



The Black Book of Healthcare Cybersecurity



Comprehensive Insights, Strategies, and Solutions

70 Critical Cybersecurity Functionalities
450 Healthcare Industry Cybersecurity Vendors
In-Depth Cybersecurity Best Practices

**2025
EDITION**

Empowering Healthcare Organizations
with the Knowledge to **Stay Resilient** in
an **Evolving Cyber Threat Landscape**

Contents

Executive Summary.....	5
Introduction.....	9
Lessons from 2024’s Major 4 HIT Cyberattacks	14
The Numbers.....	19
The State of Healthcare Cybersecurity Industry	21
Investments in Healthcare Cybersecurity	25
EHR Vendors: The Need for Vigilance	29
How EHR Vendors Can Prepare for Evolving Cyber Threats.....	32
End-to-End Healthcare Cybersecurity Vendors.....	37
Top 2025 End-to-End Healthcare Cybersecurity Vendors.....	40
Major Healthcare Cybersecurity Solutions by Functionality	50
Black Book’s 18 Cybersecurity-Centric Key Performance Indicators for Healthcare Providers and Payers.....	56
Expanded Black Book Scoring Guidance.....	61
Scoring Framework for Evaluating Healthcare Cybersecurity Vendors	62
Client Experience Satisfaction Ratings 2025	67
Alphabetical Directory of Healthcare Cybersecurity Vendors.....	93
Numeric Directory.....	217
Comprehensive Coverage of 70 Cybersecurity Tool Categories and Functionalities for Healthcare Strategies.....	235
Greatest Buyer Demand 2025-2027	269

Contents

Top AI-Driven and Comprehensive Cybersecurity Vendors in Healthcare..... 277

Index 285

About Black Book™

Black Book Market Research LLC annually evaluates leading healthcare software, information exchanges, and service providers across 18 operational excellence key performance indicators, entirely from the perspective of client experience. Independent and unbiased from vendor influence. Suppliers are also encouraged to solicit their clients to participate, producing current and objective customer service data for buyers, analysts, investors, consultants, competitive suppliers, and the media.

For more information or to order customized research results,
please contact the Client Resource Center
at: +1-800-863-7590
or
research@BlackBookMarketResearch.com.

Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Black Book disclaims all warranties as to the accuracy, completeness, or adequacy of such information. Black Book shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve intended results. The opinions expressed herein are subject to change without notice. Black Book's objectivity and credibility remain unparalleled, providing assurance amid a landscape increasingly clouded by vendor-consultancy alliances.

For more information,
visit www.blackbookmarketresearch.com.

© 2025 Black Book Market Research LLC All Rights Reserved.

Executive Summary



Healthcare cybersecurity remains a critical concern, with data breaches posing significant challenges to patient trust, financial stability, and operational efficiency. Below is an overview of recent statistics, the financial impact of breaches, effects on patient loyalty, and potential threats anticipated in 2025.

Recent Data Breach Statistics

- **Number of Breaches:** In the first half of 2024, there were 387 reported healthcare data breaches involving 500 or more records, marking an 8.4% increase from the same period in 2023.
- **Records Affected:** These breaches compromised approximately 45.6 million healthcare records, a 9.5% decrease from the 50.3 million records breached in the first half of 2023.
- **Notable Incidents:** Significant breaches in 2024 included the Kaiser Foundation Health Plan incident, affecting 13.4 million individuals, and the Change Healthcare breach, impacting over 100 million people.

Financial Impact of Data Breaches

- **Average Cost:** The healthcare sector continues to experience the highest data breach costs across industries. In 2024, the average cost of a healthcare data breach was \$9.77 million, a decrease from \$10.93 million in 2023.
- **Comparison to Other Industries:** Healthcare data breach costs are more than double the average across all industries, which stood at \$4.88 million in 2024.

Impact on Patient Loyalty and Satisfaction

- **Trust Erosion:** Data breaches undermine patient trust, leading to dissatisfaction with healthcare providers and payers. Patients expect their sensitive information to be safeguarded, and breaches can result in patients seeking services elsewhere.
- **Operational Disruptions:** Cyberattacks can disrupt healthcare services, delaying patient care and affecting outcomes, further diminishing patient satisfaction.

Potential Threats in 2025

- **Ransomware Attacks:** Ransomware continues to be a predominant threat, with cybercriminals targeting healthcare organizations to disrupt services and demand substantial ransoms.

- **Supply Chain Vulnerabilities:** As healthcare systems integrate more third-party services and technologies, vulnerabilities within the supply chain may become targets for cyberattacks.
- **Advanced Persistent Threats (APTs):** State-sponsored and organized cybercriminal groups may increase sophisticated attacks aimed at stealing sensitive patient data for espionage or financial gain.
- **IoT and Medical Device Exploits:** The proliferation of Internet of Things (IoT) devices in healthcare settings presents new attack vectors, with potential threats to patient safety if medical devices are compromised.

Healthcare organizations must remain vigilant, investing in robust cybersecurity measures, employee training, and incident response strategies to mitigate these risks and protect patient data in the evolving threat landscape of 2025.

In 2025, the healthcare sector continues to face an evolving and intensifying cybersecurity landscape. Black Book Market Research LLC surveyed 3,400 security professionals from 2,600 healthcare organizations, including hospitals, medical practices, and health plans, to assess gaps, vulnerabilities, and persistent deficiencies. The findings underscore the urgency for robust cybersecurity measures as healthcare organizations remain prime targets for data breaches and cyberattacks.

Key Findings

1. Understanding and Prioritization:

- 97% of surveyed professionals understand the risks posed by cybersecurity threats.
- 62% of healthcare organizations rank security as a top IT concern, up from 54% in 2023 and 19% in 2022.

2. Data Breaches:

- 85% of healthcare organizations experienced a data breach in the past two years.
- The average healthcare data breach cost rose to \$750 per record in 2025, the highest across industries for over a decade.

3. Cyberattack Trends:

- 2024 witnessed 500+ reported data breaches in the U.S., affecting 90 million patients.
- Ransomware attacks accounted for 42% of reported breaches.

4. **Budgetary Constraints:**

- Despite a 21% increase in cybersecurity budgets from 2023 to 2024, 72% of providers cite budget constraints as a barrier to comprehensive cybersecurity measures.

5. **Workforce Challenges:**

- The average tenure for healthcare cybersecurity professionals dropped to 1.2 years in 2025, compared to 1.5 years in 2023.
- 62% of surveyed organizations reported difficulty hiring and retaining qualified cybersecurity staff.

6. **Healthcare Cybersecurity Market:**

- Valued at \$12 billion in 2025, the market is projected to reach \$48 billion by 2028, with a CAGR of 21%.
- Spending on managed services and outsourcing has surged, comprising 38% of total cybersecurity investments.



Introduction



The healthcare sector is one of the most critical yet vulnerable industries in the global economy. The integration of digital technologies, accelerated by the COVID-19 pandemic, has brought unprecedented improvements in patient care but has also increased cybersecurity risks. In 2025, the healthcare sector is facing sophisticated threats from cybercriminals and state-sponsored actors. The value of protected health information (PHI), combined with the widespread adoption of interconnected devices and cloud-based systems, has created a vast attack surface. This paper will analyze the current state of cybersecurity in hospitals, physician organizations, medical schools, payers, government agencies, pharmaceutical companies, EHR systems, long-term care providers, and diagnostic services. It will also discuss trends, major breaches, and solutions implemented to mitigate risks.

Hospitals and Health Systems

Current State

Hospitals have been at the forefront of digital transformation, with advancements in telemedicine, remote patient monitoring, and electronic health record (EHR) systems. However, their reliance on digital infrastructure has made them vulnerable to cyberattacks. A survey conducted in 2025 found that 78% of hospitals have experienced at least one significant cybersecurity incident in the past year.

Challenges

- **Legacy Systems:** Many hospitals operate on outdated IT systems that lack the capability to counter modern threats.
- **Budget Constraints:** Smaller hospitals, especially in rural areas, struggle to allocate sufficient funds for cybersecurity.
- **Human Error:** Employee negligence remains a leading cause of breaches.

Physician Organizations and Ambulatory Care

Overview

Physician organizations, including group practices and clinics, play a crucial role in healthcare delivery but often lack the resources for robust cybersecurity defenses. The increasing use of mobile devices and telehealth platforms has introduced additional vulnerabilities.

Trends

- **Cloud Adoption:** 90% of physician organizations now use cloud-based EHR systems, increasing their exposure to cyber risks.
- **Targeted Attacks:** Cybercriminals are increasingly targeting small practices, knowing they are less likely to have sophisticated defenses.

Academic Healthcare and Medical Schools

Role in Healthcare

Academic institutions are at the intersection of patient care, education, and research. They house valuable data, including PHI, proprietary research, and intellectual property, making them attractive targets for cybercriminals and nation-state actors.

Threats

- **Research Data Theft:** Universities conducting cutting-edge research on treatments and vaccines are frequently targeted.
- **IoT Devices:** Medical schools often use IoT devices in training, which can be exploited if not secured properly.

Payers and Health Plans

Cybersecurity Landscape

Health plans are custodians of sensitive patient information, including medical histories, financial data, and claims. This makes them high-value targets for hackers looking to monetize stolen data.

Common Threats

- **Phishing Attacks:** Fraudulent emails remain the primary method of gaining unauthorized access to payer systems.
- **Social Engineering:** Employees are often tricked into revealing credentials.

Trends in 2025

- Over 60% of health plans have implemented multi-factor authentication (MFA) to enhance security.
- AI and machine learning are being used to detect unusual patterns and prevent fraud.

Government Public Health Agencies

Importance

Government agencies are responsible for managing public health crises, such as pandemics, and maintaining critical infrastructure. A successful attack on these entities can have far-reaching consequences.

Threats

- **State-Sponsored Attacks:** Foreign adversaries often target government health systems to disrupt services or steal data.
- **Supply Chain Risks:** Vulnerabilities in third-party software used by public agencies are a growing concern.

Pharmaceutical and Supply Chain Companies

Overview

Pharmaceutical companies are prime targets due to the value of their intellectual property and the critical role they play in the global healthcare supply chain.

Risks

- **R&D Breaches:** Theft of drug formulations and clinical trial data is a major concern.
- **Supply Chain Attacks:** Cybercriminals often infiltrate third-party vendors to access pharmaceutical networks.

EHRs and Healthcare Software

Vulnerabilities

EHR systems are central to modern healthcare but are also vulnerable to cyberattacks due to their complexity and the vast amounts of data they handle.

Trends

- 85% of healthcare providers use cloud-based EHRs, which require advanced security measures to prevent breaches.
- Interoperability mandates have increased the risk of data exposure during exchanges between systems.

Long-Term Care and Post-Acute Providers

Challenges

Long-term care providers often operate on tight budgets and lack dedicated IT staff, making them particularly vulnerable to cyber threats.

A 2025 survey found that 40% of long-term care facilities experienced at least one breach in the past year, with ransomware being the most common threat.

Ambulatory Care and Diagnostics

Risk Factors

Ambulatory care centers and diagnostic labs are attractive targets due to their reliance on connected devices and the sensitive nature of diagnostic data.

Trends

- The adoption of AI-driven diagnostic tools has increased, but these systems often lack proper security protocols.
- Third-party breaches remain a significant concern, with attackers targeting lab software vendors.

The healthcare industry in 2025 faces unparalleled cybersecurity challenges. To combat these risks, organizations must invest in advanced technologies, foster a culture of security awareness, and collaborate across sectors. By addressing vulnerabilities and implementing robust defense mechanisms, the industry can safeguard patient data and maintain the integrity of healthcare delivery.

Lessons from 2024's Major 4 HIT Cyberattacks



In 2024, the healthcare sector experienced several significant data breaches that underscored the critical importance of robust cybersecurity measures. Below are notable incidents, their impacts, and key lessons learned:

Change Healthcare: Ransomware Attack

Incident Overview: In February 2024, Change Healthcare, a subsidiary of UnitedHealth Group, suffered a ransomware attack that compromised approximately 100 million individuals' personal information, including patient records, financial data, and insurance details.

Impact:

- **Operational Disruption:** The attack disrupted healthcare operations nationwide, affecting thousands of hospitals, clinics, pharmacies, and medical providers that rely on Change Healthcare for patient record management and billing.
- **Financial Losses:** Change Healthcare reportedly paid a \$22 million ransom to regain access to their systems, marking one of the largest such payouts.
- **Data Exposure:** Despite the ransom payment, portions of the stolen data were published online, confirming the breach's scale and severity.

Lessons Learned:

- **Implement Strong Access Controls:** The attackers exploited stolen credentials to gain unauthorized access. Enforcing multi-factor authentication (MFA) and regular credential audits could have mitigated this risk.
- **Network Segmentation:** Proper segmentation can limit the spread of malware and restrict attackers' lateral movement within the network.
- **Regular Backups and Incident Response Planning:** Maintaining up-to-date, offline backups and having a robust incident response plan are crucial for minimizing downtime and data loss during cyber incidents.

Synnovis Ransomware Attack

Incident Overview: In 2024, Synnovis, a provider of laboratory services for the UK's National Health Service (NHS), was targeted by the Qilin ransomware group. The attackers exfiltrated 400GB of data, leading to significant operational disruptions.

Impact:

- **Service Disruption:** The attack resulted in the cancellation and delay of thousands of operations and appointments, severely impacting patient care.
- **Financial Losses:** Synnovis incurred costs of £32.7 million due to the attack, far exceeding its profits of £4.3 million in 2023.
- **Data Breach:** The incident led to one of the largest recent breaches of NHS patient data, with sensitive information leaked online.

Lessons Learned:

- **Supply Chain Security:** The attack highlighted vulnerabilities in the NHS supply chain, emphasizing the need for stringent cybersecurity measures among third-party providers.
- **Manual Contingency Plans:** Synnovis had to revert to manual methods for delivering test results, underscoring the importance of having contingency plans for critical services.
- **Regulatory Compliance:** The incident prompted discussions about mandating stronger cybersecurity measures for private providers delivering public services.

Confidant Health Data Exposure

Incident Overview: In 2024, Confidant Health, a US-based mental health care firm, inadvertently exposed thousands of sensitive health records, including therapy session audio and video, due to an unsecured database.



Impact:

- **Privacy Violations:** Personal details of patients, including detailed medical histories and therapy session notes, were accessible online, posing significant privacy risks.
- **Potential for Exploitation:** Although the firm secured the database upon discovery and claimed no malicious access occurred, the exposure highlighted vulnerabilities that could be exploited if left unaddressed.

Lessons Learned:

- **Secure Configuration Management:** Ensuring databases and storage systems are properly configured with appropriate access controls is vital to prevent unauthorized access.
- **Regular Security Audits:** Conducting routine security assessments can help identify and rectify vulnerabilities before they lead to data breaches.
- **Data Encryption:** Implementing encryption for sensitive data, both at rest and in transit, adds an additional layer of security against unauthorized access.

NHS Dumfries & Galloway Cyber-Attack

Incident Overview: In 2024, NHS Dumfries & Galloway in southwest Scotland experienced a cyber-attack that led to the leak of data from over 100,000 patients and staff after the health board refused to meet ransom demands.

Impact:

- **Data Breach:** The ransomware group, Inc Ransom, published the stolen information on the dark web, including significant amounts of personal and medical data.
- **Patient Care Disruption:** The attack caused disruptions in medical services, leading to delays in patient care and treatment.

Lessons Learned:

- **Incident Response Readiness:** Having a well-prepared incident response plan enables organizations to act swiftly and effectively during cyber-attacks, minimizing damage.
- **Stakeholder Communication:** Transparent communication with patients and staff during and after a breach is essential to maintain trust and provide guidance on protective measures.
- **Cybersecurity Training:** Regular training for staff on recognizing and responding to cyber threats can help prevent successful attacks and reduce their impact.

These incidents highlight the escalating cyber threats facing the healthcare sector and underscore the necessity for comprehensive cybersecurity strategies, including robust access controls, regular security audits, employee training, and incident response planning. Implementing these measures can significantly mitigate risks and enhance the resilience of healthcare organizations against cyber-attacks.



The Numbers

Global Perspective: The global healthcare cybersecurity market has accelerated, fueled by technological advancements, regulatory pressures, and the increasing sophistication of cyberattacks. Emerging trends include:

- **AI-Enhanced Threat Detection:** AI-driven tools are now essential for identifying and mitigating threats in real-time.
- **IoT Vulnerabilities:** The proliferation of Internet of Medical Things (IoMT) devices has expanded the attack surface significantly.
- **Zero-Trust Security Models:** Adoption of zero-trust frameworks has increased by 40% since 2023.

U.S. Status: The U.S. healthcare sector remains disproportionately affected, reporting more breaches than any other nation. High-profile incidents in 2024 include:

- **HCA Healthcare Breach:** Exposed data of 12 million patients.
- **Community Health Systems Attack:** Impacted 10 million individuals.

Top Challenges Identified in 2025:

1. **Ransomware Attacks:** 94% of respondents cite ransomware as the most disruptive cyber threat.
2. **Human Error:** Insider threats, both intentional and accidental, account for 28% of breaches.
3. **Legacy Systems:** 65% of organizations still rely on outdated systems, increasing vulnerability.
4. **IoMT Device Security:** 72% of respondents report inadequate security measures for connected devices.

Recommendations:

- **Strategic Investments:** Increase funding for modernizing legacy systems and adopting advanced threat detection technologies.
- **Workforce Development:** Establish training programs to address the talent gap in healthcare cybersecurity.
- **Vendor Management:** Implement stringent security requirements and audits for third-party vendors.
- **Incident Response:** Conduct regular drills and establish clear protocols for responding to cyber incidents.



The State of Healthcare Cybersecurity Industry

The healthcare industry is facing unprecedented challenges in cybersecurity as it transitions to digital-first systems and manages increasing cyber threats. This report by Black Book Research provides a comprehensive analysis of trends, concerns, statistics, and IT activities in the healthcare cybersecurity landscape for 2025. It includes a detailed section addressing the unique needs of electronic health record (EHR) vendors and their strategies for vigilance and preparedness.

The healthcare industry in 2025 remains one of the most targeted sectors for cyberattacks, owing to the value of protected health information (PHI) and the increasing digitalization of healthcare systems. This paper explores the current state of cybersecurity across various healthcare domains, including hospitals, physician organizations, academic institutions, payers, EHR systems, and more. It highlights trends, risks, data breaches, and the unique challenges faced by the industry.

Overview of Cybersecurity in Healthcare

Healthcare organizations have witnessed a significant increase in cyber threats due to expanded attack surfaces, remote work adoption, and the rise of interconnected devices.

Key Trends in Healthcare Cybersecurity

Escalation of Ransomware Attacks:

- **Dominance:** Ransomware remains the top threat, with 92% of healthcare organizations reporting significant concerns.
- **Financial Impact:** Average ransomware demands rose to \$5 million, with payouts averaging \$1.4 million per attack.
- **Double Extortion:** Attackers frequently steal data before encryption, threatening to release it unless additional ransom is paid.

IoMT (Internet of Medical Things) Vulnerabilities:

- 68% of IoMT devices are connected without adequate security measures.
- Hospitals report exponential growth in vulnerabilities due to unmonitored IoMT expansions.

Zero Trust Architecture Adoption:

- Zero trust frameworks were adopted by 40% more organizations compared to 2024, emphasizing "never trust, always verify" principles.

AI-Driven Threats:

- Cyber adversaries are employing AI-powered tools to mimic legitimate behavior, making attacks harder to detect.
- Healthcare organizations are deploying AI to counter these threats through real-time analytics.

Surge in Cybersecurity Budgets:

- Global spending on healthcare cybersecurity is projected to reach \$48 billion by the end of 2025, with hospitals and health systems contributing 70%.

Increased Regulation:

- Updated HIPAA rules and new global data privacy regulations require stricter cybersecurity controls and reporting.

Managed Security Services Expansion:

- Adoption of managed security services grew by 35% as organizations struggled with internal resource constraints and 24/7 monitoring demands.



Major Concerns in 2025

Budget Constraints:

- Despite increased budgets, 68% of healthcare providers cite insufficient funds to address evolving cyber risks adequately.

Cybersecurity Talent Shortage:

- Over 56% of healthcare organizations report challenges in hiring and retaining skilled professionals, with burnout and high stress levels cited as critical issues.

Human Error:

- Insider threats account for 28% of breaches, with phishing emails being a leading cause of data exposure.

Third-Party Risks:

- 61% of breaches originated from vendor vulnerabilities. Many healthcare entities lack comprehensive vendor risk assessment frameworks.

Legacy Systems:

- Older EHR systems and outdated hardware leave organizations more vulnerable to breaches.

Quick View: Cybersecurity Statistics for 2025

Global Data Breaches:

- 94 million patient records were compromised globally, marking an 18% increase from 2024.
- Healthcare organizations experienced 85% of these breaches.

Rising Costs:

- The average cost of a data breach in healthcare increased to \$11.3 million, up from \$10.1 million in 2023.

Sources of Breaches:

- **Ransomware: 42%**
- **Phishing: 29%**
- **Insider negligence: 17%**
- **Third-party vulnerabilities: 12%**

Investments in Healthcare Cybersecurity



The healthcare industry in 2025 continues to prioritize robust IT investments to address the rapidly evolving cyber threat landscape. Key focus areas include enhanced EHR security, proactive incident response strategies, cloud migration initiatives, and IoT/IoMT security measures. Below is an expanded discussion of these critical topics.

Enhanced EHR Security

Electronic Health Records (EHR) systems remain the backbone of modern healthcare, containing vast amounts of sensitive patient data. In 2025, cybersecurity investments in EHR platforms are centered around encryption, multifactor authentication (MFA), and AI-driven threat detection tools to address rising cyber threats.

- **Encryption:** Advanced encryption protocols, such as AES-256, are being widely implemented to secure patient data both at rest and in transit. These measures protect against unauthorized access, ensuring that even if data is intercepted, it cannot be decrypted without proper authorization.
- **Multifactor Authentication (MFA):** MFA has become a non-negotiable requirement for accessing EHR systems. By requiring multiple verification methods, such as biometrics, tokens, or one-time passwords, MFA significantly reduces the risk of unauthorized access due to credential theft.
- **AI-Driven Threat Detection:** Artificial intelligence (AI) is revolutionizing EHR security by identifying anomalous behaviors and potential breaches in real-time. AI tools can monitor access patterns, detect unusual activities, and flag potential insider threats, providing an additional layer of defense.

These advancements are crucial for ensuring compliance with HIPAA and GDPR regulations, maintaining patient trust, and preventing costly data breaches. As EHR systems evolve to include more interoperable features, the emphasis on robust security frameworks will continue to grow.

Proactive Incident Response

The frequency and sophistication of cyberattacks have driven healthcare organizations to adopt proactive incident response (IR) strategies. In 2025, approximately 73% of healthcare entities have formalized IR protocols, a significant increase from prior years.

- **Tabletop Exercises:** These simulated breach scenarios are becoming a cornerstone of preparedness, allowing organizations to test their response plans and refine workflows. Tabletop exercises help identify gaps in communication, escalation procedures, and technical defenses.

- **Dedicated IR Teams:** Many healthcare providers and payers have established dedicated incident response teams, often augmented by Managed Detection and Response (MDR) services. These teams ensure rapid containment and recovery when breaches occur.
- **Integration with Cyber Insurance:** Incident response plans now align closely with cyber insurance policies, ensuring compliance with coverage requirements and minimizing financial impacts.

Proactive IR strategies not only reduce the downtime and operational disruptions caused by attacks but also enhance an organization's ability to recover quickly and maintain trust with patients and stakeholders.

Cloud Migration

The adoption of cloud technologies by hospitals, payers, and suppliers has accelerated in 2025 as organizations seek to improve scalability, efficiency, and data accessibility. However, this shift brings with it unique cybersecurity challenges and the need for robust cloud security measures.

- **Data Security in the Cloud:** Healthcare organizations are leveraging tools like cloud access security brokers (CASBs), encryption, and zero-trust frameworks to protect sensitive data in multi-cloud environments.
- **Compliance and Auditing:** Cloud service providers are increasingly offering healthcare-specific compliance certifications, such as HITRUST and ISO 27001, ensuring adherence to stringent regulatory requirements.
- **Disaster Recovery and Redundancy:** Cloud-based disaster recovery solutions are enabling organizations to maintain business continuity during cyber incidents or natural disasters. Automated backups and replication capabilities are becoming standard features in healthcare cloud strategies.

By integrating these measures, healthcare entities can securely migrate workloads to the cloud, enhancing their agility and operational efficiency while minimizing risks.

IoT/loMT Security

The proliferation of Internet of Things (IoT) and Internet of Medical Things (loMT) devices in healthcare has created new vulnerabilities and attack surfaces. In 2025, investments in loMT security have grown by 45%, reflecting the urgency to address these risks.

- **loMT Monitoring Tools:** Advanced monitoring solutions provide real-time visibility into loMT ecosystems, identifying devices, assessing vulnerabilities, and detecting anomalies. Tools like Medigate and Armis are becoming essential for healthcare providers.
- **Secure Device Configurations:** Organizations are implementing strict configuration protocols to ensure that loMT devices are protected against unauthorized access and default settings are replaced with secure alternatives.
- **Device Patching and Lifecycle Management:** Regular patching and end-of-life management are critical to mitigating risks associated with outdated or unsupported devices. Automated patch management solutions are increasingly adopted to streamline this process.
- **Segmentation and Access Controls:** Network segmentation ensures that loMT devices are isolated from critical systems, preventing lateral movement in case of a breach. Role-based access control (RBAC) further limits access to authorized personnel.

These investments are driven by the need to safeguard connected devices, which play a vital role in patient monitoring, diagnostics, and treatment delivery. Strengthening loMT security not only protects patient data but also ensures the safety and reliability of life-critical devices.

Healthcare IT investments in 2025 are focused on creating resilient and secure ecosystems that can withstand evolving cyber threats. Enhanced EHR security, proactive incident response, cloud migration, and IoT/loMT security represent critical areas where organizations are channeling resources. By prioritizing these initiatives, healthcare providers, payers, and suppliers can mitigate risks, maintain regulatory compliance, and deliver uninterrupted, secure patient care.

EHR Vendors: The Need for Vigilance



Electronic Health Record (EHR) vendors are at the core of healthcare's digital transformation, enabling seamless data storage, sharing, and access across organizations. However, their central role also makes them a prime target for cyberattacks. In 2025, EHR vendors must address several key risks to maintain security, regulatory compliance, and the trust of healthcare providers and patients. These risks include vulnerabilities in legacy systems, integration challenges, and compliance issues.

Legacy Systems Vulnerabilities

Many healthcare organizations continue to rely on older EHR platforms that lack modern security features. These legacy systems were designed in an era when cybersecurity was less complex, and their outdated architectures make them susceptible to attacks.

- **Outdated Protocols and Encryption:** Legacy systems often use weak or obsolete encryption standards, making it easier for attackers to intercept and exploit sensitive patient data. For instance, systems still operating with older TLS (Transport Layer Security) versions are vulnerable to man-in-the-middle attacks.
- **Unsupported Software:** EHR platforms that are no longer supported by their vendors are particularly at risk, as they do not receive critical security patches and updates. This creates exploitable vulnerabilities, especially as threat actors develop increasingly sophisticated methods.
- **Operational Inflexibility:** Legacy systems often lack compatibility with modern security tools, such as endpoint detection and response (EDR) or advanced threat analytics, further limiting an organization's ability to detect and respond to threats.

Solution: Vendors must encourage clients to migrate to updated platforms or develop scalable solutions that incorporate advanced security features like AI-driven threat detection, real-time monitoring, and robust encryption. Additionally, offering comprehensive support for the transition process can reduce resistance from healthcare organizations.

Integration Challenges

The growing interoperability of EHR systems, driven by the need for seamless data exchange, has expanded the attack surface. EHRs are increasingly connected to telehealth platforms, billing systems, patient portals, and third-party tools, creating potential vulnerabilities.

- **Increased Points of Entry:** Each integration with a third-party tool or application introduces a potential entry point for attackers. For example, a vulnerability in a billing platform linked to an EHR could provide access to the entire database.

- **Data Flow Complexities:** Secure data exchange between systems requires robust APIs (Application Programming Interfaces) that are often targeted by hackers. Poorly secured APIs can result in data leakage or unauthorized access.
- **Dependency on Third-Party Security:** The security of an integrated EHR system is only as strong as its weakest link. If a third-party vendor fails to implement adequate cybersecurity measures, it compromises the entire system.

Solution: EHR vendors must prioritize secure integration by conducting rigorous third-party risk assessments, enforcing strict API security protocols, and employing tools like cloud access security brokers (CASBs) to monitor data exchanges. Zero Trust principles can also be applied, ensuring that every data transfer is verified and secure.

Compliance Issues

EHR vendors operate in a highly regulated environment, with frameworks like HIPAA in the United States and GDPR in Europe mandating strict standards for data protection. Non-compliance not only exposes vendors to fines but also damages their reputation, leading to loss of trust among clients.

- **Inconsistent Adherence to Standards:** As regulations evolve, some EHR vendors struggle to keep their systems compliant. For instance, updates to HIPAA guidelines on the use of telehealth services and data sharing require continuous monitoring and adaptation.
- **Regional Variations in Compliance:** Vendors operating across multiple regions face the added complexity of adhering to varying regulatory requirements. Failure to comply with local laws, such as Europe's GDPR or Brazil's LGPD, can result in significant penalties.
- **Audits and Breach Reporting:** Many vendors lack the robust logging and auditing capabilities needed to track data access and report breaches promptly, as required by regulations. This can result in delays in breach notifications and further legal liabilities.

Solution: Vendors must invest in compliance automation tools that streamline adherence to various regulatory frameworks. Regular audits, both internal and external, should be conducted to ensure compliance. Additionally, vendors can provide built-in tools for clients to generate compliance reports and monitor data access in real time.

EHR vendors play a pivotal role in safeguarding healthcare data, but their systems and processes are not immune to risks. Addressing vulnerabilities in legacy systems, securing complex integrations, and maintaining regulatory compliance are essential steps to building trust and ensuring data protection in 2025 and beyond. Proactively mitigating these risks through robust cybersecurity measures, modernized platforms, and transparent regulatory adherence will enable vendors to protect both their clients and their reputation in an increasingly interconnected healthcare ecosystem.

How EHR Vendors Can Prepare for Evolving Cyber Threats

As cyber threats become more sophisticated, Electronic Health Record (EHR) vendors must adopt advanced security strategies to safeguard sensitive patient data and maintain trust with healthcare providers. Preparation involves implementing modern frameworks, technologies, and practices to address vulnerabilities and evolving risks. Below is an expanded discussion of key measures EHR vendors can take to enhance their cybersecurity posture.

Zero Trust Frameworks

A Zero Trust framework operates under the principle of "never trust, always verify," ensuring that every user and device attempting to access sensitive data is authenticated and authorized.

- **Strict Access Control:** EHR vendors must enforce granular role-based access controls (RBAC) to ensure that users can only access data and systems relevant to their role. For example, clinicians accessing patient records should not have administrative privileges over system configurations.
- **Continuous Verification:** Implementing continuous authentication techniques, such as session monitoring and adaptive security protocols, ensures that even authenticated users are periodically re-verified.
- **Device Authentication:** Vendors should integrate device-level authentication measures, ensuring that only registered and secure devices can connect to the EHR system. This reduces the risk of unauthorized devices acting as entry points for attackers.

By adopting Zero Trust principles, vendors can significantly reduce the risk of unauthorized access and data breaches.

AI-Driven Threat Detection

Artificial intelligence (AI) and machine learning (ML) tools are revolutionizing cybersecurity by enabling real-time threat detection and automated responses.

- **Anomaly Detection:** AI can analyze user behavior and identify deviations from normal patterns, such as unusual login times, large data exports, or access from unrecognized devices. These anomalies can signal potential insider threats or compromised accounts.
- **Automated Responses:** Machine learning models can prioritize threats and initiate automated responses, such as isolating suspicious accounts or blocking unauthorized access attempts, minimizing damage.
- **Proactive Threat Hunting:** AI-driven tools can scan vast amounts of network data to identify hidden threats, such as dormant malware or advanced persistent threats (APTs), before they are activated.

Embedding AI into EHR platforms provides vendors with a proactive approach to cybersecurity, enabling them to stay ahead of emerging threats.

Robust API Security

APIs (Application Programming Interfaces) are essential for integrating EHR systems with third-party applications, but they also introduce potential vulnerabilities.

- **Authentication and Authorization:** EHR vendors must implement OAuth 2.0 or similar secure frameworks to authenticate API requests and authorize user actions. This ensures that only verified entities can interact with the system.
- **Input Validation:** APIs should be designed to validate input data rigorously, preventing attacks such as SQL injection or command injection that exploit poorly secured endpoints.
- **Rate Limiting:** Limiting the number of requests an API can handle per second reduces the risk of denial-of-service (DoS) attacks and system overloads caused by malicious actors.

Securing APIs ensures that EHR systems can integrate with other platforms without compromising the integrity or confidentiality of patient data.

Regular Security Testing

Regular security testing is critical for identifying and mitigating vulnerabilities before attackers can exploit them.

- **Penetration Testing:** Simulating real-world attacks helps identify weaknesses in EHR systems, such as unpatched software, misconfigured servers, or weak authentication protocols.
- **Vulnerability Assessments:** Regular scanning of system components ensures that known vulnerabilities are identified and patched promptly, reducing the risk of exploitation.
- **Compliance Audits:** Conducting routine compliance audits ensures that EHR systems adhere to regulatory requirements like HIPAA and GDPR, minimizing the risk of legal and financial penalties.

By incorporating frequent security testing into their operations, vendors can create a dynamic and resilient defense against evolving threats.

Data Encryption

Encryption is a cornerstone of data security, ensuring that sensitive information remains inaccessible even if intercepted or stolen.

- **Data at Rest:** Encrypting stored data using strong algorithms like AES-256 ensures that even if storage devices are compromised, the data cannot be read without decryption keys.
- **Data in Transit:** Vendors must use secure communication protocols like HTTPS and TLS to encrypt data as it travels between users, systems, and third-party applications.
- **Data During Processing:** Implementing homomorphic encryption or secure enclaves protects data during active use, reducing risks in high-volume processing environments.

Comprehensive encryption strategies ensure that patient data remains protected at every stage of its lifecycle.

Vendor Risk Management

Collaboration with healthcare clients to manage risks across interconnected systems is vital for ensuring holistic security.



- **Third-Party Risk Assessments:** EHR vendors must evaluate the security practices of third-party providers integrated with their systems, ensuring compliance with industry standards.
- **Supply Chain Security:** Establishing guidelines and frameworks for secure data exchange between vendors, clients, and third parties reduces risks introduced by supply chain vulnerabilities.
- **Shared Responsibility Models:** Clear delineation of security responsibilities between vendors and clients fosters accountability and ensures comprehensive protection.

By managing vendor-related risks, EHR providers can prevent vulnerabilities from spreading across interconnected systems.

Resilient Backup Systems

Resilient backup systems are essential for mitigating the impact of ransomware attacks and ensuring business continuity.

- **Immutable Backups:** Storing backups in a tamper-proof format ensures they remain unaffected by ransomware or malicious actions.
- **Frequent Backups:** Regularly backing up data minimizes potential loss and ensures that the latest records can be restored in case of an attack or system failure.
- **Disaster Recovery Plans:** EHR vendors should work with clients to establish disaster recovery plans, including testing backup restoration processes to ensure rapid recovery during emergencies.

Reliable backup systems provide a safety net, enabling healthcare organizations to recover quickly from cyber incidents and maintain patient care continuity.

EHR vendors must adopt a multi-layered approach to cybersecurity, combining Zero Trust frameworks, AI-driven threat detection, robust API security, regular testing, encryption, vendor risk management, and resilient backups. By proactively addressing these areas, vendors can enhance the security and reliability of their platforms, protect sensitive patient data, and build trust with healthcare providers in an increasingly interconnected and high-risk digital landscape.

The healthcare industry is at a critical juncture in its cybersecurity evolution. With data breaches and ransomware attacks on the rise, organizations must prioritize investments in cutting-edge tools, proactive planning, and skilled personnel. For EHR vendors, the emphasis must be on integrating advanced security features and collaborating closely with healthcare entities to mitigate risks. By fostering a culture of security awareness and adopting zero trust principles, healthcare organizations and their vendors can safeguard sensitive patient data and maintain operational integrity in 2025 and beyond.

For more information, contact Black Book Market Research at
research@BlackBookMarketResearch.com

or visit
www.blackbookmarketresearch.com



End-to-End Healthcare Cybersecurity Vendors



An end-to-end cybersecurity vendor provides comprehensive security solutions that address the entire spectrum of cybersecurity needs within the healthcare industry, encompassing providers, payers, and suppliers. These vendors go beyond offering standalone products; they deliver integrated frameworks that protect sensitive patient data, ensure compliance with stringent regulations, and secure diverse digital environments such as electronic health records (EHRs), IoT/IoMT devices, telehealth platforms, and cloud-based services.

Healthcare organizations face unique cybersecurity challenges, including safeguarding highly sensitive Protected Health Information (PHI), ensuring uninterrupted care delivery, and managing complex networks and interconnected systems. End-to-end vendors are distinguished by their ability to deliver cohesive, multi-layered security solutions tailored to these specific needs. They combine advanced technologies, robust risk management practices, and exceptional service excellence to protect healthcare entities from emerging threats.

Core Qualities of an End-to-End Healthcare Cybersecurity Vendor

Strategic Industry Alignment End-to-end vendors deeply understand the operational and regulatory complexities of the healthcare industry. Their solutions are designed to align with value-based care (VBC) models, support interoperability initiatives like health information exchanges (HIE), and secure telehealth platforms. This industry-specific focus ensures that their tools and services meet the unique demands of healthcare organizations.

Comprehensive Technology Stack These vendors offer a range of tools and technologies, from endpoint detection and response (EDR) to identity and access management (IAM), encryption, cloud security, and data loss prevention (DLP). Their solutions integrate seamlessly across platforms, enabling healthcare organizations to secure every layer of their IT infrastructure without gaps or redundancies.

Advanced Threat Detection and Mitigation Leveraging AI, machine learning, and behavioral analytics, end-to-end vendors provide proactive threat detection and real-time mitigation. They ensure healthcare systems are protected against sophisticated attacks, including ransomware, phishing, and insider threats. These capabilities are critical for maintaining the integrity and availability of EHR systems and other critical applications.

Regulatory Compliance Expertise Healthcare cybersecurity vendors understand the importance of compliance with regulations such as HIPAA, HITECH, GDPR, and regional data protection laws. Their solutions include built-in compliance features, automated auditing, and reporting capabilities, enabling healthcare organizations to meet regulatory requirements efficiently.

Service Excellence and Support An essential differentiator for end-to-end vendors is their focus on providing exceptional customer support and training. They equip healthcare IT teams with the knowledge and resources to effectively use their tools and stay ahead of emerging threats. This includes 24/7 support, detailed documentation, and tailored training programs.

Scalability and Customization End-to-end vendors design their solutions to scale with the needs of healthcare organizations, whether they are small clinics, large hospital systems, or multinational payers. They also offer customization options to address specific workflows, integration requirements, or compliance mandates.

Why End-to-End Vendors Are Critical for Healthcare

The healthcare industry is uniquely vulnerable to cyber threats due to its reliance on interconnected systems, the high value of patient data, and the potential impact of breaches on patient safety and care delivery. End-to-end vendors provide a holistic approach to cybersecurity, reducing risks, ensuring operational continuity, and enhancing trust among stakeholders.

These vendors also help healthcare organizations manage the complexities of digital transformation, such as cloud migration, IoT/IoMT adoption, and interoperability. By partnering with end-to-end vendors, healthcare entities can confidently navigate these changes while maintaining robust security and compliance.

Top 2025 End-to-End Healthcare Cybersecurity Vendors



The following list highlights leading vendors that exemplify the qualities of an end-to-end provider. Each has demonstrated expertise in delivering integrated solutions tailored to the specific needs of healthcare providers, payers, and suppliers, making them essential partners in addressing the evolving cybersecurity landscape.

1. Palo Alto Networks

Key Strengths:

- **Strategic Alignment:** Demonstrates deep healthcare industry expertise and supports value-based care (VBC), health information exchange (HIE), and telehealth.
- **Innovation & Product Usability:** Cutting-edge AI-driven threat detection, behavioral analytics, and proactive risk mitigation.
- **Risk Management:** Exceptional incident response and robust threat intelligence.
- **Service Excellence:** Comprehensive training and support.
- **Market Presence:** Strong market adoption and proven success in healthcare.

2. CrowdStrike

Key Strengths:

- **Strategic Alignment:** Extensive experience protecting healthcare organizations' endpoints and critical data, with deep integration into healthcare IT systems.
- **Innovation & Product Usability:** Best-in-class endpoint detection and AI-powered threat intelligence.
- **Risk Management:** Advanced incident response and proactive threat mitigation.
- **Service Excellence:** 24/7 technical support and training for healthcare teams.
- **Financial Viability:** Proven financial stability with a track record of sustained growth.

3. IBM Security

Key Strengths:

- **Strategic Alignment:** Extensive compliance capabilities (HIPAA, HITECH) and a strong presence in healthcare sectors.

- **Innovation & Product Usability:** Provides advanced threat intelligence, behavioral analytics, and proactive security measures.
- **Risk Management:** Excellent security practices with strong encryption and privacy measures.
- **Market Presence:** IBM's solutions are widely adopted in healthcare settings.
- **Financial Viability:** Solid financial backing with significant investments in R&D.

4. Microsoft

Key Strengths:

- **Strategic Alignment:** Cloud, security, and identity solutions that align with the needs of healthcare, including telehealth and VBC.
- **Innovation & Product Usability:** Continuous innovation with Azure security services, AI, and integrated data protection.
- **Risk Management:** Strong data encryption and privacy, with transparent security practices.
- **Service Excellence:** Excellent support and training options tailored to healthcare organizations.
- **Proven Success:** Significant market share in healthcare, particularly in large hospitals and payers.

5. Cisco

Key Strengths:

- **Strategic Alignment:** Strong healthcare industry alignment, supporting telehealth, IoT, and secure communication platforms.
- **Innovation & Product Usability:** Integrated solutions across networking, security, and collaboration platforms (Cisco Umbrella, WebEx).
- **Risk Management:** Cutting-edge network security and threat intelligence capabilities.
- **Service Excellence:** Reliable, robust support and ongoing training for healthcare IT staff.
- **Market Presence:** Extensive adoption in healthcare environments.

6. Fortinet

Key Strengths:

- **Strategic Alignment:** Tailored cybersecurity solutions for healthcare networks, IoT devices, and telehealth platforms.
- **Innovation & Product Usability:** Strong AI and ML capabilities for threat detection and mitigation.
- **Risk Management:** Industry-leading data protection, encryption, and incident response.
- **Service Excellence:** Responsive customer support and extensive training programs.
- **Market Presence:** Strong presence across the healthcare industry, especially in smaller to mid-sized healthcare systems.

7. Check Point Software

Key Strengths:

- **Strategic Alignment:** Healthcare-focused solutions with strong support for telehealth and data exchange.
- **Innovation & Product Usability:** Advanced network security, secure messaging, and behavioral analytics solutions.
- **Risk Management:** Robust data loss prevention (DLP) and proactive incident response.
- **Service Excellence:** Comprehensive training, support, and services tailored to healthcare needs.
- **Proven Success:** Well-established in healthcare with a track record of successful implementations.

8. McAfee

Key Strengths:

- **Strategic Alignment:** Specializes in providing integrated security for healthcare organizations' IT infrastructure and endpoints.
- **Innovation & Product Usability:** Offers cutting-edge threat detection, endpoint security, and data loss prevention.
- **Risk Management:** Strong data protection, encryption, and compliance features.

- Service Excellence: Responsive support and extensive training resources.
- Financial Viability: Solid financial stability and consistent innovation in the cybersecurity space.

9. Sophos

Key Strengths:

- Strategic Alignment: Strong healthcare-specific cybersecurity solutions with a focus on endpoint protection and data privacy.
- Innovation & Product Usability: AI-driven threat detection and advanced security features.
- Risk Management: Robust data security practices, ransomware protection, and privacy compliance.
- Service Excellence: Excellent customer support, training, and usability for healthcare IT teams.
- Proven Success: Trusted by healthcare organizations worldwide for endpoint protection and security solutions.

10. Zscaler

Key Strengths:

- Strategic Alignment: Zscaler offers strong support for telehealth, cloud security, and data privacy in healthcare.
- Innovation & Product Usability: Next-gen Zero Trust security model and cloud-native architecture.
- Risk Management: Real-time protection and proactive threat detection across healthcare environments.
- Service Excellence: High-quality customer support with strong educational resources for healthcare staff.
- Market Presence: Gaining strong adoption in healthcare, particularly in cloud and IoT security.

11. Trend Micro

Key Strengths:

- **Strategic Alignment:** Offers robust cybersecurity solutions for healthcare organizations, focusing on endpoint, cloud, and network security.
- **Innovation & Product Usability:** AI-powered threat detection and proactive cybersecurity measures.
- **Risk Management:** Strong ransomware protection, advanced threat intelligence, and encryption solutions.
- **Service Excellence:** Comprehensive training programs and excellent support tailored to healthcare needs.
- **Market Presence:** Well-established in healthcare, with a strong reputation for protecting healthcare data.

12. Splunk

Key Strengths:

- **Strategic Alignment:** Well-suited for large healthcare organizations with extensive data analytics and SIEM capabilities.
- **Innovation & Product Usability:** Real-time data monitoring and AI-based analytics for proactive threat detection.
- **Risk Management:** Strong incident response and threat intelligence platforms.
- **Service Excellence:** High-quality support and knowledge transfer, with extensive training resources.
- **Financial Viability:** Strong market presence with significant investments in innovation and security analytics.

13. SentinelOne

Key Strengths:

- **Strategic Alignment:** Focuses on endpoint protection with strong healthcare use cases for data security and privacy.
- **Innovation & Product Usability:** Cutting-edge AI and behavioral analytics for real-time threat detection and response.

- **Risk Management:** Exceptional ransomware protection, proactive risk mitigation, and automated threat response.
- **Service Excellence:** High responsiveness and tailored support for healthcare IT departments.
- **Proven Success:** Gaining traction within healthcare organizations due to its effectiveness in endpoint protection.

14. Ivanti

Key Strengths:

- **Strategic Alignment:** Strong capabilities in endpoint security, patch management, and vulnerability management, particularly for healthcare systems.
- **Innovation & Product Usability:** Comprehensive suite of solutions for endpoint protection and automated patch management.
- **Risk Management:** Provides robust data security, proactive risk identification, and real-time threat mitigation.
- **Service Excellence:** Excellent support services and training resources for healthcare teams.
- **Financial Viability:** Solid financial growth with significant investments in cybersecurity innovations.

15. CyberArk

Key Strengths:

- **Strategic Alignment:** Specializes in Privileged Access Management (PAM) and Identity and Access Management (IAM), critical for healthcare organizations managing sensitive data.
- **Innovation & Product Usability:** Advanced solutions for securing privileged access and user identities across healthcare environments.
- **Risk Management:** Strong focus on data privacy, access controls, and compliance with regulatory standards.
- **Service Excellence:** Excellent training programs and support services for healthcare organizations.
- **Proven Success:** Trusted by healthcare organizations to manage privileged access and reduce insider threats.

16. FortiNet

Key Strengths:

- **Strategic Alignment:** Tailored cybersecurity solutions for healthcare networks, IoT devices, and telehealth platforms.
- **Innovation & Product Usability:** Strong AI and ML capabilities for threat detection and mitigation.
- **Risk Management:** Industry-leading data protection, encryption, and incident response.
- **Service Excellence:** Responsive customer support and extensive training programs.
- **Market Presence:** Strong presence across the healthcare industry, especially in smaller to mid-sized healthcare systems.

17. FireEye (Trellix)

Key Strengths:

- **Strategic Alignment:** Well-positioned for healthcare organizations needing robust protection against advanced persistent threats (APTs).
- **Innovation & Product Usability:** Cutting-edge detection and response capabilities with advanced threat intelligence tools.
- **Risk Management:** Excellent incident response, vulnerability scanning, and real-time mitigation of healthcare cybersecurity risks.
- **Service Excellence:** High-quality support and extensive training resources for healthcare teams.
- **Proven Success:** Trusted by healthcare organizations globally for managing advanced cybersecurity threats.

18. Barracuda Networks

Key Strengths:

- **Strategic Alignment:** Provides network, email, and data security solutions with a strong focus on healthcare industry needs.
- **Innovation & Product Usability:** Scalable solutions for email security, cloud backup, and network protection.

- **Risk Management:** Strong data loss prevention (DLP), secure email gateways, and ransomware protection.
- **Service Excellence:** Excellent customer support and training specifically designed for healthcare teams.
- **Market Presence:** Trusted by many healthcare organizations for securing email and network communications.

19. ManageEngine

Key Strengths:

- **Strategic Alignment:** Specializes in IT management tools, including security for healthcare systems like EHRs and medical devices.
- **Innovation & Product Usability:** Comprehensive solutions for access management, monitoring, and patch management.
- **Risk Management:** Strong focus on vulnerability management, data protection, and disaster recovery.
- **Service Excellence:** Affordable solutions with extensive support and training for healthcare IT departments.
- **Proven Success:** Trusted by smaller and mid-sized healthcare organizations.

20. Kaspersky

Key Strengths:

- **Strategic Alignment:** Focuses on endpoint protection and ransomware prevention, crucial for healthcare organizations handling sensitive patient data.
- **Innovation & Product Usability:** Provides cutting-edge threat detection capabilities, including AI-based solutions and real-time malware detection.
- **Risk Management:** Offers strong encryption, data protection, and backup solutions with regulatory compliance in mind (e.g., HIPAA).
- **Service Excellence:** Excellent customer support and healthcare-specific training programs to improve usability and adoption.
- **Market Presence:** Widely adopted by healthcare organizations globally, especially for endpoint protection and malware defense.

These vendors stand out as the top choices for healthcare organizations based on their comprehensive end-to-end cybersecurity offerings that cover regulatory compliance, advanced threat protection, service excellence, and industry-specific solutions. They have demonstrated success in meeting the complex needs of healthcare providers, payers, and other stakeholders in the healthcare ecosystem.

Major Healthcare Cybersecurity Solutions by Functionality



Identity and Access Management (IAM)

- **Hospitals:** Controls access to sensitive patient records, clinical systems, and medical devices. Ensures only authorized personnel access operating rooms or pharmacy systems.
- **Physician Practices:** Manages access to electronic health records (EHRs) and practice management systems to prevent unauthorized access.
- **Payers:** Secures access to member records, claims processing systems, and underwriting data.

Endpoint Detection and Response (EDR)

- **Hospitals:** Monitors hospital devices, including workstations and connected medical devices, for potential security breaches.
- **Physician Practices:** Protects desktop computers, laptops, and mobile devices from malware and phishing attacks.
- **Payers:** Secures endpoints involved in claims processing and customer support operations.

Network Security

- **Hospitals:** Protects large, complex networks spanning multiple departments and connected devices, including firewalls and intrusion prevention.
- **Physician Practices:** Ensures a secure local network to protect patient data and secure communication with labs and pharmacies.
- **Payers:** Secures expansive networks that process vast amounts of member and claims data.

Data Loss Prevention (DLP)

- **Hospitals:** Prevents unauthorized access or transfer of sensitive patient data, especially during data-sharing with external partners.
- **Physician Practices:** Secures patient records from being shared or emailed inadvertently.
- **Payers:** Protects member data during claims review, processing, and inter-departmental communication.

Encryption

- **Hospitals:** Encrypts patient data in electronic health records and during data sharing across departments.
- **Physician Practices:** Encrypts communications with labs, pharmacies, and patients.
- **Payers:** Secures sensitive financial data, claims information, and policyholder communications.

Security Information and Event Management (SIEM)

- **Hospitals:** Aggregates and analyzes security logs from across the hospital to detect threats.
- **Physician Practices:** Provides insights into unusual activities in smaller, localized systems.
- **Payers:** Consolidates threat intelligence across nationwide systems.

Zero Trust Architecture

- **Hospitals:** Enforces strict access controls for clinicians, contractors, and vendors, assuming no inherent trust.
- **Physician Practices:** Verifies each access request to prevent unauthorized EHR usage.
- **Payers:** Ensures internal and external systems comply with rigorous authentication processes.

Cloud Security

- **Hospitals:** Protects cloud-based EHRs, imaging data, and telehealth services.
- **Physician Practices:** Safeguards practice management software hosted in the cloud.
- **Payers:** Secures cloud-based customer portals and claims processing systems.

IoT/IoMT Security

- **Hospitals:** Protects connected medical devices like infusion pumps and monitoring systems.
- **Physician Practices:** Secures diagnostic tools and wearable devices.
- **Payers:** Ensures safe data exchange from wearable health devices provided to policyholders.



Ransomware Protection and Recovery

- **Hospitals:** Prevents ransomware from locking critical hospital systems and disrupts attacks targeting emergency services.
- **Physician Practices:** Ensures rapid recovery of patient records and scheduling systems.
- **Payers:** Protects sensitive claims and policyholder data from encryption and theft.

Secure Messaging Platforms

- **Hospitals:** Enables secure communication among clinicians and staff to discuss patient care without exposing sensitive information.
- **Physician Practices:** Protects text and email communications with labs and pharmacies.
- **Payers:** Ensures encrypted communications with members and providers.

Threat Intelligence Platforms

- **Hospitals:** Tracks global cyber threats targeting healthcare institutions and updates defense mechanisms accordingly.
- **Physician Practices:** Provides alerts about regional phishing or ransomware campaigns.
- **Payers:** Monitors threats to large-scale payer operations and member-facing platforms.

Behavioral Analytics

- **Hospitals:** Identifies unusual login or access patterns to prevent insider threats.
- **Physician Practices:** Detects irregular access to patient records or billing systems.
- **Payers:** Monitors for fraudulent claims submission or unauthorized access attempts.

Mobile Device Management (MDM)

- **Hospitals:** Secures staff smartphones and tablets used for clinical decision-making.
- **Physician Practices:** Protects mobile devices used for remote patient care.
- **Payers:** Ensures security for employee devices accessing member data on the go.

Vulnerability Management

- **Hospitals:** Regularly scans for weaknesses in interconnected systems like imaging machines and EHRs.
- **Physician Practices:** Identifies vulnerabilities in smaller systems and software applications.
- **Payers:** Proactively addresses weaknesses in claims and billing software.

Privileged Access Management (PAM)

- **Hospitals:** Controls access to administrative functions of critical systems.
- **Physician Practices:** Secures access to billing and administrative software.
- **Payers:** Limits access to sensitive databases and financial systems.

Multi-Factor Authentication (MFA)

- **Hospitals:** Requires two or more verification steps to access EHRs or medical devices.
- **Physician Practices:** Ensures secure login to practice management systems.
- **Payers:** Protects member portals and internal systems from unauthorized access.

18. Secure Email Gateways

- **Hospitals:** Blocks phishing and malicious emails targeting staff.
- **Physician Practices:** Prevents malicious attachments and links from compromising systems.
- **Payers:** Protects email communication with members, providers, and partners.

Blockchain for Data Security

- **Hospitals:** Ensures immutable patient data records and secure data sharing.
- **Physician Practices:** Secures smaller-scale data exchanges with labs and pharmacies.
- **Payers:** Enables transparent and secure claims processing.

Incident Response Platforms

- **Hospitals:** Coordinates responses to breaches affecting critical hospital functions.



- **Physician Practices:** Provides structured responses to breaches or ransomware attacks.
- **Payers:** Facilitates swift action on detected breaches in member data systems.

Security Awareness Training

- **Hospitals:** Educates clinicians and staff on recognizing phishing and other cyber threats.
- **Physician Practices:** Trains staff to avoid mishandling patient data.
- **Payers:** Equips employees with skills to detect and mitigate social engineering threats.

Forensic Analysis Tools

- **Hospitals:** Investigates breaches to determine the extent of data compromise.
- **Physician Practices:** Analyzes incidents to improve future cybersecurity defenses.
- **Payers:** Tracks attack origins and methods in data breaches.

Patch Management Systems

- **Hospitals:** Ensures timely updates for medical devices and clinical software.
- **Physician Practices:** Automates updates for practice management systems.
- **Payers:** Ensures claims and billing systems remain up to date and secure.

Third-Party Risk Management

- **Hospitals:** Assesses security risks from external vendors like device manufacturers.
- **Physician Practices:** Evaluates risks from outsourced billing or IT services.
- **Payers:** Manages risks from third-party administrators and technology providers.

Telehealth Security

- **Hospitals:** Secures virtual consultations and remote monitoring systems.
- **Physician Practices:** Protects telemedicine platforms used for patient care.
- **Payers:** Ensures the security of remote health management and virtual care tools

Black Book's 18 Cybersecurity-Centric Key Performance Indicators for Healthcare Providers and Payers



Strategic Alignment and Industry Expertise

1. Compliance with Healthcare Regulations and Standards

- Assess the vendor's ability to demonstrate alignment with regulatory frameworks like HIPAA, GDPR, and HITECH through certifications, audits, and industry engagement.
- Evaluate their proactive approach to adapting to evolving regulatory requirements and communicating updates effectively.

2. Understanding and Alignment with Healthcare Needs

- Determine the vendor's ability to articulate a clear understanding of healthcare-specific cybersecurity challenges, such as EHR security and IoT device risks.
- Evaluate their use of real-world case studies and references that showcase tailored solutions for healthcare environments.

3. Alignment with Strategic Client Goals

- Assess how well the vendor integrates their solutions to support strategic healthcare goals, such as improving value-based care (VBC) initiatives, enabling health information exchanges (HIE), and advancing telehealth capabilities.
- Evaluate their ability to align their technology and services with a client's broader organizational mission and objectives.

Innovation and Product Usability

4. Integration and Interoperability with Existing Systems

- Evaluate how effectively the vendor demonstrates seamless integration with healthcare systems like EHRs, PACS, and telehealth platforms, ensuring minimal disruption during deployment.
- Assess the clarity and accessibility of their APIs and their capacity to support multi-system interoperability.

5. Scalability, Adaptability, and Cost Flexibility

- Assess the vendor's ability to articulate how their solutions can scale with organizational growth and adapt to changes in regulatory or operational needs.

- Evaluate how well the vendor communicates their pricing model's flexibility to accommodate diverse client budgets and requirements.

6. Innovation and Advanced Features

- Evaluate the vendor's focus on innovation by assessing their ability to introduce cutting-edge features, such as AI-driven threat detection or behavioral analytics, and their commitment to staying ahead of emerging threats.
- Review how well they communicate their product roadmap and investment in future technologies.

7. Usability and User Experience

- Assess the intuitiveness and accessibility of the vendor's interface, particularly for non-technical users such as clinicians and administrative staff.
- Evaluate feedback on the vendor's training and onboarding processes to ensure ease of adoption and use.

Service Excellence and Support

8. Technical Support Responsiveness and Quality

- Evaluate the vendor's ability to provide accessible, responsive, and effective support tailored to the needs of healthcare clients.
- Assess their communication style, clarity, and professionalism when resolving issues.

9. Training and Knowledge Transfer

- Determine how well the vendor supports healthcare clients with training programs, guides, and resources that improve understanding and usability of their solutions.
- Evaluate their ability to customize training to address specific healthcare workflows and compliance requirements.

10. Customization and Flexibility in Deployment

- Assess the vendor's openness to tailoring solutions to meet unique client requirements, such as integrating with legacy systems or accommodating specific regulatory constraints.
- Evaluate the range of deployment options they offer, such as cloud, on-premises, or hybrid environments.



Risk Management and Data Security

11. Incident Response and Threat Mitigation Capabilities

- Assess how effectively the vendor articulates their approach to identifying, managing, and resolving security incidents in healthcare settings.
- Evaluate their ability to communicate proactive measures for mitigating future risks.

12. Data Security, Privacy, and Backup Services

- Determine the vendor's ability to explain and implement strong data protection measures, such as encryption and secure backups.
- Evaluate their confidence in meeting privacy and reliability standards, especially in scenarios involving sensitive patient data.

13. Transparency in Security Practices and Reporting

- Assess the vendor's willingness to openly discuss their security policies, audit results, and past incidents, demonstrating accountability and trustworthiness.
- Evaluate their communication practices in providing regular updates and incident reports to clients.

Partnership and Collaboration

14. Vendor Relationship Management and Collaboration

- Assess the vendor's ability to build strong, trust-based relationships with clients, characterized by collaboration and cultural alignment.
- Evaluate feedback from other clients regarding the vendor's approach to partnership and ongoing engagement.

15. Third-Party Alliances and Ecosystem Integration

- Evaluate the vendor's ability to articulate their partnerships with other reputable cybersecurity or healthcare vendors and the added value these alliances bring to their solutions.
- Assess their ability to foster a seamless and integrated ecosystem that benefits healthcare clients.

Financial Viability and Value

16. Financial Stability and Long-Term Viability

- Evaluate the vendor's ability to demonstrate their financial health, long-term commitment to the healthcare sector, and investments in innovation.
- Assess client confidence in the vendor's sustainability and their ability to support future growth.

17. Value for Money and Return on Investment (ROI)

- Assess the vendor's ability to communicate the qualitative benefits of their solutions, such as improved security posture, reduced risk, and operational efficiency.
- Evaluate how well the vendor aligns their pricing with the perceived value of their services.

Performance Metrics and Market Presence

18. Proven Success and Adoption in Healthcare

- Assess the vendor's ability to demonstrate a strong track record of successful implementations in healthcare through case studies, testimonials, and references.
- Evaluate their market credibility and reputation as a trusted partner in the healthcare industry.

Expanded Black Book Scoring Guidance



Scoring Framework for Evaluating Healthcare Cybersecurity Vendors

To effectively assess healthcare cybersecurity vendors against the 18 Key Performance Indicators (KPIs), organizations can use a 1-to-10 scoring scale. This approach ensures a consistent and transparent evaluation process, balancing both qualitative perceptions and measurable performance metrics. Below is an explanation of how the scoring framework is tailored specifically to evaluating cybersecurity vendors in the healthcare sector.

Scoring Framework

1. 1 (Deal-Breaking Dissatisfaction)

This score indicates significant deficiencies in the vendor's performance or capabilities that pose substantial risks to cybersecurity and operations.

- **Examples in Healthcare Cybersecurity:**

- Non-compliance with HIPAA, GDPR, or other critical healthcare regulations.
- Poor incident response times resulting in prolonged downtime or unresolved breaches.
- Persistent vulnerabilities in the vendor's solutions that expose patient data to cyberattacks.
- Failure to provide adequate encryption or secure integration with healthcare systems like EHRs and telehealth platforms.

- **Implications:**

A score of 1 reflects an urgent need to replace the vendor due to unacceptable risks to the organization's security, compliance, and reputation.

2. 2–5 (Below Expectations)

Scores in this range highlight recurring problems or underperformance in critical areas, leading to concerns about the vendor's reliability and effectiveness.

- **Examples in Healthcare Cybersecurity:**

- Limited scalability of solutions, making them inadequate for growing organizations or evolving cybersecurity threats.
- Outdated technology that lacks advanced features such as AI-driven threat detection or behavioral analytics.
- Inconsistent customer support, resulting in delays during critical incidents.
- Poor user satisfaction due to non-intuitive interfaces or lack of training resources.

- **Implications:**

Vendors scoring in this range may require contract renegotiation or immediate improvement plans to address deficiencies and restore stakeholder confidence.

3. 6–7 (Meets Minimum Expectations)

Vendors scoring 6–7 meet baseline requirements but lack standout performance.

- **Examples in Healthcare Cybersecurity:**

- Solutions comply with regulatory standards but do not offer proactive features like Zero Trust architecture or threat intelligence.
- The vendor delivers adequate uptime and system availability but does not excel in incident response times or innovation.
- Training and support are provided but require improvement to enhance usability for non-technical healthcare staff.

- **Implications:**

These vendors are functional but may not provide the best long-term value. Organizations might retain them temporarily while exploring more innovative alternatives.

4. 8–9 (Exceeds Expectations)

Scores of 8–9 represent vendors that consistently exceed industry standards and deliver exceptional value in healthcare cybersecurity.

- **Examples in Healthcare Cybersecurity:**

- Seamless integration with healthcare systems like EHRs, PACS, and IoT/IoMT devices, ensuring robust interoperability.

- Advanced threat detection capabilities, such as AI-driven behavioral analytics and automated risk mitigation.
- Proactive compliance updates and clear communication about evolving regulatory requirements.
- Highly responsive 24/7 technical support and effective training programs tailored to healthcare environments.
- **Implications:**
Vendors scoring in this range are strong candidates for long-term partnerships, demonstrating a clear alignment with organizational goals and priorities.

5. 10 (Overwhelmingly Exceeds Expectations)

A score of 10 is reserved for vendors that deliver transformational benefits and consistently surpass expectations in all evaluated areas.

- **Examples in Healthcare Cybersecurity:**
 - Demonstrated ROI through detailed case studies showcasing significant risk reduction and efficiency gains.
 - Innovative solutions tailored specifically to healthcare challenges, such as securing IoMT ecosystems or preventing ransomware attacks.
 - Exceptional transparency in security practices and incident reporting, fostering trust and collaboration.
 - Unmatched customer support, proactive relationship management, and regular innovation that addresses emerging threats.
- **Implications:**
These vendors are considered indispensable strategic partners, offering unparalleled expertise and value.

Scoring Thresholds

- **Scores Below 6:**
Indicate underperformance and potential misalignment with healthcare cybersecurity requirements. Vendors in this category should be considered for replacement or immediate performance improvement.
- **Scores of 8 and Above:**
Reflect vendors that outperform industry benchmarks, demonstrating excellence in cybersecurity practices, innovation, and customer satisfaction.
- **Industry Benchmark:**
As of 2024, the average score for healthcare cybersecurity vendors across the 18 KPIs was **8.05/10**. Vendors scoring below this average may be considered subpar relative to competitors.

Scoring Considerations

1. Evidence-Based Assessment:

- Support scores with tangible evidence such as uptime statistics, ROI reports, client testimonials, and regulatory compliance certifications.
- Evaluate the effectiveness of solutions in real-world scenarios, such as during simulated breaches or tabletop exercises.

2. Stakeholder Feedback:

- Incorporate insights from IT teams, administrators, clinicians, and end-users to ensure a comprehensive evaluation.
- Focus on areas like usability, support responsiveness, and alignment with organizational goals.

3. Weighting of KPIs:

- Assign equal weight to all KPIs unless specific areas, such as compliance or incident response, are deemed more critical for the organization's priorities.

4. Trend Analysis:

- Compare the current evaluation to past assessments to identify improvements or declines in vendor performance.
- Use trend analysis to track vendors' ability to adapt to evolving cybersecurity threats.

5. Qualitative Insights:

- Document specific strengths and weaknesses for each KPI, providing actionable feedback for internal decision-making or vendor discussions.
- Include contextual factors, such as how the vendor performed during a recent cybersecurity incident.

This scoring framework provides a structured approach to evaluating healthcare cybersecurity vendors. By combining qualitative insights with evidence-based assessments, organizations can identify vendors that best align with their security needs, compliance requirements, and long-term goals. The inclusion of industry benchmarks and stakeholder feedback ensures a well-rounded evaluation process, empowering healthcare entities to make informed decisions about vendor retention, replacement, or strategic partnerships.

Client Experience Satisfaction Ratings 2025

**Rated on Black Book's 18
Cybersecurity KPIs**



Identity and Access Management (IAM)

1. Okta
2. Ping Identity
3. Imprivata
4. SailPoint
5. ForgeRock
6. CyberArk
7. OneLogin
8. Microsoft Azure Active Directory
9. IBM Security Verify
10. Duo Security (Cisco)
11. SecureAuth
12. Centrify
13. RSA SecurID
14. HID Global
15. Auth0
16. BeyondTrust
17. Trustwave
18. ManageEngine (ADSelfService Plus)
19. Saviynt
20. Keeper Security



Endpoint Detection and Response (EDR)

1. CrowdStrike
2. Carbon Black (VMware)
3. SentinelOne
4. Sophos
5. McAfee Endpoint Security
6. Trend Micro
7. Symantec Endpoint Protection
8. Bitdefender GravityZone
9. Kaspersky Endpoint Security
10. ESET Endpoint Security
11. FireEye Endpoint Security (Trellix)
12. Palo Alto Networks Cortex XDR
13. FortiEDR (Fortinet)
14. Check Point Harmony Endpoint
15. BlackBerry Cylance
16. Deep Instinct
17. Malwarebytes Endpoint Protection
18. Ivanti Endpoint Security
19. Tanium
20. SecureWorks Taegis

Network Security

1. Palo Alto Networks
2. Cisco Secure
3. Fortinet
4. Check Point Software
5. Juniper Networks
6. SonicWall
7. Barracuda Networks
8. WatchGuard
9. Arista Networks
10. Versa Networks
11. Extreme Networks
12. Zscaler
13. Forcepoint
14. Aruba Networks
15. Sophos Firewall
16. Trend Micro TippingPoint
17. Imperva
18. Netskope
19. Untangle (Arista)
20. Citrix ADC



Data Loss Prevention (DLP)

1. Symantec (Broadcom)
2. Forcepoint
3. Digital Guardian
4. McAfee Total Protection for DLP
5. Trend Micro DLP
6. Varonis
7. Code42
8. Proofpoint
9. Netwrix Auditor
10. Microsoft 365 DLP
11. Palo Alto Networks DLP
12. SecureTrust DLP
13. GTB Technologies
14. Fidelis Cybersecurity
15. Spirion
16. Teramind
17. Clearswift DLP
18. Zecurion
19. InfoWatch
20. Exabeam DLP

Encryption

1. Thales Group
2. Zscaler
3. Virtru
4. Sophos Encryption
5. Symantec Encryption
6. McAfee Complete Data Protection
7. IBM Guardium
8. BitLocker (Microsoft)
9. Dell Data Protection Encryption
10. Trend Micro Encryption
11. WinMagic SecureDoc
12. Digital Guardian Encryption
13. AxCrypt
14. VeraCrypt
15. Boxcryptor
16. ESET Endpoint Encryption
17. EncryptRIGHT (PKWARE)
18. Fortanix
19. OpenText (Carbonite Endpoint Encryption)
20. Vormetric



Security Information and Event Management (SIEM)

1. Splunk
2. IBM Security QRadar
3. LogRhythm
4. SolarWinds Security Event Manager
5. Sumo Logic
6. AlienVault (AT&T Cybersecurity)
7. Exabeam
8. Elastic Security
9. McAfee Enterprise Security Manager
10. Netsurion EventTracker
11. Fortinet FortiSIEM
12. Rapid7 InsightIDR
13. ArcSight (Micro Focus)
14. Microsoft Azure Sentinel
15. RSA NetWitness
16. SentinelOne Vigilance Respond
17. Trend Micro Vision One
18. Devo Technology
19. Blumira
20. Graylog

Zero Trust Architecture

1. Okta
2. Palo Alto Networks
3. Zscaler
4. Illumio
5. Cisco Zero Trust
6. Microsoft Zero Trust Solutions
7. Symantec Zero Trust
8. Fortinet Zero Trust
9. Duo Security (Cisco)
10. BeyondTrust Zero Trust
11. CyberArk Zero Trust
12. RSA Zero Trust
13. Netskope Zero Trust
14. Ping Identity Zero Trust
15. IBM Security Zero Trust
16. VMware Zero Trust Solutions
17. Trend Micro Zero Trust
18. Citrix Zero Trust
19. Appgate SDP
20. Forrester Zero Trust Partners



Cloud Security

1. Amazon Web Services (AWS) Security
2. Microsoft Azure Security
3. Google Cloud Security
4. Palo Alto Networks Prisma
5. Zscaler Cloud Security
6. Netskope Cloud Security
7. Fortinet Cloud Security
8. Check Point CloudGuard
9. Sophos Cloud Optix
10. Trend Micro Cloud One
11. Cisco Umbrella
12. Proofpoint Cloud Security
13. CrowdStrike Falcon Cloud
14. Oracle Cloud Security
15. IBM Cloud Security
16. FireEye Cloud Security
17. Cloudflare
18. Barracuda CloudGen
19. Akamai Cloud Security
20. Lacework

IoT/IoMT Security

1. Armis
2. Medigate (by Claroty)
3. Forescout
4. CyberMDX
5. Axonius
6. Palo Alto Networks IoT Security
7. Zingbox (Fortinet)
8. Check Point IoT Protect
9. Cisco IoT Threat Defense
10. Trend Micro IoT Security
11. Dragos (Industrial IoT)
12. Darktrace IoT
13. Senrio Insight
14. Sectigo IoT Manager
15. AWS IoT Device Defender
16. Thales IoT Solutions
17. Kaspersky IoT Security
18. Symantec IoT Security
19. Cynerio
20. Arm Pelion IoT



Ransomware Protection and Recovery

1. Sophos Intercept X
2. CrowdStrike Falcon
3. Rubrik
4. Acronis Cyber Protect
5. Carbon Black (VMware)
6. SentinelOne Singularity
7. Palo Alto Networks Cortex XDR
8. FireEye Endpoint Security
9. Malwarebytes for Business
10. Kaspersky Anti-Ransomware
11. Barracuda Ransomware Protection
12. Veritas NetBackup
13. Cohesity DataProtect
14. Commvault Complete Backup
15. Trend Micro Worry-Free
16. IBM Spectrum Protect
17. Check Point Harmony Endpoint
18. Cybereason RansomFree
19. Microsoft Defender ATP
20. Arcserve UDP

Secure Messaging Platforms

1. Spok
2. TigerConnect
3. Imprivata Cortext
4. Vocera Communications
5. Pulsara
6. Forward Advantage
7. PerfectServe
8. Halo Health
9. Klara
10. Symphony Communication Services
11. OnPage Secure Messaging
12. Telmediq (by PerfectServe)
13. Zinc Secure Messaging
14. Cerner Secure Messaging
15. Epic Secure Chat
16. WhatsApp for Business API (with encryption tools)
17. Wickr (AWS)
18. Signal Secure Messaging
19. MEDITECH Expanse Secure Messaging
20. Voalte (by Hillrom)



Threat Intelligence Platforms

1. Recorded Future
2. FireEye Threat Intelligence (Trellix)
3. Anomali
4. ThreatConnect
5. Palo Alto Networks Unit 42
6. IBM X-Force Exchange
7. Cisco Talos
8. CrowdStrike Threat Intelligence
9. Check Point ThreatCloud
10. Kaspersky Threat Intelligence
11. McAfee Advanced Threat Defense
12. Cybereason Threat Analysis
13. AlienVault Threat Intelligence
14. Fortinet FortiGuard Labs
15. ThreatQuotient
16. EclecticlQ
17. SophosLabs
18. Bitdefender Threat Intelligence
19. F-Secure Countercept
20. ZeroFox Threat Intelligence

Behavioral Analytics

1. Exabeam
2. Varonis
3. Splunk Behavioral Analytics
4. Darktrace
5. LogRhythm UEBA
6. Fortinet FortiInsight
7. ObservelT (Proofpoint)
8. Rapid7 InsightIDR
9. Sumo Logic Behavioral Analysis
10. Cynet 360 Behavioral Analytics
11. Microsoft Advanced Threat Analytics (ATA)
12. Ekran System
13. Securonix UEBA
14. Forcepoint Behavioral Analytics
15. IBM Security QRadar UEBA
16. NetWitness UEBA
17. Cybereason Defense Platform
18. ESET Inspect
19. Gurukul Behavioral Analytics
20. Balbix



Mobile Device Management (MDM)

1. VMware Workspace ONE
2. Jamf Pro
3. MobileIron (Ivanti)
4. Citrix Endpoint Management
5. BlackBerry UEM
6. Microsoft Intune
7. IBM MaaS360
8. SOTI MobiControl
9. Sophos Mobile Security
10. ManageEngine Mobile Device Manager Plus
11. Trend Micro Mobile Security
12. Symantec Endpoint Security Mobile
13. Knox Manage (Samsung)
14. Scalefusion MDM
15. 42Gears SureMDM
16. Cisco Meraki Systems Manager
17. Hexnode MDM
18. Codeproof Enterprise MDM
19. Kandji
20. Baramundi Management Suite

Vulnerability Management

1. Tenable
2. Qualys
3. Rapid7
4. Palo Alto Networks Prisma Cloud
5. Microsoft Defender Vulnerability Management
6. BeyondTrust Retina
7. CrowdStrike Falcon Spotlight
8. Ivanti Neurons for Vulnerability Management
9. SolarWinds Network Vulnerability Detection
10. F-Secure Radar
11. GFI LanGuard
12. Nexpose (Rapid7)
13. AWS Inspector
14. SecPod SanerNow
15. OpenVAS (Greenbone Networks)
16. Skybox Security
17. Tripwire IP360
18. Acunetix Vulnerability Scanner
19. InsightVM (Rapid7)
20. Censys



Privileged Access Management (PAM)

1. CyberArk
2. BeyondTrust
3. Thycotic (Delinea)
4. ManageEngine PAM360
5. IBM Security Secret Server
6. Centrify Privileged Access Service
7. ARCON PAM
8. Netwrix Privilege Secure
9. Remediant SecureONE
10. Fudo Security PAM
11. Wallix Bastion
12. Hitachi ID PAM
13. Devolutions PAM
14. KeeperPAM
15. Saviynt Privileged Access Management
16. Foxpass PAM
17. One Identity Safeguard
18. CA Privileged Access Manager
19. HashiCorp Vault
20. SolarWinds Access Rights Manager

Multi-Factor Authentication (MFA)

1. Duo Security (Cisco)
2. Okta MFA
3. Ping Identity MFA
4. Microsoft Authenticator
5. Google Authenticator
6. RSA SecurID
7. Symantec VIP Access
8. OneLogin Protect
9. Authy (Twilio)
10. Yubico YubiKey
11. SecureAuth MFA
12. HID Global ActivID
13. LastPass MFA
14. Fortinet FortiToken
15. Keycloak
16. Thales SafeNet MFA
17. Dashlane MFA
18. Entrust Identity MFA
19. Keeper Security MFA
20. ESET Secure Authentication



Secure Email Gateways

1. Proofpoint Email Protection
2. Mimecast Secure Email Gateway
3. Barracuda Email Security Gateway
4. Cisco Secure Email
5. Sophos Email Protection
6. Fortinet FortiMail
7. Symantec Email Security
8. Trend Micro Hosted Email Security
9. Zix Email Encryption
10. FireEye Email Security (Trellix)
11. SolarWinds Mail Assure
12. Ironscales
13. Vade Secure
14. TitanHQ SpamTitan
15. Check Point Email Security
16. Area 1 Security (Cloudflare)
17. Virtru Email Encryption
18. Perception Point
19. Egress Protect
20. Microsoft Defender for Office 365

Blockchain for Data Security

1. Guardtime
2. Hashed Health
3. Solve.Care
4. Blockpharma
5. Factom
6. IBM Blockchain
7. Microsoft Azure Blockchain
8. MedRec
9. PokitDok Blockchain
10. Chronicled
11. SimplyVital Health
12. HealthCombix
13. Coral Health
14. BurstIQ
15. Doc.ai
16. FarmaTrust
17. Guardtime Health
18. PeerLedger
19. EncrypGen
20. Chainalysis



Incident Response Platforms

1. Palo Alto Networks Cortex XSOAR
2. IBM Security Resilient
3. Splunk Phantom
4. Rapid7 InsightConnect
5. Microsoft Sentinel Incident Response
6. FireEye Helix (Trellix)
7. Cisco SecureX
8. D3 Security
9. Swimlane
10. Siemplify (Google Chronicle)
11. LogRhythm SOAR
12. Fortinet FortiSOAR
13. ThreatConnect IRM
14. CyberSponse (Arctic Wolf)
15. Sumo Logic SOAR
16. Symantec Managed Security Services
17. Exabeam Incident Responder
18. CrowdStrike Falcon Fusion
19. AWS Security Hub
20. Elastic Security

Security Awareness Training

1. KnowBe4
2. Infosec IQ
3. Proofpoint Security Awareness Training
4. SANS Security Awareness
5. Mimecast Awareness Training
6. CyberVista
7. Terranova Security
8. ESET Cybersecurity Awareness
9. Wombat Security (Proofpoint)
10. PhishMe (Cofense)
11. Barracuda PhishLine
12. Inspired eLearning
13. Security Mentor
14. Curricula Security Awareness Training
15. Habitu8
16. MetaCompliance
17. Webroot Security Awareness Training
18. ThreatSim
19. Arctic Wolf Managed Security Awareness
20. AttackIQ Cybersecurity Training



Forensic Analysis Tools

1. EnCase (OpenText)
2. Magnet AXIOM
3. FTK (Forensic Toolkit) by Exterro
4. Cellebrite
5. Paraben E3 Platform
6. X-Ways Forensics
7. Belkasoft Evidence Center
8. Autopsy (Sleuth Kit)
9. Oxygen Forensics
10. BlackBag Blacklight (OpenText)
11. CrowdStrike Falcon Forensics
12. Palo Alto Networks Cortex XDR Forensics
13. Kroll Artifact Parser and Extractor (KAPE)
14. FireEye Endpoint Security (Trellix)
15. AccessData Forensic Tools (Exterro)
16. Basis Technology Autopsy
17. LogRhythm Forensic Suite
18. CyFIR Investigator
19. Cado Response
20. SANS Investigative Forensics Toolkit (SIFT)

Patch Management Systems

1. Ivanti Patch Management
2. ManageEngine Patch Manager Plus
3. SolarWinds Patch Manager
4. Microsoft SCCM (System Center Configuration Manager)
5. Automox
6. PDQ Deploy
7. GFI LanGuard
8. Kaseya VSA
9. ConnectWise Automate
10. Symantec Endpoint Management (Broadcom)
11. Quest KACE Systems Management
12. Flexera Software Vulnerability Manager
13. Atera Patch Management
14. Qualys Patch Management
15. Rapid7 Patch Management
16. Patch My PC
17. Ninite Pro
18. VMware Workspace ONE Patch Management
19. CrowdStrike Falcon Spotlight Patch Management
20. Tanium Patch



Third-Party Risk Management

1. Prevalent
2. BitSight
3. RiskRecon (Mastercard)
4. SecurityScorecard
5. UpGuard
6. OneTrust Vendorpedia
7. ProcessUnity
8. Aravo
9. RSA Archer Third-Party Risk Management
10. LogicGate Risk Cloud
11. RiskWatch
12. CyberGRX
13. VendorInsight
14. Panorays
15. KY3P (S&P Global)
16. Shared Assessments Third-Party Risk Tools
17. Fortinet Vendor Risk Management
18. MetricStream Third-Party Risk
19. TrustArc Vendor Management
20. EcoVadis

Telehealth Security

1. Teladoc Health
2. Amwell (American Well)
3. Doxy.me
4. Zoom for Healthcare
5. Microsoft Teams for Healthcare
6. Cisco Webex for Healthcare
7. VSee
8. Mend Telemedicine Platform
9. eVisit
10. Medici Telehealth
11. Epic Telehealth Integration
12. Cerner Telehealth Solutions
13. InTouch Health (Teladoc)
14. SimplePractice Telehealth
15. Mend VIP Telehealth
16. Updox Telehealth
17. Chiron Health
18. CareClix
19. HealthTap
20. VidyoConnect for Telehealth



Alphabetical Directory of Healthcare Cybersecurity Vendors

**Products and Services Receiving
Black Book Scoring 2025**



1. 42Gears SureMDM

42Gears SureMDM is a comprehensive mobile device management (MDM) solution designed to secure and manage endpoints across diverse environments. The platform provides centralized control over mobile devices, wearables, and IoT endpoints, enabling healthcare organizations to maintain data security and compliance. SureMDM offers features like remote device configuration, real-time monitoring, and automated updates, critical for healthcare settings where mobile access to patient records and clinical tools is essential.

In healthcare, SureMDM ensures the secure operation of mobile devices used by clinicians, administrators, and telehealth providers. For hospitals, it supports compliance with regulations like HIPAA by controlling access to sensitive data on devices used for patient care. For payers and pharmaceutical companies, the platform safeguards devices used in remote work scenarios, ensuring secure communication and collaboration.

2. ARCON Privileged Access Management (PAM)

ARCON PAM is a robust solution for managing and securing privileged access to critical IT systems. By providing centralized control and monitoring of administrative accounts, ARCON PAM helps organizations mitigate the risk of insider threats and unauthorized access. Its key features include session monitoring, real-time alerts, and automated workflows for granting and revoking access.

In healthcare, ARCON PAM plays a vital role in protecting sensitive systems like electronic health records (EHRs), claims processing platforms, and medical device networks. Hospitals and health systems use PAM to enforce strict access controls, ensuring that only authorized personnel can manage critical infrastructure. The solution also supports compliance with regulations such as GDPR and HITECH by maintaining detailed audit trails of all privileged account activities.

3. AWS Inspector

AWS Inspector is a vulnerability management service that assesses workloads on the Amazon Web Services (AWS) cloud platform. It identifies security vulnerabilities, misconfigurations, and deviations from best practices, providing actionable insights to enhance cloud security. AWS Inspector integrates with other AWS security services for streamlined operations and automated compliance checks.



For healthcare organizations leveraging AWS for EHR hosting, telehealth platforms, or analytics, AWS Inspector ensures that workloads remain secure and compliant. Hospitals and payers can use the tool to continuously monitor cloud-based systems, safeguarding patient data from breaches. Its automated reports help organizations quickly address vulnerabilities, reducing the risk of cyberattacks.

4. AWS IoT Device Defender

AWS IoT Device Defender provides comprehensive security management for IoT devices connected to AWS. It monitors devices for unusual activity, enforces compliance policies, and mitigates risks through automated alerts. Healthcare organizations increasingly depend on IoT devices such as wearable health monitors and connected infusion pumps, making security critical.

Hospitals and health systems can leverage AWS IoT Device Defender to secure medical devices connected to the cloud. The solution supports patient safety by ensuring that devices operate without interference from cyber threats. For pharmaceutical companies using IoT devices in clinical trials, it helps maintain data integrity and regulatory compliance.

5. AWS Security Hub

AWS Security Hub is a centralized platform that aggregates and analyzes security data from various AWS services. It offers a unified view of security compliance, threat intelligence, and incident response activities. By integrating with third-party security tools, Security Hub helps organizations enhance their overall security posture.

Healthcare organizations benefit from AWS Security Hub by gaining visibility into their cloud environments. Hospitals can monitor compliance with HIPAA and other regulations, while EHR vendors and payers use it to streamline threat detection and response. Its integration capabilities make it a versatile tool for securing complex healthcare IT infrastructures.

6. AccessData Forensic Tools (Exterro)

AccessData Forensic Tools, now part of Exterro, specializes in digital forensic investigations and incident response. The tools enable organizations to investigate data breaches, analyze cyberattacks, and ensure compliance with legal requirements. Features like file recovery, timeline reconstruction, and endpoint analysis make it a powerful solution for security teams.

Healthcare organizations use AccessData to investigate breaches involving patient records, ensuring timely and thorough incident response. Hospitals can track the source of unauthorized access, while payers rely on its capabilities to safeguard claims data. The tools also assist in legal cases by preserving evidence with forensic precision.

7. Acronis Cyber Protect

Acronis Cyber Protect integrates data backup, anti-malware, and endpoint protection into a single platform. It provides healthcare organizations with a unified approach to securing data, reducing downtime, and recovering from ransomware attacks. Features like real-time threat detection, patch management, and automated backups ensure business continuity.

For hospitals, Acronis protects patient data stored in EHRs and imaging systems, ensuring compliance with HIPAA. Pharmaceutical companies use it to secure research data, while payers rely on its recovery capabilities to maintain operational efficiency during cyber incidents. Its multi-layered security approach is ideal for complex healthcare environments.

8. Acunetix Vulnerability Scanner

Acunetix Vulnerability Scanner is a web application security testing tool designed to identify and remediate vulnerabilities like SQL injection, XSS, and misconfigurations. It automates scanning for security flaws, providing actionable reports to prioritize remediation.

In healthcare, Acunetix helps protect web applications such as patient portals, telehealth platforms, and insurance websites. Hospitals use it to secure public-facing systems from exploitation, while payers rely on it to safeguard online claims portals. Its integration with CI/CD pipelines also supports secure application development in EHR and health IT projects.

9. Akamai Cloud Security

Akamai Cloud Security provides web application protection, DDoS mitigation, and zero-trust security for cloud environments. Its edge platform enhances performance and security by minimizing latency and delivering scalable threat protection.

For healthcare providers, Akamai secures patient portals, telehealth systems, and cloud-hosted EHR platforms. Payers and health systems use it to prevent downtime during cyberattacks, maintaining patient trust and operational integrity. Its robust security features ensure compliance with healthcare regulations and safeguard sensitive data.



10. AlienVault (AT&T Cybersecurity)

AlienVault, now part of AT&T Cybersecurity, offers Unified Security Management (USM) tools that combine SIEM, threat intelligence, and incident response capabilities. It provides organizations with comprehensive visibility into their security posture, enabling proactive threat mitigation.

Hospitals and health systems benefit from AlienVault's ability to monitor complex networks and detect advanced threats. Payers and EHR vendors use the platform to maintain regulatory compliance and respond to potential breaches effectively. Its affordability and ease of deployment make it a preferred choice for mid-sized healthcare organizations.

11. AlienVault Threat Intelligence

AlienVault Threat Intelligence, a component of AT&T Cybersecurity's suite, provides organizations with actionable insights into emerging threats. By aggregating global threat data and correlating it with local security logs, it helps identify potential vulnerabilities and anomalous activities in real time.

Healthcare providers use AlienVault Threat Intelligence to protect sensitive patient data from evolving cyber threats. Hospitals and payers benefit from its ability to monitor threat landscapes, including ransomware and phishing campaigns, enabling proactive defense strategies. The platform also helps ensure compliance by identifying and addressing security gaps in EHR systems and other critical infrastructure.

12. Amazon Web Services (AWS) Security

AWS Security encompasses a range of services designed to secure cloud workloads and infrastructure. With offerings like Identity and Access Management (IAM), encryption, and network firewalls, AWS Security ensures robust protection for data hosted on the cloud. Its automation capabilities streamline compliance with healthcare regulations like HIPAA and GDPR.

Healthcare organizations leverage AWS Security to protect cloud-hosted EHRs, analytics platforms, and telehealth services. Hospitals use it to ensure secure data exchange, while pharmaceutical companies trust its encryption tools for safeguarding clinical trial data. Its scalable solutions make it ideal for health systems of all sizes.

13. Amwell (American Well)

Amwell is a leading telehealth provider that enables secure, high-quality virtual healthcare experiences. Its platform supports video consultations, remote monitoring, and integration with EHR systems. Amwell's robust security features, including end-to-end encryption and compliance with HIPAA, ensure patient data protection during telehealth sessions.

Hospitals use Amwell to extend care delivery beyond physical facilities, improving access for rural and underserved populations. For payers, the platform reduces costs by offering virtual care alternatives. Pharmaceutical companies also benefit by using Amwell for remote clinical trial consultations and patient monitoring.

14. Anomali

Anomali specializes in threat intelligence and cybersecurity analytics, offering solutions to detect, investigate, and respond to advanced threats. Its platform aggregates threat data from multiple sources, correlating it with internal logs to identify vulnerabilities and breaches.

In healthcare, Anomali helps hospitals monitor threats targeting EHR systems and medical devices. Payers use its predictive analytics to protect claims processing systems from fraud, while pharmaceutical companies leverage it to safeguard intellectual property from cyber espionage. Its advanced threat hunting capabilities enhance overall security posture.

15. Appgate SDP

Appgate Software-Defined Perimeter (SDP) delivers a zero-trust network access solution that protects applications and resources from unauthorized access. By dynamically granting access based on user identity and context, it ensures that only legitimate users can interact with critical systems.

Healthcare providers use Appgate SDP to secure access to EHRs, billing systems, and telehealth platforms. For payers, it enhances protection for member portals and claims processing systems. Pharmaceutical companies also leverage its zero-trust architecture to secure R&D environments and collaboration tools.

16. Aravo

Aravo provides third-party risk management solutions that help organizations assess, monitor, and mitigate risks from vendors and suppliers. Its platform enables continuous monitoring of third-party relationships, ensuring compliance with healthcare regulations.

Hospitals and health systems use Aravo to manage risks associated with medical device suppliers and outsourced IT services. Payers leverage its capabilities to evaluate third-party claims processors, while EHR vendors use it to ensure their software integrates securely with external platforms.

17. ArcSight (Micro Focus)

ArcSight, a product by Micro Focus, is a security information and event management (SIEM) platform that consolidates log data, detects threats, and automates responses. Its real-time monitoring capabilities enable organizations to identify and neutralize security incidents quickly.

Healthcare organizations use ArcSight to monitor networks for unauthorized access to patient data and medical systems. Hospitals benefit from its integration with IoT devices, while payers rely on it to secure claims processing systems. Its compliance reporting features are essential for meeting HIPAA and GDPR requirements.

18. Arcserve UDP

Arcserve UDP (Unified Data Protection) combines backup, disaster recovery, and ransomware protection in a single platform. Its continuous data replication ensures minimal downtime and rapid recovery in the event of a cyberattack.

Hospitals use Arcserve UDP to protect critical systems like EHRs and imaging databases, ensuring uninterrupted care delivery. Payers rely on its backup capabilities to safeguard claims data, while pharmaceutical companies benefit from its disaster recovery solutions to maintain operational continuity during cybersecurity incidents.

19. Arctic Wolf Managed Security Awareness

Arctic Wolf Managed Security Awareness focuses on employee training and education to combat social engineering and phishing threats. Its personalized training programs adapt to organizational needs, ensuring that staff remain vigilant against cyber risks.

Healthcare providers use Arctic Wolf to educate clinicians and administrative staff on safeguarding patient data. Payers benefit from its tailored modules that address risks specific to claims processing and member portals. The platform's continuous reinforcement of best practices reduces human-related vulnerabilities.

20. Area 1 Security (Cloudflare)

Area 1 Security, a Cloudflare company, specializes in preemptive email security to block phishing attacks before they reach inboxes. Its cloud-based platform analyzes email traffic in real time, identifying and mitigating threats like malware and credential theft.

Hospitals use Area 1 Security to protect staff email systems from phishing campaigns targeting EHR credentials. Payers rely on it to secure communications with members and providers. Its proactive approach minimizes the risk of breaches originating from email-based attacks, safeguarding patient and financial data.

21. Arista Networks

Arista Networks specializes in high-performance networking solutions designed for large-scale data centers and cloud environments. Their software-driven approach ensures secure and efficient network management. With capabilities like real-time telemetry, network segmentation, and automation, Arista supports advanced cybersecurity practices.

In healthcare, Arista is ideal for hospitals and health systems managing extensive networks with high data volumes, such as imaging and EHR systems. Payers use its networking solutions to streamline claims processing and secure data exchange. Its robust network security features help meet compliance requirements like HIPAA.

22. Arm Pelion IoT

Arm Pelion IoT is a comprehensive IoT platform that provides device management, data analysis, and secure connectivity. It simplifies the deployment and management of connected devices, ensuring secure communication and data exchange.

Healthcare organizations leverage Pelion IoT to manage medical devices such as infusion pumps, patient monitors, and wearables. For pharmaceutical companies, it supports clinical trials by securely gathering data from IoT-enabled devices. Its security features protect patient data and ensure compliance with healthcare regulations.

23. Armis

Armis is a leading IoT security platform that provides visibility and control over connected devices. It identifies, monitors, and protects unmanaged devices, including medical equipment and IoT endpoints, from cyber threats.

Hospitals use Armis to safeguard medical devices such as imaging systems and ventilators from cyberattacks. Payers and health systems rely on it to secure IoT devices used in patient care and operational processes. Its ability to integrate with existing IT infrastructure ensures comprehensive protection without disrupting workflows.

24. Aruba Networks

Aruba Networks, a Hewlett Packard Enterprise company, delivers secure wireless and wired networking solutions. With features like network access control (NAC) and AI-powered threat detection, Aruba ensures secure connectivity for healthcare organizations.

Hospitals use Aruba to support reliable Wi-Fi access for clinicians and patients while protecting sensitive data. Health systems benefit from its ability to segment networks, isolating medical devices to prevent breaches. Its scalability makes it a preferred choice for expanding healthcare facilities.

25. Atera Patch Management

Atera offers an all-in-one remote monitoring and management (RMM) platform that includes patch management capabilities. It automates the deployment of security updates to ensure endpoint protection and compliance.

Healthcare providers use Atera to maintain up-to-date software on endpoints like workstations and mobile devices. Payers benefit from its automated patching, which reduces vulnerabilities in claims processing systems. Its real-time monitoring ensures that IT teams can address potential issues proactively.

26. AttackIQ Cybersecurity Training

AttackIQ focuses on adversary emulation and security validation, providing organizations with tools to test and improve their defenses. Its platform trains IT teams to identify and mitigate vulnerabilities effectively.

Hospitals use AttackIQ to simulate cyberattacks on EHR systems and evaluate their response readiness. Health systems and payers leverage its training modules to enhance staff awareness and preparedness against advanced threats, reducing the likelihood of successful breaches.

27. Auth0

Auth0, now part of Okta, specializes in identity and access management (IAM) solutions that secure user authentication and authorization processes. Its platform supports multi-factor authentication (MFA), single sign-on (SSO), and user identity verification.

Healthcare providers use Auth0 to secure patient portals and telehealth platforms, ensuring only authorized access. Payers rely on it to protect member-facing systems, while EHR vendors integrate its authentication features to enhance system security.

28. Authy (Twilio)

Authy provides multi-factor authentication (MFA) solutions that strengthen login security. By requiring an additional layer of verification, Authy protects against unauthorized access and credential theft.

In healthcare, Authy secures access to EHR systems, patient portals, and mobile apps. Hospitals and payers use its features to safeguard sensitive data, while pharmaceutical companies integrate it to protect intellectual property. Its ease of use ensures widespread adoption across healthcare staff.

29. Automox

Automox is a cloud-native endpoint management platform that automates patching, configuration, and compliance tasks. It simplifies vulnerability management and reduces the attack surface across distributed IT environments.

Hospitals use Automox to manage security updates for EHR systems and connected devices. Payers and health systems benefit from its scalability, enabling centralized patch management across multiple locations. Its real-time visibility into endpoint health ensures robust security compliance.

30. Autopsy (Sleuth Kit)

Autopsy is an open-source digital forensics platform that supports incident investigation and analysis. It provides tools to recover deleted files, analyze disk images, and trace malicious activities.

Healthcare organizations use Autopsy to investigate data breaches involving patient records or financial systems. Hospitals benefit from its ability to trace unauthorized access to medical devices, while payers rely on it for detailed forensic analysis of security incidents.

31. AxCrypt

AxCrypt is an encryption software that provides simple and effective file-level security. It allows users to encrypt, decrypt, and securely share sensitive files with minimal setup. AxCrypt supports AES-256 encryption, ensuring robust protection against unauthorized access.

In healthcare, AxCrypt is used to secure patient data, financial records, and administrative documents. Hospitals employ it to encrypt files containing protected health information (PHI), while payers use it to secure claims processing data. Its ease of integration and lightweight design make it suitable for small clinics and large health systems alike.

32. Axonius

Axonius is a cybersecurity asset management platform that provides visibility into all devices, users, and applications within an IT environment. By integrating with existing security tools, Axonius identifies unmanaged assets and potential security gaps.

Healthcare organizations use Axonius to manage the growing number of connected devices, including medical equipment and IoT devices. Hospitals benefit from its ability to enforce security policies across diverse endpoints, while payers leverage its insights to protect claims systems. Its automated workflows simplify compliance with regulations like HIPAA and GDPR.

33. Balbix

Balbix is a cybersecurity posture automation platform that uses AI and machine learning to identify and prioritize vulnerabilities. It provides actionable insights into security risks, helping organizations mitigate potential threats effectively.

In healthcare, Balbix assists hospitals in identifying weaknesses in EHR systems, medical devices, and network infrastructure. Payers use its predictive analytics to prevent data breaches in claims systems. Its risk-based prioritization ensures that limited resources are focused on addressing the most critical vulnerabilities.

34. Baramundi Management Suite

Baramundi Management Suite is an endpoint management platform that automates IT tasks like patch management, device monitoring, and software distribution. It ensures secure and efficient management of endpoints across healthcare environments.

Hospitals use Baramundi to maintain secure and compliant endpoints, such as clinician workstations and administrative systems. Payers rely on its patching capabilities to protect claims processing systems from vulnerabilities. Its centralized dashboard provides real-time visibility into endpoint health and security.

35. Barracuda CloudGen Firewall

Barracuda CloudGen Firewall is a network security solution that protects cloud and on-premises environments from cyber threats. It offers advanced features like intrusion detection, web filtering, and DDoS protection.

Healthcare providers use Barracuda CloudGen Firewall to secure their networks, ensuring that patient data and medical systems are protected from breaches. Payers rely on its scalability to secure large networks supporting member portals and claims systems. Its ease of deployment makes it a popular choice for healthcare organizations transitioning to hybrid environments.

36. Barracuda Email Security Gateway

Barracuda Email Security Gateway provides comprehensive email protection against phishing, spam, and malware. It uses AI-driven threat detection and real-time analytics to prevent email-based attacks.

Hospitals use Barracuda Email Security Gateway to safeguard communication between staff and patients. Payers benefit from its ability to protect email exchanges with members and providers. Its compliance-focused features ensure secure handling of sensitive information in line with healthcare regulations.

37. Barracuda Networks

Barracuda Networks offers a wide range of cybersecurity solutions, including email protection, network security, and data backup. Its integrated approach ensures comprehensive protection against cyber threats.



Healthcare organizations use Barracuda to secure critical systems like EHRs, telehealth platforms, and financial applications. Payers leverage its tools to protect member data, while pharmaceutical companies use its backup solutions to safeguard research data. Its user-friendly interfaces and scalable solutions make it a preferred choice in healthcare.

38. Barracuda PhishLine

Barracuda PhishLine is a security awareness training platform designed to educate employees about phishing threats. It includes simulated phishing campaigns, interactive training modules, and real-time reporting.

Hospitals use PhishLine to train staff on recognizing and avoiding phishing attempts that target EHR credentials. Payers benefit from its ability to reduce human error in handling sensitive claims data. Its interactive approach ensures high engagement and better retention of security best practices.

39. Barracuda Ransomware Protection

Barracuda Ransomware Protection provides advanced tools to detect, prevent, and recover from ransomware attacks. It includes features like anomaly detection, automated backups, and rapid recovery options.

Healthcare providers use Barracuda to protect critical systems, such as imaging archives and patient databases, from ransomware. Payers rely on its recovery capabilities to minimize downtime during cyber incidents. Its proactive threat mitigation ensures continuous operations in healthcare environments.

40. Basis Technology Autopsy

Basis Technology Autopsy is a forensic tool designed for investigating digital evidence. It supports data recovery, malware analysis, and case management, making it suitable for incident response teams.

Healthcare organizations use Autopsy to analyze breaches involving EHRs, billing systems, or patient portals. Hospitals employ its forensic capabilities to trace unauthorized access, while payers rely on it for investigating fraud-related incidents. Its open-source nature makes it a cost-effective solution for healthcare cybersecurity teams.

41. Belkasoft Evidence Center

Belkasoft Evidence Center is a digital forensic tool designed to collect, analyze, and preserve digital evidence. It supports data recovery from devices, applications, and cloud services, providing a comprehensive toolkit for incident response and investigations.

In healthcare, Belkasoft is used to investigate breaches involving sensitive patient data and medical systems. Hospitals leverage its capabilities to track unauthorized access to EHRs, while payers utilize it to uncover fraud in claims processing systems. Its ability to handle a wide range of data sources makes it a versatile tool for healthcare cybersecurity teams.

42. BeyondTrust

BeyondTrust specializes in privileged access management (PAM) and endpoint security solutions. It helps organizations manage and monitor privileged accounts, enforce least privilege policies, and secure endpoints against cyber threats.

Healthcare providers use BeyondTrust to protect critical systems like EHRs and imaging devices from insider threats and unauthorized access. Payers and pharmaceutical companies rely on its tools to enforce strict access controls and ensure compliance with regulations like HIPAA and GDPR. Its advanced analytics capabilities provide actionable insights into privileged activity.

43. BeyondTrust Retina

BeyondTrust Retina is a vulnerability management platform that identifies and prioritizes security risks across IT environments. It offers comprehensive scanning and reporting features to help organizations address vulnerabilities proactively.

Hospitals use Retina to identify weaknesses in medical devices, networks, and EHR systems. Payers benefit from its ability to scan claims processing platforms for vulnerabilities, while pharmaceutical companies leverage it to secure research data. Its integration with other BeyondTrust products enhances overall cybersecurity resilience.

44. BeyondTrust Zero Trust

BeyondTrust Zero Trust implements a zero-trust approach to access control, ensuring that users and devices are continuously verified before gaining access to critical resources. It supports identity verification, session monitoring, and policy enforcement.



In healthcare, BeyondTrust Zero Trust secures access to sensitive systems like patient records and billing platforms. Hospitals use it to protect against insider threats and unauthorized access, while payers rely on its zero-trust architecture to safeguard member data and claims systems. Its scalability supports large and distributed healthcare networks.

45. BitLocker (Microsoft)

Microsoft BitLocker is a full-disk encryption solution that protects data stored on drives by encrypting it and requiring authentication for access. Its seamless integration with Windows systems ensures minimal disruption to workflows.

Healthcare organizations use BitLocker to secure laptops, workstations, and mobile devices used for accessing patient records and financial systems. Hospitals rely on its encryption to meet HIPAA requirements, while payers use it to safeguard member data. Its user-friendly interface and centralized management make it a popular choice in healthcare.

46. BitSight

BitSight provides security ratings that assess an organization's cybersecurity posture based on external indicators. Its platform helps identify vulnerabilities, benchmark performance, and monitor third-party risks.

Healthcare organizations use BitSight to evaluate their own security practices and those of their partners, such as vendors and contractors. Hospitals rely on its insights to assess the risk of data breaches, while payers use it to monitor the cybersecurity performance of outsourced claims processors. Its comprehensive reporting supports informed decision-making.

47. Bitdefender GravityZone

Bitdefender GravityZone is an endpoint security platform that combines anti-malware, ransomware protection, and behavior monitoring. Its AI-driven capabilities ensure advanced threat detection and response.

Hospitals use GravityZone to protect clinician workstations, mobile devices, and EHR systems from malware and phishing attacks. Payers rely on its centralized management to secure claims platforms and member portals. Its lightweight design ensures robust protection without impacting system performance.

48. Bitdefender Threat Intelligence

Bitdefender Threat Intelligence provides real-time insights into global cyber threats, helping organizations strengthen their defenses. Its data-driven approach enables early detection of emerging threats and vulnerabilities.

Healthcare providers use Bitdefender Threat Intelligence to anticipate and mitigate risks targeting EHR systems and medical devices. Payers benefit from its ability to identify phishing campaigns aimed at claims systems. Its actionable insights enhance overall security posture, ensuring compliance and patient safety.

49. BlackBag Blacklight (OpenText)

BlackBag Blacklight is a forensic analysis tool designed to investigate macOS, Windows, and iOS devices. It offers comprehensive capabilities for data recovery, file system analysis, and timeline reconstruction.

Healthcare organizations use Blacklight to investigate breaches involving clinician workstations, mobile devices, and administrative systems. Hospitals rely on it to uncover unauthorized access to sensitive data, while payers use it to investigate potential fraud. Its intuitive interface simplifies complex forensic workflows.

50. BlackBerry Cylance

BlackBerry Cylance leverages AI and machine learning to provide predictive endpoint security. Its platform detects and blocks threats before they can execute, ensuring proactive protection against malware, ransomware, and zero-day attacks.

In healthcare, BlackBerry Cylance protects medical devices, workstations, and telehealth systems from cyber threats. Hospitals use it to safeguard patient records and imaging systems, while payers rely on its predictive capabilities to secure claims processing platforms. Its low resource consumption ensures seamless integration into existing IT environments.



51. BlackBerry UEM

BlackBerry Unified Endpoint Management (UEM) provides secure management of endpoints, including mobile devices, desktops, and IoT systems. It supports containerization, app management, and secure communications, ensuring compliance with data protection standards like HIPAA.

Hospitals use BlackBerry UEM to manage clinician devices and secure access to EHRs and imaging systems. Payers rely on its capabilities to enforce security policies for remote work environments. Its robust management tools ensure consistent security across all connected devices in healthcare organizations.

52. Blockpharma

Blockpharma leverages blockchain technology to ensure the authenticity of pharmaceutical products and prevent counterfeit drugs. It provides real-time traceability across the supply chain, enhancing transparency and security.

Pharmaceutical companies use Blockpharma to track medicines from manufacturing to distribution, ensuring regulatory compliance and consumer trust. Hospitals benefit by verifying the authenticity of drugs used in patient care, reducing risks associated with counterfeit medications. Its integration capabilities make it a valuable tool in the healthcare supply chain.

53. Blumira

Blumira offers cloud-based security information and event management (SIEM) solutions designed to detect and respond to cybersecurity threats quickly. It integrates with various IT systems to provide real-time threat detection and actionable insights.

Healthcare organizations use Blumira to monitor networks for suspicious activity, such as unauthorized access to EHRs. Hospitals rely on its automated response capabilities to minimize downtime during incidents, while payers use it to safeguard claims processing systems. Its ease of deployment and affordability make it suitable for mid-sized healthcare providers.

54. Boxcryptor

Boxcryptor provides end-to-end encryption for cloud storage services, ensuring that data remains secure during storage and transit. It supports a wide range of cloud providers, making it a flexible solution for securing sensitive files.

Hospitals use Boxcryptor to encrypt patient records stored in cloud platforms like Google Drive and Dropbox. Payers rely on it to protect member data shared across distributed teams. Its user-friendly interface and strong encryption standards make it ideal for healthcare organizations managing sensitive information.

55. BurstIQ

BurstIQ utilizes blockchain technology to create secure data exchanges between healthcare entities. Its platform enables secure sharing of patient data, research information, and analytics while maintaining compliance with regulations like HIPAA.

Hospitals use BurstIQ to manage patient data exchanges securely, supporting interoperability initiatives like health information exchanges (HIEs). Pharmaceutical companies leverage it for secure collaboration during clinical trials. Its ability to combine security with data accessibility makes it a vital tool for advancing digital health innovation.

56. CA Privileged Access Manager

CA Privileged Access Manager (PAM), now part of Broadcom, provides advanced access control for managing privileged accounts. It includes features like session monitoring, credential management, and automated access provisioning.

Hospitals use CA PAM to enforce access controls for administrators managing EHR systems and medical devices. Payers rely on it to protect claims processing platforms from insider threats. Its compliance reporting features ensure alignment with regulatory requirements like GDPR and HIPAA.

57. Cado Response

Cado Response is a cloud-native digital forensics and incident response (DFIR) platform. It automates the investigation of cybersecurity incidents, providing rapid insights into the root cause of breaches.

Healthcare organizations use Cado Response to investigate incidents involving cloud-hosted EHRs and telehealth platforms. Hospitals benefit from its ability to analyze large-scale data breaches quickly, while payers use it to identify vulnerabilities in claims systems. Its scalability makes it a preferred choice for healthcare entities using cloud infrastructure.

58. Carbon Black (VMware)

Carbon Black, a VMware solution, provides endpoint detection and response (EDR) capabilities to protect against advanced threats. Its platform uses behavioral analytics to detect and mitigate malware, ransomware, and zero-day attacks.

Hospitals use Carbon Black to safeguard EHR systems, imaging devices, and telehealth platforms from cyberattacks. Payers benefit from its centralized management and real-time threat detection to protect claims systems. Its robust analytics ensure proactive cybersecurity across healthcare environments.

59. CareClix

CareClix is a telemedicine platform that enables secure virtual consultations, remote monitoring, and patient engagement. It integrates with EHR systems, ensuring seamless data exchange and continuity of care.

Hospitals use CareClix to expand access to healthcare services, particularly for rural and underserved populations. Payers leverage the platform to reduce costs by offering telehealth options for routine care. Its robust encryption and compliance with HIPAA ensure patient data remains secure during virtual visits.

60. Cellebrite

Cellebrite specializes in digital intelligence and forensic solutions, enabling organizations to extract and analyze data from devices, cloud platforms, and applications. It supports investigations with tools for data recovery, timeline analysis, and reporting.

Healthcare organizations use Cellebrite to investigate breaches involving mobile devices or administrative systems. Hospitals rely on its capabilities to track unauthorized access to patient data, while payers use it to analyze security incidents affecting claims systems. Its advanced forensic tools ensure thorough and accurate investigations.

61. Censys

Censys provides continuous attack surface management by identifying and monitoring exposed assets across the internet. Its platform offers insights into vulnerabilities and misconfigurations that could be exploited by attackers.

In healthcare, hospitals use Censys to secure external-facing systems such as patient portals and telehealth platforms. Payers leverage its capabilities to identify weaknesses in online claims systems. Its continuous monitoring ensures that healthcare organizations stay ahead of potential threats and remain compliant with data protection regulations.

62. Centrify

Centrify, now part of Delinea, specializes in identity and access management (IAM) and privileged access management (PAM). It enforces zero-trust principles by verifying every access request based on identity, context, and risk.

Hospitals use Centrify to secure administrative access to EHR systems and medical devices. Payers benefit from its ability to control privileged access to claims processing systems. Its real-time monitoring and session recording ensure compliance with regulations like HIPAA and GDPR.

63. Centrify Privileged Access Service

The Centrify Privileged Access Service provides advanced tools for managing privileged accounts across hybrid environments. It supports secure access to cloud, on-premises, and DevOps resources, ensuring minimal risk of unauthorized access.

Healthcare organizations use this service to control access to sensitive systems such as EHR platforms and financial databases. Hospitals leverage it to secure infrastructure supporting critical operations, while pharmaceutical companies rely on it to protect R&D environments. Its robust auditing features ensure regulatory compliance.

64. Cerner Secure Messaging

Cerner Secure Messaging enables secure communication between healthcare providers, ensuring the protection of sensitive patient information. The platform supports real-time collaboration, encrypted messaging, and integration with EHR systems.

Hospitals use Cerner Secure Messaging to streamline communication among clinicians and administrative staff while maintaining compliance with HIPAA. For payers, it ensures the secure exchange of member information with providers. Its user-friendly interface supports efficient and secure communication in healthcare settings.

65. Cerner Telehealth Solutions

Cerner Telehealth Solutions provide a secure platform for virtual care delivery, integrating with EHRs for seamless patient management. It includes features like video consultations, remote monitoring, and appointment scheduling.

Hospitals use Cerner Telehealth to expand care access, particularly for rural and underserved communities. Payers leverage the platform to reduce costs by supporting virtual consultations as an alternative to in-person visits. Its encryption and compliance capabilities ensure patient data remains secure throughout virtual interactions.

66. Chainalysis

Chainalysis is a blockchain analytics platform that monitors and investigates cryptocurrency transactions for fraud and compliance risks. It helps organizations identify illicit activity and maintain regulatory adherence.

In healthcare, Chainalysis is used by pharmaceutical companies to ensure secure and compliant transactions involving blockchain-based supply chain solutions. Hospitals and payers exploring blockchain for secure data exchange can rely on its insights to identify and mitigate risks.

67. Check Point CloudGuard

Check Point CloudGuard provides comprehensive cloud security, including threat prevention, compliance monitoring, and advanced threat intelligence. Its automated tools secure workloads and applications in public, private, and hybrid cloud environments.

Healthcare organizations use CloudGuard to protect cloud-hosted EHR platforms, patient portals, and telehealth systems. Hospitals rely on its compliance tools to meet HIPAA requirements, while payers use it to secure claims data in cloud environments. Its multi-layered security ensures robust protection for sensitive healthcare data.

68. Check Point Email Security

Check Point Email Security safeguards organizations from email-based attacks, including phishing, malware, and ransomware. It leverages AI and advanced threat detection techniques to block malicious emails before they reach users.

Hospitals use Check Point Email Security to protect staff from phishing campaigns targeting EHR credentials. Payers benefit from its ability to secure communications with members and providers. Its focus on proactive protection helps healthcare organizations reduce the risk of email-related breaches.

69. Check Point Harmony Endpoint

Check Point Harmony Endpoint provides endpoint security with features like threat detection, anti-ransomware, and data loss prevention. It ensures continuous monitoring and protection against advanced threats.

Hospitals use Harmony Endpoint to secure workstations and mobile devices accessing EHRs and imaging systems. Payers rely on its robust protection to safeguard claims systems and member portals. Its centralized management simplifies security across distributed healthcare environments.

70. Check Point IoT Protect

Check Point IoT Protect delivers specialized security for IoT devices, offering visibility, threat prevention, and compliance enforcement. It ensures that connected devices remain secure against cyber threats.

Healthcare organizations use IoT Protect to safeguard medical devices such as infusion pumps and patient monitors. Hospitals benefit from its ability to identify and mitigate vulnerabilities in IoT networks. Its real-time protection ensures patient safety and data integrity.

71. Check Point Software

Check Point Software provides comprehensive cybersecurity solutions, including firewalls, threat intelligence, endpoint security, and cloud protection. Its unified platform ensures robust protection against advanced threats.

Hospitals use Check Point to secure networks and protect critical systems like EHRs and imaging platforms. Payers benefit from its scalability to secure claims processing systems, while pharmaceutical companies rely on its threat intelligence to protect sensitive research data. Its compliance-focused tools help healthcare organizations meet regulatory standards.

72. Check Point ThreatCloud

ThreatCloud, powered by Check Point, is a collaborative threat intelligence platform that aggregates global data on cyber threats. It provides real-time insights into malware, phishing campaigns, and advanced persistent threats (APTs).

Healthcare organizations use ThreatCloud to stay informed about emerging threats targeting EHR systems, telehealth platforms, and IoT devices. Hospitals rely on its intelligence to enhance incident response, while payers use it to prevent fraud targeting member data. Its predictive analytics empower proactive defense strategies.

73. Chiron Health

Chiron Health offers a secure telemedicine platform designed for virtual consultations and remote patient monitoring. It integrates with EHR systems, enabling seamless patient data exchange and appointment management.

Hospitals use Chiron Health to expand care delivery, providing virtual visits for routine checkups and chronic disease management. Payers leverage the platform to reduce healthcare costs while maintaining access for members. Its compliance with HIPAA ensures secure and private telehealth interactions.

74. Chronicled

Chronicled uses blockchain technology to secure supply chain processes, ensuring the authenticity and traceability of pharmaceuticals. Its platform enables healthcare organizations to track products from manufacturing to distribution.

Pharmaceutical companies use Chronicled to combat counterfeit drugs and ensure regulatory compliance. Hospitals benefit from its ability to verify the authenticity of medications used in patient care. Its integration with existing supply chain systems enhances transparency and security.

75. Cisco IoT Threat Defense

Cisco IoT Threat Defense protects connected devices and IoT ecosystems from cyber threats. It provides visibility, segmentation, and real-time threat detection for IoT networks.

Hospitals use IoT Threat Defense to secure medical devices like patient monitors and infusion pumps. Health systems benefit from its ability to isolate compromised devices, preventing the spread of threats. Its integration with Cisco's broader security portfolio ensures comprehensive protection for healthcare IoT environments.

76. Cisco Meraki Systems Manager

Cisco Meraki Systems Manager is a cloud-based endpoint management solution that simplifies device provisioning, monitoring, and security. It supports centralized control for diverse endpoint types, including mobile devices and desktops.

Hospitals use Meraki Systems Manager to secure devices accessing EHRs and clinical tools. Payers rely on its capabilities to enforce security policies for remote employees. Its user-friendly interface and automated workflows make it ideal for large and distributed healthcare organizations.

77. Cisco Secure

Cisco Secure offers a suite of cybersecurity solutions, including network security, endpoint protection, and threat intelligence. Its platform provides comprehensive security for hybrid and multi-cloud environments.

Hospitals use Cisco Secure to protect critical systems like imaging platforms and EHRs, ensuring uninterrupted operations. Payers leverage its advanced threat detection capabilities to secure claims systems and member portals. Its scalable solutions meet the needs of healthcare organizations of all sizes.

78. Cisco Secure Email

Cisco Secure Email protects healthcare organizations from phishing, ransomware, and email fraud. It leverages advanced threat intelligence and machine learning to block malicious emails before they reach users.

Hospitals use Secure Email to safeguard communications between staff and patients, protecting sensitive health information. Payers benefit from its ability to secure member communications, ensuring trust and compliance with regulations. Its proactive approach reduces email-based vulnerabilities in healthcare.

79. Cisco SecureX

Cisco SecureX is a cloud-native platform that integrates security tools and automates threat detection and response. It provides unified visibility and streamlined workflows for security operations teams.

Healthcare organizations use SecureX to coordinate responses to cybersecurity incidents across EHR systems, medical devices, and telehealth platforms. Hospitals benefit from its automation capabilities, which reduce response times, while payers use it to manage threats targeting claims data. Its centralized approach enhances operational efficiency.

80. Cisco Talos

Cisco Talos is a global threat intelligence team that provides actionable insights into emerging cyber threats. Its research supports Cisco's security products, helping organizations stay ahead of attackers.

Hospitals use Talos intelligence to protect networks and EHR systems from advanced threats. Payers benefit from its insights into fraud schemes targeting claims systems. Its predictive capabilities empower healthcare organizations to strengthen their defenses proactively.

81. Cisco Umbrella

Cisco Umbrella is a cloud-delivered security platform that provides secure internet access and threat protection for users across all devices. It includes features like DNS-layer security, content filtering, and malware blocking to prevent threats before they reach endpoints.

Hospitals use Cisco Umbrella to secure internet traffic and prevent unauthorized access to patient data. Payers rely on its capabilities to safeguard member portals and internal systems. Its scalability and ease of deployment make it an ideal solution for healthcare organizations of all sizes.

82. Cisco Webex for Healthcare

Cisco Webex for Healthcare is a secure collaboration platform designed to support virtual care delivery and internal communication. It includes encrypted video conferencing, messaging, and file-sharing capabilities to ensure compliance with healthcare regulations.

Hospitals use Webex to facilitate telehealth consultations, enabling remote patient care. Payers leverage the platform for secure communication with providers and members. Its HIPAA-compliant features and seamless integration with clinical workflows make it a trusted tool for healthcare organizations.

83. Citrix ADC

Citrix ADC (Application Delivery Controller) is a load-balancing and application security solution that optimizes application performance and ensures secure delivery. It provides advanced traffic management and DDoS protection, making it essential for high-demand environments.

Hospitals use Citrix ADC to optimize access to EHRs, patient portals, and telehealth platforms. Payers benefit from its ability to enhance the performance of claims processing systems and member-facing applications. Its robust security features protect against cyber threats while maintaining operational efficiency.

84. Citrix Endpoint Management

Citrix Endpoint Management secures and manages devices across healthcare environments, ensuring compliance and productivity. It supports mobile device management (MDM) and app management, enabling secure access to clinical and administrative systems.

Hospitals use Citrix Endpoint Management to protect clinician devices accessing sensitive patient information. Payers leverage its capabilities to enforce security policies for remote employees. Its centralized management dashboard ensures efficient device monitoring and policy enforcement.

85. Citrix Zero Trust

Citrix Zero Trust delivers secure access to applications and data by enforcing strict authentication and authorization policies. It supports a zero-trust approach, ensuring that all users and devices are continuously verified.

Healthcare organizations use Citrix Zero Trust to protect EHR systems and telehealth platforms from unauthorized access. Hospitals benefit from its ability to secure critical workflows, while payers rely on it to safeguard member data. Its integration with Citrix's broader portfolio provides end-to-end security.

86. Clearswift DLP

Clearswift DLP (Data Loss Prevention) protects sensitive healthcare data by preventing unauthorized sharing or access. Its adaptive redaction and encryption capabilities ensure compliance with data protection regulations like HIPAA.

Hospitals use Clearswift DLP to safeguard patient records and imaging data during internal and external communication. Payers rely on its tools to protect claims data and member information. Its ability to redact sensitive data in real time makes it a trusted solution in healthcare.

87. Cloudflare

Cloudflare provides a suite of security solutions, including DDoS protection, web application firewalls (WAFs), and secure content delivery. Its platform ensures fast and secure access to online resources.

Healthcare organizations use Cloudflare to protect patient portals, telehealth systems, and other online applications. Hospitals benefit from its DDoS protection to ensure uninterrupted operations, while payers rely on its WAFs to secure claims portals. Its global network enhances both security and performance.

88. Code42

Code42 specializes in insider threat detection and data loss prevention. Its platform monitors data movement across endpoints, cloud applications, and email to identify potential risks and prevent breaches.

Hospitals use Code42 to monitor data exfiltration from EHR systems and research databases. Payers leverage its insights to prevent unauthorized sharing of member data. Its focus on insider threats makes it a valuable tool for addressing one of healthcare's most significant risks.

89. Codeproof Enterprise MDM

Codeproof Enterprise MDM offers robust mobile device management solutions to secure and manage endpoints in healthcare settings. It includes features like device tracking, app management, and compliance monitoring.

Hospitals use Codeproof to secure mobile devices used by clinicians and administrative staff. Payers rely on its centralized management capabilities to enforce security policies for remote employees. Its user-friendly interface and compliance-focused tools ensure safe and efficient device operations.

90. Cohesity DataProtect

Cohesity DataProtect is a modern backup and recovery solution designed for hybrid and multi-cloud environments. It provides ransomware protection, data replication, and rapid recovery capabilities to ensure business continuity.

Hospitals use Cohesity to protect critical data stored in EHR systems and imaging databases. Payers benefit from its ability to ensure the integrity of claims and financial data. Its ransomware recovery features minimize downtime and maintain operational efficiency in healthcare organizations.

91. Commvault Complete Backup

Commvault Complete Backup is a comprehensive data management solution offering backup, recovery, and data protection for on-premises, cloud, and hybrid environments. It includes features like automated backups, disaster recovery, and ransomware protection.

Hospitals use Commvault to secure EHR systems, imaging data, and other critical information. Payers rely on its data protection capabilities to ensure the availability and integrity of claims and financial records. Its scalability makes it a preferred choice for healthcare organizations of all sizes.

92. ConnectWise Automate

ConnectWise Automate is a remote monitoring and management (RMM) platform that automates IT tasks like patch management, endpoint monitoring, and security updates. It provides centralized visibility into IT assets, ensuring proactive maintenance.

Healthcare providers use ConnectWise to monitor and secure endpoints such as workstations and medical devices. Payers leverage its automation capabilities to streamline IT operations across multiple locations. Its real-time monitoring helps identify and mitigate potential vulnerabilities before they impact operations.

93. Coral Health

Coral Health uses blockchain technology to enable secure, patient-controlled health data exchanges. Its platform supports interoperability, allowing patients and providers to share medical records seamlessly and securely.

Hospitals and clinics use Coral Health to facilitate secure sharing of EHR data while maintaining compliance with regulations like HIPAA. Payers benefit from its ability to streamline claims processing by ensuring data accuracy and authenticity. Its patient-centric approach promotes trust and transparency in healthcare.

94. CrowdStrike

CrowdStrike provides endpoint detection and response (EDR) solutions powered by AI and machine learning. Its Falcon platform delivers real-time threat detection, automated incident response, and advanced threat intelligence.

Hospitals use CrowdStrike to protect EHR systems, medical devices, and telehealth platforms from advanced threats. Payers benefit from its proactive threat detection to secure claims processing systems and member data. Its lightweight design ensures minimal impact on system performance.

95. CrowdStrike Falcon Cloud

CrowdStrike Falcon Cloud is a cloud-native EDR solution that provides endpoint protection, threat intelligence, and real-time monitoring. Its platform integrates seamlessly with existing IT systems for comprehensive security.

Healthcare providers use Falcon Cloud to secure cloud-hosted EHRs and other critical applications. Hospitals rely on its advanced analytics to detect and respond to cyber threats, while payers use it to safeguard cloud-based claims processing systems. Its scalability supports organizations of all sizes.

96. CrowdStrike Falcon Forensics

CrowdStrike Falcon Forensics provides advanced incident analysis and reporting tools to investigate cybersecurity breaches. Its platform helps identify the root cause of attacks and recommends remediation strategies.

Hospitals use Falcon Forensics to analyze breaches involving patient data or medical devices. Payers rely on it to investigate incidents affecting claims systems. Its detailed reporting ensures healthcare organizations can respond effectively and prevent future incidents.

97. CrowdStrike Falcon Fusion

Falcon Fusion is a threat hunting and incident orchestration platform from CrowdStrike. It automates workflows and integrates with existing security tools to enhance threat detection and response capabilities.

Healthcare organizations use Falcon Fusion to streamline security operations and respond quickly to incidents. Hospitals benefit from its integration capabilities, which support complex IT infrastructures, while payers use it to automate threat mitigation processes for member data security.

98. CrowdStrike Falcon Spotlight

CrowdStrike Falcon Spotlight focuses on vulnerability management, providing real-time insights into endpoint vulnerabilities. It prioritizes remediation efforts based on risk levels, ensuring efficient resource allocation.

Hospitals use Spotlight to identify vulnerabilities in workstations, mobile devices, and medical systems. Payers leverage its analytics to protect claims processing platforms from exploitation. Its integration with the broader Falcon platform enhances overall cybersecurity resilience.

99. CrowdStrike Threat Intelligence

CrowdStrike Threat Intelligence delivers actionable insights into global cyber threats, enabling organizations to anticipate and mitigate risks effectively. It provides in-depth analyses of malware, threat actors, and attack trends.

Healthcare providers use CrowdStrike Threat Intelligence to protect EHR systems and telehealth platforms from targeted attacks. Hospitals benefit from its predictive capabilities, while payers use it to defend against fraud schemes. Its real-time updates ensure organizations remain vigilant against emerging threats.

100. Curricula Security Awareness Training

Curricula provides engaging security awareness training to educate employees on recognizing and responding to cyber threats. Its interactive modules cover topics like phishing, social engineering, and password security.



Hospitals use Curricula to train staff on safeguarding patient data and EHR access credentials. Payers benefit from its focus on reducing human error in claims processing workflows. Its gamified approach ensures higher engagement and retention of security best practices.

101. CyFIR Investigator

CyFIR Investigator is a forensic and incident response tool designed to quickly detect, analyze, and remediate cybersecurity threats. It enables real-time visibility into endpoints and supports comprehensive threat hunting and data recovery.

Hospitals use CyFIR Investigator to analyze breaches affecting EHR systems and medical devices. Payers rely on its capabilities to investigate unauthorized access to claims processing platforms. Its rapid analysis tools ensure healthcare organizations can respond effectively to incidents, minimizing downtime and data loss.

102. CyberArk

CyberArk specializes in privileged access management (PAM) solutions, securing administrative credentials and controlling access to critical systems. Its platform prevents unauthorized access and enforces least-privilege policies.

Healthcare providers use CyberArk to protect privileged accounts for EHR systems, medical devices, and financial applications. Payers rely on its tools to secure claims systems and enforce compliance with regulations like HIPAA. Its session monitoring and auditing features provide transparency and security across IT environments.

103. CyberArk Zero Trust

CyberArk Zero Trust integrates zero-trust principles into privileged access management, requiring continuous verification for every access request. It ensures that no user or device is inherently trusted.

Hospitals use CyberArk Zero Trust to protect sensitive systems like EHRs and telehealth platforms. Payers rely on its strict access controls to secure member data and claims platforms. Its seamless integration with existing IT infrastructure makes it a scalable solution for healthcare organizations.

104. CyberGRX

CyberGRX is a third-party risk management platform that assesses and monitors the cybersecurity posture of vendors and partners. It provides detailed risk profiles and actionable recommendations to mitigate potential threats.

Hospitals use CyberGRX to evaluate risks associated with medical device manufacturers and IT service providers. Payers leverage its tools to monitor the security of outsourced claims processors. Its centralized dashboard simplifies third-party risk management, ensuring compliance and data protection.

105. CyberMDX

CyberMDX focuses on securing connected medical devices and IoT endpoints within healthcare environments. Its platform provides visibility, risk assessment, and threat detection for medical device networks.

Hospitals use CyberMDX to protect devices like infusion pumps, imaging systems, and patient monitors. Health systems benefit from its ability to enforce security policies across diverse IoT networks. Its compliance features help ensure adherence to regulations like HIPAA and FDA cybersecurity guidelines.

106. CyberSponse (Arctic Wolf)

CyberSponse, now part of Arctic Wolf, provides security orchestration, automation, and response (SOAR) capabilities. It streamlines incident response workflows, enabling faster threat mitigation.

Healthcare organizations use CyberSponse to coordinate responses to cybersecurity incidents across EHR systems, telehealth platforms, and medical devices. Hospitals benefit from its automation capabilities, while payers use it to manage threats targeting claims data. Its integration with other security tools enhances overall cybersecurity resilience.

107. CyberVista

CyberVista offers cybersecurity training and skills development programs tailored to IT and security professionals. Its courses cover topics like risk management, threat detection, and compliance best practices.



Hospitals use CyberVista to train IT teams on securing medical devices and EHR platforms. Payers leverage its programs to enhance staff skills in protecting claims systems and member data. Its industry-specific content ensures healthcare organizations remain prepared to address evolving cyber threats.

108. Cybereason Defense Platform

The Cybereason Defense Platform provides endpoint detection and response (EDR), threat hunting, and ransomware protection. Its AI-powered tools detect advanced threats and automate incident response.

Hospitals use Cybereason to safeguard EHR systems and medical devices from ransomware and malware attacks. Payers rely on its real-time monitoring to protect claims processing platforms. Its proactive threat detection ensures healthcare organizations can respond to incidents before they escalate.

109. Cybereason RansomFree

Cybereason RansomFree is a ransomware protection solution designed to detect and block ransomware before it encrypts data. It uses behavioral analysis to identify suspicious activities and neutralize threats.

Healthcare organizations use RansomFree to protect critical systems like patient databases, imaging archives, and financial platforms. Hospitals rely on its advanced algorithms to prevent disruptions to care delivery, while payers use it to secure member data and operational systems.

110. Cybereason Threat Analysis

Cybereason Threat Analysis provides actionable insights into emerging cyber threats, helping organizations strengthen their defenses. Its platform combines real-time monitoring with advanced analytics to identify vulnerabilities and attack vectors.

Hospitals use Cybereason Threat Analysis to protect networks and medical devices from targeted attacks. Payers benefit from its predictive capabilities, which help prevent fraud schemes targeting claims systems. Its detailed reports enhance decision-making and cybersecurity planning in healthcare environments.

111. Cynerio

Cynerio is a specialized IoT cybersecurity platform designed for the healthcare industry. It provides visibility, threat detection, and risk mitigation for medical devices and connected healthcare systems.

Hospitals use Cynerio to secure critical medical devices like infusion pumps, ventilators, and patient monitors. Its real-time monitoring ensures that threats are detected and neutralized before impacting patient care. Cynerio's focus on healthcare-specific use cases makes it a valuable solution for protecting IoT ecosystems in hospitals and health systems.

112. Cynet 360 Behavioral Analytics

Cynet 360 Behavioral Analytics is a comprehensive endpoint protection platform that leverages user behavior analytics (UBA) to identify and mitigate advanced threats. Its AI-driven detection capabilities ensure proactive security.

Healthcare providers use Cynet 360 to protect EHR systems, telehealth platforms, and connected devices from insider threats and malware. Payers benefit from its behavior monitoring to detect anomalous activities within claims systems. Its automated threat response minimizes downtime and enhances operational security.

113. D3 Security

D3 Security offers a security orchestration, automation, and response (SOAR) platform that streamlines incident management processes. It integrates with various security tools to enhance threat detection and response.

Hospitals use D3 Security to coordinate responses to cybersecurity incidents affecting EHR systems and medical devices. Payers leverage its automation capabilities to manage threats targeting claims processing platforms. Its customizable workflows ensure alignment with healthcare-specific compliance requirements.

114. Darktrace

Darktrace leverages AI and machine learning to provide real-time threat detection and response across IT, IoT, and cloud environments. Its platform identifies anomalous activities and neutralizes potential threats autonomously.



Hospitals use Darktrace to secure medical devices, EHR systems, and telehealth platforms from advanced threats. Payers benefit from its predictive analytics to prevent fraud and data breaches. Its self-learning AI adapts to evolving threats, making it a reliable choice for healthcare cybersecurity.

115. Darktrace IoT

Darktrace IoT extends the capabilities of Darktrace's core platform to IoT devices, providing visibility and protection for connected medical equipment and networks. It autonomously identifies and mitigates IoT-specific threats.

Healthcare providers use Darktrace IoT to secure medical devices such as imaging systems and infusion pumps. Hospitals benefit from its ability to detect unusual device behavior that could indicate cyberattacks. Its focus on IoT security ensures patient safety and data integrity.

116. Dashlane MFA

Dashlane MFA (Multi-Factor Authentication) enhances login security by requiring additional verification steps beyond passwords. It supports various authentication methods, including biometrics and one-time passwords.

Hospitals use Dashlane MFA to secure access to EHRs, billing systems, and administrative tools. Payers rely on it to protect member portals and internal systems from unauthorized access. Its user-friendly implementation encourages widespread adoption among healthcare staff.

117. Deep Instinct

Deep Instinct employs deep learning to prevent and detect cybersecurity threats, including ransomware, malware, and zero-day attacks. Its platform provides endpoint protection with minimal false positives.

Hospitals use Deep Instinct to safeguard EHR systems and medical devices from advanced threats. Payers benefit from its proactive threat prevention for claims processing platforms and member data. Its predictive capabilities ensure robust security against emerging attack vectors.

118. Dell Data Protection Encryption

Dell Data Protection Encryption is an enterprise-grade encryption solution that secures sensitive data at rest and in transit. It ensures compliance with regulations like HIPAA and GDPR by providing robust encryption protocols.

Healthcare organizations use Dell Data Protection to encrypt patient records, financial data, and communications. Hospitals rely on its seamless integration with existing Dell infrastructure, while payers use it to secure claims systems and member information. Its centralized management simplifies compliance monitoring.

119. Devo Technology

Devo Technology provides a cloud-native security analytics platform that delivers real-time visibility into IT environments. It enables organizations to detect and respond to cybersecurity threats efficiently.

Hospitals use Devo to monitor EHR systems, medical devices, and network infrastructure for suspicious activities. Payers leverage its advanced analytics to secure claims processing systems and member portals. Its scalability supports the needs of large healthcare organizations with complex IT environments.

120. Devolutions PAM

Devolutions Privileged Access Management (PAM) provides tools to manage and monitor privileged accounts. It enforces access controls, session monitoring, and credential management to reduce the risk of insider threats.

Hospitals use Devolutions PAM to secure administrative access to EHR systems and medical networks. Payers rely on it to protect sensitive financial systems and claims data. Its user-friendly design ensures efficient management of privileged accounts across healthcare environments.

121. Digital Guardian

Digital Guardian specializes in data loss prevention (DLP) and endpoint protection. Its platform secures sensitive information across devices, networks, and cloud environments, ensuring compliance with regulations like HIPAA and GDPR.

Hospitals use Digital Guardian to protect patient records and imaging data from unauthorized access or accidental sharing. Payers rely on its capabilities to secure member data and prevent data breaches in claims systems. Its robust monitoring features enhance visibility into data movement within healthcare organizations.

122. Doc.ai

Doc.ai is an AI-powered platform that processes healthcare data to generate actionable insights. It supports applications like predictive analytics, research acceleration, and personalized patient care while maintaining data privacy and security.

Hospitals use Doc.ai to optimize clinical workflows and improve patient outcomes through data-driven insights. Pharmaceutical companies benefit from its ability to accelerate drug discovery and clinical trials. Its secure architecture ensures compliance with healthcare regulations during data processing.

123. Doxy.me

Doxy.me is a telehealth platform designed for secure video consultations. It features end-to-end encryption, HIPAA compliance, and an easy-to-use interface, making it accessible for providers and patients alike.

Hospitals and clinics use Doxy.me to offer virtual care services, expanding access to healthcare for underserved populations. Payers leverage the platform to reduce costs by supporting telehealth for routine care. Its simplicity and compliance features make it a preferred solution for small practices and large systems alike.

124. Dragos (Industrial IoT)

Dragos specializes in industrial IoT cybersecurity, protecting operational technology (OT) networks and devices from cyber threats. It provides visibility, threat detection, and incident response tailored to industrial environments.

In healthcare, Dragos is used to secure connected medical devices and critical infrastructure, such as HVAC systems in hospitals. Its ability to detect and mitigate OT-specific threats ensures the safety and reliability of healthcare operations.

125. Duo Security (Cisco)

Duo Security provides multi-factor authentication (MFA) and zero-trust security solutions. Its platform ensures secure access to applications and systems by verifying user identity and device health.

Hospitals use Duo Security to secure EHR systems, telehealth platforms, and administrative tools. Payers rely on its MFA capabilities to protect member portals and internal systems from unauthorized access. Its integration with Cisco's broader security portfolio enhances its utility in healthcare environments.

126. ESET Cybersecurity Awareness

ESET Cybersecurity Awareness provides training programs that educate employees on recognizing and mitigating cyber threats. Its interactive modules cover phishing, ransomware, and other common attack vectors.

Hospitals use ESET to train staff on safeguarding patient data and EHR access credentials. Payers benefit from its focus on reducing human error in claims processing workflows. Its practical, scenario-based training improves employee readiness against cybersecurity risks.

127. ESET Endpoint Security

ESET Endpoint Security delivers comprehensive protection for devices against malware, ransomware, and phishing attacks. It features advanced threat detection, behavior monitoring, and data encryption.

Hospitals use ESET Endpoint Security to protect clinician workstations and administrative systems. Payers rely on its lightweight yet robust protection to secure claims platforms and member data. Its centralized management simplifies security across diverse IT environments.

128. ESET Inspect

ESET Inspect is an advanced endpoint detection and response (EDR) solution that provides visibility into endpoint activity and automates threat mitigation. Its platform helps organizations detect and respond to advanced threats effectively.

Healthcare providers use ESET Inspect to monitor EHR systems and medical devices for anomalous activity. Hospitals benefit from its detailed forensic capabilities, while payers use it to protect sensitive claims data. Its integration with other ESET solutions enhances overall security.

129. ESET Secure Authentication

ESET Secure Authentication offers multi-factor authentication (MFA) to protect user accounts and systems from unauthorized access. It supports a variety of authentication methods, including biometrics and one-time passwords.

Hospitals use ESET Secure Authentication to secure access to EHRs and telehealth platforms. Payers rely on its capabilities to protect member portals and financial systems. Its user-friendly implementation ensures seamless adoption across healthcare staff.

130. Eclectiq

Eclectiq provides threat intelligence and incident response solutions, helping organizations enhance their cybersecurity posture. Its platform integrates threat intelligence with security workflows to enable proactive defense.

Hospitals use Eclectiq to identify and respond to emerging threats targeting EHR systems and medical devices. Payers leverage its insights to protect claims processing platforms from fraud. Its comprehensive threat analysis supports informed decision-making in healthcare security operations.

131. EcoVadis

EcoVadis provides sustainability and risk management ratings for vendors and suppliers. Its platform evaluates cybersecurity and compliance practices as part of broader third-party risk assessments.

Hospitals use EcoVadis to ensure that medical device manufacturers and IT vendors meet security and sustainability standards. Payers leverage its ratings to evaluate third-party claims processors. Its comprehensive assessments help healthcare organizations build secure and ethical supply chains.

132. Egress Protect

Egress Protect provides secure email encryption and data protection to prevent unauthorized sharing of sensitive information. Its platform ensures compliance with regulations like HIPAA while maintaining user-friendly workflows.

Hospitals use Egress Protect to secure communications involving patient data and clinical information. Payers rely on it to protect sensitive correspondence with members and providers. Its seamless integration with email platforms enhances security without disrupting operations.

133. Ekran System

Ekran System delivers insider threat detection and privileged access management (PAM) solutions. It provides real-time monitoring, session recording, and access control to protect sensitive systems.

Hospitals use Ekran System to monitor privileged access to EHRs and administrative systems. Payers leverage its capabilities to secure claims processing platforms. Its detailed activity logs and reporting features help meet compliance requirements like HIPAA and GDPR.

134. Elastic Security

Elastic Security is an open-source platform that provides endpoint protection, SIEM capabilities, and advanced threat hunting. It integrates seamlessly with other Elastic tools to deliver comprehensive visibility and security.

Hospitals use Elastic Security to monitor EHR systems, medical devices, and network activity for suspicious behavior. Payers benefit from its real-time analytics to protect claims data. Its open-source nature makes it a cost-effective option for healthcare organizations seeking scalable security solutions.

135. EncrypGen

EncrypGen leverages blockchain technology to securely store and share genomic data. Its platform enables researchers, providers, and patients to exchange data while maintaining privacy and regulatory compliance.

Hospitals and research institutions use EncrypGen to manage genomic data for personalized medicine and clinical research. Pharmaceutical companies benefit from its secure sharing capabilities during drug development. Its blockchain infrastructure ensures data integrity and accessibility.

136. EncryptRIGHT (PKWARE)

EncryptRIGHT by PKWARE is a data security platform that automates encryption, masking, and tokenization processes. It ensures that sensitive healthcare data remains secure at rest and in transit.

Hospitals use EncryptRIGHT to protect patient records and financial information. Payers leverage its tools to secure member data and claims systems. Its automation capabilities reduce the risk of human error and ensure compliance with data protection regulations.

137. Entrust Identity MFA

Entrust Identity MFA provides secure multi-factor authentication (MFA) to protect access to critical systems. It supports adaptive authentication, biometrics, and mobile-based security tokens.

Hospitals use Entrust Identity MFA to secure access to EHRs, telehealth platforms, and administrative systems. Payers rely on its capabilities to protect member portals and financial applications. Its flexible deployment options make it suitable for diverse healthcare environments.

138. Epic Secure Chat

Epic Secure Chat is an encrypted messaging platform integrated into Epic's EHR system. It enables real-time communication between clinicians while maintaining compliance with healthcare regulations like HIPAA.

Hospitals use Epic Secure Chat to streamline communication between care teams, improving coordination and patient outcomes. Its integration with Epic EHR ensures that clinical data remains secure and accessible only to authorized users.

139. Epic Telehealth Integration

Epic Telehealth Integration extends Epic's EHR capabilities to support virtual care delivery. It provides a secure platform for video consultations, remote monitoring, and appointment management.

Hospitals use Epic Telehealth Integration to offer virtual visits, enhancing access to care for patients in remote or underserved areas. Payers leverage it to reduce costs associated with in-person consultations. Its seamless integration ensures continuity of care and data security.

140. Exabeam DLP

Exabeam Data Loss Prevention (DLP) provides comprehensive protection against unauthorized data sharing and breaches. Its platform leverages user behavior analytics (UBA) to identify and mitigate risks.

Hospitals use Exabeam DLP to protect patient data and ensure compliance with regulations like HIPAA. Payers rely on its capabilities to secure sensitive claims data and financial records. Its advanced analytics enhance visibility and control over data movement within healthcare organizations.

141. Exabeam Incident Responder

Exabeam Incident Responder automates and streamlines incident response workflows. It integrates with security tools to detect, analyze, and mitigate threats efficiently, reducing response times.

Hospitals use Exabeam Incident Responder to address breaches affecting EHR systems and medical devices. Payers leverage its capabilities to respond to threats targeting claims processing systems. Its automation ensures consistent and effective responses, minimizing the impact of cybersecurity incidents.

142. Extreme Networks

Extreme Networks provides high-performance networking solutions, including secure wireless and wired connectivity for complex IT environments. Its tools support real-time monitoring, segmentation, and threat prevention.

Hospitals use Extreme Networks to ensure reliable and secure connections for EHR systems, imaging platforms, and IoT devices. Payers rely on its scalability to support secure member portals and claims systems. Its advanced security features protect healthcare organizations from network-based threats.

143. F-Secure Countercept

F-Secure Countercept is a managed detection and response (MDR) service that provides continuous threat monitoring, detection, and response. It uses proactive threat hunting to identify advanced attacks.



Healthcare providers use Countercept to protect EHR systems and telehealth platforms from targeted threats. Payers benefit from its 24/7 monitoring and rapid response capabilities to secure claims processing systems. Its managed service model ensures healthcare organizations have expert support to handle complex threats.

144. F-Secure Radar

F-Secure Radar is a vulnerability management platform that identifies, prioritizes, and remediates security risks across IT environments. It includes tools for network scanning, risk assessment, and compliance reporting.

Hospitals use F-Secure Radar to identify vulnerabilities in medical devices, workstations, and networks. Payers rely on its risk prioritization to focus on critical threats affecting claims systems. Its reporting features support compliance with healthcare regulations like HIPAA.

145. FTK (Forensic Toolkit) by Exterro

FTK is a digital forensics platform that supports incident investigation and evidence analysis. It includes tools for data recovery, email analysis, and case management.

Hospitals use FTK to investigate breaches involving patient data or administrative systems. Payers leverage its forensic capabilities to analyze fraud-related incidents affecting claims processing platforms. Its robust reporting features ensure that evidence is preserved for legal and compliance purposes.

146. Factom

Factom leverages blockchain technology to ensure the security and integrity of healthcare data. It provides tamper-proof records for audits, compliance, and secure data sharing.

Hospitals use Factom to securely store and verify patient records, ensuring data integrity for clinical workflows. Payers rely on it to streamline claims processing by verifying data authenticity. Its blockchain-based approach enhances trust and transparency in healthcare operations.

147. FarmaTrust

FarmaTrust is a blockchain-based platform that ensures the traceability and authenticity of pharmaceuticals throughout the supply chain. It combats counterfeit drugs and enhances regulatory compliance.

Pharmaceutical companies use FarmaTrust to secure the supply chain, ensuring the safety and authenticity of medications. Hospitals benefit by verifying the legitimacy of drugs used in patient care. Its real-time tracking capabilities improve efficiency and reduce risks in healthcare supply chains.

148. Fidelis Cybersecurity

Fidelis Cybersecurity provides tools for threat detection, data protection, and incident response. Its platform integrates network, endpoint, and deception technologies to deliver comprehensive security.

Hospitals use Fidelis to monitor and protect EHR systems, medical devices, and IoT networks. Payers leverage its advanced threat detection to safeguard claims platforms and member data. Its proactive approach ensures healthcare organizations can respond quickly to evolving threats.

149. FireEye Cloud Security

FireEye Cloud Security protects cloud workloads and applications from cyber threats. It provides visibility into cloud environments and integrates with other security tools to deliver comprehensive protection.

Healthcare providers use FireEye Cloud Security to secure cloud-hosted EHR platforms, telehealth applications, and patient portals. Payers rely on its capabilities to protect claims systems and member-facing services. Its real-time monitoring ensures the safety and compliance of sensitive healthcare data.

150. FireEye Email Security (Trellix)

FireEye Email Security provides advanced protection against phishing, malware, and business email compromise (BEC). It uses machine learning and threat intelligence to detect and block malicious emails.

Hospitals use FireEye Email Security to secure communications involving patient data and clinical workflows. Payers rely on its capabilities to protect member correspondence and financial systems. Its proactive threat detection reduces email-related vulnerabilities in healthcare organizations.

151. FireEye Endpoint Security (Trellix)

FireEye Endpoint Security offers advanced endpoint detection and response (EDR) capabilities to protect devices from malware, ransomware, and other threats. Its platform uses behavioral analysis and machine learning to detect and mitigate attacks.

Hospitals use FireEye Endpoint Security to protect workstations, medical devices, and systems accessing EHRs. Payers leverage its capabilities to secure claims processing platforms and member data. Its proactive detection and detailed forensics enhance overall endpoint security in healthcare environments.

152. FireEye Threat Intelligence (Trellix)

FireEye Threat Intelligence provides actionable insights into global cyber threats, enabling organizations to proactively address vulnerabilities. Its comprehensive database includes information on attack methods, threat actors, and mitigation strategies.

Healthcare providers use FireEye Threat Intelligence to anticipate and defend against threats targeting EHR systems and telehealth platforms. Payers rely on its insights to secure claims systems from fraud and other attacks. Its detailed analyses help healthcare organizations prioritize their cybersecurity efforts.

153. Flexera Software Vulnerability Manager

Flexera Software Vulnerability Manager identifies and prioritizes vulnerabilities across IT environments. It provides patch management and compliance tools to ensure that systems remain secure and up-to-date.

Hospitals use Flexera to manage vulnerabilities in EHR platforms, medical devices, and administrative systems. Payers rely on its automated patching to secure claims processing and financial applications. Its compliance-focused tools simplify adherence to healthcare regulations.

154. Forcepoint

Forcepoint provides data security and threat protection solutions, including data loss prevention (DLP), user behavior analytics (UBA), and cloud security. Its platform focuses on protecting sensitive information across devices and applications.

Hospitals use Forcepoint to safeguard patient data and prevent unauthorized access to clinical systems. Payers rely on its DLP capabilities to secure claims data and financial records. Its integration with existing IT infrastructure ensures seamless implementation for healthcare organizations.

155. Forescout

Forescout offers visibility and control over connected devices, including IoT and medical devices. Its platform identifies unmanaged assets, monitors device behavior, and enforces security policies to mitigate risks.

Hospitals use Forescout to manage and secure IoT devices such as infusion pumps and patient monitors. Payers leverage its capabilities to protect connected systems involved in claims processing. Its real-time monitoring ensures comprehensive protection for healthcare IT environments.

156. ForgeRock

ForgeRock provides identity and access management (IAM) solutions that secure user identities across healthcare systems. Its platform supports single sign-on (SSO), multi-factor authentication (MFA), and access controls to enhance security.

Hospitals use ForgeRock to secure access to EHRs, telehealth platforms, and administrative systems. Payers rely on its tools to protect member portals and financial applications. Its scalability and compliance-focused features make it ideal for large healthcare organizations.

157. Forrester Zero Trust Partners

Forrester Zero Trust Partners provides frameworks and recommendations for implementing zero-trust security architectures. It focuses on minimizing attack surfaces and continuously verifying user and device identities.

Healthcare organizations use Forrester's guidance to secure EHR systems, IoT devices, and telehealth platforms. Hospitals benefit from its insights into best practices for segmenting networks and enforcing strict access controls. Its expertise helps healthcare entities enhance their security posture.

158. Fortanix

Fortanix specializes in confidential computing and data protection. Its platform secures sensitive data using advanced encryption methods and supports compliance with healthcare regulations like HIPAA.

Hospitals use Fortanix to protect patient records and research data in hybrid and multi-cloud environments. Payers leverage its tools to secure claims processing systems and financial transactions. Its focus on data security and privacy ensures trust and compliance in healthcare operations.

159. FortiEDR (Fortinet)

FortiEDR provides real-time endpoint detection and response (EDR) capabilities, protecting devices from advanced threats like ransomware and zero-day attacks. It features automated threat mitigation and forensic analysis tools.

Hospitals use FortiEDR to secure clinician devices, medical equipment, and systems accessing EHRs. Payers rely on its proactive threat detection to protect claims data and member portals. Its lightweight design ensures minimal impact on system performance.

160. Fortinet

Fortinet delivers a comprehensive suite of cybersecurity solutions, including firewalls, endpoint protection, and threat intelligence. Its Security Fabric architecture integrates various tools to provide unified protection across IT environments.

Healthcare providers use Fortinet to protect EHR systems, telehealth platforms, and medical devices from cyberattacks. Payers leverage its advanced security features to safeguard claims systems and financial records. Its scalability and ease of management make it a trusted choice for healthcare organizations.

161. Fortinet FortiGuard Labs

FortiGuard Labs provides advanced threat intelligence services, offering real-time insights into global cyber threats. It continuously updates Fortinet's Security Fabric with actionable intelligence to protect against emerging vulnerabilities.

Hospitals use FortiGuard Labs to stay ahead of threats targeting EHR systems, telehealth platforms, and medical devices. Payers benefit from its insights into fraud schemes and data breaches targeting claims systems. Its comprehensive threat intelligence enhances security strategies across healthcare organizations.

162. Fortinet FortiInsight

Fortinet FortiInsight delivers insider threat detection by analyzing user behavior and identifying anomalies. It provides actionable insights to prevent data breaches caused by human error or malicious intent.

Hospitals use FortiInsight to monitor staff access to EHRs and administrative systems, ensuring compliance with access policies. Payers leverage its behavior analytics to identify suspicious activities within claims processing platforms. Its proactive approach helps reduce the risk of insider threats in healthcare settings.

163. Fortinet FortiMail

Fortinet FortiMail is a secure email gateway that protects organizations from phishing, malware, and other email-borne threats. It uses AI-driven threat detection and sandboxing to block malicious content.

Hospitals use FortiMail to secure communications involving patient data and clinical workflows. Payers rely on its capabilities to protect email exchanges with members and providers. Its focus on healthcare compliance ensures the secure handling of sensitive information.

164. Fortinet FortiSIEM

FortiSIEM is a security information and event management (SIEM) platform that provides real-time visibility, threat detection, and compliance monitoring. It integrates with Fortinet's Security Fabric for comprehensive protection.

Healthcare providers use FortiSIEM to monitor EHR systems, medical devices, and telehealth platforms for suspicious activities. Hospitals rely on its advanced analytics to detect and respond to threats, while payers use it to ensure compliance with HIPAA and other regulations. Its centralized management simplifies security operations in complex healthcare environments.

165. Fortinet FortiSOAR

FortiSOAR is a security orchestration, automation, and response (SOAR) platform that streamlines incident response workflows. It integrates with other Fortinet tools to automate threat detection and mitigation.

Hospitals use FortiSOAR to coordinate responses to breaches affecting EHRs and medical devices. Payers leverage its capabilities to manage threats targeting claims systems. Its customizable playbooks ensure efficient and consistent incident responses in healthcare settings.

166. Fortinet FortiToken

FortiToken provides multi-factor authentication (MFA) solutions to secure access to critical systems. It supports one-time passwords (OTPs) and mobile-based authentication methods for enhanced security.

Hospitals use FortiToken to secure access to EHRs, administrative systems, and telehealth platforms. Payers rely on its MFA capabilities to protect member portals and financial applications. Its seamless integration with Fortinet's Security Fabric ensures comprehensive access control in healthcare environments.

167. Forward Advantage

Forward Advantage offers secure communication and data exchange solutions tailored to healthcare organizations. Its products include secure messaging, data migration, and interoperability tools.

Hospitals use Forward Advantage to facilitate secure communication between clinicians and administrative staff. Payers leverage its data exchange capabilities to integrate claims systems with provider networks. Its focus on healthcare workflows ensures compliance and operational efficiency.

168. Foxpass PAM

Foxpass Privileged Access Management (PAM) secures administrative access to critical IT systems by enforcing strong authentication and access controls. It integrates with cloud and on-premises environments for comprehensive protection.

Healthcare providers use Foxpass PAM to protect privileged accounts accessing EHRs and other sensitive systems. Payers rely on its capabilities to enforce access policies for claims processing platforms. Its user-friendly design ensures seamless adoption across healthcare teams.

169. Fudo Security PAM

Fudo Security PAM delivers advanced privileged access management solutions, including session recording, real-time monitoring, and access control. It helps organizations mitigate the risk of insider threats and unauthorized access.

Hospitals use Fudo Security PAM to secure administrative access to EHR systems and medical devices. Payers leverage its session monitoring capabilities to track activity within claims systems. Its robust auditing features support compliance with regulations like HIPAA and GDPR.

170. GFI LanGuard

GFI LanGuard is a network security scanner and patch management tool that identifies vulnerabilities and ensures systems remain up-to-date. It provides comprehensive reporting to support compliance and risk management.

Hospitals use GFI LanGuard to secure networks connecting EHR platforms and medical devices. Payers rely on its automated patching capabilities to protect claims processing systems. Its ease of deployment makes it a valuable tool for maintaining security in healthcare environments.

171. GTB Technologies

GTB Technologies specializes in data loss prevention (DLP) solutions that safeguard sensitive information from unauthorized access or sharing. Its platform includes tools for real-time monitoring, encryption, and compliance enforcement.

Hospitals use GTB Technologies to protect patient records and imaging data from accidental or malicious leaks. Payers rely on its capabilities to secure claims data and financial records. Its customizable policies and robust analytics ensure effective data protection across healthcare organizations.

172. Google Authenticator

Google Authenticator provides multi-factor authentication (MFA) for securing user accounts. It generates time-based one-time passwords (TOTPs) to enhance login security across various systems and applications.

Healthcare providers use Google Authenticator to secure access to EHR systems, administrative tools, and telehealth platforms. Payers leverage it to protect member portals and financial systems from unauthorized access. Its simplicity and wide compatibility make it a popular choice for healthcare environments.

173. Google Cloud Security

Google Cloud Security offers a suite of tools to secure cloud environments, including encryption, access controls, and threat detection. Its platform ensures compliance with healthcare regulations like HIPAA.

Hospitals use Google Cloud Security to protect cloud-hosted EHRs, patient portals, and telehealth services. Payers rely on its capabilities to secure claims data and member-facing applications. Its scalability and integration with other Google services make it ideal for large healthcare organizations.

174. Graylog

Graylog is an open-source log management and security information and event management (SIEM) platform. It enables real-time monitoring, threat detection, and forensic analysis.

Healthcare organizations use Graylog to monitor network activity, EHR systems, and medical devices for suspicious behavior. Hospitals benefit from its detailed log analysis to investigate breaches, while payers use it to secure claims platforms. Its affordability and flexibility make it a valuable tool for healthcare IT teams.

175. Guardtime

Guardtime uses blockchain technology to provide tamper-proof records for data integrity and security. Its platform is designed to ensure compliance with regulatory standards and enhance trust in data transactions.

Hospitals use Guardtime to securely store patient data and ensure the integrity of clinical workflows. Payers rely on it to streamline claims processing by verifying data authenticity. Its blockchain-based approach enhances transparency and reduces fraud in healthcare operations.

176. Guardtime Health

Guardtime Health extends Guardtime's blockchain capabilities to healthcare-specific use cases. It provides solutions for securing patient data, improving interoperability, and ensuring compliance with HIPAA.

Hospitals use Guardtime Health to securely exchange patient information across health systems. Payers benefit from its ability to validate claims data and prevent fraud. Its focus on healthcare applications makes it a trusted solution for enhancing security and operational efficiency.

177. Gurukul Behavioral Analytics

Gurukul Behavioral Analytics uses machine learning to detect anomalies in user and device behavior. It provides proactive threat detection and insider threat mitigation across IT environments.

Healthcare organizations use Gurukul to monitor staff access to EHRs, medical devices, and telehealth platforms. Hospitals benefit from its ability to detect unusual activities that could indicate security breaches, while payers leverage its analytics to secure claims systems. Its real-time insights enhance overall cybersecurity resilience.

178. HID Global

HID Global offers identity and access management (IAM) solutions, including smart cards, biometrics, and mobile authentication. Its platform ensures secure access to critical healthcare systems and data.

Hospitals use HID Global to control access to EHRs, administrative systems, and physical facilities. Payers rely on its tools to secure member portals and financial systems. Its comprehensive IAM capabilities support compliance and data protection in healthcare environments.

179. HID Global ActivID

HID Global ActivID provides advanced multi-factor authentication (MFA) solutions, including token-based and biometric authentication. It ensures secure access to sensitive healthcare systems.

Healthcare providers use ActivID to secure clinician access to EHRs and administrative tools. Payers leverage its capabilities to protect member data and financial systems. Its flexibility and integration options make it suitable for diverse healthcare environments.

180. Habitu8

Habitu8 delivers engaging cybersecurity awareness training tailored to healthcare environments. Its content includes phishing simulations, policy reminders, and best practices for data security.

Hospitals use Habitu8 to educate staff on protecting patient data and avoiding cyber threats. Payers rely on its training modules to reduce risks in claims processing workflows. Its interactive approach ensures better retention and adoption of cybersecurity best practices.

181. Halo Health

Halo Health provides secure communication solutions designed specifically for healthcare teams. Its platform includes features like encrypted messaging, on-call scheduling, and voice communication to enhance care coordination.

Hospitals use Halo Health to streamline communication among clinicians, ensuring quick and secure information exchange. Payers leverage its capabilities for secure collaboration with providers and members. Its compliance with healthcare regulations like HIPAA ensures the protection of sensitive information.

182. Hashed Health

Hashed Health leverages blockchain technology to improve healthcare processes, including data sharing, identity management, and claims processing. Its solutions enhance security and transparency across healthcare systems.

Hospitals use Hashed Health to securely share patient data and improve interoperability. Payers benefit from its blockchain-based claims processing to reduce fraud and ensure accuracy. Its innovative approach fosters trust and efficiency in healthcare transactions.

183. HashiCorp Vault

HashiCorp Vault provides secrets management and encryption services, allowing organizations to secure sensitive data like passwords, API keys, and certificates. It ensures that only authorized users and applications have access to critical resources.

Hospitals use HashiCorp Vault to protect credentials for EHR systems, medical devices, and cloud applications. Payers rely on it to secure sensitive claims data and administrative systems. Its robust access controls and encryption capabilities make it a trusted solution for healthcare security.

184. HealthCombix

HealthCombix is a blockchain-based platform designed for secure health data management and interoperability. It provides tools for privacy-preserving data exchanges and compliance with healthcare regulations.

Hospitals use HealthCombix to securely exchange patient data across health systems and organizations. Payers leverage its capabilities to streamline claims processing and reduce administrative inefficiencies. Its focus on blockchain ensures the integrity and transparency of healthcare transactions.

185. HealthTap

HealthTap is a virtual healthcare platform that provides secure telehealth services, including video consultations, health advice, and remote monitoring. It integrates with EHR systems to support seamless care delivery.

Hospitals use HealthTap to offer telehealth options for routine and specialized care, improving access for underserved populations. Payers benefit from its ability to reduce healthcare costs by supporting virtual consultations. Its compliance with HIPAA ensures patient data security and privacy.

186. Hexnode MDM

Hexnode MDM (Mobile Device Management) provides tools to manage and secure mobile devices in healthcare environments. It supports device tracking, app management, and compliance monitoring to ensure security.

Hospitals use Hexnode MDM to secure mobile devices used by clinicians for accessing EHRs and other clinical tools. Payers rely on its centralized management capabilities to enforce security policies across remote workforces. Its ease of deployment and comprehensive features make it suitable for healthcare organizations of all sizes.

187. Hitachi ID PAM

Hitachi ID Privileged Access Management (PAM) provides secure access controls for privileged accounts. It includes features like session monitoring, credential management, and real-time threat detection.



Hospitals use Hitachi ID PAM to secure administrative access to EHR systems, medical devices, and cloud applications. Payers leverage its capabilities to protect sensitive claims data and financial systems. Its robust auditing features ensure compliance with healthcare regulations like HIPAA.

188. IBM Blockchain

IBM Blockchain provides secure and scalable blockchain solutions for healthcare. Its platform supports use cases like supply chain management, patient data exchange, and fraud prevention.

Hospitals use IBM Blockchain to enhance interoperability and ensure the authenticity of medical records. Payers leverage its capabilities to improve transparency in claims processing and combat fraud. Its blockchain infrastructure ensures data integrity and compliance with healthcare regulations.

189. IBM Cloud Security

IBM Cloud Security delivers advanced tools to protect cloud environments, including encryption, access controls, and threat detection. It ensures compliance with healthcare standards like HIPAA and GDPR.

Healthcare providers use IBM Cloud Security to secure cloud-hosted EHRs, patient portals, and telehealth applications. Payers rely on its capabilities to protect claims systems and member-facing services. Its comprehensive security suite supports large-scale healthcare cloud deployments.

190. IBM Guardium

IBM Guardium provides data security and compliance solutions, offering real-time monitoring, vulnerability management, and encryption. Its platform ensures the protection of sensitive healthcare data across databases and applications.

Hospitals use IBM Guardium to monitor access to patient records and financial data, ensuring compliance with HIPAA. Payers rely on its capabilities to secure claims systems and reduce the risk of data breaches. Its robust reporting features support regulatory audits and risk assessments.

191. IBM MaaS360

IBM MaaS360 is a unified endpoint management (UEM) platform that provides mobile device management (MDM), app management, and threat defense. It ensures secure and compliant access to healthcare systems from mobile devices.

Hospitals use MaaS360 to manage and secure devices accessing EHRs, telehealth platforms, and clinical tools. Payers leverage its capabilities to enforce security policies for remote employees and contractors. Its AI-driven insights enhance device management and security in healthcare environments.

192. IBM Security QRadar

IBM Security QRadar is a security information and event management (SIEM) platform that provides real-time threat detection and response. It analyzes security logs and network activity to identify and prioritize threats.

Hospitals use QRadar to monitor EHR systems, IoT devices, and telehealth platforms for suspicious activities. Payers rely on its advanced analytics to detect and mitigate threats targeting claims processing systems. Its integration capabilities support comprehensive security operations in healthcare.

193. IBM Security QRadar UEBA

IBM Security QRadar UEBA (User Entity Behavior Analytics) enhances QRadar's capabilities by analyzing user and entity behaviors to detect insider threats and anomalous activities.

Healthcare organizations use QRadar UEBA to identify unusual access patterns to EHRs, financial systems, and administrative tools. Hospitals benefit from its ability to detect insider threats, while payers use it to safeguard member data. Its advanced behavior analytics improve security posture across healthcare environments.

194. IBM Security Resilient

IBM Security Resilient is an incident response platform that helps organizations manage and automate responses to cybersecurity threats. It integrates with other security tools to provide a unified approach to incident management.



Hospitals use Resilient to streamline responses to breaches affecting EHR systems and medical devices. Payers leverage its automation capabilities to handle incidents targeting claims platforms. Its customizable playbooks ensure healthcare-specific responses to security incidents.

195. IBM Security Secret Server

IBM Security Secret Server provides privileged access management (PAM) solutions, including credential storage, session monitoring, and access control. It ensures secure management of administrative accounts.

Hospitals use Secret Server to protect privileged accounts accessing EHR systems, medical devices, and administrative tools. Payers rely on its capabilities to enforce access policies for claims platforms and financial applications. Its auditing features support compliance with healthcare regulations.

196. IBM Security Verify

IBM Security Verify offers identity and access management (IAM) solutions, including single sign-on (SSO), multi-factor authentication (MFA), and risk-based access controls. It secures user identities across cloud and on-premises environments.

Healthcare providers use Verify to secure access to EHRs, telehealth platforms, and administrative systems. Payers leverage its tools to protect member portals and internal applications. Its integration with IBM's broader security portfolio enhances identity management in healthcare.

197. IBM Spectrum Protect

IBM Spectrum Protect provides data backup and recovery solutions for hybrid and multi-cloud environments. It offers ransomware protection, encryption, and automated recovery to ensure business continuity.

Hospitals use Spectrum Protect to safeguard EHR data, imaging archives, and financial records. Payers rely on its capabilities to secure claims systems and member data. Its robust recovery features minimize downtime during cyber incidents, ensuring operational resilience.

198. IBM X-Force Exchange

IBM X-Force Exchange is a threat intelligence platform that provides actionable insights into global cyber threats. It includes tools for threat sharing, analysis, and collaboration among security teams.

Hospitals use X-Force Exchange to stay informed about emerging threats targeting EHR systems and telehealth platforms. Payers leverage its insights to protect claims systems from fraud and cyberattacks. Its collaborative features enhance information sharing within the healthcare security community.

199. Illumio

Illumio provides zero-trust segmentation solutions to protect critical systems by isolating applications and workloads. Its platform limits the lateral movement of threats within networks, reducing the risk of breaches.

Hospitals use Illumio to secure EHR systems, medical devices, and administrative tools by segmenting sensitive data. Payers rely on its capabilities to protect claims systems from advanced threats. Its real-time visibility and enforcement ensure robust network security for healthcare organizations.

200. Imperva

Imperva delivers data and application security solutions, including web application firewalls (WAFs), DDoS protection, and database security. Its platform protects healthcare systems from advanced cyber threats.

Hospitals use Imperva to secure patient portals, telehealth platforms, and EHR systems from online attacks. Payers leverage its tools to protect claims systems and member-facing applications. Its focus on data and application security ensures compliance with healthcare regulations like HIPAA.

201. Infosec IQ

Infosec IQ provides cybersecurity awareness training tailored to various industries, including healthcare. Its platform offers phishing simulations, interactive training modules, and compliance tracking to educate employees on recognizing and responding to cyber threats.

Hospitals use Infosec IQ to train staff on safeguarding patient data and avoiding common attack vectors like phishing. Payers leverage its training programs to reduce human error in claims processing workflows. Its practical and engaging approach ensures improved retention of cybersecurity best practices.

202. InsightVM (Rapid7)

InsightVM by Rapid7 is a vulnerability management platform that identifies and prioritizes security risks across IT environments. It provides real-time data on vulnerabilities and automated remediation tracking.

Hospitals use InsightVM to identify weaknesses in EHR systems, medical devices, and network infrastructure. Payers rely on its analytics to secure claims processing platforms and member portals. Its robust reporting features support compliance with healthcare regulations like HIPAA and GDPR.

203. Inspired eLearning

Inspired eLearning offers customizable cybersecurity awareness training programs designed to improve employee behavior and reduce risks. Its courses cover phishing, social engineering, and compliance requirements.

Healthcare providers use Inspired eLearning to train staff on recognizing threats and maintaining data security. Payers benefit from its focus on compliance training to ensure adherence to HIPAA and other regulations. Its engaging content helps healthcare organizations build a strong security culture.

204. InTouch Health (Teladoc)

InTouch Health, now part of Teladoc Health, provides telehealth solutions for secure virtual consultations and remote patient monitoring. Its platform integrates with EHR systems to support continuity of care.

Hospitals use InTouch Health to expand access to healthcare services, particularly for rural and underserved populations. Payers leverage its capabilities to reduce costs and improve member satisfaction by offering virtual care options. Its HIPAA-compliant features ensure secure and private interactions.

205. Ironscales

Ironscales delivers an AI-powered email security platform designed to detect and respond to phishing and email-based threats. It provides tools for real-time threat detection, user training, and automated remediation.

Hospitals use Ironscales to protect staff from phishing attacks targeting EHR credentials and financial data. Payers rely on its capabilities to secure member communication and prevent fraud. Its proactive and automated approach reduces the risks associated with email-based vulnerabilities.

206. Ivanti Endpoint Security

Ivanti Endpoint Security protects endpoints from malware, ransomware, and unauthorized access. Its platform includes threat detection, patch management, and compliance tools for securing healthcare IT environments.

Hospitals use Ivanti to secure workstations, mobile devices, and systems accessing EHRs. Payers leverage its capabilities to protect claims processing platforms and member data. Its centralized management simplifies endpoint security across large and distributed healthcare organizations.

207. Ivanti Neurons for Vulnerability Management

Ivanti Neurons for Vulnerability Management uses AI-driven insights to identify and prioritize vulnerabilities. It automates remediation processes to reduce risks and ensure compliance with security policies.

Healthcare providers use Ivanti Neurons to secure medical devices, clinical systems, and networks from emerging threats. Payers benefit from its predictive analytics to protect claims systems and financial platforms. Its focus on automation enhances efficiency and reduces human error in vulnerability management.

208. Ivanti Patch Management

Ivanti Patch Management automates the deployment of security patches across IT environments. It ensures that healthcare systems remain updated and protected against known vulnerabilities.

Hospitals use Ivanti Patch Management to secure EHR platforms, medical devices, and administrative systems. Payers rely on its capabilities to maintain the integrity of claims processing platforms. Its ease of use and robust reporting features support compliance with healthcare regulations.

209. Jamf Pro

Jamf Pro is a mobile device management (MDM) solution designed for Apple devices. It supports device tracking, app management, and security enforcement to protect healthcare IT environments.

Hospitals use Jamf Pro to manage iPads and iPhones used by clinicians for accessing EHRs and telehealth platforms. Payers leverage its capabilities to secure employee devices accessing member data. Its seamless integration with Apple's ecosystem ensures efficient management and security.

210. Juniper Networks

Juniper Networks provides advanced networking and security solutions, including firewalls, secure access gateways, and network monitoring tools. Its platform ensures reliable and secure connectivity for healthcare organizations.

Hospitals use Juniper Networks to protect large, complex networks spanning multiple departments and connected devices. Payers rely on its scalability to secure claims systems and member-facing applications. Its AI-driven threat detection enhances security while maintaining high network performance.

211. Kandji

Kandji provides advanced device management for macOS, enabling healthcare organizations to securely manage and configure Apple devices. It supports compliance enforcement, patch management, and device tracking.

Hospitals use Kandji to secure Apple devices used by clinicians and administrative staff for accessing EHRs and telehealth platforms. Payers rely on its capabilities to manage remote employee devices. Its automated compliance checks ensure adherence to healthcare regulations like HIPAA.

212. Kaseya VSA

Kaseya VSA is a remote monitoring and management (RMM) platform that automates IT tasks like patch management, endpoint monitoring, and network management. It provides real-time visibility into healthcare IT environments.

Hospitals use Kaseya VSA to secure and manage endpoints such as workstations and medical devices. Payers leverage its tools to maintain operational efficiency and secure claims processing platforms. Its automation features reduce the administrative burden on healthcare IT teams.

213. Kaspersky Anti-Ransomware

Kaspersky Anti-Ransomware provides robust protection against ransomware attacks by detecting and blocking malicious activities in real-time. It offers recovery options to minimize disruption and data loss.

Hospitals use Kaspersky to protect critical systems like EHRs and imaging archives from ransomware. Payers leverage its capabilities to secure claims data and member portals. Its lightweight design ensures seamless integration with existing healthcare IT systems.

214. Kaspersky Endpoint Security

Kaspersky Endpoint Security delivers comprehensive protection for healthcare devices, including workstations, laptops, and servers. Its features include malware detection, vulnerability management, and data encryption.

Hospitals use Kaspersky Endpoint Security to protect clinical systems and administrative workstations. Payers rely on its robust threat detection to secure member data and claims platforms. Its centralized management console simplifies endpoint security in large healthcare organizations.

215. Kaspersky IoT Security

Kaspersky IoT Security provides specialized protection for connected devices in healthcare environments. It includes tools for threat detection, risk assessment, and compliance monitoring.

Hospitals use Kaspersky IoT Security to safeguard medical devices like infusion pumps and patient monitors from cyber threats. Health systems benefit from its ability to secure IoT ecosystems while maintaining compliance with healthcare regulations. Its focus on IoT vulnerabilities ensures patient safety and data integrity.

216. Kaspersky Threat Intelligence

Kaspersky Threat Intelligence offers actionable insights into global cyber threats, including malware trends, phishing campaigns, and attack methods. Its database provides in-depth analyses to enhance security operations.

Hospitals use Kaspersky Threat Intelligence to protect EHR systems and telehealth platforms from targeted attacks. Payers leverage its capabilities to prevent fraud and secure claims systems. Its real-time updates ensure healthcare organizations stay ahead of emerging threats.

217. Keycloak

Keycloak is an open-source identity and access management (IAM) solution that provides single sign-on (SSO), multi-factor authentication (MFA), and role-based access control. It supports integration with various healthcare IT systems.

Hospitals use Keycloak to secure access to EHRs, telehealth platforms, and administrative tools. Payers rely on its capabilities to protect member portals and internal applications. Its open-source flexibility makes it a cost-effective option for healthcare organizations.

218. KnowBe4

KnowBe4 provides cybersecurity awareness training and simulated phishing campaigns to educate employees on recognizing and avoiding cyber threats. Its platform focuses on reducing human error in healthcare security.

Hospitals use KnowBe4 to train staff on protecting patient data and avoiding phishing scams. Payers benefit from its simulations to test and improve employee awareness of cyber threats targeting claims workflows. Its interactive content ensures better engagement and retention of security practices.

219. Knox Manage (Samsung)

Knox Manage is a mobile device management (MDM) solution from Samsung that provides secure device configuration, monitoring, and compliance enforcement. It supports a wide range of mobile and IoT devices.

Hospitals use Knox Manage to secure mobile devices used by clinicians for accessing EHRs and telehealth tools. Payers rely on its centralized management to enforce security policies for remote workforces. Its compatibility with Samsung devices ensures seamless integration in healthcare settings.

220. Klara

Klara is a secure communication platform designed for healthcare providers. It offers features like encrypted messaging, appointment reminders, and patient engagement tools, ensuring compliance with HIPAA.

Hospitals use Klara to improve communication between clinicians and patients, streamlining workflows and enhancing care delivery. Payers benefit from its ability to securely communicate with members and providers. Its user-friendly interface supports efficient and secure interactions in healthcare environments.

221. Kroll Artifact Parser and Extractor (KAPE)

KAPE is a forensic tool that enables quick collection and analysis of forensic artifacts from endpoints. It is designed for rapid triage and evidence gathering in incident response scenarios.

Hospitals use KAPE to investigate breaches affecting EHR systems and medical devices. Payers rely on its capabilities to analyze incidents involving claims data. Its lightweight design and targeted artifact collection make it a valuable tool for healthcare cybersecurity investigations.

222. KY3P (S&P Global)

KY3P (Know Your Third Party) by S&P Global provides a centralized platform for managing third-party risks. It evaluates vendors' security, compliance, and operational capabilities to reduce risks.

Healthcare organizations use KY3P to assess the cybersecurity posture of vendors providing medical devices, IT services, and administrative tools. Payers benefit from its ability to monitor third-party risks associated with claims processing and outsourcing. Its detailed assessments ensure vendor compliance with healthcare regulations.

223. Lacework

Lacework delivers automated security and compliance solutions for cloud environments. It provides visibility into cloud workloads, threat detection, and configuration monitoring to protect healthcare data.

Hospitals use Lacework to secure cloud-hosted EHR systems, telehealth platforms, and patient portals. Payers leverage its capabilities to protect claims systems and ensure compliance with HIPAA and GDPR. Its automation reduces the burden on IT teams while enhancing security.

224. LastPass MFA

LastPass MFA enhances access security with multi-factor authentication (MFA) features, including biometrics, one-time passwords, and contextual authentication. It integrates seamlessly with existing IT systems.

Healthcare providers use LastPass MFA to secure access to EHRs, telehealth platforms, and administrative systems. Payers rely on its capabilities to protect member portals and financial applications. Its user-friendly implementation encourages adoption across healthcare organizations.

225. LogRhythm

LogRhythm provides security information and event management (SIEM) solutions with advanced analytics, threat detection, and response capabilities. It integrates with existing IT tools to deliver comprehensive security.

Hospitals use LogRhythm to monitor networks, medical devices, and EHR systems for suspicious activity. Payers leverage its real-time threat detection to protect claims systems and member data. Its automation and advanced analytics improve incident response times in healthcare environments.

226. LogRhythm Forensic Suite

LogRhythm Forensic Suite offers digital forensics tools for investigating cybersecurity incidents. It includes features like log analysis, anomaly detection, and evidence collection to support breach investigations.

Healthcare organizations use LogRhythm Forensic Suite to analyze breaches affecting patient data and medical devices. Hospitals benefit from its forensic capabilities to identify vulnerabilities, while payers use it to investigate fraud and data breaches. Its detailed reporting ensures compliance with regulatory requirements.

227. LogRhythm SOAR

LogRhythm SOAR (Security Orchestration, Automation, and Response) streamlines incident management workflows by integrating and automating security tools. It enhances efficiency in responding to cybersecurity threats.

Hospitals use LogRhythm SOAR to automate responses to threats targeting EHR systems and IoT devices. Payers leverage its capabilities to mitigate risks in claims systems. Its customizable playbooks ensure healthcare-specific incident management strategies.

228. LogRhythm UEBA

LogRhythm User and Entity Behavior Analytics (UEBA) provides advanced monitoring of user behavior to detect insider threats and anomalies. It leverages AI and machine learning to identify risks.

Healthcare providers use LogRhythm UEBA to monitor access patterns to EHRs and administrative systems, ensuring compliance with access policies. Payers rely on its behavior analytics to detect suspicious activities in claims platforms. Its real-time insights enhance threat detection and response.

229. LogicGate Risk Cloud

LogicGate Risk Cloud is a governance, risk, and compliance (GRC) platform that centralizes risk management processes. It includes tools for tracking and mitigating cybersecurity risks in healthcare.

Hospitals use LogicGate to manage risks associated with medical devices, IT systems, and supply chains. Payers leverage its compliance tracking features to ensure adherence to HIPAA and other regulations. Its flexible workflows support tailored risk management strategies.

230. ManageEngine (ADSelfService Plus)

ManageEngine ADSelfService Plus provides self-service password management and multi-factor authentication (MFA) for secure access to IT systems. It helps reduce administrative workloads and improve security.

Hospitals use ADSelfService Plus to secure clinician and staff access to EHRs and administrative tools. Payers benefit from its self-service features to enhance the user experience while maintaining data security. Its integration with Active Directory simplifies access management in healthcare organizations.

231. ManageEngine Mobile Device Manager Plus

ManageEngine Mobile Device Manager Plus is an enterprise-grade mobile device management (MDM) solution that secures and manages healthcare devices, including smartphones, tablets, and wearables.

Hospitals use Mobile Device Manager Plus to ensure that mobile devices accessing sensitive patient data remain secure and compliant with healthcare regulations. Payers leverage its capabilities to manage remote employee devices and ensure secure access to claims systems. Its automation features simplify device configuration and security policy enforcement.

232. ManageEngine PAM360

ManageEngine PAM360 is a privileged access management (PAM) solution designed to control and monitor privileged access across IT environments. It ensures that only authorized personnel have access to critical systems and data.

Hospitals use PAM360 to secure administrative access to EHRs and medical devices, ensuring compliance with healthcare regulations. Payers rely on its capabilities to protect financial systems and claims processing platforms. Its session monitoring and auditing features support regulatory audits and enhance security.

233. ManageEngine Patch Manager Plus

ManageEngine Patch Manager Plus automates the deployment of security patches across IT systems, ensuring that healthcare environments stay up to date and secure.

Hospitals use Patch Manager Plus to secure EHR systems, medical devices, and administrative tools by deploying critical security patches. Payers benefit from its automated patching capabilities to protect claims systems and member data. Its centralized management ensures consistent patching across healthcare networks.

234. Magnet AXIOM

Magnet AXIOM is a digital forensics tool that helps organizations collect, analyze, and report on evidence during cybersecurity investigations. It provides detailed insights into incidents involving data breaches or cyberattacks.

Hospitals use Magnet AXIOM to analyze cybersecurity incidents affecting EHR systems and medical devices. Payers leverage its forensic capabilities to investigate fraud and unauthorized access to claims data. Its robust analysis tools ensure that healthcare organizations can quickly assess the impact of cyber incidents.

235. Malwarebytes Endpoint Protection

Malwarebytes Endpoint Protection provides advanced security features to protect endpoints from malware, ransomware, and other threats. It includes real-time protection, threat detection, and automated remediation.

Hospitals use Malwarebytes to secure clinician devices, workstations, and medical equipment from cyber threats. Payers rely on its capabilities to protect claims systems and member-facing platforms. Its lightweight design ensures minimal disruption to healthcare workflows while maintaining strong protection.

236. Malwarebytes for Business

Malwarebytes for Business offers endpoint protection, malware removal, and cybersecurity tools tailored to business environments. It provides automated remediation and advanced threat detection to protect sensitive data.

Hospitals use Malwarebytes for Business to secure patient data, EHR systems, and clinical applications. Payers leverage its features to secure claims processing systems and member data. Its easy-to-manage platform makes it suitable for healthcare organizations of all sizes.

237. McAfee Advanced Threat Defense

McAfee Advanced Threat Defense provides multi-layered protection against malware, ransomware, and zero-day attacks. It uses a combination of machine learning, sandboxing, and heuristic analysis to identify emerging threats.

Hospitals use McAfee Advanced Threat Defense to secure critical systems like EHRs and medical devices. Payers rely on its capabilities to protect claims platforms and financial data. Its proactive threat detection ensures that healthcare organizations can quickly respond to new attack vectors.

238. McAfee Complete Data Protection

McAfee Complete Data Protection offers encryption, data loss prevention (DLP), and endpoint security to safeguard sensitive information across IT environments.

Hospitals use McAfee Complete Data Protection to secure patient records, imaging data, and medical device configurations. Payers leverage its encryption and DLP features to protect member data and claims information. Its comprehensive data protection ensures compliance with healthcare regulations like HIPAA and GDPR.

239. McAfee Endpoint Security

McAfee Endpoint Security provides advanced protection against malware, ransomware, and phishing attacks. It includes real-time threat detection, behavior analysis, and automated remediation.

Hospitals use McAfee Endpoint Security to protect workstations, laptops, and medical devices from cyber threats. Payers rely on its capabilities to secure claims systems and member portals. Its centralized management simplifies security across healthcare organizations with diverse IT environments.

240. McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) is a security information and event management (SIEM) platform that provides real-time monitoring, threat detection, and compliance reporting.

Hospitals use McAfee ESM to monitor network activity, medical devices, and clinical systems for suspicious activities. Payers rely on its advanced analytics to secure claims platforms and prevent fraud. Its robust reporting features ensure healthcare organizations stay compliant with regulatory standards like HIPAA.

241. McAfee Total Protection for DLP

McAfee Total Protection for Data Loss Prevention (DLP) provides tools to monitor, detect, and prevent the unauthorized transfer of sensitive data. It helps healthcare organizations secure patient data and meet compliance requirements.

Hospitals use McAfee Total Protection to safeguard patient records and ensure that sensitive health information is not inadvertently shared or leaked. Payers rely on its capabilities to protect claims data and financial records. Its compliance tools ensure adherence to healthcare regulations like HIPAA and GDPR.

242. MedRec

MedRec is a blockchain-based healthcare data management system that enables secure and interoperable health record sharing. It ensures data integrity and transparency, allowing patients and providers to securely exchange medical records.

Hospitals use MedRec to streamline data sharing across multiple healthcare providers, ensuring the accuracy and integrity of patient records. Payers benefit from its ability to verify claims and prevent fraud. Its blockchain technology ensures that health data is tamper-proof and secure.

243. Medici Telehealth

Medici Telehealth offers a secure platform for virtual care delivery, including video consultations, messaging, and patient monitoring. It integrates with EHR systems to ensure continuity of care for patients.

Hospitals use Medici Telehealth to offer remote consultations and virtual follow-ups, improving access to care. Payers leverage its capabilities to reduce healthcare costs by supporting telehealth for routine care. Its HIPAA-compliant features ensure the security and privacy of patient data during telehealth interactions.

244. Medigate (by Claroty)

Medigate, now part of Claroty, provides healthcare-focused IoT security solutions that protect connected medical devices and operational technology (OT). It offers real-time threat detection, risk assessment, and compliance monitoring.

Hospitals use Medigate to secure connected medical devices such as infusion pumps, patient monitors, and imaging systems. Health systems benefit from its ability to identify and mitigate risks associated with medical devices. Its healthcare-specific focus ensures comprehensive protection across IoT and OT environments.

245. MEDITECH Expanse Secure Messaging

MEDITECH Expanse Secure Messaging is a communication platform designed for healthcare teams to securely exchange patient information and coordinate care. It integrates seamlessly with MEDITECH's EHR system.

Hospitals use MEDITECH Expanse Secure Messaging to improve communication between clinicians and staff, ensuring that sensitive patient data is protected during discussions. Payers rely on it for secure collaboration with providers. Its integration with MEDITECH's EHR enhances workflow efficiency in healthcare environments.

246. Mend Telemedicine Platform

Mend provides a secure telemedicine platform that supports virtual consultations, patient scheduling, and follow-up care. It integrates with EHR systems to enhance the continuity of care for patients.

Hospitals use Mend to provide virtual care services and improve access to healthcare for underserved populations. Payers benefit from its ability to reduce healthcare costs while maintaining high-quality care. Its HIPAA-compliant platform ensures secure communication and data exchange in healthcare settings.

247. Mend VIP Telehealth

Mend VIP Telehealth is a telehealth platform designed for high-touch, personalized patient care. It offers features like secure video consultations, patient communication, and appointment management.

Hospitals use Mend VIP Telehealth to offer personalized virtual consultations for patients with chronic conditions or those requiring specialized care. Payers leverage its capabilities to enhance patient engagement and reduce in-person visit costs. Its HIPAA-compliant features ensure secure and private patient interactions.

248. MetaCompliance

MetaCompliance offers cybersecurity awareness training and compliance management solutions. Its platform includes phishing simulations, policy enforcement, and tracking tools to help organizations reduce cyber risks.

Hospitals use MetaCompliance to train staff on recognizing and mitigating cyber threats, such as phishing and social engineering. Payers rely on its training modules to reduce risks in claims processing workflows. Its compliance tracking features help healthcare organizations meet regulatory requirements.

249. MetricStream Third-Party Risk

MetricStream provides a comprehensive platform for third-party risk management, allowing organizations to assess, monitor, and mitigate risks posed by vendors and partners.

Hospitals use MetricStream to evaluate the cybersecurity posture of medical device manufacturers, IT service providers, and other third-party vendors. Payers rely on it to assess risks associated with claims processors and other external service providers. Its detailed assessments ensure compliance with healthcare regulations.

250. Mimecast Awareness Training

Mimecast Awareness Training provides cybersecurity education for employees, focusing on the most common attack vectors such as phishing and social engineering. Its platform includes interactive training modules and assessments.

Hospitals use Mimecast to educate staff on safeguarding patient data and avoiding phishing attacks targeting EHR systems. Payers benefit from its phishing simulations to improve employee awareness of cybersecurity risks in claims processing. Its user-friendly content ensures better retention of security best practices across healthcare organizations.

251. Mimecast Secure Email Gateway

Mimecast Secure Email Gateway provides protection against phishing, malware, and other email-based threats. It uses AI-driven threat intelligence to detect malicious emails and prevent data breaches.

Hospitals use Mimecast Secure Email Gateway to protect communications involving patient data, ensuring that emails remain secure and comply with healthcare regulations. Payers rely on its capabilities to safeguard email exchanges with members and providers. Its robust detection and remediation features reduce the risk of cyberattacks via email.

252. Microsoft 365 DLP

Microsoft 365 Data Loss Prevention (DLP) helps organizations protect sensitive data across Office 365 applications. It provides policies and tools to prevent accidental or intentional data leaks.

Hospitals use Microsoft 365 DLP to safeguard patient data, including emails, documents, and communications within EHR systems. Payers benefit from its DLP features to protect claims data and financial records. Its integration with Microsoft 365 applications ensures that data protection is seamlessly embedded into everyday workflows.

253. Microsoft Advanced Threat Analytics (ATA)

Microsoft Advanced Threat Analytics (ATA) helps organizations detect suspicious activity and advanced threats in real-time. It uses machine learning to analyze user behavior and network traffic for anomalies.

Hospitals use Microsoft ATA to monitor access to EHR systems, medical devices, and sensitive patient data. Payers rely on its advanced threat detection to secure claims systems and member portals. Its behavior analytics help identify insider threats and prevent data breaches in healthcare environments.

254. Microsoft Azure Active Directory

Microsoft Azure Active Directory (Azure AD) is an identity and access management (IAM) solution that provides secure authentication and authorization for cloud-based applications. It supports single sign-on (SSO) and multi-factor authentication (MFA).

Hospitals use Azure AD to manage access to EHR systems, telehealth platforms, and administrative tools. Payers rely on its IAM capabilities to secure member portals and internal applications. Its integration with Microsoft's ecosystem ensures seamless access management and compliance with healthcare regulations.

255. Microsoft Azure Blockchain

Microsoft Azure Blockchain provides a platform for developing and deploying blockchain applications in the cloud. It enables secure and transparent data sharing and helps improve compliance with industry standards.

Hospitals use Azure Blockchain to securely share patient data across healthcare providers, ensuring data integrity and privacy. Payers benefit from its capabilities to verify claims data and reduce fraud. Its blockchain infrastructure ensures that all data exchanges are secure and compliant with healthcare regulations.

256. Microsoft Azure Security

Microsoft Azure Security offers a comprehensive suite of security tools to protect cloud environments, including encryption, access controls, and real-time monitoring. It helps ensure compliance with healthcare standards like HIPAA and GDPR.

Hospitals use Azure Security to protect cloud-hosted EHR systems, patient portals, and telehealth services. Payers leverage its capabilities to secure cloud-based claims platforms and member data. Its integration with Microsoft Azure enhances security across healthcare cloud infrastructures.

257. Microsoft Azure Sentinel

Microsoft Azure Sentinel is a cloud-native security information and event management (SIEM) solution that provides threat detection, investigation, and response capabilities. It uses AI and automation to improve security operations.

Hospitals use Azure Sentinel to monitor EHR systems, medical devices, and telehealth platforms for potential security threats. Payers benefit from its capabilities to detect fraud and cyberattacks targeting claims systems. Its cloud-native architecture ensures scalability and flexibility in large healthcare environments.

258. Microsoft Defender ATP

Microsoft Defender Advanced Threat Protection (ATP) provides endpoint protection, threat detection, and incident response capabilities. It uses machine learning and behavior analytics to identify and block advanced threats.

Hospitals use Microsoft Defender ATP to secure endpoints accessing sensitive healthcare data, including clinician workstations and medical devices. Payers rely on it to protect claims systems and financial platforms. Its AI-driven protection provides robust defenses against emerging threats in healthcare.

259. Microsoft Defender for Office 365

Microsoft Defender for Office 365 protects email accounts and Office 365 applications from phishing, malware, and other cyber threats. It includes automated threat detection, incident response, and threat intelligence.

Hospitals use Defender for Office 365 to protect communications involving patient data and medical records. Payers rely on it to secure email exchanges with members and providers. Its integration with Office 365 ensures that healthcare organizations can secure their entire suite of communication tools.

260. Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management provides a comprehensive solution for identifying, prioritizing, and remediating security vulnerabilities across IT environments. It integrates with Defender ATP to deliver a unified security posture.

Hospitals use Defender Vulnerability Management to identify and patch vulnerabilities in EHR systems, medical devices, and clinical infrastructure. Payers rely on its capabilities to ensure claims systems and financial platforms remain secure. Its integration with Microsoft Defender ensures a cohesive security framework across healthcare organizations.

261. Microsoft Intune

Microsoft Intune is a mobile device management (MDM) and mobile application management (MAM) solution that secures devices and applications across healthcare environments. It enables secure access to healthcare systems from mobile devices.

Hospitals use Intune to manage and secure devices accessing EHR systems, telehealth platforms, and patient data. Payers rely on it to enforce security policies across mobile devices used by employees and contractors. Its integration with Azure AD ensures seamless identity management and secure access to sensitive data.

262. Microsoft SCCM (System Center Configuration Manager)

Microsoft SCCM provides endpoint management and patching solutions to ensure that healthcare devices remain up-to-date and secure. It supports compliance and risk management by automating software updates and configuration changes.

Hospitals use SCCM to manage medical devices, clinician workstations, and administrative systems. Payers rely on its capabilities to secure claims systems and financial platforms. Its comprehensive endpoint management features enhance security across diverse healthcare environments.

263. Microsoft Teams for Healthcare

Microsoft Teams for Healthcare is a collaboration and communication platform designed for healthcare organizations. It provides secure video conferencing, instant messaging, and document sharing, all integrated into the healthcare ecosystem.

Hospitals use Microsoft Teams for virtual care delivery, facilitating telehealth consultations, team collaborations, and patient engagement. Payers leverage it for secure communications with healthcare providers and members. Its HIPAA-compliant features ensure secure and confidential interactions, enhancing healthcare communication efficiency.

264. Microsoft Zero Trust Solutions

Microsoft Zero Trust Solutions adopt a security framework that continuously verifies every user, device, and network request before granting access, assuming that no entity is trusted by default.

Hospitals use Microsoft Zero Trust Solutions to secure access to EHR systems, medical devices, and administrative tools. Payers benefit from its continuous monitoring and enforcement to protect claims systems and member data. Its seamless integration with other Microsoft tools helps healthcare organizations implement a robust zero-trust architecture.

265. MobileIron (Ivanti)

MobileIron, now part of Ivanti, provides a mobile device management (MDM) and mobile application management (MAM) solution designed to secure healthcare devices. It helps organizations manage and monitor devices accessing sensitive healthcare data.

Hospitals use MobileIron to secure clinician devices and ensure that mobile access to EHRs, medical devices, and telehealth platforms complies with healthcare regulations. Payers rely on its capabilities to secure member-facing applications and financial platforms accessed by mobile devices. Its comprehensive security features ensure compliance with HIPAA.

266. Netskope

Netskope provides a cloud-native security platform that delivers data and threat protection across cloud applications, cloud infrastructure, and web traffic. Its solution enables secure cloud adoption and ensures compliance with regulations like HIPAA.

Hospitals use Netskope to secure cloud-hosted EHR systems, telehealth platforms, and patient portals. Payers benefit from its capabilities to protect cloud-based claims systems and member data. Its real-time visibility into cloud traffic allows healthcare organizations to monitor and control data access and movement.

267. Netskope Cloud Security

Netskope Cloud Security is a data-centric security solution designed to protect cloud applications and services. It provides real-time data and threat protection, ensuring compliance with healthcare standards.

Hospitals use Netskope Cloud Security to monitor and protect cloud-hosted patient data, including EHRs and telehealth services. Payers leverage its data loss prevention (DLP) capabilities to secure claims platforms. Its advanced analytics and real-time threat detection ensure comprehensive cloud security for healthcare organizations.

268. Netskope Zero Trust

Netskope Zero Trust enforces the zero-trust security model by ensuring that every access request to cloud applications is authenticated and authorized. It continuously monitors user behavior and device health to mitigate risks.

Hospitals use Netskope Zero Trust to secure access to EHRs, medical devices, and telehealth platforms, ensuring that only authorized users and devices can access sensitive information. Payers rely on its security controls to protect claims systems and financial data. Its integration with other security tools enhances healthcare cybersecurity infrastructure.

269. Netsurion EventTracker

Netsurion EventTracker is a security information and event management (SIEM) platform that provides real-time monitoring, log management, and threat detection. It helps healthcare organizations detect and respond to cybersecurity threats.

Hospitals use EventTracker to monitor activity across EHR systems, medical devices, and IT networks. Payers benefit from its threat detection and log analysis capabilities to secure claims platforms. Its comprehensive reporting and analytics support compliance with healthcare regulations like HIPAA.

270. NetWitness UEBA

NetWitness UEBA (User and Entity Behavior Analytics) uses machine learning to detect anomalies in user and device behaviors. It helps healthcare organizations identify insider threats and other suspicious activities.

Hospitals use NetWitness UEBA to monitor clinician access to sensitive systems, such as EHRs and medical devices, and to detect abnormal user activities that could indicate security breaches. Payers rely on it to secure claims systems by identifying fraudulent access attempts. Its behavior analytics improve overall security in healthcare environments.

271. Netwrix Auditor

Netwrix Auditor provides auditing and compliance tools to monitor and report on user activity across IT systems. It ensures that healthcare organizations can detect unauthorized access and maintain compliance with regulations like HIPAA.

Hospitals use Netwrix Auditor to track access to patient records, medical devices, and clinical applications, ensuring compliance with access control policies. Payers rely on its capabilities to monitor claims systems and financial records for unauthorized changes or access. Its reporting features support regulatory audits in healthcare organizations.

272. Netwrix Privilege Secure

Netwrix Privilege Secure is a privileged access management (PAM) solution that provides visibility and control over sensitive access permissions. It ensures that only authorized personnel have access to critical systems and data.

Hospitals use Privilege Secure to secure administrative access to EHR systems, medical devices, and IT infrastructure. Payers benefit from its capabilities to protect claims systems and financial data from unauthorized access. Its session recording and auditing features support compliance with healthcare regulations.

Would you like to continue with the next set of vendors? Let me know!

4o mini

You said:

yes

ChatGPT said:

ChatGPT

273. Nexpose (Rapid7)

Nexpose by Rapid7 is a vulnerability management platform that identifies, prioritizes, and remediates security vulnerabilities across IT environments. It provides real-time visibility and automated patching tools to ensure systems remain secure.

Hospitals use Nexpose to scan EHR systems, medical devices, and clinical infrastructure for vulnerabilities. Payers leverage its capabilities to identify and fix security flaws in claims processing platforms. Its detailed reports help healthcare organizations prioritize remediation efforts and ensure compliance with HIPAA and other regulations.

274. Ninite Pro

Ninite Pro is an automated patch management and software deployment tool that simplifies the process of keeping IT systems up to date. It supports patching for multiple applications, reducing the risk of vulnerabilities.

Hospitals use Ninite Pro to automatically update medical devices, clinician workstations, and administrative tools. Payers benefit from its ability to patch claims systems and financial applications. Its automated patching ensures consistent and timely updates, which are essential for maintaining secure healthcare IT environments.

275. Okta

Okta is an identity and access management (IAM) platform that provides secure authentication and access control. It supports single sign-on (SSO), multi-factor authentication (MFA), and adaptive access management.

Hospitals use Okta to secure access to EHRs, medical devices, and telehealth platforms. Payers rely on its IAM capabilities to protect claims platforms and member portals. Its integration with a wide range of healthcare applications enhances user authentication while maintaining compliance with regulations like HIPAA.

276. Okta MFA

Okta MFA adds an extra layer of security to authentication processes by requiring multiple forms of verification. It helps healthcare organizations secure access to critical systems, such as EHRs, financial applications, and telehealth platforms.

Hospitals use Okta MFA to prevent unauthorized access to sensitive patient data and medical devices. Payers rely on it to protect member portals and claims data. Its seamless integration with Okta's IAM platform ensures that multi-factor authentication is implemented efficiently across healthcare environments.

277. One Identity Safeguard

One Identity Safeguard is a privileged access management (PAM) solution that secures and audits privileged accounts to prevent unauthorized access. It helps healthcare organizations manage access to critical systems and data.

Hospitals use One Identity Safeguard to control administrative access to EHR systems, medical devices, and hospital networks. Payers leverage its capabilities to protect claims processing systems from unauthorized access. Its robust monitoring and auditing features enhance compliance with healthcare security standards.

278. OneLogin

OneLogin provides a unified identity and access management (IAM) solution that secures user authentication and enables single sign-on (SSO). It ensures secure access to cloud-based and on-premises applications across healthcare organizations.

Hospitals use OneLogin to simplify clinician access to EHR systems, telehealth platforms, and administrative tools. Payers rely on it to secure member portals and financial systems. Its ease of use and integration with existing healthcare IT infrastructure ensure seamless adoption across organizations.

279. OneLogin Protect

OneLogin Protect is a mobile app-based multi-factor authentication (MFA) solution that enhances the security of healthcare systems. It provides users with an extra layer of protection to ensure only authorized individuals can access sensitive data.

Hospitals use OneLogin Protect to secure access to patient records, EHR systems, and clinical applications. Payers rely on it to protect claims data and financial systems from unauthorized access. Its simplicity and integration with OneLogin's IAM platform ensure a user-friendly MFA solution.

280. OneTrust Vendorpedia

OneTrust Vendorpedia is a third-party risk management platform that helps organizations assess and monitor the cybersecurity posture of vendors. It provides insights into vendors' security practices to mitigate risks associated with third-party relationships.

Hospitals use OneTrust Vendorpedia to evaluate the security practices of medical device manufacturers, IT service providers, and other healthcare vendors. Payers leverage it to monitor the risks associated with claims processing and outsourcing partners. Its detailed assessments ensure that third-party vendors meet healthcare security and compliance requirements.

281. OpenText (Carbonite Endpoint Encryption)

OpenText (Carbonite) Endpoint Encryption protects sensitive data on endpoints by encrypting it both at rest and in transit. This solution helps organizations prevent unauthorized access and ensure compliance with data protection regulations.

Hospitals use OpenText Endpoint Encryption to secure patient records, medical devices, and imaging systems. Payers rely on its capabilities to protect claims data and financial transactions. Its automated encryption ensures data security without disrupting the workflow in healthcare environments.

282. OpenVAS (Greenbone Networks)

OpenVAS (Open Vulnerability Assessment System) is an open-source vulnerability scanning tool that helps organizations identify and remediate security vulnerabilities across IT systems. It provides detailed vulnerability assessments and risk reports.

Hospitals use OpenVAS to identify vulnerabilities in EHR systems, medical devices, and hospital networks. Payers leverage its scanning tools to assess and secure claims systems. Its open-source nature and robust reporting features make it a cost-effective vulnerability management solution for healthcare organizations.

283. Oracle Cloud Security

Oracle Cloud Security provides comprehensive protection for cloud-based applications, including identity management, encryption, and compliance monitoring. It ensures that sensitive healthcare data hosted in the cloud remains secure.

Hospitals use Oracle Cloud Security to secure cloud-hosted EHR systems, telehealth platforms, and patient data storage. Payers rely on its capabilities to protect cloud-based claims systems and member portals. Its integration with Oracle's broader cloud platform enhances security and operational efficiency.

284. Oxygen Forensics

Oxygen Forensics provides advanced mobile device forensics and data recovery tools. It helps organizations recover and analyze data from smartphones, tablets, and other mobile devices in response to cybersecurity incidents.

Hospitals use Oxygen Forensics to investigate incidents involving mobile devices that access EHR systems or clinical applications. Payers rely on it to analyze mobile-based fraud or unauthorized access to claims systems. Its detailed forensic capabilities support compliance with regulatory requirements in healthcare.

285. Palo Alto Networks

Palo Alto Networks offers a wide range of cybersecurity solutions, including firewalls, endpoint protection, and cloud security. Its integrated platform delivers comprehensive protection across IT environments.

Hospitals use Palo Alto Networks to secure EHR systems, medical devices, and networks from cyberattacks. Payers rely on its capabilities to protect claims platforms and member data. Its next-gen firewalls and threat detection systems provide robust security for healthcare organizations of all sizes.

286. Palo Alto Networks Cortex XDR

Palo Alto Networks Cortex XDR integrates endpoint detection and response (EDR) with network traffic analysis to provide advanced protection against cyber threats. It uses machine learning to detect and mitigate threats in real time.

Hospitals use Cortex XDR to monitor medical devices, EHR systems, and administrative tools for suspicious activity. Payers leverage its capabilities to protect claims systems and member data. Its unified approach to endpoint and network security ensures comprehensive protection in healthcare environments.

287. Palo Alto Networks Cortex XDR Forensics

Palo Alto Networks Cortex XDR Forensics provides advanced forensic analysis tools for investigating cybersecurity incidents. It enables organizations to track the origin and scope of attacks across endpoints and networks.

Hospitals use Cortex XDR Forensics to investigate breaches involving EHR systems and medical devices. Payers rely on it to analyze fraud or unauthorized access incidents affecting claims systems. Its in-depth analysis and real-time capabilities enhance security investigations in healthcare environments.

288. Palo Alto Networks Cortex XSOAR

Palo Alto Networks Cortex XSOAR is a security orchestration, automation, and response (SOAR) platform that automates and streamlines incident response processes. It integrates with other security tools to provide a unified response to threats.

Hospitals use Cortex XSOAR to automate responses to cybersecurity incidents affecting EHR systems, medical devices, and clinical applications. Payers leverage its orchestration capabilities to mitigate risks in claims platforms. Its customizable workflows ensure efficient and consistent incident responses.

289. Palo Alto Networks IoT Security

Palo Alto Networks IoT Security protects connected medical devices and operational technology (OT) from cyber threats. It provides real-time visibility and risk management for healthcare IoT environments.

Hospitals use Palo Alto Networks IoT Security to safeguard devices such as infusion pumps, patient monitors, and imaging systems. Payers rely on it to protect IoT systems involved in claims processing. Its comprehensive security features ensure that connected devices remain secure and compliant with healthcare regulations.

290. Palo Alto Networks Prisma

Palo Alto Networks Prisma provides cloud security solutions, including threat detection, data protection, and compliance monitoring. It secures cloud applications and infrastructure, ensuring that healthcare organizations' cloud environments remain safe.

Hospitals use Prisma to secure cloud-hosted EHRs, telehealth platforms, and patient data. Payers rely on it to protect cloud-based claims systems and member portals. Its unified security features enhance compliance and reduce the risk of cloud-specific threats in healthcare organizations.

291. Palo Alto Networks Prisma Cloud

Prisma Cloud offers comprehensive security for cloud-native applications and infrastructure. It includes tools for vulnerability management, data protection, and compliance monitoring, ensuring secure cloud environments for healthcare.

Hospitals use Prisma Cloud to protect cloud-hosted applications, including EHR systems, telehealth platforms, and patient portals. Payers leverage its capabilities to secure claims systems and ensure compliance with healthcare regulations like HIPAA. Its real-time monitoring and threat intelligence protect healthcare data across cloud environments.

292. Palo Alto Networks Unit 42

Unit 42 is Palo Alto Networks' threat intelligence team, providing comprehensive insights into emerging cybersecurity threats, attack methods, and mitigation strategies. Its reports help organizations stay ahead of evolving threats.

Hospitals use Unit 42's threat intelligence to anticipate and defend against cyberattacks targeting EHR systems, medical devices, and telehealth platforms. Payers benefit from its insights into fraud schemes and cyberattacks targeting claims systems. Its real-time threat intelligence improves overall security posture in healthcare environments.

293. Panorays

Panorays is a third-party risk management platform that helps organizations assess and manage the cybersecurity posture of vendors and partners. It provides continuous monitoring of third-party risks to ensure compliance and reduce exposure.

Hospitals use Panorays to evaluate the cybersecurity practices of vendors providing medical devices, IT services, and cloud platforms. Payers rely on it to assess risks associated with claims processors and outsourced administrative functions. Its continuous monitoring ensures that third-party vendors meet healthcare security and compliance standards.

294. Paraben E3 Platform

The Paraben E3 Platform is a comprehensive digital forensics tool that provides investigative capabilities for mobile devices, computers, and cloud data. It helps organizations collect, preserve, and analyze evidence from a wide range of digital sources.

Hospitals use Paraben E3 to investigate incidents involving mobile devices, EHR systems, and medical devices. Payers rely on its forensic capabilities to analyze fraud or unauthorized access to claims data. Its extensive support for various device types and data sources makes it a valuable tool for healthcare cybersecurity investigations.

295. Patch My PC

Patch My PC automates patching for third-party applications and software. It ensures that critical software vulnerabilities are patched in a timely manner, reducing the risk of exploitation.

Hospitals use Patch My PC to ensure that clinical software, EHR systems, and other healthcare applications remain up-to-date with security patches. Payers benefit from its capabilities to secure claims processing platforms and administrative tools. Its simplicity and automation ensure that patch management is efficient and compliant with healthcare security standards.

296. PerfectServe

PerfectServe provides secure messaging and communication tools for healthcare teams. Its platform ensures that sensitive patient information is shared securely and efficiently across healthcare environments.

Hospitals use PerfectServe to streamline communication among care teams, ensuring that patient data is shared securely during clinical workflows. Payers rely on it for secure communication with healthcare providers and members. Its HIPAA-compliant features guarantee that healthcare organizations adhere to data privacy and security regulations.

297. Perception Point

Perception Point is an advanced threat prevention platform that provides email, web, and cloud security. It uses machine learning and threat intelligence to detect and block malicious content before it can impact the organization.

Hospitals use Perception Point to secure email communications involving patient data, clinical updates, and administrative information. Payers rely on it to protect claims processing systems and member communications from phishing and malware attacks. Its advanced detection capabilities provide comprehensive protection for healthcare organizations.

298. PhishMe (Cofense)

PhishMe (now Cofense) provides phishing detection and training tools that help organizations identify, report, and respond to phishing attacks. Its platform includes simulations, training, and threat intelligence to reduce phishing risks.

Hospitals use PhishMe to train staff on recognizing phishing attempts that target EHR systems, medical devices, and other critical healthcare applications. Payers benefit from its capabilities to mitigate phishing risks in claims processing workflows. Its user-friendly platform improves cybersecurity awareness across healthcare organizations.

299. Ping Identity

Ping Identity offers identity and access management (IAM) solutions that provide secure authentication, single sign-on (SSO), and adaptive access management. It ensures that only authorized users can access sensitive systems and data.

Hospitals use Ping Identity to secure access to EHRs, telehealth platforms, and administrative tools. Payers rely on its capabilities to protect member portals and internal applications. Its seamless integration with existing healthcare systems enhances identity management while ensuring compliance with regulations like HIPAA.

300. Ping Identity MFA

Ping Identity MFA provides multi-factor authentication (MFA) to secure user access to healthcare systems. It supports various authentication methods, including biometrics, push notifications, and one-time passwords (OTPs).

Hospitals use Ping Identity MFA to prevent unauthorized access to patient records, EHR systems, and medical devices. Payers benefit from its capabilities to secure claims systems and member portals from unauthorized access. Its flexibility and compatibility ensure that MFA is easily integrated into healthcare IT environments.

301. Ping Identity Zero Trust

Ping Identity Zero Trust provides a security model that ensures every user, device, and application is continuously verified before granting access. It helps healthcare organizations implement robust access controls and reduce the risk of unauthorized access.

Hospitals use Ping Identity Zero Trust to secure access to EHR systems, medical devices, and telehealth platforms. Payers rely on it to protect claims systems and member data from unauthorized access. Its continuous verification of access requests enhances security and compliance across healthcare organizations.

302. PKWARE EncryptRIGHT

PKWARE's EncryptRIGHT provides data encryption and data masking solutions to protect sensitive healthcare data. It helps organizations secure data at rest and in transit, ensuring compliance with regulations like HIPAA.

Hospitals use EncryptRIGHT to protect patient records, medical device configurations, and clinical data during storage and transmission. Payers benefit from its encryption capabilities to secure claims data and financial transactions. Its automated encryption ensures data security without disrupting healthcare workflows.

303. Prevalent

Prevalent is a third-party risk management platform that helps organizations assess, monitor, and mitigate risks from vendors and partners. It offers tools for continuous monitoring, risk assessments, and compliance tracking.

Hospitals use Prevalent to evaluate the cybersecurity practices of vendors providing IT services, medical devices, and software. Payers rely on its platform to assess the risks associated with third-party claims processors and outsourcing partners. Its continuous monitoring capabilities ensure that third-party vendors meet healthcare security and compliance standards.

304. ProcessUnity

ProcessUnity provides a third-party risk management platform that helps organizations manage vendor risks, compliance, and cybersecurity vulnerabilities. It offers tools for assessment, monitoring, and mitigation of third-party risks.

Hospitals use ProcessUnity to assess the security posture of medical device manufacturers, IT service providers, and cloud vendors. Payers rely on it to monitor risks associated with claims processors and other third-party partners. Its continuous monitoring and detailed assessments ensure that vendors meet strict healthcare security standards.

305. Proofpoint

Proofpoint provides comprehensive email security, data loss prevention (DLP), and threat intelligence solutions. Its platform is designed to detect and block phishing, malware, and other email-based threats targeting healthcare organizations.

Hospitals use Proofpoint to secure communications involving patient data, clinical information, and administrative details. Payers benefit from its email security tools to protect claims systems and financial data. Its DLP capabilities ensure that sensitive healthcare information is not inadvertently shared or compromised.

306. Proofpoint Cloud Security

Proofpoint Cloud Security provides threat protection for cloud applications, including Office 365, G Suite, and Salesforce. It ensures that sensitive data is protected from cloud-specific vulnerabilities and compliance risks.

Hospitals use Proofpoint Cloud Security to secure cloud-hosted EHR systems, patient portals, and telehealth services. Payers rely on its capabilities to protect claims systems and financial applications from cyberattacks. Its DLP and threat detection tools help maintain compliance with healthcare regulations.

307. Proofpoint Email Protection

Proofpoint Email Protection is a solution that safeguards against phishing, malware, and other email threats. It uses advanced filtering and AI to detect malicious content and prevent it from reaching users.

Hospitals use Proofpoint Email Protection to secure email communications involving sensitive patient information and medical records. Payers rely on it to protect email exchanges with providers and members. Its real-time protection and content filtering ensure that healthcare organizations remain secure from email-based cyber threats.

308. Proofpoint Security Awareness Training

Proofpoint Security Awareness Training offers interactive training modules and phishing simulations to educate employees on cybersecurity risks. It aims to reduce human error and enhance security awareness in organizations.

Hospitals use Proofpoint Security Awareness Training to educate staff on recognizing phishing attempts, safeguarding patient data, and maintaining HIPAA compliance. Payers benefit from its training programs to reduce risks in claims processing workflows. Its engaging modules ensure better retention of cybersecurity best practices across healthcare teams.

309. Pulsara

Pulsara is a communication platform designed for healthcare teams, providing secure messaging and collaboration tools to coordinate patient care. It ensures compliance with healthcare regulations and protects sensitive patient data.

Hospitals use Pulsara to streamline communication between clinical teams, ensuring that patient information is shared securely and efficiently. Payers leverage its secure messaging tools to communicate with healthcare providers about claims and member data. Its HIPAA-compliant platform ensures the confidentiality of healthcare interactions.

310. Qualys

Qualys offers a comprehensive cloud-based security and compliance platform that includes vulnerability management, policy compliance, and web application security. Its solution helps healthcare organizations secure their networks, endpoints, and data.

Hospitals use Qualys to scan EHR systems, medical devices, and networks for vulnerabilities, ensuring compliance with healthcare regulations like HIPAA. Payers rely on its platform to secure claims systems and financial records. Its automated patch management and compliance reporting help streamline security operations in healthcare environments.

311. Qualys Patch Management

Qualys Patch Management automates the patching of vulnerabilities across IT environments, helping organizations keep their systems secure and up-to-date. It ensures that critical security updates are applied in a timely manner.

Hospitals use Qualys Patch Management to apply patches to EHR systems, medical devices, and workstations. Payers rely on it to ensure that claims processing platforms remain secure. Its automation capabilities ensure that healthcare organizations can stay on top of patching requirements without manual intervention.

312. Rapid7

Rapid7 provides a suite of cybersecurity solutions, including vulnerability management, incident detection, and response. Its platform helps healthcare organizations identify and mitigate threats across networks, endpoints, and applications.

Hospitals use Rapid7 to monitor and secure EHR systems, medical devices, and telehealth platforms. Payers benefit from its capabilities to protect claims systems and financial applications. Its centralized platform integrates threat detection, vulnerability management, and incident response to provide comprehensive security for healthcare organizations.

313. Rapid7 InsightConnect

Rapid7 InsightConnect is a security orchestration, automation, and response (SOAR) platform that automates and streamlines incident response workflows. It helps healthcare organizations respond to cyber incidents quickly and efficiently.

Hospitals use InsightConnect to automate incident responses related to EHR systems and medical devices. Payers leverage its capabilities to mitigate risks in claims systems and financial platforms. Its customizable workflows ensure efficient and consistent responses to cybersecurity threats in healthcare environments.

314. Rapid7 InsightIDR

Rapid7 InsightIDR is a security information and event management (SIEM) platform designed to detect and respond to cybersecurity threats. It integrates with other security tools to provide comprehensive visibility across an organization's IT environment.

Hospitals use InsightIDR to monitor activity across EHR systems, medical devices, and clinical applications for potential threats. Payers rely on it to detect and mitigate fraud and cyberattacks targeting claims platforms. Its ability to analyze network traffic and user behavior enhances threat detection and response in healthcare environments.

315. Recorded Future

Recorded Future offers a threat intelligence platform that provides real-time insights into global cyber threats. It uses machine learning and data analytics to predict and mitigate emerging security risks.

Hospitals use Recorded Future to stay ahead of cyber threats targeting EHR systems, telehealth platforms, and medical devices. Payers leverage its threat intelligence to secure claims systems and member data from fraud and cyberattacks. Its real-time insights enhance healthcare organizations' ability to anticipate and respond to evolving threats.

316. Remediant SecureONE

Remediant SecureONE is a privileged access management (PAM) solution that provides secure, least-privilege access to critical systems. It enables healthcare organizations to control who has access to sensitive data and applications.

Hospitals use SecureONE to secure administrative access to EHR systems, medical devices, and network infrastructure. Payers rely on it to protect claims systems and financial platforms. Its real-time monitoring and auditing capabilities ensure compliance with healthcare regulations like HIPAA.

317. RiskRecon (Mastercard)

RiskRecon, now part of Mastercard, provides third-party risk management and vendor assessment solutions. It evaluates the cybersecurity posture of vendors and helps organizations manage risks from their external partners.

Hospitals use RiskRecon to assess the cybersecurity practices of medical device manufacturers, IT vendors, and cloud service providers. Payers rely on it to evaluate the risks associated with third-party claims processors and outsourcing partners. Its continuous monitoring ensures that vendors meet healthcare security standards.

318. RiskWatch

RiskWatch provides a comprehensive risk management platform that helps healthcare organizations assess, manage, and mitigate cybersecurity risks. It offers vulnerability assessments, policy compliance tracking, and continuous risk monitoring.

Hospitals use RiskWatch to assess vulnerabilities in EHR systems, medical devices, and clinical applications. Payers benefit from its tools to monitor risks in claims processing platforms and financial records. Its automated risk assessments help healthcare organizations maintain compliance and improve security.

319. RSA Archer Third-Party Risk Management

RSA Archer Third-Party Risk Management is a platform designed to help organizations assess and manage third-party risks. It provides tools for vendor assessments, risk monitoring, and compliance management.

Hospitals use RSA Archer to evaluate the security posture of vendors supplying medical devices, IT services, and software. Payers rely on it to assess risks from claims processors and outsourcing partners. Its detailed reporting and automated workflows improve third-party risk management and ensure healthcare organizations stay compliant with regulations.

320. RSA NetWitness

RSA NetWitness provides advanced threat detection and monitoring capabilities. It combines network traffic analysis, endpoint monitoring, and security information event management (SIEM) to provide comprehensive visibility into cyber threats.

Hospitals use RSA NetWitness to monitor networks, EHR systems, and medical devices for potential security breaches. Payers benefit from its threat detection capabilities to secure claims systems and member data. Its integration of multiple security technologies provides healthcare organizations with robust, real-time threat detection.

321. RSA SecurID

RSA SecurID offers multi-factor authentication (MFA) and identity and access management (IAM) solutions. It secures user access to critical systems and applications, ensuring only authorized personnel can access sensitive healthcare data.

Hospitals use RSA SecurID to secure access to EHRs, medical devices, and administrative systems. Payers rely on it to protect claims platforms and member data. Its flexible MFA options and integration with existing healthcare systems ensure robust authentication and compliance with healthcare security standards.

322. RSA Zero Trust

RSA Zero Trust implements a security framework that continuously verifies all access requests, regardless of the source. It helps healthcare organizations ensure that only trusted users and devices can access sensitive systems and data.

Hospitals use RSA Zero Trust to secure access to EHRs, medical devices, and telehealth platforms. Payers rely on its ability to mitigate risks associated with third-party access and ensure that claims systems and financial data remain secure. Its continuous monitoring of access requests helps enforce a zero-trust security posture.

323. Rubrik

Rubrik provides cloud data management and ransomware protection solutions. It offers backup, recovery, and archival capabilities that ensure critical healthcare data remains secure and easily recoverable.

Hospitals use Rubrik to protect patient records, imaging data, and EHR systems from ransomware and other cyber threats. Payers benefit from its backup and recovery features to secure claims systems and financial data. Its cloud-native platform ensures that healthcare organizations can recover quickly from cyber incidents.

324. SANS Investigative Forensics Toolkit (SIFT)

SIFT, developed by SANS Institute, is a comprehensive digital forensics toolkit that provides tools for analyzing and investigating cybersecurity incidents. It is widely used in incident response and forensic analysis.

Hospitals use SIFT to analyze cybersecurity incidents affecting EHR systems, medical devices, and clinical applications. Payers rely on it to investigate fraud or unauthorized access to claims systems. Its open-source nature and extensive tools make it a valuable resource for healthcare cybersecurity investigations.

325. SANS Security Awareness

SANS Security Awareness offers comprehensive cybersecurity training programs designed to educate employees on identifying and responding to threats. It includes phishing simulations, security best practices, and compliance training.

Hospitals use SANS Security Awareness to train staff on recognizing phishing attacks, safeguarding patient data, and complying with healthcare regulations like HIPAA. Payers benefit from its educational tools to enhance security awareness among claims processors and customer service representatives. Its interactive training modules ensure better retention of cybersecurity knowledge across healthcare organizations.

326. Saviynt

Saviynt provides identity governance and administration (IGA) solutions that help healthcare organizations manage user access, enforce policies, and ensure compliance. It integrates with existing IT systems to secure sensitive healthcare data.

Hospitals use Saviynt to manage user access to EHR systems, medical devices, and telehealth platforms. Payers rely on its capabilities to ensure that only authorized individuals can access claims systems and member data. Its robust policy enforcement tools help healthcare organizations stay compliant with regulations like HIPAA and GDPR.

327. Saviynt Privileged Access Management

Saviynt Privileged Access Management (PAM) helps organizations secure and manage privileged accounts that have access to sensitive systems and data. It provides real-time monitoring, session recording, and access controls.

Hospitals use Saviynt PAM to secure access to critical EHR systems, medical devices, and hospital networks. Payers rely on its capabilities to protect privileged access to claims systems and financial records. Its detailed auditing features support compliance with regulatory requirements and improve overall security.

328. Scalefusion MDM

Scalefusion is a mobile device management (MDM) solution designed to secure and manage healthcare devices, including smartphones, tablets, and IoT devices. It provides features like remote device management, security policy enforcement, and app management.

Hospitals use Scalefusion MDM to secure mobile devices used by clinicians for accessing EHRs and patient data. Payers rely on it to manage devices accessing member data and financial platforms. Its user-friendly platform ensures healthcare organizations can easily enforce security policies across mobile and IoT devices.

329. SecureAuth

SecureAuth offers identity and access management (IAM) solutions that provide multi-factor authentication (MFA), single sign-on (SSO), and adaptive authentication. It helps healthcare organizations secure access to critical systems and data.

Hospitals use SecureAuth to manage user access to EHR systems, telehealth platforms, and medical devices. Payers rely on its IAM capabilities to protect claims systems and member data. Its adaptive authentication features ensure that access requests are continuously verified, improving security across healthcare environments.

330. SecureAuth MFA

SecureAuth MFA is a multi-factor authentication solution that provides an additional layer of security for healthcare systems. It supports various authentication methods, including biometrics, push notifications, and one-time passwords (OTPs).

Hospitals use SecureAuth MFA to secure access to patient records, medical devices, and clinical applications. Payers rely on its capabilities to protect claims systems and financial platforms from unauthorized access. Its flexibility and user-friendly design make it an ideal solution for securing healthcare IT environments.

331. SecureTrust DLP

SecureTrust Data Loss Prevention (DLP) provides tools to prevent the unauthorized sharing or leakage of sensitive healthcare data. It helps organizations monitor data transfers and ensure compliance with privacy regulations.

Hospitals use SecureTrust DLP to prevent accidental or intentional sharing of patient records, medical data, and clinical communications. Payers rely on it to secure claims data and financial records. Its detailed reporting and monitoring capabilities help healthcare organizations comply with HIPAA and other regulatory standards.

332. SecureWorks Taegis

SecureWorks Taegis is a cloud-native security platform that provides threat detection, incident response, and security monitoring. It uses machine learning and analytics to detect and respond to advanced cyber threats.

Hospitals use SecureWorks Taegis to monitor EHR systems, medical devices, and telehealth platforms for potential security breaches. Payers leverage its threat detection capabilities to protect claims platforms and member data. Its cloud-native architecture ensures scalability and flexibility for large healthcare organizations.

333. Sectigo IoT Manager

Sectigo IoT Manager provides secure management and monitoring of connected devices in healthcare environments. It offers features like device authentication, certificate management, and encryption to protect IoT devices from cyber threats.

Hospitals use Sectigo IoT Manager to secure connected medical devices, including infusion pumps, patient monitors, and diagnostic tools. Payers rely on its capabilities to ensure that claims systems and member devices remain secure. Its end-to-end device management features ensure compliance with healthcare cybersecurity regulations.

334. Security Mentor

Security Mentor offers cybersecurity awareness training that helps employees identify and mitigate risks. It provides interactive training programs that focus on phishing, social engineering, and other common attack vectors.

Hospitals use Security Mentor to train staff on safeguarding patient data, recognizing phishing attempts, and adhering to cybersecurity best practices. Payers benefit from its training tools to improve security awareness within claims processing teams. Its engaging training modules ensure better retention and awareness across healthcare organizations.



335. SecurityScorecard

SecurityScorecard provides a platform for assessing and monitoring the cybersecurity posture of vendors and third-party partners. It helps healthcare organizations manage third-party risks and ensure vendor compliance with security standards.

Hospitals use SecurityScorecard to assess the cybersecurity practices of vendors providing IT services, medical devices, and cloud platforms. Payers rely on it to monitor the security posture of third-party claims processors and service providers. Its continuous monitoring ensures that vendors meet healthcare security and compliance requirements.

336. Senrio Insight

Senrio Insight provides IoT and medical device security solutions, offering real-time monitoring, threat detection, and vulnerability management. Its platform helps healthcare organizations secure connected medical devices and operational technology (OT).

Hospitals use Senrio Insight to monitor and protect IoT devices like infusion pumps, patient monitors, and imaging systems from cyber threats. Payers rely on it to ensure that IoT systems involved in claims processing and healthcare administration remain secure. Its proactive threat detection helps prevent attacks on critical healthcare infrastructure.

337. SentinelOne

SentinelOne provides endpoint security solutions that deliver real-time protection against malware, ransomware, and advanced persistent threats. It uses machine learning and AI to detect and mitigate threats at the endpoint level.

Hospitals use SentinelOne to secure clinician devices, medical equipment, and administrative systems from cyberattacks. Payers rely on it to protect claims processing systems and financial applications from malware and ransomware. Its autonomous response capabilities ensure quick action against emerging threats in healthcare environments.

338. SentinelOne Singularity

SentinelOne Singularity is an advanced endpoint protection platform that integrates endpoint detection and response (EDR) with extended detection and response (XDR). It offers real-time threat hunting and automated remediation.

Hospitals use Singularity to monitor and protect EHR systems, medical devices, and clinical applications from cyber threats. Payers benefit from its advanced detection and response capabilities to secure claims systems and financial data. Its AI-driven threat detection and automated remediation improve security efficiency in healthcare organizations.

339. SentinelOne Vigilance Respond

SentinelOne Vigilance Respond is a managed detection and response (MDR) service that provides 24/7 threat monitoring, analysis, and incident response. It helps healthcare organizations detect and respond to cybersecurity incidents in real time.

Hospitals use Vigilance Respond to monitor EHR systems, medical devices, and telehealth platforms for cyber threats. Payers rely on it to secure claims processing systems and member data. Its expert-led incident response and threat detection capabilities ensure healthcare organizations can quickly respond to security breaches.

340. SentinelOne Vigilance

SentinelOne Vigilance offers a managed security service that provides real-time monitoring, threat intelligence, and incident response. It is designed to detect and mitigate threats across endpoints, networks, and cloud environments.

Hospitals use Vigilance to secure clinical systems, EHRs, and medical devices from cyber threats. Payers benefit from its capabilities to protect claims platforms and financial data from cyberattacks. Its managed services provide healthcare organizations with continuous protection and expert guidance on cybersecurity best practices.

341. Shared Assessments Third-Party Risk Tools

Shared Assessments provides a suite of third-party risk management tools that help organizations assess, monitor, and mitigate risks posed by vendors and external partners. It includes questionnaires, assessments, and continuous monitoring features.

Hospitals use Shared Assessments tools to evaluate the cybersecurity practices of third-party vendors, including medical device suppliers, IT service providers, and software vendors. Payers rely on it to monitor the risks associated with claims processors and outsourced service providers. Its robust vendor risk assessments ensure that third-party partners meet healthcare security and compliance standards.

342. Signal Secure Messaging

Signal is a secure messaging platform that uses end-to-end encryption to protect communications. It is widely used in healthcare for secure, private communication between healthcare teams, patients, and members.

Hospitals use Signal to securely exchange patient data and clinical updates between clinicians and care teams. Payers rely on it for secure communication with providers and members regarding claims and benefits. Its encryption ensures that all healthcare-related interactions remain private and comply with data protection regulations.

343. SimplePractice Telehealth

SimplePractice provides a comprehensive telehealth platform designed for healthcare providers. It offers secure video consultations, online scheduling, and electronic health record (EHR) integration.

Hospitals use SimplePractice Telehealth to expand access to healthcare services through virtual care. Payers benefit from its ability to reduce healthcare costs by facilitating virtual consultations. Its HIPAA-compliant features ensure secure and confidential virtual interactions for both patients and providers.

344. Siemplify (Google Chronicle)

Siemplify, now part of Google Chronicle, offers a security orchestration, automation, and response (SOAR) platform that helps organizations automate incident response and integrate threat intelligence.

Hospitals use Siemplify to streamline incident management processes related to EHR systems, medical devices, and clinical applications. Payers leverage its capabilities to automate responses to fraud or cybersecurity incidents targeting claims systems. Its integration with other security tools enhances overall security operations in healthcare.

345. Skybox Security

Skybox Security provides comprehensive vulnerability management and network security solutions, helping healthcare organizations detect, prioritize, and remediate vulnerabilities across their IT environments.

Hospitals use Skybox to secure EHR systems, medical devices, and clinical networks by identifying and addressing vulnerabilities before they can be exploited. Payers rely on its capabilities to secure claims platforms and member-facing applications. Its robust reporting and analytics tools help healthcare organizations comply with regulations and improve overall security.

346. SolarWinds Access Rights Manager

SolarWinds Access Rights Manager is a user access management solution that helps organizations control and monitor user access to sensitive data and applications. It provides tools for auditing and enforcing access policies.

Hospitals use SolarWinds Access Rights Manager to secure access to EHR systems, medical devices, and clinical applications. Payers rely on it to control access to claims platforms and financial systems. Its auditing features support compliance with healthcare regulations like HIPAA, ensuring that only authorized personnel have access to sensitive healthcare data.

347. SolarWinds Mail Assure

SolarWinds Mail Assure is a secure email platform that provides protection against email-based threats, including phishing, spam, and malware. It ensures that sensitive healthcare communications remain secure and compliant with data privacy regulations.

Hospitals use Mail Assure to protect email communications involving patient data, clinical information, and administrative records. Payers rely on it to secure email exchanges with providers and members regarding claims and benefits. Its spam filtering and phishing protection capabilities help prevent email-based cyberattacks in healthcare environments.

348. SolarWinds Network Vulnerability Detection

SolarWinds Network Vulnerability Detection provides real-time scanning and monitoring of network infrastructure to identify vulnerabilities and potential threats. It helps healthcare organizations ensure the security of their networks and connected devices.

Hospitals use SolarWinds Network Vulnerability Detection to monitor medical device networks, EHR systems, and clinical applications for vulnerabilities. Payers leverage it to secure claims systems and financial networks. Its continuous monitoring capabilities ensure that healthcare networks are proactively protected against emerging threats.

349. SolarWinds Patch Manager

SolarWinds Patch Manager automates the patching process across IT systems, ensuring that critical security updates are applied in a timely manner. It helps healthcare organizations reduce the risk of vulnerabilities and cyberattacks.

Hospitals use Patch Manager to apply security patches to EHR systems, medical devices, and clinical infrastructure. Payers rely on it to ensure that claims systems and financial platforms remain up-to-date and secure. Its automation features ensure that patch management is streamlined and compliant with healthcare regulations.

350. SolarWinds Security Event Manager

SolarWinds Security Event Manager (SEM) is a security information and event management (SIEM) platform that provides real-time monitoring and threat detection. It helps healthcare organizations identify and respond to security incidents.

Hospitals use SEM to monitor EHR systems, medical devices, and hospital networks for suspicious activities. Payers rely on it to detect threats targeting claims systems and member data. Its centralized logging and real-time monitoring capabilities ensure that healthcare organizations can quickly respond to security incidents.

351. Sophos

Sophos provides a comprehensive suite of cybersecurity solutions, including endpoint protection, firewall management, and encryption. Its platform protects healthcare organizations from cyber threats like malware, ransomware, and phishing attacks.

Hospitals use Sophos to secure endpoints such as clinician devices, medical equipment, and workstations. Payers rely on it to protect claims systems and financial platforms. Its integrated security solutions, including encryption and DLP, ensure that sensitive healthcare data remains secure across all platforms.

352. Sophos Cloud Optix

Sophos Cloud Optix is a cloud security platform designed to monitor and protect cloud environments. It provides real-time threat detection, compliance monitoring, and automated remediation for cloud-based healthcare systems.

Hospitals use Sophos Cloud Optix to secure cloud-hosted EHRs, telehealth platforms, and patient data. Payers rely on its capabilities to protect cloud-based claims systems and member portals. Its continuous monitoring ensures that cloud environments are secure and compliant with healthcare regulations.

353. Sophos Email Protection

Sophos Email Protection provides advanced security for email systems, including protection against phishing, malware, and spam. It helps healthcare organizations secure email communications and reduce the risk of data breaches.

Hospitals use Sophos Email Protection to secure email communications involving patient data, medical records, and clinical updates. Payers rely on it to protect claims-related email exchanges from cyberattacks. Its AI-driven threat detection capabilities ensure that email security is robust and compliant with healthcare regulations.

354. Sophos Encryption

Sophos Encryption provides strong encryption solutions for protecting sensitive healthcare data at rest and in transit. It ensures that patient records, medical data, and financial transactions remain secure and compliant with regulations like HIPAA.

Hospitals use Sophos Encryption to secure patient data, EHRs, and medical device configurations. Payers rely on it to protect claims data and financial records. Its easy-to-deploy encryption capabilities ensure that sensitive healthcare information remains protected from unauthorized access.

355. Sophos Firewall

Sophos Firewall offers advanced protection for healthcare organizations by securing networks against cyber threats. It provides features such as intrusion prevention, VPN support, and advanced threat detection.

Hospitals use Sophos Firewall to protect hospital networks, medical devices, and EHR systems from cyber threats. Payers rely on it to secure claims platforms and member-facing applications. Its real-time threat detection capabilities help ensure that healthcare organizations remain protected from evolving cyberattacks.

356. Sophos Intercept X

Sophos Intercept X is an advanced endpoint protection solution that combines deep learning, anti-ransomware capabilities, and behavioral analytics to detect and stop cyber threats. It provides healthcare organizations with comprehensive protection against malware and ransomware.

Hospitals use Intercept X to secure endpoints such as workstations, laptops, and medical devices from cyberattacks. Payers rely on it to protect claims systems and financial applications from malware, ransomware, and other advanced threats. Its proactive defense features enhance overall security across healthcare environments.

357. Sophos Mobile Security

Sophos Mobile Security provides mobile device management (MDM) and mobile threat defense (MTD) capabilities. It helps healthcare organizations secure mobile devices used by clinicians and administrative staff to access sensitive patient data.

Hospitals use Sophos Mobile Security to protect smartphones, tablets, and medical devices from malware and unauthorized access. Payers leverage its MDM features to secure mobile access to claims systems and member data. Its comprehensive protection ensures that mobile devices used in healthcare environments remain secure and compliant with privacy regulations.

358. Sophos Worry-Free

Sophos Worry-Free is an endpoint protection solution designed for small and medium-sized healthcare organizations. It offers advanced security features, including anti-malware, web filtering, and email protection, to safeguard healthcare data and systems.

Hospitals use Sophos Worry-Free to secure workstations, medical devices, and clinical systems from cyber threats. Payers rely on it to protect claims processing systems and member-facing platforms. Its easy-to-manage features and cloud-based capabilities provide strong security for smaller healthcare organizations with limited IT resources.

359. SophosLabs

SophosLabs is a threat intelligence and research division that provides cybersecurity insights and data to help organizations defend against emerging threats. It analyzes malware, ransomware, and attack techniques to deliver actionable threat intelligence.

Hospitals use SophosLabs' threat intelligence to stay ahead of cyberattacks targeting EHR systems, medical devices, and clinical infrastructure. Payers rely on it to detect and mitigate threats to claims systems and member data. Its continuous research into cybersecurity trends helps healthcare organizations prepare for evolving risks.

360. SophosLabs Behavioral Analytics

SophosLabs Behavioral Analytics leverages machine learning and AI to detect anomalous behavior across healthcare networks, applications, and endpoints. It provides healthcare organizations with the tools to identify potential insider threats and data breaches.

Hospitals use SophosLabs Behavioral Analytics to detect abnormal access patterns to EHRs, medical devices, and administrative systems. Payers rely on it to identify suspicious activities in claims processing systems and member portals. Its real-time threat detection helps prevent data breaches and insider threats in healthcare environments.

361. Solve.Care

Solve.Care offers a blockchain-based healthcare management platform that helps coordinate and automate care delivery. It provides secure data exchanges, appointment scheduling, and payment management, improving healthcare operations and reducing administrative overhead.

Hospitals use Solve.Care to automate patient care workflows, ensuring that data sharing between clinicians and departments remains secure. Payers benefit from its platform to streamline care coordination and claims processing. Its blockchain-based technology ensures data integrity and compliance with healthcare security standards.

362. SonicWall

SonicWall provides advanced network security solutions, including firewalls, VPNs, and secure SD-WAN capabilities. Its platform is designed to protect healthcare networks, remote workers, and connected devices from cyber threats.

Hospitals use SonicWall to protect hospital networks, medical devices, and EHR systems from cyberattacks. Payers rely on it to secure claims systems and member portals from unauthorized access. Its scalable and flexible network security solutions are ideal for healthcare organizations of all sizes.

363. Sophos Endpoint Security Mobile

Sophos Endpoint Security Mobile provides mobile threat defense and MDM features that secure smartphones and tablets used by healthcare professionals. It protects against mobile malware, unauthorized access, and data breaches.

Hospitals use Sophos Endpoint Security Mobile to secure clinician devices and medical equipment that access EHRs and patient data. Payers rely on it to protect mobile access to claims systems and financial data. Its comprehensive mobile security features ensure that sensitive healthcare information is protected across mobile platforms.

364. Sophos TippingPoint

Sophos TippingPoint is an intrusion prevention system (IPS) that provides network security and threat prevention for healthcare organizations. It helps detect and block cyberattacks targeting critical infrastructure, including EHR systems and medical devices.

Hospitals use TippingPoint to protect their networks from malicious traffic and cyberattacks targeting patient data and clinical systems. Payers rely on it to secure claims platforms and ensure the integrity of financial data. Its real-time detection and threat blocking capabilities help mitigate risks across healthcare networks.

365. Sophos Vision One

Sophos Vision One is an integrated cybersecurity platform that combines endpoint, network, and cloud security to provide comprehensive threat detection and response. It uses AI to identify, block, and remediate threats across the healthcare ecosystem.

Hospitals use Sophos Vision One to secure EHR systems, medical devices, and administrative networks from cyber threats. Payers benefit from its AI-driven capabilities to protect claims systems and member-facing applications. Its unified approach to security ensures comprehensive protection for healthcare organizations.

366. Sophos Behavioral Analytics

Sophos Behavioral Analytics uses machine learning and AI to analyze user and entity behavior across endpoints, networks, and cloud environments. It helps detect anomalies and insider threats by tracking deviations from normal activity patterns.

Hospitals use Sophos Behavioral Analytics to monitor access to EHRs, medical devices, and sensitive patient data, identifying potential insider threats or unauthorized access. Payers rely on it to detect fraudulent activities or security breaches within claims systems. Its behavioral insights help healthcare organizations identify risks before they escalate into serious incidents.

367. Spok

Spok provides secure messaging solutions for healthcare organizations, allowing clinicians to communicate securely in real-time. Its platform includes features like encrypted messaging, alerts, and collaboration tools for improved patient care coordination.

Hospitals use Spok to securely communicate between care teams, ensuring that sensitive patient data is exchanged in compliance with healthcare regulations like HIPAA. Payers benefit from its secure messaging capabilities to communicate with providers regarding claims and member data. Its user-friendly interface ensures smooth communication in fast-paced healthcare environments.

368. Splunk

Splunk is a security information and event management (SIEM) platform that provides real-time monitoring, threat detection, and security analytics. It helps healthcare organizations gain visibility into their entire IT infrastructure to detect cyber threats.

Hospitals use Splunk to monitor EHR systems, medical devices, and hospital networks for suspicious activities. Payers rely on it to detect threats targeting claims platforms and financial systems. Its advanced analytics and dashboards enable healthcare organizations to quickly respond to security incidents and improve their overall security posture.

369. Splunk Phantom

Splunk Phantom is a security orchestration, automation, and response (SOAR) platform that helps organizations automate and streamline their security operations. It integrates with existing security tools to improve incident response and threat management.

Hospitals use Splunk Phantom to automate incident response workflows related to EHR systems and medical devices. Payers rely on it to streamline the response to fraud or cyberattacks targeting claims systems. Its automation capabilities ensure quick and efficient remediation of security incidents in healthcare environments.

370. Splunk Behavioral Analytics

Splunk Behavioral Analytics integrates with Splunk's SIEM platform to provide advanced analytics for detecting anomalous behavior and insider threats. It uses machine learning to identify patterns in user activity across networks and systems.

Hospitals use Splunk Behavioral Analytics to monitor clinician access to sensitive systems like EHRs and medical devices, detecting potential insider threats or unauthorized activity. Payers rely on it to identify fraud or irregular access attempts in claims systems. Its deep behavioral insights improve threat detection and help prevent data breaches in healthcare environments.

371. Spirion

Spirion provides data discovery and data loss prevention (DLP) solutions that help organizations protect sensitive data from unauthorized access or leakage. It ensures that sensitive patient information remains secure across healthcare systems.

Hospitals use Spirion to discover and classify sensitive patient data across their IT infrastructure, ensuring compliance with regulations like HIPAA. Payers rely on it to protect claims data and financial records. Its real-time data protection capabilities prevent unauthorized sharing or transfer of healthcare data.

372. SOTI MobiControl

SOTI MobiControl is a mobile device management (MDM) solution that helps organizations secure and manage mobile devices in healthcare environments. It provides capabilities for remote monitoring, security policy enforcement, and application management.

Hospitals use SOTI MobiControl to secure clinician devices, mobile workstations, and medical equipment accessing patient data. Payers rely on it to secure mobile access to claims systems and financial data. Its robust security features ensure that healthcare devices remain compliant with privacy regulations.

373. Swimlane

Swimlane is a security orchestration, automation, and response (SOAR) platform that helps organizations automate and manage their security operations. It streamlines incident response processes and integrates with a wide range of security tools.

Hospitals use Swimlane to automate incident responses related to EHR systems, medical devices, and telehealth platforms. Payers leverage its capabilities to streamline the response to threats targeting claims systems and member data. Its automation capabilities improve the efficiency and speed of incident resolution in healthcare environments.

374. Sumo Logic

Sumo Logic provides cloud-native security information and event management (SIEM) solutions that enable real-time threat detection, log management, and security analytics. It helps healthcare organizations identify and respond to cybersecurity incidents.

Hospitals use Sumo Logic to monitor EHR systems, medical devices, and hospital networks for potential security threats. Payers rely on it to detect threats targeting claims platforms and financial data. Its cloud-native platform ensures scalability and flexibility, making it ideal for large healthcare organizations.

375. Sumo Logic SOAR

Sumo Logic SOAR is a security orchestration, automation, and response platform that enables healthcare organizations to automate security processes and streamline incident response. It integrates with existing security tools to enhance overall cybersecurity operations.

Hospitals use Sumo Logic SOAR to automate incident responses related to critical systems like EHRs and medical devices. Payers rely on it to mitigate risks in claims systems and member data. Its automation capabilities help healthcare organizations respond quickly and effectively to security threats.

376. Sumo Logic Behavioral Analytics

Sumo Logic Behavioral Analytics leverages machine learning to detect anomalies in user and entity behavior. It provides healthcare organizations with insights into potential insider threats, account compromises, and other suspicious activities.

Hospitals use Sumo Logic Behavioral Analytics to monitor clinician access to EHR systems and medical devices, detecting abnormal behavior that could indicate security breaches. Payers rely on it to identify fraudulent claims or unauthorized access to sensitive member data. Its advanced behavioral analytics help improve security visibility and threat detection in healthcare environments.

377. Symphony Communication Services

Symphony Communication Services offers a secure collaboration platform for healthcare organizations. It includes features like encrypted messaging, voice, video, and file sharing to ensure secure communications among healthcare teams and with external partners.

Hospitals use Symphony for secure communication between clinical teams, ensuring that patient data remains private and compliant with HIPAA. Payers rely on it to communicate securely with healthcare providers regarding claims and member data. Its end-to-end encryption ensures the confidentiality and integrity of healthcare communications.

378. Symantec (Broadcom)

Symantec, now part of Broadcom, provides cybersecurity solutions that include endpoint protection, email security, cloud security, and threat intelligence. Its platform is designed to protect healthcare organizations from a wide range of cyber threats.

Hospitals use Symantec to secure EHR systems, medical devices, and hospital networks from malware, ransomware, and phishing attacks. Payers rely on it to protect claims systems and member-facing platforms. Its threat intelligence capabilities help healthcare organizations stay ahead of evolving threats, ensuring comprehensive protection for sensitive healthcare data.

379. Symantec Email Security

Symantec Email Security provides advanced protection against email-based threats, such as phishing, malware, and spam. It helps healthcare organizations secure their email communications, ensuring that sensitive patient data remains private.

Hospitals use Symantec Email Security to protect email exchanges involving patient information, clinical updates, and administrative details. Payers rely on it to secure communication with providers and members regarding claims. Its AI-driven email filtering helps prevent email-based attacks, ensuring compliance with HIPAA and other privacy regulations.

380. Symantec Encryption

Symantec Encryption provides data encryption solutions for securing sensitive information at rest, in transit, and in use. It ensures that healthcare data remains protected from unauthorized access, meeting regulatory compliance requirements.

Hospitals use Symantec Encryption to secure patient records, medical images, and other critical healthcare data. Payers rely on it to protect claims data and financial transactions. Its seamless integration with existing IT infrastructures ensures that sensitive healthcare information remains secure across all platforms and devices.

381. Symantec IoT Security

Symantec IoT Security provides advanced protection for connected devices in healthcare environments, such as infusion pumps, patient monitors, and imaging systems. It helps prevent cyberattacks targeting healthcare IoT devices and networks.

Hospitals use Symantec IoT Security to monitor and secure medical devices, ensuring they remain free from malware and unauthorized access. Payers benefit from its capabilities to protect IoT devices involved in claims processing and healthcare administration. Its real-time threat detection helps mitigate risks in healthcare IoT environments.

382. Symantec Managed Security Services

Symantec Managed Security Services offers a comprehensive suite of security operations, including monitoring, threat detection, incident response, and vulnerability management. It helps healthcare organizations strengthen their security posture and respond effectively to cyber threats.

Hospitals use Symantec Managed Security Services to secure EHR systems, medical devices, and clinical applications from evolving cyber threats. Payers rely on it for comprehensive protection of claims systems and member data. Its 24/7 monitoring and expert response services ensure that healthcare organizations can address incidents quickly and effectively.

383. Symantec VIP Access

Symantec VIP Access provides multi-factor authentication (MFA) to secure access to sensitive healthcare data and systems. It includes token-based authentication and support for biometric methods to ensure that only authorized users can access patient data.

Hospitals use VIP Access to protect access to EHR systems, medical devices, and administrative tools. Payers rely on it to secure claims systems and member portals. Its flexible MFA options provide enhanced security while ensuring seamless access for authorized users across healthcare organizations.

384. Symantec Zero Trust

Symantec Zero Trust implements a security model where trust is never assumed, and all access requests are continuously verified. It ensures that only authorized users and devices can access sensitive healthcare data and applications.

Hospitals use Symantec Zero Trust to secure access to EHRs, medical devices, and telehealth platforms, ensuring that every access request is validated. Payers benefit from its ability to secure claims systems and financial data by enforcing strict access controls. Its real-time verification capabilities ensure compliance with the zero-trust security model.

385. Symantec Endpoint Protection

Symantec Endpoint Protection provides advanced threat defense for endpoints, including malware protection, firewall controls, and device management. It helps healthcare organizations protect their devices from cyber threats like ransomware and viruses.

Hospitals use Symantec Endpoint Protection to secure clinician workstations, laptops, and medical devices from cyber threats. Payers rely on it to protect claims systems and internal financial applications. Its centralized management and advanced threat detection capabilities improve overall security and reduce the risk of endpoint attacks.

386. Symantec Endpoint Management

Symantec Endpoint Management provides comprehensive tools for managing and securing endpoints across an organization. It includes features like device management, software deployment, and patching to ensure that endpoints remain secure and compliant.

Hospitals use Symantec Endpoint Management to manage and secure clinician devices, medical workstations, and mobile devices that access sensitive patient data. Payers benefit from its patch management and software deployment capabilities to keep claims processing systems secure. Its centralized management ensures healthcare organizations remain compliant with data privacy regulations like HIPAA.

387. Tanium

Tanium provides endpoint management and security solutions that enable organizations to manage, secure, and monitor all endpoints in real time. It offers capabilities such as patch management, vulnerability scanning, and incident response.

Hospitals use Tanium to monitor medical devices, EHR systems, and clinical workstations for vulnerabilities and threats. Payers rely on it to secure claims systems and financial data, ensuring that endpoints are continuously protected. Its real-time visibility into endpoint status allows healthcare organizations to respond rapidly to security threats.

388. Teladoc Health

Teladoc Health provides telehealth solutions that enable remote consultations, virtual care, and healthcare delivery through video, phone, and messaging. It allows healthcare organizations to expand access to care and improve patient outcomes.

Hospitals use Teladoc to offer virtual consultations, reducing in-person visits and improving access to care. Payers benefit from its telehealth platform to reduce healthcare costs by supporting remote care for patients with chronic conditions. Its secure, HIPAA-compliant platform ensures that patient data remains protected during virtual care interactions.

389. Telmediq (by PerfectServe)

Telmediq provides a secure communication platform for healthcare organizations, including encrypted messaging, alerts, and collaboration tools. It helps ensure that healthcare professionals can communicate quickly and securely, improving care coordination.

Hospitals use Telmediq to securely communicate with clinicians, ensuring that sensitive patient information is shared in compliance with HIPAA. Payers leverage its secure messaging capabilities to coordinate with healthcare providers on claims and patient care. Its real-time communication features improve operational efficiency and enhance patient outcomes.

390. Tenable

Tenable offers a vulnerability management platform that helps organizations identify, assess, and remediate security vulnerabilities across their IT infrastructure. It provides insights into risk exposure and helps prioritize remediation efforts.

Hospitals use Tenable to scan and assess vulnerabilities in EHR systems, medical devices, and clinical applications. Payers rely on its capabilities to identify risks in claims systems and financial platforms. Its risk-based approach ensures that healthcare organizations can prioritize their patching and remediation efforts based on the severity of vulnerabilities.

391. Terranova Security

Terranova Security provides cybersecurity awareness training and phishing simulation solutions to help organizations educate employees on recognizing and responding to cyber threats. It aims to reduce the risk of human error in security incidents.

Hospitals use Terranova Security to train staff on phishing threats, social engineering attacks, and data protection practices. Payers benefit from its training modules to reduce the risk of security breaches within claims processing workflows. Its engaging simulations and easy-to-deploy training programs improve security awareness across healthcare organizations.

392. Thales Group

Thales Group offers data protection, encryption, and identity management solutions designed to secure sensitive information and ensure compliance with industry regulations. Its platform helps healthcare organizations safeguard patient data across various systems and platforms.

Hospitals use Thales Group's solutions to encrypt patient records, EHRs, and medical device configurations to ensure confidentiality. Payers rely on its encryption capabilities to protect claims data and financial records. Its extensive security portfolio helps healthcare organizations comply with data privacy regulations like HIPAA and GDPR.

393. Thales IoT Solutions

Thales IoT Solutions provide comprehensive security for IoT devices, including encryption, authentication, and lifecycle management. It helps protect connected healthcare devices from cyber threats and ensures secure communication between devices.

Hospitals use Thales IoT Solutions to secure connected medical devices such as infusion pumps, patient monitors, and diagnostic tools. Payers rely on its IoT security features to protect IoT systems involved in claims processing and patient care. Its end-to-end security ensures that healthcare IoT devices remain secure throughout their lifecycle.

394. Thales SafeNet MFA

Thales SafeNet MFA offers multi-factor authentication (MFA) to ensure secure access to sensitive healthcare systems and data. It supports various authentication methods such as biometrics, smart cards, and OTPs.

Hospitals use Thales SafeNet MFA to secure access to EHRs, medical devices, and clinical applications. Payers benefit from its MFA capabilities to protect claims systems and member data. Its flexible authentication options help healthcare organizations meet compliance requirements while ensuring that only authorized personnel can access sensitive information.

395. ThreatConnect

ThreatConnect provides a threat intelligence platform that helps organizations collect, analyze, and respond to cyber threats. It offers real-time intelligence sharing, threat hunting, and automated threat response to enhance cybersecurity operations.

Hospitals use ThreatConnect to stay ahead of cyber threats targeting EHR systems, medical devices, and clinical applications. Payers rely on it to secure claims systems and financial platforms. Its integration with other security tools helps healthcare organizations enhance their threat detection and incident response capabilities.

396. ThreatQuotient

ThreatQuotient is a threat intelligence platform that helps organizations collect, analyze, and operationalize threat data. It enables security teams to prioritize threats and integrate intelligence into their cybersecurity workflows.

Hospitals use ThreatQuotient to enhance their security operations by integrating threat intelligence into their EHR systems, medical devices, and clinical applications. Payers rely on its platform to detect and mitigate threats targeting claims systems and financial data. Its real-time intelligence sharing improves overall cybersecurity posture in healthcare environments.

397. ThreatSim

ThreatSim provides phishing simulation and training solutions to help organizations educate their employees about cyber threats. It enables healthcare organizations to test their staff's ability to recognize and respond to phishing attacks.



Hospitals use ThreatSim to simulate phishing attacks targeting staff, helping them identify potential vulnerabilities in EHR systems, medical devices, and clinical applications. Payers rely on it to educate employees involved in claims processing and customer service to prevent phishing attacks. Its simulation-based approach to training reduces the risk of human error in healthcare organizations.

398. TigerConnect

TigerConnect is a secure messaging and collaboration platform designed for healthcare teams. It allows clinicians and staff to communicate in real time while ensuring compliance with privacy regulations such as HIPAA.

Hospitals use TigerConnect to securely communicate between care teams, improving patient care coordination and data sharing. Payers rely on it to securely communicate with providers regarding claims and member data. Its HIPAA-compliant platform ensures that sensitive healthcare information is protected during communication.

399. TitanHQ SpamTitan

TitanHQ SpamTitan is a secure email gateway solution that protects organizations from spam, phishing, malware, and other email-based threats. It ensures that sensitive healthcare communications remain secure and compliant with regulations like HIPAA.

Hospitals use SpamTitan to filter malicious emails and prevent spam and phishing attacks targeting patient data, medical records, and clinical communications. Payers rely on it to secure email exchanges regarding claims and financial information. Its real-time threat filtering ensures that healthcare organizations' email systems remain secure.

400. Tripwire IP360

Tripwire IP360 is a vulnerability management platform that helps organizations identify, prioritize, and remediate security vulnerabilities across their IT infrastructure. It offers automated scanning and reporting tools to improve security and compliance.

Hospitals use Tripwire IP360 to scan EHR systems, medical devices, and clinical networks for vulnerabilities, ensuring that they are protected against cyber threats. Payers benefit from its capabilities to secure claims systems and financial platforms. Its comprehensive vulnerability assessments help healthcare organizations prioritize remediation efforts and maintain compliance with healthcare regulations.

401. TrustArc Vendor Management

TrustArc provides a privacy management platform that helps organizations assess, manage, and monitor third-party risks. It helps healthcare organizations ensure that their vendors and partners comply with privacy regulations such as HIPAA and GDPR.

Hospitals use TrustArc to evaluate the cybersecurity practices of third-party vendors, including medical device suppliers, IT service providers, and cloud platforms. Payers rely on it to assess risks associated with third-party claims processors and service providers. Its continuous monitoring helps ensure that healthcare organizations' third-party vendors meet data protection and compliance requirements.

402. Trustwave

Trustwave offers a wide range of cybersecurity solutions, including managed security services, compliance management, and threat detection. It helps healthcare organizations protect their IT environments from cyber threats and maintain regulatory compliance.

Hospitals use Trustwave to secure EHR systems, medical devices, and hospital networks from cyberattacks. Payers rely on its solutions to protect claims platforms and financial systems. Its managed services and threat detection capabilities help healthcare organizations detect and respond to threats quickly and efficiently.

403. Untangle (Arista)

Untangle, part of Arista Networks, provides network security solutions that include firewalls, VPNs, and advanced threat protection. It helps healthcare organizations secure their networks, protect patient data, and prevent cyberattacks.

Hospitals use Untangle to secure hospital networks, medical devices, and clinical systems from cyber threats. Payers rely on it to protect claims systems and member-facing applications. Its advanced network security features ensure that healthcare organizations can prevent unauthorized access and data breaches.

404. UpGuard

UpGuard provides third-party risk management and cybersecurity assessment tools. It helps organizations assess, monitor, and mitigate risks associated with vendors and service providers to reduce the threat of supply chain attacks.

Hospitals use UpGuard to evaluate and manage the cybersecurity risks of medical device manufacturers, IT service providers, and cloud platforms. Payers rely on it to assess risks from third-party claims processors and outsourced service providers. Its continuous monitoring helps ensure that vendors meet healthcare cybersecurity standards.

405. Vade Secure

Vade Secure provides email security solutions designed to protect organizations from phishing, spear-phishing, malware, and other email-based threats. It uses machine learning to detect and block malicious emails in real time.

Hospitals use Vade Secure to protect email communications involving patient data, clinical information, and administrative records. Payers rely on it to secure claims-related email exchanges and communication with members. Its machine learning algorithms ensure that email security is robust and effective in preventing email-based attacks.

406. Varonis

Varonis provides a data security and analytics platform that helps organizations monitor and protect sensitive data, track user activity, and detect insider threats. It uses advanced analytics to detect abnormal behaviors and protect data from unauthorized access.

Hospitals use Varonis to monitor access to EHR systems, medical devices, and patient data, detecting any suspicious activity that could indicate an insider threat or data breach. Payers benefit from its capabilities to monitor claims systems and financial records for unauthorized access. Its real-time alerts and analytics help improve data protection and ensure compliance with healthcare regulations.

407. VeraCrypt

VeraCrypt is an open-source disk encryption software that provides strong encryption for data stored on endpoints and servers. It helps healthcare organizations protect sensitive patient data and clinical records from unauthorized access.

Hospitals use VeraCrypt to encrypt EHR systems, medical device configurations, and clinical data stored on endpoints. Payers rely on it to secure claims data and financial records. Its robust encryption capabilities ensure that sensitive healthcare information remains protected from unauthorized access, meeting regulatory standards like HIPAA.

408. Versa Networks

Versa Networks offers a secure SD-WAN solution that integrates networking and security functions, helping organizations secure cloud and branch-office environments. It ensures that healthcare organizations can securely connect remote sites and manage data flows across multiple locations.

Hospitals use Versa Networks to securely connect branch offices, telehealth platforms, and remote healthcare providers to their main healthcare infrastructure. Payers rely on it to secure the connection between claims processing centers and remote offices. Its SD-WAN and security features provide secure and scalable connectivity across healthcare environments.

409. VidyoConnect for Telehealth

VidyoConnect for Telehealth is a video conferencing platform designed specifically for healthcare organizations, offering secure and HIPAA-compliant virtual care solutions. It provides high-quality video consultations and communication tools for healthcare professionals and patients.

Hospitals use VidyoConnect to facilitate virtual consultations, enabling clinicians to provide care to patients remotely. Payers benefit from its telehealth capabilities to support virtual care programs for members, improving patient access and reducing healthcare costs. Its secure, encrypted communication tools ensure the privacy of patient data during virtual consultations.

410. Virtru

Virtru provides email encryption solutions that protect sensitive information exchanged through email. It offers seamless integration with email platforms like Gmail and Outlook and helps organizations ensure that their communications remain private and compliant with data protection regulations.

Hospitals use Virtru to encrypt email communications involving patient data, medical records, and clinical updates. Payers rely on it to secure communications with healthcare providers regarding claims and financial data. Its easy-to-use encryption tools ensure that sensitive healthcare information is protected during transmission, meeting HIPAA and GDPR compliance standards.

411. VMware Workspace ONE

VMware Workspace ONE is an enterprise mobility management (EMM) solution that provides unified endpoint management (UEM) and secure access to applications. It helps healthcare organizations secure and manage devices accessing sensitive healthcare data.



Hospitals use Workspace ONE to manage and secure clinician devices, medical devices, and workstations that access EHRs and patient data. Payers rely on it to secure mobile access to claims systems and financial records. Its centralized management platform ensures compliance with healthcare regulations while protecting endpoints across the organization.

412. VMware Zero Trust Solutions

VMware Zero Trust Solutions offer a framework for securing access to applications and data by continuously verifying the identity of users and devices. It ensures that only trusted entities can access sensitive healthcare systems, reducing the risk of unauthorized access.

Hospitals use VMware Zero Trust Solutions to secure access to EHR systems, medical devices, and patient portals by continuously verifying the identity of users and devices. Payers rely on it to protect claims systems and financial data from unauthorized access. Its ability to enforce strict access controls ensures compliance with healthcare security standards.

413. Vocalcom

Vocalcom provides cloud-based contact center solutions that enhance communication and customer service in healthcare organizations. It offers features such as voice, chat, email, and social media integration, improving patient and member engagement.

Hospitals use Vocalcom to improve patient communication, including appointment scheduling, billing inquiries, and support for telehealth services. Payers rely on it for secure communication with members regarding claims and benefits. Its multi-channel capabilities ensure seamless communication between healthcare providers and patients, enhancing the patient experience.

414. Vocera Communications

Vocera Communications provides a secure communication platform for healthcare teams, enabling clinicians and staff to communicate in real-time. Its platform includes voice, text, and alerting capabilities to improve workflow and coordination.

Hospitals use Vocera to streamline communication between healthcare teams, ensuring that patient data is exchanged securely and efficiently. Payers rely on it to communicate with providers regarding claims and member data. Its HIPAA-compliant messaging features ensure that sensitive healthcare information remains private.

415. Vormetric

Vormetric provides data-centric security solutions, including encryption, access controls, and data masking. It helps healthcare organizations protect sensitive patient data and comply with data privacy regulations like HIPAA and GDPR.

Hospitals use Vormetric to encrypt EHR systems, medical records, and clinical data to protect patient privacy. Payers benefit from its encryption and access control features to secure claims systems and financial records. Its comprehensive data protection capabilities help ensure compliance with healthcare regulations and prevent unauthorized access.

416. Voalte (by Hillrom)

Voalte provides secure, HIPAA-compliant communication tools for healthcare organizations, including messaging, voice, and alarm management. It helps improve workflow efficiency and patient care coordination across healthcare teams.

Hospitals use Voalte to improve communication between clinical teams, ensuring that sensitive patient information is shared securely. Payers rely on it to securely communicate with healthcare providers about claims and member data. Its user-friendly interface and secure communication capabilities enhance patient care and operational efficiency.

417. Wallix Bastion

Wallix Bastion provides privileged access management (PAM) solutions that secure and monitor privileged accounts and access to critical IT systems. It helps organizations control and audit access to sensitive data, ensuring compliance with privacy regulations.

Hospitals use Wallix Bastion to secure administrative access to EHR systems, medical devices, and hospital networks. Payers rely on it to manage access to claims platforms and financial systems. Its real-time session monitoring and detailed access auditing features help healthcare organizations maintain compliance with regulations like HIPAA and ensure secure access to critical healthcare systems.

418. WatchGuard

WatchGuard provides network security solutions, including firewalls, VPNs, and secure Wi-Fi services. It offers multi-layered protection against cyber threats, ensuring that healthcare organizations can safeguard their networks and sensitive data from attacks.

Hospitals use WatchGuard to secure hospital networks, medical devices, and EHR systems from cyber threats like malware, ransomware, and data breaches. Payers rely on it to protect claims platforms and financial applications. Its comprehensive security features, including advanced threat detection and prevention, ensure that healthcare organizations remain protected from evolving cyber threats.

419. Webroot Security Awareness Training

Webroot Security Awareness Training provides cybersecurity education to employees, focusing on preventing phishing attacks, social engineering, and other common cyber threats. It includes interactive training modules and phishing simulations to improve user awareness and reduce risk.

Hospitals use Webroot Security Awareness Training to educate staff on recognizing phishing attempts and protecting patient data. Payers benefit from its training programs to reduce the risk of fraud or cyberattacks targeting claims systems. Its engaging and interactive training modules ensure that employees at all levels of the organization are equipped to handle cybersecurity risks.

420. Wickr (AWS)

Wickr, now part of AWS, offers secure messaging and collaboration tools that provide end-to-end encryption for communication across healthcare organizations. It allows secure messaging, voice, video calls, and file sharing while ensuring compliance with HIPAA and other privacy regulations.

Hospitals use Wickr to enable secure communication between clinicians, ensuring that patient data and clinical information remain confidential. Payers rely on it for secure communications with healthcare providers regarding claims and member data. Its end-to-end encryption ensures that all communication is protected against unauthorized access.

421. WinMagic SecureDoc

WinMagic SecureDoc provides full disk encryption (FDE) solutions to help organizations secure their sensitive data at rest. It protects patient data, financial records, and clinical information from unauthorized access and meets compliance requirements like HIPAA.

Hospitals use SecureDoc to encrypt medical devices, EHR systems, and clinical data to prevent unauthorized access. Payers benefit from its capabilities to encrypt claims data and financial records. Its strong encryption algorithms ensure that sensitive healthcare information is always protected, even when devices are lost or stolen.

422. Wombat Security (Proofpoint)

Wombat Security, now part of Proofpoint, provides security awareness training, phishing simulations, and other educational tools to help organizations mitigate the risks of human error in cybersecurity. It helps healthcare organizations reduce their vulnerability to phishing and social engineering attacks.

Hospitals use Wombat Security to train staff on identifying phishing attacks and protecting patient data. Payers rely on it to reduce the risk of fraud and phishing attacks targeting claims systems and member data. Its interactive training and realistic simulations ensure that healthcare staff can recognize and respond to cyber threats effectively.

423. X-Ways Forensics

X-Ways Forensics is a digital forensics and data recovery software suite that provides powerful tools for investigating security incidents and breaches. It helps healthcare organizations analyze and recover data from compromised systems.

Hospitals use X-Ways Forensics to investigate incidents involving EHR systems, medical devices, and patient data. Payers rely on it to analyze potential fraud or data breaches involving claims systems. Its powerful forensic tools help healthcare organizations understand the scope of a security incident and recover lost or compromised data.

424. Yubico YubiKey

Yubico YubiKey is a hardware-based multi-factor authentication (MFA) solution that provides strong security for user access to sensitive systems and applications. It ensures that only authorized users can access healthcare data and systems, reducing the risk of unauthorized access.

Hospitals use Yubico YubiKey to secure access to EHR systems, medical devices, and clinical applications. Payers benefit from its capabilities to protect claims systems and financial data. Its physical authentication keys provide an additional layer of security to prevent unauthorized access and comply with HIPAA and other privacy regulations.

425. Zinc Secure Messaging

Zinc Secure Messaging is a HIPAA-compliant, encrypted messaging platform designed for healthcare organizations. It enables secure, real-time communication between care teams, patients, and other healthcare professionals.

Hospitals use Zinc Secure Messaging to communicate securely between clinicians, ensuring that patient data is exchanged in compliance with privacy regulations. Payers rely on it to securely communicate with providers regarding claims and benefits. Its easy-to-use interface and secure messaging features ensure that sensitive healthcare information remains confidential.

426. Zix Email Encryption

Zix Email Encryption is a secure email platform that provides end-to-end encryption to protect sensitive communications. It is designed to ensure that email communications, including patient records and financial information, are protected from unauthorized access and comply with healthcare regulations.

Hospitals use Zix Email Encryption to protect email communications involving patient data, medical records, and clinical updates. Payers benefit from its secure email capabilities for communication related to claims, reimbursements, and member data. Its easy-to-use encryption features ensure that all sensitive healthcare communications remain secure and compliant with regulations like HIPAA.

427. Zscaler

Zscaler offers a cloud-based security platform that provides secure internet access, data protection, and threat prevention. Its platform helps healthcare organizations secure data as it travels across the internet, ensuring that sensitive information is protected from external threats.

Hospitals use Zscaler to secure internet access for clinical staff, ensuring that patient data and medical records are protected during online exchanges. Payers rely on it to secure claims processing platforms and member data as they interact with external partners and networks. Its cloud-native platform ensures that healthcare organizations can scale their security as they grow.

428. Zscaler Cloud Security

Zscaler Cloud Security provides comprehensive protection for cloud-based applications and services. It helps healthcare organizations ensure that their cloud-hosted EHR systems, telehealth platforms, and patient portals remain secure and compliant with privacy regulations.

Hospitals use Zscaler Cloud Security to protect cloud-based EHRs, telehealth services, and other clinical applications from cyber threats. Payers rely on it to secure cloud-based claims systems and member portals. Its advanced threat detection and data loss prevention capabilities help healthcare organizations safeguard sensitive data in the cloud.

429. Zscaler Zero Trust

Zscaler Zero Trust is a security model that ensures no user, device, or application is trusted by default. It continuously verifies the identity of users and devices before granting access to sensitive healthcare data and systems.

Hospitals use Zscaler Zero Trust to secure access to EHR systems, medical devices, and telehealth platforms, ensuring that each access request is authenticated and authorized. Payers rely on it to enforce strict access controls for claims platforms and member data. Its zero-trust model reduces the risk of unauthorized access and enhances compliance with HIPAA and other regulations.

430. Zscaler IoT Security

Zscaler IoT Security protects connected medical devices and IoT systems from cyber threats. It provides real-time monitoring, anomaly detection, and secure network access, ensuring that healthcare IoT devices remain secure and compliant with regulations.

Hospitals use Zscaler IoT Security to monitor and protect medical devices like infusion pumps, patient monitors, and diagnostic tools from cyberattacks. Payers benefit from its capabilities to secure IoT systems involved in claims processing and healthcare administration. Its real-time security features help ensure the confidentiality and integrity of healthcare IoT devices.

.



Numeric Directory

**Vendor Listing Cybersecurity
Products Offered Healthcare
Organizations**



2. **42Gears SureMDM:** Mobile Device Management (MDM)
3. **AccessData Forensic Tools (Exterro):** Forensic Analysis Tools, Incident Response Platforms
4. **Acunetix Vulnerability Scanner:** Vulnerability Management
5. **Acronis Cyber Protect:** Ransomware Protection and Recovery, Endpoint Detection and Response (EDR)
6. **Akamai Cloud Security:** Cloud Security, Network Security
7. **AlienVault (AT&T Cybersecurity):** SIEM, Threat Intelligence Platforms
8. **AlienVault Threat Intelligence:** Threat Intelligence Platforms
9. **Amazon Web Services (AWS) Security:** Cloud Security, IoT Security, Network Security
10. **Amazon Web Services (AWS) IoT Device Defender:** IoT/IoMT Security
11. **Amazon Web Services (AWS) Security Hub:** SIEM, Cloud Security
12. **Amwell (American Well):** Telehealth Security
13. **Anomali:** Threat Intelligence Platforms
14. **Appgate SDP:** Zero Trust Architecture
15. **Aravo:** Third-Party Risk Management
16. **ArcSight (Micro Focus):** SIEM
17. **Arcserve UDP:** Backup and Disaster Recovery, Ransomware Protection and Recovery
18. **Arctic Wolf Managed Security Awareness:** Security Awareness Training
19. **Area 1 Security (Cloudflare):** Secure Email Gateways, Network Security
20. **Arista Networks:** Network Security
21. **Arm Pelion IoT:** IoT/IoMT Security
22. **Armis:** IoT/IoMT Security
23. **Aruba Networks:** Network Security
24. **Atera Patch Management:** Patch Management Systems
25. **AttackIQ Cybersecurity Training:** Security Awareness Training
26. **Auth0:** Identity and Access Management (IAM), Multi-Factor Authentication (MFA)
27. **Authy (Twilio):** Multi-Factor Authentication (MFA)



28. **Automox:** Patch Management Systems
29. **Autopsy (Sleuth Kit):** Forensic Analysis Tools
30. **AxCrypt:** Encryption
31. **Axonius:** Asset Management, IoT/IoMT Security
32. **Balbix:** Behavioral Analytics
33. **Baramundi Management Suite:** Mobile Device Management (MDM), Endpoint Management
34. **Barracuda CloudGen:** Cloud Security, Network Security
35. **Barracuda Email Security Gateway:** Secure Email Gateways
36. **Barracuda Networks:** Network Security, Cloud Security
37. **Barracuda PhishLine:** Security Awareness Training
38. **Barracuda Ransomware Protection:** Ransomware Protection and Recovery
39. **Basis Technology Autopsy:** Forensic Analysis Tools
40. **Belkasoft Evidence Center:** Forensic Analysis Tools
41. **BeyondTrust:** Privileged Access Management (PAM), Identity and Access Management (IAM), Zero Trust Architecture
42. **BeyondTrust Retina:** Vulnerability Management
43. **BeyondTrust Zero Trust:** Zero Trust Architecture
44. **BitLocker (Microsoft):** Encryption
45. **BitSight:** Third-Party Risk Management
46. **Bitdefender GravityZone:** Endpoint Detection and Response (EDR)
47. **Bitdefender Threat Intelligence:** Threat Intelligence Platforms
48. **BlackBag Blacklight (OpenText):** Forensic Analysis Tools
49. **BlackBerry Cylance:** Endpoint Detection and Response (EDR), Artificial Intelligence and Machine Learning
50. **BlackBerry UEM:** Unified Endpoint Management (UEM)
51. **Blockpharma:** Blockchain for Data Security
52. **Blumira:** SIEM

53. **Boxcryptor:** Encryption
54. **BurstIQ:** Blockchain for Data Security
55. **CA Privileged Access Manager:** Privileged Access Management (PAM)
56. **Cado Response:** Incident Response Platforms
57. **Carbon Black (VMware):** Endpoint Detection and Response (EDR), Cloud Security
58. **CareClix:** Telehealth Security
59. **Cellebrite:** Forensic Analysis Tools
60. **Censys:** Threat Intelligence Platforms
61. **Centrify:** Identity and Access Management (IAM), Privileged Access Management (PAM)
62. **Centrify Privileged Access Service:** Privileged Access Management (PAM)
63. **Cerner Secure Messaging:** Secure Messaging Platforms
64. **Cerner Telehealth Solutions:** Telehealth Security
65. **Chainalysis:** Blockchain for Data Security
66. **Check Point CloudGuard:** Cloud Security
67. **Check Point Email Security:** Secure Email Gateways
68. **Check Point Harmony Endpoint:** Endpoint Detection and Response (EDR)
69. **Check Point IoT Protect:** IoT/IoMT Security
70. **Check Point Software:** Network Security, Cloud Security, IoT/IoMT Security
71. **Check Point ThreatCloud:** Threat Intelligence Platforms
72. **Chiron Health:** Telehealth Security
73. **Chronicled:** Blockchain for Data Security
74. **Cisco IoT Threat Defense:** IoT/IoMT Security
75. **Cisco Meraki Systems Manager:** Unified Endpoint Management (UEM)
76. **Cisco Secure:** Network Security, Cloud Security
77. **Cisco Secure Email:** Secure Email Gateways
78. **Cisco SecureX:** SIEM
79. **Cisco Talos:** Threat Intelligence Platforms



80. **Cisco Umbrella:** Network Security
81. **Cisco Webex for Healthcare:** Telehealth Security
82. **Citrix ADC:** Network Security
83. **Citrix Endpoint Management:** Unified Endpoint Management (UEM)
84. **Citrix Zero Trust:** Zero Trust Architecture
85. **Clearswift DLP:** Data Loss Prevention (DLP)
86. **Cloudflare:** Cloud Security
87. **Code42:** Data Loss Prevention (DLP)
88. **Codeproof Enterprise MDM:** Mobile Device Management (MDM)
89. **Cohesity DataProtect:** Backup and Disaster Recovery
90. **Commvault Complete Backup:** Backup and Disaster Recovery
91. **ConnectWise Automate:** Patch Management Systems
92. **Coral Health:** Blockchain for Data Security
93. **CrowdStrike:** Endpoint Detection and Response (EDR), Cloud Security
94. **CrowdStrike Falcon Cloud:** Cloud Security
95. **CrowdStrike Falcon Forensics:** Forensic Analysis Tools
96. **CrowdStrike Falcon Fusion:** Incident Response Platforms
97. **CrowdStrike Falcon Spotlight:** Endpoint Detection and Response (EDR)
98. **CrowdStrike Threat Intelligence:** Threat Intelligence Platforms
99. **Curricula Security Awareness Training:** Security Awareness Training
100. **CyFIR Investigator:** Forensic Analysis Tools
101. **CyberArk:** Identity and Access Management (IAM), Privileged Access Management (PAM)
102. **CyberArk Zero Trust:** Zero Trust Architecture, Privileged Access Management (PAM)
103. **CyberGRX:** Third-Party Risk Management
104. **CyberMDX:** IoT/IoMT Security
105. **CyberSponse (Arctic Wolf):** Incident Response Platforms
106. **CyberVista:** Security Awareness Training

107. **Cybereason Defense Platform:** Endpoint Detection and Response (EDR), Threat Intelligence Platforms
108. **Cybereason RansomFree:** Ransomware Protection and Recovery
109. **Cybereason Threat Analysis:** Threat Intelligence Platforms
110. **Cynerio:** IoT/IoMT Security
111. **Cynet 360 Behavioral Analytics:** Behavioral Analytics
112. **D3 Security:** Incident Response Platforms
113. **Darktrace:** Endpoint Detection and Response (EDR), Threat Intelligence Platforms, Behavioral Analytics
114. **Darktrace IoT:** IoT/IoMT Security
115. **Dashlane MFA:** Multi-Factor Authentication (MFA)
116. **Deep Instinct:** Endpoint Detection and Response (EDR), Behavioral Analytics
117. **Dell Data Protection Encryption:** Encryption
118. **Devo Technology:** SIEM
119. **Devolutions PAM:** Privileged Access Management (PAM)
120. **Digital Guardian:** Data Loss Prevention (DLP)
121. **Doc.ai:** Blockchain for Data Security
122. **Doxy.me:** Telehealth Security
123. **Dragos (Industrial IoT):** IoT/IoMT Security
124. **Duo Security (Cisco):** Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Zero Trust Architecture
125. **ESET Cybersecurity Awareness:** Security Awareness Training
126. **ESET Endpoint Security:** Endpoint Detection and Response (EDR)
127. **ESET Inspect:** Endpoint Detection and Response (EDR)
128. **ESET Secure Authentication:** Multi-Factor Authentication (MFA)
129. **EclecticIQ:** Threat Intelligence Platforms
130. **EcoVadis:** Third-Party Risk Management
131. **Egress Protect:** Data Loss Prevention (DLP)



- 132. **Ekran System:** Privileged Access Management (PAM)
- 133. **Elastic Security:** SIEM
- 134. **EncrypGen:** Blockchain for Data Security
- 135. **EncryptRIGHT (PKWARE):** Encryption
- 136. **Entrust Identity MFA:** Multi-Factor Authentication (MFA)
- 137. **Epic Secure Chat:** Secure Messaging Platforms
- 138. **Epic Telehealth Integration:** Telehealth Security
- 139. **Exabeam DLP:** Data Loss Prevention (DLP)
- 140. **Exabeam Incident Responder:** Incident Response Platforms
- 141. **Extreme Networks:** Network Security
- 142. **F-Secure Countercept:** Endpoint Detection and Response (EDR)
- 143. **F-Secure Radar:** Vulnerability Management
- 144. **FTK (Forensic Toolkit) by Exterro:** Forensic Analysis Tools
- 145. **Factom:** Blockchain for Data Security
- 146. **FarmaTrust:** Blockchain for Data Security
- 147. **Fidelis Cybersecurity:** Data Loss Prevention (DLP), Threat Intelligence Platforms
- 148. **FireEye Cloud Security:** Cloud Security
- 149. **FireEye Email Security (Trellix):** Secure Email Gateways
- 150. **FireEye Endpoint Security:** Endpoint Detection and Response (EDR)
- 151. **FireEye Endpoint Security (Trellix):** Endpoint Detection and Response (EDR)
- 152. **FireEye Threat Intelligence (Trellix):** Threat Intelligence Platforms
- 153. **Flexera Software Vulnerability Manager:** Vulnerability Management
- 154. **Forcepoint:** Network Security, Data Loss Prevention (DLP)
- 155. **Forescout:** IoT/IoMT Security, Network Security
- 156. **ForgeRock:** Identity and Access Management (IAM), Zero Trust Architecture
- 157. **Forrester Zero Trust Partners:** Zero Trust Architecture
- 158. **Fortanix:** Encryption, Zero Trust Architecture

- 159. **FortiEDR (Fortinet):** Endpoint Detection and Response (EDR)
- 160. **Fortinet:** Network Security, Zero Trust Architecture, IoT Security
- 161. **Fortinet FortiGuard Labs:** Threat Intelligence Platforms
- 162. **Fortinet FortiInsight:** Behavioral Analytics
- 163. **Fortinet FortiMail:** Secure Email Gateways
- 164. **Fortinet FortiSIEM:** SIEM
- 165. **Fortinet FortiSOAR:** Incident Response Platforms
- 166. **Fortinet FortiToken:** Multi-Factor Authentication (MFA)
- 167. **Forward Advantage:** Secure Messaging Platforms
- 168. **Foxpass PAM:** Privileged Access Management (PAM)
- 169. **Fudo Security PAM:** Privileged Access Management (PAM)
- 170. **GFI LanGuard:** Vulnerability Management, Patch Management Systems
- 171. **GTB Technologies:** Data Loss Prevention (DLP)
- 172. **Google Authenticator:** Multi-Factor Authentication (MFA)
- 173. **Google Cloud Security:** Cloud Security
- 174. **Graylog:** SIEM
- 175. **Guardtime:** Blockchain for Data Security
- 176. **Guardtime Health:** Blockchain for Data Security
- 177. **Gurukul Behavioral Analytics:** Behavioral Analytics
- 178. **HID Global:** Identity and Access Management (IAM)
- 179. **HID Global ActivID:** Multi-Factor Authentication (MFA)
- 180. **Habitu8:** Security Awareness Training
- 181. **Halo Health:** Secure Messaging Platforms
- 182. **Hashed Health:** Blockchain for Data Security
- 183. **HashiCorp Vault:** Privileged Access Management (PAM), Encryption
- 184. **HealthCombix:** Blockchain for Data Security
- 185. **HealthTap:** Telehealth Security



- 186. **Hexnode MDM:** Mobile Device Management (MDM)
- 187. **Hitachi ID PAM:** Privileged Access Management (PAM)
- 188. **IBM Blockchain:** Blockchain for Data Security
- 189. **IBM Cloud Security:** Cloud Security
- 190. **IBM Guardium:** Data Loss Prevention (DLP), Encryption
- 191. **IBM MaaS360:** Mobile Device Management (MDM)
- 192. **IBM Security QRadar:** SIEM
- 193. **IBM Security QRadar UEBA:** SIEM
- 194. **IBM Security Resilient:** Incident Response Platforms
- 195. **IBM Security Secret Server:** Privileged Access Management (PAM)
- 196. **IBM Security Verify:** Identity and Access Management (IAM)
- 197. **IBM Spectrum Protect:** Backup and Disaster Recovery
- 198. **IBM X-Force Exchange:** Threat Intelligence Platforms
- 199. **Illumio:** Zero Trust Architecture
- 200. **Imperva:** Network Security
- 201. **Infosec IQ:** Security Awareness Training
- 202. **InsightVM (Rapid7):** Vulnerability Management
- 203. **Inspired eLearning:** Security Awareness Training
- 204. **InTouch Health (Teladoc):** Telehealth Security
- 205. **Ironscales:** Secure Email Gateways, Behavioral Analytics
- 206. **Ivanti Endpoint Security:** Endpoint Detection and Response (EDR), Vulnerability Management
- 207. **Ivanti Neurons for Vulnerability Management:** Vulnerability Management
- 208. **Ivanti Patch Management:** Patch Management Systems
- 209. **Jamf Pro:** Mobile Device Management (MDM)
- 210. **Juniper Networks:** Network Security
- 211. **Kandji:** Mobile Device Management (MDM)
- 212. **Kaseya VSA:** Patch Management Systems, Endpoint Management

- 213. **Kaspersky Anti-Ransomware:** Ransomware Protection and Recovery
- 214. **Kaspersky Endpoint Security:** Endpoint Detection and Response (EDR)
- 215. **Kaspersky IoT Security:** IoT/IoMT Security
- 216. **Kaspersky Threat Intelligence:** Threat Intelligence Platforms
- 217. **Keycloak:** Identity and Access Management (IAM), Multi-Factor Authentication (MFA)
- 218. **KnowBe4:** Security Awareness Training
- 219. **Knox Manage (Samsung):** Mobile Device Management (MDM)
- 220. **Klara:** Secure Messaging Platforms
- 221. **Kroll Artifact Parser and Extractor (KAPE):** Forensic Analysis Tools
- 222. **KY3P (S&P Global):** Third-Party Risk Management
- 223. **Lacework:** Cloud Security
- 224. **LastPass MFA:** Multi-Factor Authentication (MFA)
- 225. **LogRhythm:** SIEM
- 226. **LogRhythm Forensic Suite:** Forensic Analysis Tools, SIEM
- 227. **LogRhythm SOAR:** Incident Response Platforms
- 228. **LogRhythm UEBA:** Behavioral Analytics, SIEM
- 229. **LogicGate Risk Cloud:** Third-Party Risk Management
- 230. **ManageEngine (ADSelfService Plus):** Identity and Access Management (IAM)
- 231. **ManageEngine Mobile Device Manager Plus:** Mobile Device Management (MDM)
- 232. **ManageEngine PAM360:** Privileged Access Management (PAM)
- 233. **ManageEngine Patch Manager Plus:** Patch Management Systems
- 234. **Magnet AXIOM:** Forensic Analysis Tools
- 235. **Malwarebytes Endpoint Protection:** Endpoint Detection and Response (EDR)
- 236. **Malwarebytes for Business:** Endpoint Detection and Response (EDR)
- 237. **McAfee Advanced Threat Defense:** Endpoint Detection and Response (EDR)
- 238. **McAfee Complete Data Protection:** Encryption, Endpoint Detection and Response (EDR)
- 239. **McAfee Endpoint Security:** Endpoint Detection and Response (EDR)



- 240. **McAfee Enterprise Security Manager:** SIEM
- 241. **McAfee Total Protection for DLP:** Data Loss Prevention (DLP)
- 242. **MedRec:** Blockchain for Data Security
- 243. **Medici Telehealth:** Telehealth Security
- 244. **Medigate (by Claroty):** IoT/IoMT Security
- 245. **MEDITECH Expanse Secure Messaging:** Secure Messaging Platforms
- 246. **Mend Telemedicine Platform:** Telehealth Security
- 247. **Mend VIP Telehealth:** Telehealth Security
- 248. **MetaCompliance:** Security Awareness Training
- 249. **MetricStream Third-Party Risk:** Third-Party Risk Management
- 250. **Mimecast Awareness Training:** Security Awareness Training
- 251. **Mimecast Secure Email Gateway:** Secure Email Gateways
- 252. **Microsoft 365 DLP:** Data Loss Prevention (DLP)
- 253. **Microsoft Advanced Threat Analytics (ATA):** Threat Intelligence Platforms
- 254. **Microsoft Azure Active Directory:** Identity and Access Management (IAM), Cloud Security
- 255. **Microsoft Azure Blockchain:** Blockchain for Data Security
- 256. **Microsoft Azure Security:** Cloud Security
- 257. **Microsoft Azure Sentinel:** SIEM, Cloud Security
- 258. **Microsoft Defender ATP:** Endpoint Detection and Response (EDR)
- 259. **Microsoft Defender for Office 365:** Secure Email Gateways
- 260. **Microsoft Defender Vulnerability Management:** Vulnerability Management
- 261. **Microsoft Intune:** Mobile Device Management (MDM)
- 262. **Microsoft SCCM (System Center Configuration Manager):** Endpoint Management
- 263. **Microsoft Teams for Healthcare:** Telehealth Security
- 264. **Microsoft Zero Trust Solutions:** Zero Trust Architecture
- 265. **MobileIron (Ivanti):** Mobile Device Management (MDM)
- 266. **Netskope:** Cloud Security, Network Security, Zero Trust Architecture

- 267. **Netskope Cloud Security:** Cloud Security
- 268. **Netskope Zero Trust:** Zero Trust Architecture
- 269. **Netsurion EventTracker:** SIEM
- 270. **NetWitness UEBA:** Behavioral Analytics, SIEM
- 271. **Netwrix Auditor:** Data Loss Prevention (DLP), SIEM
- 272. **Netwrix Privilege Secure:** Privileged Access Management (PAM)
- 273. **Nexpose (Rapid7):** Vulnerability Management
- 274. **Ninite Pro:** Patch Management Systems
- 275. **Okta:** Identity and Access Management (IAM), Zero Trust Architecture, Cloud Security
- 276. **Okta MFA:** Multi-Factor Authentication (MFA)
- 277. **OnPage Secure Messaging:** Secure Messaging Platforms
- 278. **One Identity Safeguard:** Privileged Access Management (PAM)
- 279. **OneLogin:** Identity and Access Management (IAM), Multi-Factor Authentication (MFA)
- 280. **OneLogin Protect:** Multi-Factor Authentication (MFA)
- 281. **OneTrust Vendorpedia:** Third-Party Risk Management
- 282. **OpenText (Carbonite Endpoint Encryption):** Encryption
- 283. **OpenVAS (Greenbone Networks):** Vulnerability Management
- 284. **Oracle Cloud Security:** Cloud Security
- 285. **Oxygen Forensics:** Forensic Analysis Tools
- 286. **Palo Alto Networks:** IoT/IoMT Security, Network Security, Cloud Security, Zero Trust Architecture
- 287. **Palo Alto Networks Cortex XDR:** Endpoint Detection and Response (EDR)
- 288. **Palo Alto Networks Cortex XDR Forensics:** Forensic Analysis Tools, Endpoint Detection and Response (EDR)
- 289. **Palo Alto Networks Cortex XSOAR:** Incident Response Platforms
- 290. **Palo Alto Networks IoT Security:** IoT/IoMT Security
- 291. **Palo Alto Networks Prisma:** Cloud Security
- 292. **Palo Alto Networks Prisma Cloud:** Cloud Security



- 293. **Palo Alto Networks Unit 42:** Threat Intelligence Platforms
- 294. **Panorays:** Third-Party Risk Management
- 295. **Paraben E3 Platform:** Forensic Analysis Tools
- 296. **Patch My PC:** Patch Management Systems
- 297. **PerfectServe:** Secure Messaging Platforms
- 298. **Perception Point:** Secure Email Gateways
- 299. **PhishMe (Cofense):** Security Awareness Training
- 300. **Ping Identity:** Identity and Access Management (IAM), Zero Trust Architecture
- 301. **Ping Identity MFA:** Multi-Factor Authentication (MFA)
- 302. **Ping Identity Zero Trust:** Zero Trust Architecture
- 303. **PKWARE EncryptRIGHT:** Encryption
- 304. **Prevalent:** Third-Party Risk Management
- 305. **ProcessUnity:** Third-Party Risk Management
- 306. **Proofpoint:** Data Loss Prevention (DLP), Secure Email Gateways, Threat Intelligence Platforms
- 307. **Proofpoint Cloud Security:** Cloud Security
- 308. **Proofpoint Email Protection:** Secure Email Gateways
- 309. **Proofpoint Security Awareness Training:** Security Awareness Training
- 310. **Pulsara:** Secure Messaging Platforms
- 311. **Qualys:** Vulnerability Management
- 312. **Qualys Patch Management:** Patch Management Systems
- 313. **Rapid7:** SIEM, Vulnerability Management
- 314. **Rapid7 InsightConnect:** Incident Response Platforms
- 315. **Rapid7 InsightIDR:** SIEM
- 316. **Recorded Future:** Threat Intelligence Platforms
- 317. **Remediant SecureONE:** Privileged Access Management (PAM)
- 318. **RiskRecon (Mastercard):** Third-Party Risk Management
- 319. **RiskWatch:** Third-Party Risk Management

- 320. **RSA Archer Third-Party Risk Management:** Third-Party Risk Management
- 321. **RSA NetWitness:** SIEM
- 322. **RSA SecurID:** Identity and Access Management (IAM), Multi-Factor Authentication (MFA)
- 323. **RSA Zero Trust:** Zero Trust Architecture
- 324. **Rubrik:** Ransomware Protection and Recovery, Backup and Disaster Recovery
- 325. **SANS Investigative Forensics Toolkit (SIFT):** Forensic Analysis Tools
- 326. **SANS Security Awareness:** Security Awareness Training
- 327. **Saviynt:** Identity and Access Management (IAM), Privileged Access Management (PAM)
- 328. **Saviynt Privileged Access Management:** Privileged Access Management (PAM)
- 329. **Scalefusion MDM:** Mobile Device Management (MDM)
- 330. **SecureAuth:** Identity and Access Management (IAM), Multi-Factor Authentication (MFA)
- 331. **SecureAuth MFA:** Multi-Factor Authentication (MFA)
- 332. **SecureTrust DLP:** Data Loss Prevention (DLP)
- 333. **SecureWorks Taegis:** SIEM
- 334. **Sectigo IoT Manager:** IoT/IoMT Security
- 335. **Security Mentor:** Security Awareness Training
- 336. **SecurityScorecard:** Third-Party Risk Management
- 337. **Senrio Insight:** IoT/IoMT Security
- 338. **SentinelOne:** Endpoint Detection and Response (EDR)
- 339. **SentinelOne Singularity:** Endpoint Detection and Response (EDR)
- 340. **SentinelOne Vigilance Respond:** Incident Response Platforms
- 341. **Shared Assessments Third-Party Risk Tools:** Third-Party Risk Management
- 342. **Signal Secure Messaging:** Secure Messaging Platforms
- 343. **SimplePractice Telehealth:** Telehealth Security
- 344. **Siemplify (Google Chronicle):** Incident Response Platforms
- 345. **Skybox Security:** Vulnerability Management
- 346. **SolarWinds Access Rights Manager:** Privileged Access Management (PAM)



- 347. **SolarWinds Mail Assure:** Secure Email Gateways
- 348. **SolarWinds Network Vulnerability Detection:** Vulnerability Management
- 349. **SolarWinds Patch Manager:** Patch Management Systems
- 350. **SolarWinds Security Event Manager:** SIEM
- 351. **Sophos:** Endpoint Detection and Response (EDR), Cloud Security, Network Security
- 352. **Sophos Cloud Optix:** Cloud Security
- 353. **Sophos Email Protection:** Secure Email Gateways
- 354. **Sophos Encryption:** Encryption
- 355. **Sophos Firewall:** Network Security
- 356. **Sophos Intercept X:** Endpoint Detection and Response (EDR)
- 357. **Sophos Mobile Security:** Mobile Device Management (MDM)
- 358. **Sophos Worry-Free:** Endpoint Detection and Response (EDR)
- 359. **SophosLabs:** Threat Intelligence Platforms
- 360. **SophosLabs Behavioral Analytics:** Behavioral Analytics
- 361. **Sophos Vision One:** Endpoint Detection and Response (EDR)
- 362. **Sophos Behavioral Analytics:** Behavioral Analytics
- 363. **Solve.Care:** Blockchain for Data Security
- 364. **SonicWall:** Network Security
- 365. **Sophos Endpoint Security Mobile:** Mobile Device Management (MDM)
- 366. **Sophos TippingPoint:** Network Security
- 367. **Sophos Vision One:** Endpoint Detection and Response (EDR)
- 368. **Sophos Behavioral Analytics:** Behavioral Analytics
- 369. **Spok:** Secure Messaging Platforms
- 370. **Splunk:** SIEM
- 371. **Splunk Phantom:** Incident Response Platforms
- 372. **Splunk Behavioral Analytics:** Behavioral Analytics
- 373. **Spirion:** Data Loss Prevention (DLP)

- 374. **SOTI MobiControl:** Mobile Device Management (MDM)
- 375. **Swimlane:** Incident Response Platforms
- 376. **Sumo Logic:** SIEM
- 377. **Sumo Logic SOAR:** Incident Response Platforms
- 378. **Sumo Logic Behavioral Analytics:** Behavioral Analytics
- 379. **Symphony Communication Services:** Secure Messaging Platforms
- 380. **Symantec (Broadcom):** Data Loss Prevention (DLP), Endpoint Protection, Cloud Security
- 381. **Symantec Email Security:** Secure Email Gateways
- 382. **Symantec Encryption:** Encryption
- 383. **Symantec IoT Security:** IoT/IoMT Security
- 384. **Symantec Managed Security Services:** Managed Security Services
- 385. **Symantec VIP Access:** Multi-Factor Authentication (MFA)
- 386. **Symantec Zero Trust:** Zero Trust Architecture
- 387. **Symantec Endpoint Protection:** Endpoint Detection and Response (EDR)
- 388. **Symantec Endpoint Management:** Endpoint Management
- 389. **Tanium:** Endpoint Detection and Response (EDR), Network Security
- 390. **Teladoc Health:** Telehealth Security
- 391. **Telmediq (by PerfectServe):** Secure Messaging Platforms
- 392. **Tenable:** Vulnerability Management
- 393. **Terranova Security:** Security Awareness Training
- 394. **Thales Group:** Encryption, Data Loss Prevention (DLP)
- 395. **Thales IoT Solutions:** IoT/IoMT Security
- 396. **Thales SafeNet MFA:** Multi-Factor Authentication (MFA)
- 397. **ThreatConnect:** Threat Intelligence Platforms
- 398. **ThreatQuotient:** Threat Intelligence Platforms
- 399. **ThreatSim:** Security Awareness Training
- 400. **TigerConnect:** Secure Messaging Platforms



- 401. **TitanHQ SpamTitan:** Secure Email Gateways
- 402. **TrustArc Vendor Management:** Third-Party Risk Management
- 403. **Trustwave:** Network Security, SIEM, Incident Response Platforms
- 404. **Untangle (Arista):** Network Security
- 405. **UpGuard:** Third-Party Risk Management
- 406. **Vade Secure:** Secure Email Gateways
- 407. **Varonis:** Data Loss Prevention (DLP), Insider Threat Detection, Behavioral Analytics
- 408. **VeraCrypt:** Encryption
- 409. **Versa Networks:** Network Security, Cloud Security
- 410. **VidyoConnect for Telehealth:** Telehealth Security
- 411. **Virtru:** Encryption, Secure Email Gateways
- 412. **VMware Workspace ONE:** Mobile Device Management (MDM), Unified Endpoint Management (UEM)
- 413. **VMware Zero Trust Solutions:** Zero Trust Architecture
- 414. **Vocalcom:** Secure Messaging Platforms
- 415. **Vocera Communications:** Secure Messaging Platforms
- 416. **Vormetric:** Encryption, Data Loss Prevention (DLP)
- 417. **Voalte (by Hillrom):** Secure Messaging Platforms
- 418. **Wallix Bastion:** Privileged Access Management (PAM)
- 419. **WatchGuard:** Network Security
- 420. **Webroot Security Awareness Training:** Security Awareness Training
- 421. **Wickr (AWS):** Secure Messaging Platforms
- 422. **WinMagic SecureDoc:** Encryption
- 423. **Wombat Security (Proofpoint):** Security Awareness Training
- 424. **X-Ways Forensics:** Forensic Analysis Tools
- 425. **Yubico YubiKey:** Multi-Factor Authentication (MFA)
- 426. **Zinc Secure Messaging:** Secure Messaging Platforms
- 427. **Zix Email Encryption:** Secure Email Gateways

- 428. **Zscaler:** Network Security, Cloud Security, Zero Trust Architecture, IoT/IoMT Security
- 429. **Zscaler Cloud Security:** Cloud Security
- 430. **Zscaler Zero Trust:** Zero Trust Architecture
- 431. **Zscaler IoT Security:** IoT/IoMT Security



Comprehensive Coverage of 70 Cybersecurity Tool Categories and Functionalities for Healthcare Strategies



1. Identity and Access Management (IAM)

IAM tools ensure that only authorized individuals can access sensitive healthcare systems and data, reducing insider threats and external breaches. These tools enforce multi-factor authentication (MFA), single sign-on (SSO), and role-based access control, ensuring appropriate access levels based on user roles. They also help monitor and log access activities, providing audit trails for compliance with HIPAA and GDPR. By implementing IAM, healthcare organizations can mitigate unauthorized data access risks, improve operational efficiency, and maintain regulatory compliance.

Available Healthcare Cybersecurity Tools:

- **Okta:** Provides SSO and MFA to streamline secure user access.
- **Ping Identity:** Focuses on adaptive authentication and intelligent access.
- **Imprivata:** Tailored for healthcare, offering fast and secure clinician access.
- **SailPoint:** Automates access provisioning and ensures compliance.

2. Endpoint Detection and Response (EDR)

EDR tools provide real-time monitoring, detection, and response capabilities for devices like workstations, laptops, and servers. They leverage behavioral analytics and machine learning to identify suspicious activities, such as ransomware attempts or unauthorized data transfers. With automated threat mitigation, EDR tools isolate infected endpoints to prevent the spread of malware. These capabilities are critical for healthcare providers to protect patient data and ensure uninterrupted access to critical systems.

Available Healthcare Cybersecurity Tools:

- **CrowdStrike:** Cloud-based threat detection with AI-powered analytics.
- **SentinelOne:** Autonomous endpoint protection with real-time remediation.
- **Carbon Black:** Focuses on advanced threat detection and incident response.
- **Sophos:** Combines endpoint protection with cloud-based threat intelligence.

3. Network Security

Network security tools protect healthcare networks from external threats like phishing, DDoS attacks, and unauthorized access. These tools include firewalls, intrusion detection/prevention systems (IDS/IPS), and VPNs to secure data transmission. By inspecting traffic, enforcing security policies, and blocking malicious activities, they safeguard the sensitive information exchanged across hospital networks, clinics, and payer systems. Enhanced network security ensures continuity of healthcare operations and patient trust.

Available Healthcare Cybersecurity Tools:

- **Palo Alto Networks:** Offers next-generation firewalls and AI-powered threat prevention.
- **Fortinet:** Provides integrated solutions, including firewalls and secure VPNs.
- **Cisco Secure:** Delivers network visibility and malware protection.
- **Check Point Software:** Focuses on advanced threat prevention for healthcare networks.

4. Data Loss Prevention (DLP)

DLP tools prevent unauthorized data access, transfer, or leakage of sensitive patient and organizational data. These tools monitor data at rest, in transit, and in use, applying encryption and access controls to protect against breaches. DLP is particularly crucial for healthcare providers to safeguard PHI and comply with regulatory standards. By implementing DLP, organizations can prevent accidental or malicious data exfiltration and ensure compliance with HIPAA and GDPR.

Available Healthcare Cybersecurity Tools:

- **Symantec DLP:** Monitors and protects data across endpoints and networks.
- **Forcepoint:** Focuses on content and behavioral analysis for risk mitigation.
- **Digital Guardian:** Offers data visibility and protection for endpoints and cloud services.
- **McAfee Total Protection for DLP:** Provides real-time data tracking and protection.

5. Encryption

Encryption tools ensure that data is securely encoded, protecting it from unauthorized access during storage or transmission. These tools are essential for securing patient records, financial transactions, and communications across healthcare organizations. With robust encryption standards, such as AES-256, they enable safe data sharing between providers, payers, and patients. Encryption helps healthcare organizations achieve regulatory compliance while safeguarding data integrity and confidentiality.

Available Healthcare Cybersecurity Tools:

- **Thales Group:** Offers hardware security modules and data encryption solutions.
- **Virtu:** Provides email and file encryption with easy sharing controls.
- **Sophos Encryption:** Ensures data security across devices and cloud platforms.
- **Microsoft BitLocker:** Encrypts full drives to protect data from physical theft.

6. Security Information and Event Management (SIEM)

SIEM tools collect, analyze, and correlate security logs from multiple systems, providing a centralized platform for threat detection and response. They use advanced analytics to detect anomalies and alert IT teams to potential breaches. SIEM solutions support compliance by maintaining detailed audit trails and generating reports for regulatory bodies. In healthcare, they help protect critical systems from threats while enabling rapid incident response.

Available Healthcare Cybersecurity Tools:

- **Splunk:** Provides advanced threat detection and operational intelligence.
- **IBM QRadar:** Automates threat detection and compliance management.
- **LogRhythm:** Offers real-time security event monitoring and response.
- **Microsoft Azure Sentinel:** A cloud-native SIEM with AI-driven analytics.

7. Zero Trust Architecture

Zero Trust Architecture (ZTA) ensures that every access request is verified, regardless of origin, adhering to the principle of "never trust, always verify." ZTA tools enforce strict identity verification and least-privilege access policies. They also monitor user activities and device health, dynamically adjusting permissions based on risk. In healthcare, ZTA ensures secure access to EHR systems and patient data while reducing insider and external threats.



AvailableHealthcare Cybersecurity Tools:

- **Okta:** Provides identity verification for Zero Trust strategies.
- **Zscaler:** Offers secure access to cloud applications and data.
- **Cisco Zero Trust:** Focuses on securing endpoints, users, and applications.
- **Microsoft Zero Trust Solutions:** Integrates identity, access, and threat protection.

8. Cloud Security

Cloud security tools protect healthcare applications and data hosted on cloud platforms, mitigating risks like unauthorized access, misconfigurations, and data breaches. These tools include workload protection, encryption, and continuous monitoring to ensure data security in multi-cloud environments. By leveraging cloud security, healthcare providers can safely adopt cloud-based EHR systems, telehealth platforms, and collaborative tools. Enhanced cloud security also enables compliance with healthcare regulations.

AvailableHealthcare Cybersecurity Tools:

- **Amazon Web Services (AWS) Security:** Offers end-to-end security for AWS workloads.
- **Microsoft Azure Security:** Integrates identity management, encryption, and threat analytics.
- **Google Cloud Security:** Focuses on protecting healthcare data through advanced AI tools.
- **Palo Alto Prisma Cloud:** Provides visibility and compliance tools for cloud applications.

9. IoT/IoMT Security

IoT/IoMT (Internet of Medical Things) security tools protect connected medical devices, such as wearable monitors, infusion pumps, and imaging systems, from cyber threats. These tools provide visibility into connected devices, assess vulnerabilities, and ensure proper device configurations. They also detect anomalous behavior, such as unauthorized communication or data exfiltration, to mitigate potential breaches. By securing IoT/IoMT devices, healthcare providers ensure the safety of patient data and uninterrupted operation of critical medical equipment.

AvailableHealthcare Cybersecurity Tools:

- **Armis:** Offers comprehensive device visibility and threat detection for healthcare environments.

- **Medigate (Claroty):** Focuses on securing IoMT devices through network segmentation and monitoring.
- **Palo Alto IoT Security:** Uses machine learning to detect device vulnerabilities and enforce policies.
- **CyberMDX:** Specializes in protecting connected medical devices and clinical networks.

10. Ransomware Protection and Recovery

Ransomware protection tools prevent, detect, and recover from ransomware attacks, which remain one of the most significant threats to healthcare systems. These tools use advanced threat intelligence, automated backups, and rapid response capabilities to minimize downtime and data loss. They also include endpoint and network-level defenses to stop ransomware before it can spread. For healthcare, effective ransomware solutions ensure continuity of patient care and prevent sensitive data breaches.

Available Healthcare Cybersecurity Tools:

- **Sophos Intercept X:** Combines behavioral analysis and AI for ransomware detection and prevention.
- **CrowdStrike Falcon:** Offers real-time threat monitoring and automated incident response.
- **Rubrik:** Provides immutable backups and instant recovery options to counter ransomware.
- **SentinelOne Singularity:** Delivers endpoint detection and response with rollback capabilities.

11. Secure Messaging Platforms

Secure messaging platforms facilitate encrypted communication between healthcare staff, ensuring patient data confidentiality. These tools comply with HIPAA and other privacy regulations by securing text messages, emails, and multimedia exchanges. They also provide audit trails and real-time messaging for efficient collaboration in hospitals, clinics, and remote settings. Secure messaging ensures that sensitive patient data remains protected while enabling seamless communication among care teams.

Available Healthcare Cybersecurity Tools:

- **TigerConnect:** Provides secure, HIPAA-compliant messaging for healthcare teams.
- **Imprivata Cortex:** Focuses on clinical workflows with secure messaging and authentication.

- **Vocera Communications:** Enhances real-time communication for clinical teams in high-pressure environments.
- **Spok:** Integrates secure messaging with critical alert delivery.

12. Threat Intelligence Platforms

Threat intelligence platforms provide real-time information on cyber threats, enabling healthcare organizations to stay ahead of attackers. These tools aggregate data from multiple sources, including malware analysis, threat feeds, and industry-specific insights, to identify emerging risks. They also help automate response workflows and prioritize vulnerabilities based on potential impact. For healthcare, threat intelligence tools protect against ransomware, phishing, and targeted attacks on critical infrastructure.

Available Healthcare Cybersecurity Tools:

- **Recorded Future:** Combines machine learning and human analysis to provide actionable threat insights.
- **FireEye Threat Intelligence (Trellix):** Focuses on advanced threat detection and response strategies.
- **Anomali:** Integrates threat intelligence with SIEM systems for a comprehensive security approach.
- **Cisco Talos:** Offers global threat insights and mitigates advanced threats.

13. Behavioral Analytics

Behavioral analytics tools monitor user and device activity to detect deviations from normal patterns that may indicate a security threat. These tools leverage AI and machine learning to identify anomalous behaviors, such as unauthorized access attempts or unusual data transfers. They also provide detailed visibility into user activities, supporting forensic investigations and compliance reporting. Behavioral analytics tools help healthcare organizations detect insider threats and enhance overall security posture.

Available Healthcare Cybersecurity Tools:

- **Darktrace:** Uses AI to identify behavioral anomalies and respond to threats in real-time.
- **Exabeam:** Focuses on user behavior analytics and automated threat detection.
- **Varonis:** Provides data-centric security by analyzing access patterns to sensitive information.

- **LogRhythm UEBA:** Integrates behavioral analytics into security event monitoring.

14. Mobile Device Management (MDM)

MDM tools secure mobile devices used in healthcare settings, such as smartphones, tablets, and laptops, ensuring compliance with security policies. These tools enable remote device management, encryption, and application control to protect sensitive data. They also support device tracking and remote wiping in case of loss or theft. MDM is essential for securing telehealth platforms and mobile access to EHR systems, reducing the risk of data breaches.

Available Healthcare Cybersecurity Tools:

- **VMware Workspace ONE:** Provides unified endpoint management and app security.
- **Jamf Pro:** Focuses on managing Apple devices in healthcare environments.
- **Microsoft Intune:** Offers device management and conditional access policies.
- **BlackBerry UEM:** Specializes in securing mobile communications and healthcare workflows.

15. Vulnerability Management

Vulnerability management tools identify, assess, and remediate security weaknesses across IT systems and devices. These tools scan networks, endpoints, and applications for vulnerabilities and prioritize remediation efforts based on risk. They also provide actionable insights to prevent exploitation of known vulnerabilities. For healthcare providers, vulnerability management ensures the protection of critical systems, such as EHR platforms, medical devices, and patient data.

Available Healthcare Cybersecurity Tools:

- **Tenable:** Offers comprehensive vulnerability scanning and risk prioritization.
- **Qualys:** Focuses on cloud-based vulnerability management for hybrid environments.
- **Rapid7 InsightVM:** Delivers real-time vulnerability insights and remediation tracking.
- **Ivanti Neurons:** Automates vulnerability discovery and patch management.

16. Privileged Access Management (PAM)

PAM tools control and monitor access to sensitive systems and data, ensuring that privileged accounts are used securely. These tools enforce least-privilege policies, provide session monitoring, and secure credentials in encrypted vaults. PAM solutions also offer automated workflows for access approval and revocation, reducing insider and external threats. In healthcare, PAM tools protect administrative access to EHR systems, databases, and critical infrastructure.

Available Healthcare Cybersecurity Tools:

- **CyberArk:** Specializes in privileged account security and session management.
- **BeyondTrust:** Focuses on endpoint and privileged access management for healthcare.
- **Thycotic (Delinea):** Provides user-friendly PAM solutions for rapid implementation.
- **ManageEngine PAM360:** Delivers integrated PAM for hybrid healthcare environments.

17. Multi-Factor Authentication (MFA)

MFA tools add an extra layer of security by requiring users to provide multiple forms of verification before gaining access to healthcare systems. This typically involves something the user knows (password), something they have (a mobile device or security token), and sometimes something they are (biometric authentication). MFA significantly reduces the risk of unauthorized access caused by stolen or compromised credentials. In healthcare, MFA ensures that access to EHR systems, patient portals, and administrative platforms remains secure, even if primary login credentials are breached.

Available Healthcare Cybersecurity Tools:

- **Duo Security (Cisco):** Provides flexible MFA solutions, including biometrics and push notifications.
- **Okta MFA:** Offers adaptive authentication with dynamic risk assessment.
- **RSA SecurID:** Uses hardware tokens and biometrics for robust authentication.
- **Google Authenticator:** A simple, widely used tool for time-based one-time passwords (TOTP).

18. Secure Email Gateways

Secure email gateways protect healthcare organizations from email-based threats such as phishing, ransomware, and spam. These tools scan incoming and outgoing emails for malicious content, enforce encryption, and ensure compliance with regulations like HIPAA. Advanced solutions include sandboxing, machine learning, and real-time threat intelligence to detect sophisticated attacks. For healthcare providers and payers, secure email gateways protect patient communications and prevent breaches that could lead to significant fines and reputational damage.

Available Healthcare Cybersecurity Tools:

- **Proofpoint Email Protection:** Offers advanced phishing and malware detection.
- **Mimecast Secure Email Gateway:** Focuses on email continuity and protection.
- **Barracuda Email Security Gateway:** Provides encryption, spam filtering, and data loss prevention.
- **Cisco Secure Email:** Delivers end-to-end email security with advanced threat protection.

19. Blockchain for Data Security

Blockchain tools enhance data security by creating immutable records that are tamper-proof and verifiable. These tools are increasingly used in healthcare for secure patient data sharing, drug supply chain tracking, and interoperability across systems. Blockchain ensures that data is accessible only to authorized parties, with a transparent log of all transactions. For healthcare organizations, blockchain technology enhances trust, reduces fraud, and ensures compliance with data protection regulations.

Available Healthcare Cybersecurity Tools:

- **Guardtime:** Offers blockchain solutions for healthcare data integrity.
- **Hashed Health:** Focuses on secure healthcare data exchanges and credentialing.
- **Solve.Care:** Uses blockchain for transparent healthcare administration and payments.
- **MedRec:** A blockchain-based system for managing patient records securely.



20. Incident Response Platforms

Incident response platforms help healthcare organizations prepare for, detect, and recover from cyberattacks. These tools provide automated workflows, threat analysis, and real-time response capabilities to minimize damage during a security event. They also enable post-incident forensics to improve future security measures. Incident response platforms are crucial for healthcare providers to ensure rapid recovery from breaches and maintain patient care continuity.

Available Healthcare Cybersecurity Tools:

- **Palo Alto Cortex XSOAR:** Offers automated incident response and threat management.
- **IBM Security Resilient:** Focuses on orchestrating and streamlining incident response processes.
- **Splunk Phantom:** Provides automation and playbooks for fast and effective response.
- **Microsoft Sentinel Incident Response:** Combines AI and human expertise for coordinated incident handling.

21. Security Awareness Training

Security awareness training tools educate healthcare staff on recognizing and responding to cybersecurity threats such as phishing, social engineering, and ransomware. These programs use interactive modules, simulated attacks, and ongoing assessments to reinforce best practices. By fostering a culture of security, these tools reduce human error, which is a leading cause of breaches in healthcare. For providers and payers, security awareness training ensures compliance with regulatory requirements and strengthens overall security posture.

Available Healthcare Cybersecurity Tools:

- **KnowBe4:** Offers customizable training programs and simulated phishing tests.
- **Proofpoint Security Awareness Training:** Combines threat intelligence with tailored education.
- **Mimecast Awareness Training:** Focuses on reducing risky behaviors in employees.
- **SANS Security Awareness:** Provides industry-recognized training modules for healthcare.

22. Forensic Analysis Tools

Forensic analysis tools support healthcare organizations in investigating and understanding cybersecurity incidents. These tools collect and analyze digital evidence, reconstruct events, and identify root causes. They also provide detailed reports for legal and compliance purposes. In healthcare, forensic tools are critical for addressing breaches, ensuring accountability, and implementing effective corrective measures.

Available Healthcare Cybersecurity Tools:

- **EnCase (OpenText):** Offers comprehensive digital forensics for breach investigations.
- **Magnet AXIOM:** Focuses on endpoint and cloud-based forensic analysis.
- **FTK (Forensic Toolkit):** Provides advanced evidence processing and reporting capabilities.
- **Cellebrite:** Specializes in mobile device forensics for healthcare security incidents.

23. Patch Management Systems

Patch management systems automate the process of identifying and deploying updates to software and hardware, ensuring vulnerabilities are addressed promptly. These tools minimize risks by keeping systems up-to-date and secure from exploits. For healthcare providers, timely patch management protects critical systems, such as EHRs and connected medical devices, from emerging threats. Automated patching reduces manual effort, ensuring compliance with security policies and regulatory standards.

Available Healthcare Cybersecurity Tools:

- **Ivanti Patch Management:** Automates patch deployment for endpoints and servers.
- **ManageEngine Patch Manager Plus:** Provides multi-platform patching with compliance reporting.
- **SolarWinds Patch Manager:** Focuses on patch management for Windows environments.
- **Qualys Patch Management:** Integrates vulnerability scanning with patch deployment.



24. Third-Party Risk Management

Third-party risk management tools assess and mitigate risks associated with vendors and partners who access healthcare systems or data. These tools provide vendor risk scoring, compliance tracking, and continuous monitoring to ensure third-party security. For healthcare organizations, managing third-party risks is essential to protect patient data and maintain regulatory compliance. These tools reduce the likelihood of breaches originating from vulnerabilities in third-party systems.

Available Healthcare Cybersecurity Tools:

- **Prevalent:** Offers automated vendor risk assessments and continuous monitoring.
- **BitSight:** Provides cybersecurity ratings for third-party risk evaluation.
- **RiskRecon (Mastercard):** Focuses on vendor risk profiling and real-time monitoring.
- **OneTrust Vendorpedia:** Streamlines third-party risk assessments and compliance management.

25. Telehealth Security

Telehealth security tools protect virtual healthcare services by securing video consultations, patient portals, and data exchanges. These tools use encryption, authentication, and secure communication protocols to ensure privacy and compliance. They also guard against threats like session hijacking and data breaches. For healthcare providers, telehealth security tools are vital for delivering safe and confidential virtual care to patients.

Available Healthcare Cybersecurity Tools:

- **Teladoc Health:** Provides secure telehealth platforms with encrypted communication.
- **Zoom for Healthcare:** Offers HIPAA-compliant video conferencing solutions.
- **Doxy.me:** Specializes in secure, user-friendly telemedicine platforms.
- **Microsoft Teams for Healthcare:** Integrates collaboration and telehealth capabilities with enterprise-grade security.

26. Vulnerability Scanning and Management

Vulnerability scanning and management tools identify and prioritize vulnerabilities in healthcare systems, networks, and applications. These tools use continuous scanning to uncover weaknesses, assess their severity, and provide actionable recommendations for remediation. By integrating with patch management systems, they ensure prompt resolution of vulnerabilities, reducing the attack surface. In healthcare, these tools are critical for protecting sensitive patient data and maintaining compliance with regulations like HIPAA and GDPR.

Available Healthcare Cybersecurity Tools:

- **Tenable:** Offers advanced scanning and risk prioritization with a focus on healthcare applications.
- **Qualys:** Provides continuous monitoring and automated remediation suggestions.
- **Rapid7 InsightVM:** Combines asset discovery with real-time vulnerability tracking.
- **F-Secure Radar:** Specializes in vulnerability detection for network and endpoint devices.

27. Privileged Identity Management (PIM)

Privileged identity management (PIM) tools secure and monitor the use of privileged accounts, which have elevated access to critical healthcare systems. These tools enforce least-privilege access policies, manage credentials in encrypted vaults, and monitor privileged session activities in real-time. They also provide automated workflows for access approvals and revocations, reducing the risk of insider threats and credential misuse. For healthcare, PIM ensures secure administration of EHR systems, databases, and IT infrastructure.

Available Healthcare Cybersecurity Tools:

- **CyberArk Privileged Identity Management:** Offers robust access controls and session monitoring.
- **BeyondTrust PIM:** Focuses on privileged access and endpoint security integration.
- **Thycotic Secret Server:** Delivers secure storage and automated credential rotation.
- **Saviynt PIM:** Provides advanced analytics to identify and mitigate privilege misuse.



28. Endpoint Encryption

Endpoint encryption tools protect sensitive data on devices such as laptops, tablets, and desktops by encrypting files and storage drives. These tools prevent unauthorized access to data, even if devices are lost or stolen. Endpoint encryption also includes features like remote wiping and encryption key management to enhance security. In healthcare, endpoint encryption ensures compliance with regulations and protects PHI stored on portable devices used in telehealth and mobile care.

Available Healthcare Cybersecurity Tools:

- **Sophos Encryption:** Provides full-disk and file-level encryption with central management.
- **Microsoft BitLocker:** Secures data on Windows devices with hardware-based encryption.
- **ESET Endpoint Encryption:** Offers flexible encryption options for files, emails, and drives.
- **Thales Endpoint Encryption:** Focuses on encryption key management and regulatory compliance.

29. Security Orchestration, Automation, and Response (SOAR)

SOAR tools streamline incident response by automating repetitive security tasks and orchestrating workflows across tools. They integrate with existing cybersecurity solutions like SIEM, threat intelligence, and endpoint protection to enhance threat detection and remediation. By reducing response times and providing playbooks for common scenarios, SOAR tools improve healthcare organizations' ability to mitigate threats. These tools are essential for managing complex healthcare IT environments with limited security resources.

Available Healthcare Cybersecurity Tools:

- **Palo Alto Cortex XSOAR:** Offers playbooks and automation for threat management.
- **IBM Resilient SOAR:** Focuses on coordinating incident response across security tools.
- **Splunk Phantom:** Provides extensive integrations and visual workflow automation.
- **Fortinet FortiSOAR:** Delivers customizable automation and real-time incident management.

30. Insider Threat Detection

Insider threat detection tools monitor user behavior and system activities to identify risks posed by employees, contractors, or third-party vendors. These tools use behavioral analytics and machine learning to detect unusual patterns, such as unauthorized data access or policy violations. They provide actionable insights and alerts to mitigate potential breaches caused by negligence or malicious intent. In healthcare, insider threat detection helps protect sensitive patient data and prevent accidental or intentional data misuse.

Available Healthcare Cybersecurity Tools:

- **Varonis:** Focuses on monitoring file access and permissions to prevent data misuse.
- **ObserveIT (Proofpoint):** Provides user behavior tracking and session recording for risk mitigation.
- **Securonix UEBA:** Uses advanced analytics to detect insider threats and anomalies.
- **Exabeam Insider Threat Detection:** Integrates with SIEM tools to enhance threat detection.

31. Threat Hunting Platforms

Threat hunting platforms proactively search for undetected threats within an organization's network and systems. These tools use advanced analytics, threat intelligence, and behavioral patterns to uncover potential risks that traditional defenses might miss. They also support investigation and root-cause analysis to improve overall security posture. In healthcare, threat hunting platforms ensure that advanced persistent threats (APTs) targeting critical infrastructure are identified and mitigated.

Available Healthcare Cybersecurity Tools:

- **CrowdStrike Falcon:** Provides AI-driven threat hunting and incident response.
- **FireEye Helix (Trellix):** Offers integrated threat detection and forensics capabilities.
- **Darktrace:** Uses machine learning to detect hidden threats in real-time.
- **Elastic Security:** Focuses on threat visibility and anomaly detection for healthcare environments.

32. Remote Access Security

Remote access security tools ensure secure connections for healthcare staff accessing systems from outside the organization. These tools include virtual private networks (VPNs), zero trust network access (ZTNA), and multi-factor authentication to verify user identities. They also monitor remote sessions for suspicious activities and enforce access control policies. With the rise of telehealth and remote work, these tools are critical for securing access to EHR systems, telemedicine platforms, and administrative networks.

Available Healthcare Cybersecurity Tools:

- **Cisco AnyConnect:** Provides secure remote access with integrated endpoint protection.
- **Palo Alto Prisma Access:** Offers cloud-based secure access for remote healthcare workers.
- **Zscaler Private Access:** Focuses on zero trust security for remote connections.
- **Fortinet FortiClient:** Combines VPN access with endpoint protection.

33. Biometric Security

Biometric security tools use unique physical or behavioral characteristics, such as fingerprints, facial recognition, or voice patterns, to authenticate users. These tools provide an additional layer of security by ensuring that only authorized individuals can access systems or data. They are particularly effective in healthcare environments, where quick yet secure authentication is critical for clinicians accessing patient records or medical devices. Biometric security reduces the risk of credential theft and enhances overall access control.

Available Healthcare Cybersecurity Tools:

- **HID Global Biometrics:** Offers multimodal biometric authentication for healthcare applications.
- **Imprivata OneSign:** Provides biometric login solutions tailored for healthcare environments.
- **Aware Biometrics:** Focuses on scalable biometric authentication for secure healthcare access.
- **NEC NeoFace:** Specializes in facial recognition for access management and surveillance.

34. Application Security

Application security tools protect healthcare software, such as EHR systems, patient portals, and telehealth platforms, from vulnerabilities and attacks. These tools scan for coding flaws, misconfigurations, and security gaps during development and deployment. They also provide runtime protection, blocking attacks like SQL injection and cross-site scripting (XSS). In healthcare, application security ensures that critical software remains secure against breaches, maintaining patient data confidentiality and system availability.

Available Healthcare Cybersecurity Tools:

- **Veracode:** Offers static and dynamic application security testing to identify vulnerabilities.
- **Checkmarx:** Provides secure coding tools and continuous application security scanning.
- **WhiteHat Security:** Focuses on application vulnerability detection and remediation.
- **Synopsys Coverity:** Automates software testing and security flaw detection for healthcare applications.

35. Threat Deception Platforms

Threat deception platforms deploy decoys, honeypots, and traps to detect and distract attackers. These tools mimic real systems and data to lure cybercriminals away from critical assets while gathering intelligence on their tactics. Threat deception helps healthcare organizations identify and mitigate threats early, minimizing the impact of cyberattacks. By adding layers of fake infrastructure, these tools increase the cost and complexity of attacks for adversaries.

Available Healthcare Cybersecurity Tools:

- **TrapX Security:** Focuses on healthcare-specific deception technologies, such as fake medical devices.
- **Attivo Networks:** Provides endpoint and network deception solutions for proactive threat detection.
- **Illusive Networks:** Creates deceptive environments to identify attackers' movements.
- **Acalvio ShadowPlex:** Integrates with security ecosystems for enhanced deception strategies.



36. Managed Detection and Response (MDR)

MDR services combine human expertise with advanced technology to monitor and respond to cyber threats in real-time. These services offer continuous threat detection, investigation, and remediation, tailored to healthcare organizations with limited internal cybersecurity resources. MDR providers deliver actionable insights and rapid incident response to minimize the impact of breaches. For healthcare, MDR ensures constant protection of sensitive data and critical systems.

Available Healthcare Cybersecurity Tools:

- **Arctic Wolf:** Provides 24/7 threat detection and response with a dedicated security team.
- **Secureworks Taegis:** Offers comprehensive MDR services for healthcare environments.
- **Rapid7 MDR:** Combines technology and expertise for advanced threat management.
- **Cynet 360 AutoXDR:** Automates detection and response workflows with built-in MDR capabilities.

37. Compliance Management

Compliance management tools help healthcare organizations adhere to regulatory frameworks like HIPAA, GDPR, and PCI DSS. These tools monitor data access, enforce policies, and provide detailed reports for audits. They also offer automated workflows for risk assessments and compliance gap remediation. Compliance management tools reduce the risk of fines, legal issues, and reputational damage while ensuring patient data protection.

Available Healthcare Cybersecurity Tools:

- **OneTrust:** Automates privacy and compliance workflows for healthcare organizations.
- **LogicGate:** Provides customizable solutions for regulatory compliance management.
- **Netwrix Auditor:** Focuses on data access visibility and compliance reporting.
- **TrustArc:** Helps healthcare organizations streamline data privacy compliance processes.

38. Identity Governance and Administration (IGA)

IGA tools manage user identities, access rights, and roles across healthcare organizations. These tools automate user provisioning, de-provisioning, and access reviews to ensure that only authorized personnel can access sensitive data. They also provide visibility into user activities and compliance reporting. In healthcare, IGA supports secure access to EHR systems and protects patient data from unauthorized use.

AvailableHealthcare Cybersecurity Tools:

- **SailPoint IdentityNow:** Offers identity lifecycle management and access certification.
- **Saviynt IGA:** Integrates identity governance with application security.
- **IBM Security Identity Governance:** Focuses on managing access and mitigating identity risks.
- **Microsoft Azure AD Governance:** Provides automated identity management for cloud environments.

39. Backup and Disaster Recovery

Backup and disaster recovery tools protect healthcare organizations against data loss caused by cyberattacks, natural disasters, or hardware failures. These tools ensure that data is regularly backed up, encrypted, and stored securely, with options for rapid restoration. They also include features like snapshot recovery and continuous data replication to minimize downtime. For healthcare, robust backup and disaster recovery systems are essential to maintain uninterrupted patient care and compliance with data retention policies.

AvailableHealthcare Cybersecurity Tools:

- **Veeam Backup & Replication:** Offers fast and reliable data recovery for healthcare organizations.
- **Rubrik:** Provides cloud-based backup and ransomware recovery solutions.
- **Commvault Complete Backup:** Focuses on data protection and recovery for hybrid environments.
- **Acronis Cyber Protect:** Combines backup with integrated cybersecurity features.

40. Endpoint Privilege Management (EPM)

EPM tools enforce least-privilege policies on endpoints, ensuring that users and applications have access only to the resources they need. These tools remove admin rights from endpoints, reducing the risk of malware execution and privilege escalation attacks. EPM solutions also provide granular control over application execution and privilege elevation requests. In healthcare, EPM ensures secure endpoint management, protecting devices used for accessing patient records and critical systems.

AvailableHealthcare Cybersecurity Tools:

- **BeyondTrust Endpoint Privilege Management:** Offers seamless privilege elevation and endpoint security.
- **CyberArk Endpoint Privilege Manager:** Focuses on reducing endpoint attack surfaces.
- **Thycotic Privilege Manager:** Provides flexible policies for managing endpoint privileges.
- **Ivanti EPM:** Combines privilege management with automated patching for endpoint protection.

41. Secure File Sharing

Secure file-sharing tools enable encrypted transmission of sensitive healthcare data between providers, patients, and payers. These tools include access controls, activity tracking, and data expiration features to prevent unauthorized access. They also support compliance by maintaining audit logs and enforcing encryption standards. Secure file-sharing ensures that patient data, such as medical reports and imaging results, remains protected during exchanges.

Available Healthcare Cybersecurity Tools:

- **Boxcryptor:** Encrypts files stored in cloud services for secure sharing.
- **Citrix ShareFile:** Provides secure file sharing with granular access controls.
- **Egnyte:** Combines secure file-sharing with compliance reporting.
- **Virtu:** Adds end-to-end encryption to email attachments and shared files.

42. Cyber Resilience Platforms

Cyber resilience platforms help healthcare organizations prepare for, withstand, and recover from cyberattacks. These tools integrate threat detection, incident response, and business continuity planning to ensure minimal disruption during an attack. They also include features like automated playbooks and resilience testing to improve preparedness. Cyber resilience platforms enable healthcare providers to maintain operations and protect patient safety even during large-scale incidents.

Available Healthcare Cybersecurity Tools:

- **Symantec Cyber Resilience Platform:** Combines endpoint security with backup and disaster recovery.
- **Trend Micro Vision One:** Focuses on threat detection and incident response for resilience.

- **Microsoft Defender for Endpoint:** Provides end-to-end protection and recovery capabilities.
- **Fortinet Cyber Resilience:** Integrates network security with resilience planning.

43. Micro-Segmentation Tools

Micro-segmentation tools enhance network security by dividing networks into smaller, isolated segments to limit lateral movement during an attack. Each segment has its own security controls and access policies, ensuring that even if one segment is compromised, others remain secure. These tools are particularly useful in healthcare for protecting sensitive systems like EHRs, medical devices, and financial data from cross-contamination. Micro-segmentation helps organizations achieve Zero Trust by enforcing granular controls across their infrastructure.

Available Healthcare Cybersecurity Tools:

- **VMware NSX:** Provides software-defined micro-segmentation with automated policies.
- **Illumio Core:** Offers real-time application dependency mapping and segmentation.
- **Cisco Secure Workload:** Focuses on protecting applications and data with micro-segmentation.
- **Palo Alto Networks Prisma Cloud:** Integrates micro-segmentation with cloud security capabilities.

44. Secure DevOps (DevSecOps) Tools

DevSecOps tools integrate security into the software development lifecycle, ensuring that healthcare applications are built with security in mind from the outset. These tools automate vulnerability scanning, secure code analysis, and compliance checks during development and deployment. By embedding security into DevOps workflows, healthcare organizations can prevent vulnerabilities in applications like telehealth platforms and EHR systems. DevSecOps tools help accelerate software delivery without compromising on security.

Available Healthcare Cybersecurity Tools:

- **GitLab Security:** Provides built-in security testing for code repositories.
- **Snyk:** Focuses on identifying and fixing vulnerabilities in open-source dependencies.
- **Aqua Security:** Offers container security and runtime protection for DevOps environments.

- **Checkmarx Codebashing:** Provides secure coding education and integrated testing tools.

45. Real-Time Threat Analysis Tools

Real-time threat analysis tools monitor healthcare systems continuously to detect and respond to emerging threats. These tools use machine learning and behavioral analytics to identify anomalies and suspicious activities before they escalate. By correlating threat data across multiple sources, they provide actionable insights for rapid response. In healthcare, real-time threat analysis is crucial for protecting patient data and ensuring the uninterrupted operation of critical systems.

Available Healthcare Cybersecurity Tools:

- **Darktrace:** Uses AI to provide autonomous detection and response capabilities.
- **Splunk Enterprise Security:** Delivers real-time visibility into threats across healthcare environments.
- **Elastic Security:** Offers continuous monitoring and alerting for advanced threats.
- **FireEye Helix (Trellix):** Integrates intelligence-driven threat analysis with incident response.

46. Data Masking Tools

Data masking tools protect sensitive healthcare data by obfuscating it in non-production environments, such as during testing or training. These tools replace real data with fake, yet realistic, values to prevent unauthorized access or misuse. They ensure that patient data remains secure while enabling developers and analysts to work with representative datasets. Data masking is critical for maintaining HIPAA compliance and protecting sensitive information in healthcare workflows.

Available Healthcare Cybersecurity Tools:

- **Informatica Data Masking:** Automates data masking for on-premises and cloud environments.
- **Oracle Data Masking and Subsetting:** Protects sensitive data in large-scale databases.
- **Delphix Masking:** Focuses on secure data provisioning for testing and development.
- **IBM Optim Data Privacy:** Provides dynamic and static data masking capabilities.

47. Mobile Application Security Tools

Mobile application security tools safeguard healthcare apps used by patients and providers for accessing medical records, telehealth, and appointment scheduling. These tools scan mobile apps for vulnerabilities, enforce encryption, and secure communications. They also include runtime application self-protection (RASP) to detect and block attacks in real time. For healthcare organizations, mobile app security ensures that patient-facing platforms are resilient to breaches and compliant with regulatory standards.

Available Healthcare Cybersecurity Tools:

- **Zimperium zIPS:** Focuses on mobile threat detection and application security.
- **AppDome:** Provides no-code mobile app security and fraud prevention.
- **Lookout Mobile Endpoint Security:** Protects mobile devices and apps with integrated threat intelligence.
- **NowSecure:** Specializes in vulnerability testing for healthcare mobile applications.

48. Phishing Protection Tools

Phishing protection tools identify and block malicious emails, websites, and messages designed to steal credentials or deploy malware. These tools analyze email headers, links, and attachments to detect phishing attempts and prevent them from reaching users. They also include training modules to help healthcare staff recognize phishing attacks. By reducing the risk of credential theft and malware infections, phishing protection tools play a key role in securing healthcare organizations.

Available Healthcare Cybersecurity Tools:

- **Proofpoint Phishing Protection:** Offers advanced threat detection and user awareness training.
- **Mimecast Targeted Threat Protection:** Focuses on email-based phishing and impersonation attacks.
- **Barracuda Sentinel:** Provides AI-driven phishing detection and response.
- **Cofense PhishMe:** Combines phishing simulation and training for healthcare staff.



49. Secure Access Service Edge (SASE) Solutions

SASE solutions combine network security and wide-area networking (WAN) into a unified, cloud-delivered service. These tools integrate technologies like secure web gateways, cloud access security brokers (CASBs), and Zero Trust network access (ZTNA) to provide secure and seamless connectivity. For healthcare organizations, SASE ensures secure access to cloud-based EHR systems, telehealth platforms, and patient data, regardless of the user's location.

Available Healthcare Cybersecurity Tools:

- **Zscaler SASE:** Offers cloud-native security with integrated threat protection.
- **Cisco Umbrella:** Combines DNS-layer security with secure remote access.
- **Netskope SASE:** Focuses on securing cloud applications and user activities.
- **Fortinet SASE:** Integrates network security with Zero Trust principles.

50. Data Governance Tools

Data governance tools enable healthcare organizations to manage, protect, and utilize their data effectively while ensuring compliance. These tools enforce policies for data access, quality, and retention, reducing the risk of breaches and regulatory violations. They also provide dashboards and reporting features to maintain visibility into data usage and compliance status. In healthcare, data governance tools help manage the vast amounts of sensitive information generated by EHRs, diagnostics, and telehealth services.

Available Healthcare Cybersecurity Tools:

- **Collibra Data Governance:** Provides a unified platform for data policy management.
- **Informatica Data Governance:** Focuses on automating governance workflows and data cataloging.
- **SAP Data Governance:** Integrates with enterprise systems for holistic data management.
- **Talend Data Governance:** Offers tools for data integration, quality, and compliance.

51. Cloud Access Security Brokers (CASB)

Cloud Access Security Brokers (CASB) tools provide visibility and control over the use of cloud-based applications and services in healthcare organizations. These tools enforce security policies such as data encryption, access control, and user activity monitoring across cloud environments. CASBs also help identify shadow IT, where unauthorized applications may introduce risks. For healthcare, CASBs ensure compliance with data protection regulations while enabling secure adoption of cloud services like EHR systems and telehealth platforms.

Available Healthcare Cybersecurity Tools:

- **Netskope CASB:** Offers real-time data protection and threat detection for cloud services.
- **Microsoft Defender for Cloud Apps:** Integrates seamlessly with Microsoft Azure and Office 365 environments.
- **McAfee MVISION Cloud:** Focuses on securing sensitive data in SaaS applications.
- **Forcepoint CASB:** Provides deep visibility and control for healthcare cloud usage.

52. Unified Threat Management (UTM) Tools

Unified Threat Management (UTM) tools consolidate multiple security functions—such as firewalls, intrusion detection/prevention, VPNs, and antivirus—into a single platform. These tools simplify security management and provide comprehensive protection against various cyber threats. UTMs are particularly beneficial for smaller healthcare providers with limited IT resources, offering a cost-effective solution for safeguarding networks and systems. By centralizing security, UTMs reduce complexity and enhance threat visibility.

Available Healthcare Cybersecurity Tools:

- **Sophos XG Firewall:** Combines advanced threat protection with user-friendly management.
- **Fortinet FortiGate UTM:** Offers integrated security features with high performance.
- **Cisco Meraki MX:** Provides cloud-managed security for healthcare networks.
- **WatchGuard Firebox:** Focuses on multi-layered defense for small to mid-sized healthcare organizations.



53. Secure File Transfer Protocol (SFTP) Tools

Secure File Transfer Protocol (SFTP) tools ensure that sensitive healthcare data is transmitted securely between systems, providers, and payers. These tools use encryption to protect files during transfer and implement authentication mechanisms to verify user identities. SFTP is essential for exchanging large datasets, such as medical imaging files or insurance claims, without risking unauthorized access. By securing data transfers, these tools ensure compliance and prevent breaches.

Available Healthcare Cybersecurity Tools:

- **FileZilla Pro:** A user-friendly SFTP solution with encryption and transfer management.
- **SolarWinds Serv-U:** Offers enterprise-grade SFTP for healthcare data transfers.
- **GoAnywhere MFT:** Provides secure, automated file transfers with audit logging.
- **WS_FTP Professional:** Focuses on secure file sharing and advanced encryption features.

54. Privileged Session Management (PSM)

Privileged Session Management (PSM) tools monitor and record the activities of privileged users during their sessions on critical systems. These tools provide real-time oversight, ensuring that privileged accounts are not misused or exploited. PSM solutions also offer session replay capabilities for forensic investigations and compliance audits. In healthcare, PSM protects access to sensitive systems, such as databases containing patient records or financial data, by reducing the risk of insider threats.

Available Healthcare Cybersecurity Tools:

- **CyberArk PSM:** Offers session monitoring and risk mitigation for privileged users.
- **BeyondTrust Privileged Remote Access:** Provides secure access for vendors and IT administrators.
- **Wallix Bastion:** Focuses on real-time session oversight and recording for compliance.
- **One Identity Safeguard:** Integrates privileged session management with access controls.

55. Threat Simulation Platforms

Threat simulation platforms test the security posture of healthcare organizations by simulating real-world cyberattacks. These tools identify vulnerabilities, test incident response capabilities, and provide actionable recommendations for improvement. Threat simulations, such as phishing campaigns or ransomware attacks, prepare healthcare staff and systems to handle actual threats. By proactively identifying weaknesses, these platforms enhance organizational resilience and reduce the likelihood of successful attacks.

Available Healthcare Cybersecurity Tools:

- **AttackIQ:** Provides automated breach and attack simulations with actionable insights.
- **SafeBreach:** Focuses on continuous security validation for healthcare environments.
- **Cymulate:** Offers pre-configured simulations for phishing, ransomware, and data exfiltration.
- **Picus Security:** Integrates with existing security tools to validate effectiveness against threats.

56. Security Policy Management Tools

Security policy management tools help healthcare organizations define, implement, and enforce cybersecurity policies across their IT infrastructure. These tools provide centralized dashboards for monitoring policy compliance, automating rule updates, and detecting policy violations. They also ensure that security policies align with regulatory requirements like HIPAA and GDPR. By simplifying policy management, these tools reduce operational overhead and improve security posture.

Available Healthcare Cybersecurity Tools:

- **AlgoSec:** Automates policy management and compliance for complex environments.
- **Tufin:** Provides visibility and control over security policies across hybrid networks.
- **FireMon:** Focuses on continuous policy monitoring and optimization.
- **Skybox Security Policy Management:** Helps manage rules and configurations for healthcare firewalls and devices.

57. Security Ratings Platforms

Security ratings platforms evaluate and score the cybersecurity posture of healthcare organizations and their third-party vendors. These tools analyze public data, threat intelligence, and network configurations to identify potential vulnerabilities. Security ratings provide a benchmark for assessing risk levels and improving security practices. For healthcare, these tools help mitigate third-party risks and ensure vendor compliance with security standards.

Available Healthcare Cybersecurity Tools:

- **BitSight:** Provides detailed security ratings based on continuous risk assessment.
- **SecurityScorecard:** Offers real-time insights into organizational and vendor security posture.
- **RiskRecon:** Focuses on third-party risk assessments with detailed reporting.
- **Panorays:** Automates third-party risk evaluations with actionable recommendations.

58. File Integrity Monitoring (FIM) Tools

File Integrity Monitoring (FIM) tools track changes to critical files and directories, ensuring that unauthorized modifications are detected promptly. These tools generate alerts for suspicious activities, such as changes to patient records or financial documents, helping healthcare organizations respond quickly to potential breaches. FIM solutions also maintain audit logs for compliance reporting and forensic investigations. By protecting sensitive data, FIM tools reduce the risk of tampering and data loss.

Available Healthcare Cybersecurity Tools:

- **Tripwire File Integrity Manager:** Monitors changes to critical files and provides detailed reports.
- **ManageEngine Log360:** Integrates FIM with log management and compliance tracking.
- **SolarWinds Server Configuration Monitor:** Tracks file and system changes across healthcare servers.
- **OSSEC:** An open-source solution for file integrity monitoring and intrusion detection.

59. Cyber Risk Quantification (CRQ) Platforms

Cyber Risk Quantification (CRQ) platforms analyze the financial and operational impact of cybersecurity risks on healthcare organizations. These tools simulate attack scenarios, assess potential losses, and provide recommendations for risk mitigation. CRQ platforms help healthcare leaders prioritize investments in security measures by quantifying the return on investment (ROI). By understanding the financial implications of cyber risks, organizations can make informed decisions to protect critical assets.

Available Healthcare Cybersecurity Tools:

- **RiskLens:** Provides financial risk modeling for healthcare cybersecurity threats.
- **X-Analytics:** Focuses on quantifying the impact of cyber risks for executive decision-making.
- **Axio360:** Integrates risk assessment with financial impact analysis.
- **AIR Worldwide Cyber Risk Modeling:** Offers scenario-based modeling for large-scale cyber incidents.

60. Proactive Vulnerability Remediation Platforms

Proactive vulnerability remediation platforms identify, prioritize, and resolve vulnerabilities before they can be exploited. These tools integrate with vulnerability scanners, patch management systems, and threat intelligence feeds to automate remediation workflows. In healthcare, proactive remediation protects EHR systems, IoT devices, and critical infrastructure from exploitation. These platforms reduce the attack surface and ensure compliance with security standards.

Available Healthcare Cybersecurity Tools:

- **Tenable.io:** Provides proactive vulnerability assessments with real-time remediation guidance.
- **Rapid7 InsightVM:** Combines vulnerability scanning with actionable remediation insights.
- **Qualys Patch Management:** Automates the remediation process for detected vulnerabilities.
- **Ivanti Neurons for Patch Management:** Focuses on endpoint and server patching in healthcare environments.

61. AI-Powered Cybersecurity Tools

AI-powered cybersecurity tools use machine learning and artificial intelligence to detect, analyze, and respond to sophisticated threats. These tools identify patterns and anomalies in real-time, adapting to evolving attack methods. AI enhances incident response by automating threat prioritization, minimizing human error, and accelerating remediation. In healthcare, AI-powered solutions help protect dynamic environments like IoT medical devices, EHR systems, and telehealth platforms.

Available Healthcare Cybersecurity Tools:

- **Darktrace:** Provides self-learning AI to identify and neutralize threats autonomously.
- **Cynet 360:** Combines AI with endpoint and network security for comprehensive protection.
- **Fortinet FortiAI:** Focuses on AI-driven threat detection and response for healthcare networks.
- **Vectra AI:** Specializes in detecting hidden threats and insider activities.

62. Healthcare-Specific Security Suites

These tailored solutions address the unique cybersecurity challenges faced by healthcare providers and payers, including regulatory compliance and safeguarding patient data. They integrate tools like endpoint protection, secure messaging, and compliance reporting into a unified platform. Healthcare-specific security suites simplify deployment and management, ensuring a secure and compliant operational environment.

Available Healthcare Cybersecurity Tools:

- **Imprivata Secure Suite:** Combines identity, access, and endpoint protection for clinicians.
- **HealthCast SecureVue:** Focuses on access management and session monitoring for healthcare workflows.
- **Spok Care Connect:** Offers secure messaging and alert systems tailored to healthcare needs.
- **Protenus Privacy:** Provides patient data monitoring and HIPAA compliance tracking.

63. Physical Security Integration Tools

These tools combine physical and cybersecurity measures to protect healthcare facilities, equipment, and data. They integrate video surveillance, badge access systems, and IoT monitoring with cybersecurity dashboards, enabling unified threat management. Physical security integration ensures that both digital and physical assets are secured against breaches or tampering.

AvailableHealthcare Cybersecurity Tools:

- **Genetec Security Center:** Combines physical access control with cybersecurity analytics.
- **LenelS2:** Integrates physical and logical security systems for healthcare environments.
- **Avigilon:** Offers video analytics integrated with network security tools.
- **Honeywell Pro-Watch:** Provides centralized management of physical and cybersecurity systems.

64. Compliance-Driven Data Archiving

Compliance-driven data archiving tools securely store healthcare data for long-term retention, ensuring it remains accessible for audits and legal purposes. These tools use encryption and access controls to protect archived data from breaches. They also support healthcare regulations by automating data lifecycle management, including secure disposal after retention periods.

AvailableHealthcare Cybersecurity Tools:

- **Mimecast Archiving:** Offers secure, compliant archiving for email and files.
- **Barracuda Message Archiver:** Provides scalable storage for long-term email archiving.
- **Proofpoint Enterprise Archive:** Focuses on regulatory compliance and eDiscovery.
- **Dell EMC Isilon:** Delivers scalable, compliant storage for healthcare data.

65. Social Engineering Prevention Tools

These tools focus on mitigating risks from phishing, pretexting, and other social engineering attacks. They combine simulation training, real-time email scanning, and behavioral analytics to identify and neutralize threats. In healthcare, social engineering prevention is critical for protecting staff who may be targeted to gain access to sensitive data or systems.

AvailableHealthcare Cybersecurity Tools:

- **KnowBe4 Phishing Simulation:** Provides realistic phishing tests and employee training.
- **Barracuda Sentinel:** Detects and blocks impersonation attempts in real-time.
- **Cofense Triage:** Automates the analysis and response to phishing attacks reported by users.
- **PhishLabs:** Focuses on training and active threat detection for healthcare staff.

66. Secure Collaboration Platforms

Secure collaboration platforms ensure that healthcare teams can share information and work together without risking data breaches. These tools encrypt communications, provide role-based access, and support compliance with HIPAA and other standards. They are essential for telehealth, interdisciplinary care coordination, and administrative workflows.

Available Healthcare Cybersecurity Tools:

- **Microsoft Teams (Healthcare Edition):** Offers secure video calls, messaging, and file sharing.
- **Zoom for Healthcare:** Provides HIPAA-compliant video conferencing for telemedicine.
- **Cisco Webex for Healthcare:** Delivers secure collaboration tools with data protection.
- **Doxy.me:** Specializes in secure telehealth communications for patient care.

67. Cybersecurity Awareness Gamification

Gamification tools make security awareness training more engaging and effective by incorporating interactive elements like quizzes, challenges, and simulations. These tools help healthcare staff understand cybersecurity threats, recognize phishing attempts, and adopt best practices. By fostering a culture of security, these tools reduce the risk of human error, which is a leading cause of breaches.

Available Healthcare Cybersecurity Tools:

- **CyberVista:** Combines interactive training with personalized learning paths.
- **Wombat Security (Proofpoint):** Offers gamified security awareness training.
- **Habitu8:** Focuses on engaging content and real-world scenarios for healthcare staff.
- **MetaCompliance:** Provides gamified training modules tailored to healthcare environments.

68. API Security Tools

API security tools protect the interfaces that enable communication between healthcare systems, such as EHRs, patient portals, and third-party applications. These tools monitor API traffic, enforce authentication, and detect anomalies to prevent unauthorized access or data leakage. Securing APIs is essential for maintaining interoperability while protecting patient data.

Available Healthcare Cybersecurity Tools:

- **Salt Security:** Focuses on real-time API protection and threat detection.
- **Imperva API Security:** Provides advanced protection for healthcare APIs.
- **Cequence Security:** Uses AI to prevent API abuse and data exfiltration.
- **Traceable AI:** Specializes in API visibility and behavioral analysis for healthcare applications.

69. Network Forensics Tools

Network forensics tools capture and analyze network traffic to investigate and respond to cyber incidents. These tools provide detailed insights into how an attack occurred, what systems were affected, and whether sensitive data was compromised. For healthcare, network forensics ensures thorough breach investigations and supports compliance reporting.

Available Healthcare Cybersecurity Tools:

- **Wireshark:** Open-source tool for analyzing network protocols and traffic.
- **NetWitness Network (RSA):** Provides real-time packet capture and threat analysis.
- **SolarWinds NetFlow Traffic Analyzer:** Monitors network traffic and identifies anomalies.
- **Corelight:** Focuses on high-performance network visibility and forensic analysis.

70. Automated Security Testing

Automated security testing tools streamline vulnerability assessments and penetration testing for healthcare applications and systems. These tools simulate attacks, identify weaknesses, and provide actionable remediation steps. Automation ensures continuous security testing, reducing the risk of vulnerabilities being exploited.

Available Healthcare Cybersecurity Tools:

- **Burp Suite:** Offers automated testing for web application vulnerabilities.
- **Qualys Web Application Scanning:** Focuses on identifying security gaps in healthcare portals.
- **Nessus Professional:** Provides comprehensive vulnerability assessments for healthcare environments.
- **OWASP ZAP:** An open-source tool for automated web application security testing.



Greatest Buyer Demand 2025-2027

Healthcare Cybersecurity Products



The demand for specific cybersecurity tools in the healthcare industry for 2025–2026 will be driven by evolving threats, regulatory pressures, and the increasing digitalization of healthcare systems. Based on industry trends, the following categories and tools are expected to see the greatest demand:

1. Identity and Access Management (IAM)

Why in Demand:

- The shift to cloud-based healthcare systems and remote work increases the need for secure identity management.
- Regulatory requirements emphasize protecting patient data by limiting unauthorized access.
- IAM is critical for managing access to Electronic Health Records (EHR) and telehealth platforms.

High Demand Vendors:

- Okta: For seamless single sign-on (SSO) and multi-factor authentication (MFA).
- CyberArk: For managing privileged accounts in critical systems.
- Microsoft Azure Active Directory: For integration with Microsoft's healthcare cloud solutions.
- Imprivata: Specifically tailored for fast and secure clinical workflows.

2. Endpoint Detection and Response (EDR)

Why in Demand:

- Ransomware attacks targeting healthcare are expected to grow, making endpoint protection a top priority.
- Increased use of mobile devices, IoT/IoMT, and remote access in healthcare heightens endpoint risks.
- EDR tools provide real-time monitoring and automated threat response.

High Demand Vendors:

- CrowdStrike: For AI-driven threat detection and response.
- SentinelOne: Known for autonomous endpoint protection and rollback capabilities.

- Sophos: Combines endpoint and network security for holistic protection.
- Carbon Black (VMware): Focuses on advanced ransomware detection and mitigation.

3. Network Security

Why in Demand:

- The rise of IoT/IoMT devices creates a larger attack surface for healthcare networks.
- Interconnected systems across providers, payers, and ancillary services require secure communication.
- Advanced firewalls and intrusion prevention systems are necessary to secure sensitive patient data.

High Demand Vendors:

- Palo Alto Networks: Offers AI-driven threat prevention for complex healthcare networks.
- Fortinet: Focuses on integrated network security with high performance.
- Cisco Secure: Combines network visibility with advanced malware protection.
- Zscaler: Ideal for securing hybrid and cloud environments.

4. Zero Trust Architecture

Why in Demand:

- Healthcare organizations are increasingly adopting Zero Trust principles to secure access to sensitive data.
- Zero Trust is critical for ensuring compliance and preventing lateral movement in case of a breach.
- Growing adoption of remote and hybrid work models necessitates Zero Trust solutions.

High Demand Vendors:

- Okta: For identity-centric Zero Trust access control.
- Palo Alto Networks: Integrates Zero Trust principles with robust network and endpoint security.
- Zscaler: Focuses on secure access to cloud applications and data.
- Microsoft Zero Trust Solutions: Combines identity, device, and network protection.

5. Data Loss Prevention (DLP)

Why in Demand:

- Stringent regulations like HIPAA and GDPR mandate the prevention of unauthorized data sharing.
- The rise in cloud storage and collaboration tools increases the risk of accidental or malicious data leaks.
- DLP is essential for safeguarding PHI during exchanges between healthcare entities.

High Demand Vendors:

- Symantec DLP: Provides comprehensive data protection across endpoints and cloud environments.
- Forcepoint DLP: Uses behavioral analytics to prevent data exfiltration.
- Digital Guardian: Focuses on protecting sensitive data across healthcare workflows.
- Microsoft 365 DLP: Ensures data security in Microsoft-based healthcare environments.

6. IoT/IoMT Security

Why in Demand:

- The rapid proliferation of connected medical devices increases vulnerabilities.
- Attacks targeting IoMT devices can disrupt patient care and compromise safety.
- Regulatory frameworks are starting to focus on securing IoMT devices.

High Demand Vendors:

- Medigate (Claroty): Specifically designed for IoMT device visibility and threat management.
- Armis: Provides asset management and security for IoT/IoMT ecosystems.
- Forescout: Focuses on identifying and securing connected devices in healthcare networks.
- Cisco IoT Threat Defense: Offers end-to-end IoT security for healthcare settings.



7. Ransomware Protection and Recovery

Why in Demand:

- Healthcare remains one of the top targets for ransomware attacks, with high financial and operational impacts.
- Organizations are focusing on robust ransomware detection, response, and recovery plans.
- Immutable backups and automated recovery capabilities are increasingly essential.

High Demand Vendors:

- Sophos Intercept X: Combines behavioral detection with ransomware-specific defenses.
- Rubrik: Provides immutable backups and rapid ransomware recovery.
- SentinelOne Singularity: Known for AI-driven detection and rollback capabilities.
- CrowdStrike Falcon: Offers comprehensive ransomware protection with threat intelligence.

8. Cloud Security

Why in Demand:

- The growing adoption of cloud-based EHR systems, telehealth platforms, and data storage demands robust cloud security.
- Compliance with data protection regulations requires secure cloud environments.
- Hybrid and multi-cloud setups in healthcare create complex security challenges.

High Demand Vendors:

- Microsoft Azure Security: Tailored for healthcare organizations leveraging Azure-based solutions.
- Palo Alto Networks Prisma Cloud: Provides full-stack security for healthcare cloud applications.
- Netskope Cloud Security: Ensures secure use of SaaS applications in healthcare.
- AWS Security: Offers end-to-end protection for cloud-hosted healthcare environments.

9. Security Information and Event Management (SIEM)

Why in Demand:

- SIEM tools are critical for detecting and responding to sophisticated threats in real-time.
- Healthcare organizations need centralized logging and reporting to ensure compliance.
- Advanced analytics and machine learning in SIEM tools enhance threat visibility.

High Demand Vendors:

- Splunk: Provides real-time threat detection and operational insights.
- IBM QRadar: Automates compliance and incident response for healthcare environments.
- Microsoft Azure Sentinel: Combines AI-driven analytics with scalability for healthcare organizations.
- LogRhythm: Focuses on detecting and mitigating insider and external threats.

10. Backup and Disaster Recovery

Why in Demand:

- Healthcare organizations require robust recovery solutions to ensure continuity of care during cyber incidents.
- Immutable backups are critical for ransomware resilience.
- Disaster recovery solutions help maintain compliance with data retention and availability requirements.

High Demand Vendors:

- Veeam Backup & Replication: Offers fast and reliable data recovery for healthcare systems.
- Rubrik: Focuses on ransomware recovery and secure data archiving.
- Commvault Complete Backup: Provides comprehensive protection for hybrid environments.
- Acronis Cyber Protect: Combines backup with integrated cybersecurity features.

Projected Key Focus Areas for 2025–2026:

- **Ransomware Protection:** Given its persistent threat to healthcare, ransomware protection will dominate investment priorities.
- **IoT/loMT Security:** The rapid growth of connected medical devices makes this a critical area.
- **Zero Trust Adoption:** Healthcare organizations will increasingly adopt Zero Trust models to secure remote and hybrid workflows.
- **Cloud Security and Compliance:** As more healthcare systems migrate to the cloud, cloud security tools will be in high demand.
- **Data Loss Prevention:** Ensuring PHI protection and compliance will remain a central concern.

By focusing on these tools and categories, healthcare organizations can address emerging threats and enhance their security posture in 2025–2026.

AI in Healthcare Cybersecurity: Transforming Protection for Providers, Payers, and Suppliers

The integration of artificial intelligence (AI) into healthcare cybersecurity represents a revolutionary shift in how the industry addresses increasingly sophisticated threats. As the healthcare sector becomes more digitally interconnected, with sensitive patient data, interconnected devices, and cloud-based platforms, the need for robust and intelligent security solutions has never been more critical. AI applications in cybersecurity empower healthcare providers, payers, and suppliers to protect their infrastructure and data more effectively, ensuring patient safety, regulatory compliance, and operational resilience.

For **providers**, AI-driven cybersecurity tools offer proactive threat detection and mitigation. Hospitals and clinics often operate with complex IT ecosystems that include electronic health records (EHRs), medical devices, and telemedicine platforms, all of which are potential targets for cyberattacks. AI algorithms can monitor network traffic in real-time, identify anomalies, and flag potential breaches before they escalate. This minimizes downtime and ensures continuity of care. Furthermore, AI tools can streamline compliance reporting, reducing administrative burdens for healthcare IT teams by automating audits and ensuring adherence to regulations like HIPAA and GDPR.

In the case of **payers**, such as insurance companies, AI enhances the ability to protect sensitive financial and personal health information from fraud and unauthorized access. AI-driven fraud detection systems can analyze patterns in claims and transactions, identifying discrepancies or potential fraudulent activities in real time. Additionally, payers benefit from AI-powered risk assessment tools that evaluate the cybersecurity postures of third-party vendors and partners, ensuring the integrity of their extended networks.

For **suppliers**, including medical device manufacturers and pharmaceutical companies, AI provides a vital layer of protection in securing intellectual property and ensuring the integrity of their supply chains. As suppliers increasingly adopt IoT-enabled devices and digital manufacturing processes, AI tools can safeguard against cyberattacks targeting these systems. AI also supports software patching and updates by identifying vulnerabilities and prioritizing fixes, reducing the risk of exploitation in connected devices.



For **IT vendors**, AI-driven cybersecurity solutions enable them to offer tailored, high-performance products to healthcare organizations. Vendors can use AI to develop adaptive security platforms that learn and evolve with each client's unique environment. By integrating machine learning algorithms, vendors provide predictive threat analytics, automated response systems, and advanced data encryption. These capabilities differentiate their products in a competitive market and ensure that healthcare organizations remain well-equipped to handle emerging cybersecurity challenges.

The benefits of AI in healthcare cybersecurity extend beyond mere defense. AI-powered systems enhance visibility, efficiency, and collaboration across the healthcare ecosystem. By automating repetitive tasks, prioritizing risks, and providing actionable insights, AI empowers stakeholders to focus on strategic goals and patient-centered care. In a landscape where cyber threats grow more sophisticated each day, AI serves as a cornerstone for building resilient, secure, and innovative healthcare infrastructures.

Top AI-Driven and Comprehensive Cybersecurity Vendors in Healthcare

The healthcare industry faces a unique blend of cybersecurity challenges, requiring advanced technologies and AI-driven solutions to protect sensitive patient data, ensure regulatory compliance, and maintain operational resilience. Below is a comprehensive list of top vendors specializing in healthcare cybersecurity, highlighting those leading in AI innovation as well as those offering robust, broader solutions.

Top AI-Driven Vendors

1. Palo Alto Networks

- **AI Role:** Industry leader in AI-driven threat detection and prevention.
- **Innovations:** Automated threat analysis, Zero Trust frameworks, and cloud-native AI tools that protect patient records and digital assets.

2. CrowdStrike

- **AI Role:** Pioneering AI-powered endpoint protection.
- **Innovations:** Machine learning algorithms for real-time detection, advanced threat hunting, and proactive response strategies.

3. Sophos

- **AI Role:** Synchronized security powered by advanced AI.
- **Innovations:** Machine learning algorithms for automated threat response and behavioral analysis across healthcare IT systems.

4. BlackBerry Cylance

- **AI Role:** Focus on predictive AI for endpoint security.
- **Innovations:** Preventative protection against ransomware, malware, and phishing using cutting-edge AI tools.

5. FireEye (Trellix)

- **AI Role:** AI-integrated threat detection and incident response.
- **Innovations:** Advanced AI analytics for identifying and mitigating sophisticated cyber threats in healthcare environments.

6. Claroty

- **AI Role:** AI-enhanced security for healthcare IoT (IoMT).
- **Innovations:** The Medigate platform, providing AI-driven risk assessment and protection for connected medical devices and critical systems.

7. Trend Micro

- **AI Role:** Multi-layered defense powered by AI.
- **Innovations:** Advanced endpoint, network, and cloud security solutions tailored for healthcare, using AI to predict and counteract cyber threats.

8. Bitdefender

- **AI Role:** Cutting-edge malware detection using AI.
- **Innovations:** Behavioral analysis and AI-powered defense mechanisms for ransomware prevention and real-time threat detection.

9. Armis

- **AI Role:** Focused on healthcare IoT and device security.
- **Innovations:** AI-driven real-time device visibility, risk assessment, and vulnerability management for connected systems.

10. Proofpoint

- **AI Role:** AI-powered email and insider threat security.
- **Innovations:** AI-based phishing detection, email threat mitigation, and management of insider risks.

11. Fortinet

- **Focus:** Comprehensive cybersecurity for healthcare networks.

- **Innovations:** AI-driven firewalls, intrusion prevention systems, and secure access solutions for robust network protection.

12. Check Point Software Technologies

- **Focus:** End-to-end security for healthcare.
- **Innovations:** Real-time threat prevention, mobile security, and tailored solutions for healthcare IT infrastructure.

13. CyberArk

- **Focus:** Privileged access management.
- **Innovations:** AI-enhanced credential monitoring and secure access for privileged accounts.

14. GE HealthCare

- **Focus:** Securing medical devices and IT systems.
- **Innovations:** Integrated security features like the Skeye solution, offering real-time device monitoring and risk management.

15. Imperva

- **Focus:** Data and application security.
- **Innovations:** AI-driven solutions to safeguard critical healthcare data and prevent application-level breaches.

16. Zscaler

- **Focus:** Cloud-based security tailored for healthcare.
- **Innovations:** AI-enabled Zero Trust Exchange to secure digital and cloud environments.

17. Symantec (Broadcom)

- **Focus:** Comprehensive endpoint and data security.
- **Innovations:** AI-powered encryption, malware protection, and endpoint security tools for healthcare organizations.

18. Cisco

- **Focus:** Network security and secure access.
- **Innovations:** AI-integrated Secure Access Service Edge (SASE) and threat analytics for seamless protection.

19. Kaspersky Lab

- **Focus:** Endpoint protection and ransomware prevention.
- **Innovations:** AI-based threat intelligence to combat advanced cyber threats in healthcare environments.

20. McAfee

- **Focus:** Endpoint security and data loss prevention.
- **Innovations:** AI-powered threat intelligence and malware protection solutions tailored for healthcare needs.

These vendors collectively represent the forefront of healthcare cybersecurity, blending AI-powered innovations with robust, comprehensive solutions. By addressing the specific challenges of providers, payers, and suppliers, they enable the healthcare industry to stay ahead of emerging threats while maintaining the highest standards of patient care and data security.

Black Book of Healthcare Cybersecurity

Setting the Gold Standard in 2025

Black Book™ continues to define excellence in evaluating healthcare IT solutions with its 2025 Cybersecurity Competitive Intelligence research. This authoritative annual report provides unparalleled insights into the healthcare industry's most critical cybersecurity tools and vendors. Black Book evaluates industry leaders across 18 key performance indicators, focusing on operational excellence, client satisfaction, and real-world effectiveness. This year's research emphasizes artificial intelligence (AI)-driven cybersecurity innovations and their impact on healthcare providers, payers, and suppliers.



Our research also draws on feedback from our extensive annual surveys, which represent the experiences of more than 2.9 million healthcare IT users globally. This approach ensures robust, actionable insights that reflect the needs and experiences of end-users, empowering healthcare stakeholders—including buyers, analysts, consultants, and investors—to make informed decisions. Our transparent and client-centric methodology ensures the integrity of our findings, free from vendor or consultancy influence.

A Comprehensive View of Healthcare Cybersecurity for 2025

The Black Book of Healthcare Cybersecurity provides insights powered by the collective voice of the global healthcare community. Leveraging feedback from over 3 million respondents, Black Book’s surveys assess nearly 8,000 vendors specializing in software, services, and solutions for critical areas like cybersecurity, EHRs, outsourcing, and IT innovation. In its 7th year, this research continues to highlight real-world performance, focusing on AI-driven cybersecurity tools that address evolving threats across healthcare networks and IoT ecosystems.

Black Book’s independence ensures credibility in an industry often influenced by vendor-consultancy relationships. We have no financial ties or incentives to favor specific providers, allowing us to deliver unbiased, transparent, and trustworthy intelligence. By capturing the authentic experiences of end-users, including CIOs, cybersecurity experts, and healthcare administrators, Black Book’s insights enable organizations to benchmark vendors, enhance their cybersecurity strategies, and navigate complex IT ecosystems with confidence.

Disclaimer and Copyright

Black Book™ research findings are based on data sourced from reliable references, including vendor websites, news articles, industry directories, and insights derived from multiple sources analyzed through five advanced large language models (LLMs). While every effort is made to ensure accuracy and completeness, Black Book™, Black Book Market Research LLC, and The Black Book of Outsourcing® disclaim all warranties regarding the adequacy or application of this information. Black Book assumes no liability for errors, omissions, or misinterpretations, and the application of this data is the sole responsibility of the reader. Opinions expressed are subject to change without notice.

Black Book™, its founder, management, and staff do not own or hold any fiscal interest in any vendors covered in its surveys.

© 2024, 2025 Black Book Market Research LLC. All Rights Reserved. Unauthorized reproduction or distribution of this publication in any form is strictly prohibited without prior written consent.

For more information or customized research results, contact our Client Resource Center at
+1 800-863-7590
or
info@blackbookmarketresearch.com.

Visit us at
www.BlackBookMarketResearch.com for further details.

Index

A

AccessData Forensic Tools, 89, 95, 218

Acronis Cyber Protect, 77, 96, 218, 254, 274

Acunetix Vulnerability Scanner, 82, 96, 218

advanced threat detection, 38, 107, 130, 136, 160, 165, 184, 194, 213, 216, 236, 241

Advanced Threat Protection (ATP), 49, 166, 208, 244, 260

AES-256, 26, 34, 238

AI-Driven Threat Detection, 26, 33

Akamai Cloud Security, 75, 96, 218

AlienVault, 73, 97, 218

AlienVault Threat Intelligence, 79, 97, 218

Amazon Web Services. *See* AWS

Amwell, 92, 98, 218

analytics platforms, 97, 209

Anomali, 79, 98, 218, 241

APIs, 33, 57

Appgate SDP, 74, 98, 218

Apple devices, 152–53

applications, cloud-based, 165, 174, 216, 260

application security, 150, 252, 254, 258, 281

approach, zero-trust, 106, 118

APTs (advanced persistent threats), 7, 33, 47, 115, 189, 250

Aravo, 91, 98–99, 218

ARCON PAM, 83, 94

Arcserve UDP, 77, 99, 218

ArcSight, 73, 99, 218

Arctic Wolf, 87, 99, 124, 221, 253

Arctic Wolf Managed Security Awareness, 88, 99, 218

Arista, 70, 100, 208, 233

Arista Networks, 70, 100, 208, 218

Arm Pelion IoT, 76, 100, 218

Aruba Networks, 70, 101, 218

ATA (Advanced Threat Analytics), 30, 80, 165, 227

Atera Patch Management, 90, 101, 218

ATP. *See* Advanced Threat Protection

AttackIQ, 101–2, 262

AttackIQ Cybersecurity Training, 88, 101, 218

AT&T Cybersecurity, 73, 97, 218

Auth0, 68, 102, 218

authentication methods, 127, 131, 179, 187, 206

authorization, 26, 33, 165

Authy, 84, 102, 218

automated remediation, 151, 160–61, 189–90, 193

Automox, 90, 102, 219
Autopsy, 89, 102–3, 105, 219
AvailableHealthcare Cybersecurity Tools, 236–68
AWS (Amazon Web Services), 75, 78, 94–95, 97, 213, 218, 233, 239
AWS Inspector, 82, 94–95
AWS IoT Device Defender, 76, 95
AWS Security, 97, 273
AWS Security Hub, 87, 95
AxCrypt, 72, 103, 219
Axonius, 76, 103, 219

B

Balbix, 80, 103, 219
Baramundi Management, 81, 104, 219
Barracuda Email Security Gateway, 85, 104, 219, 244
Barracuda Networks, 47, 70, 104, 219
Barracuda Ransomware Protection, 77, 105, 219
behavioral analysis, 125, 137, 237, 240, 268, 279–80
behavior analytics, 140, 158, 166, 170
Belkasoft Evidence Center, 89, 106, 219
BeyondTrust, 68, 83, 106, 219, 243
BeyondTrust Retina, 82, 106, 219
BeyondTrust Zero Trust, 74, 106–7, 219
biometrics, 26, 127, 131, 133, 144, 157, 179, 187, 206, 243, 251
Bitdefender GravityZone, 69, 107, 219
Bitdefender Threat Intelligence, 79, 108, 219

BitLocker, 72, 107, 219
BitSight, 91, 107, 219, 247, 263
BlackBag Blacklight, 89, 108, 219
BlackBerry Cylance, 69, 108, 219, 279
BlackBerry UEM, 81, 109, 219, 242
Black Book Market Research LLC, 7, 285
Blockchain, 113, 146, 244
Blockchain for Data Security, 54, 86, 219–25, 227, 231, 244
Blockpharma, 86, 109, 219
Blumira, 73, 109, 219
Boxcryptor, 72, 109–10, 220, 255
Broadcom, 71, 90, 110, 201, 232, 281
BurstIQ, 86, 110, 220

C

Cado Response, 89, 110, 220
capabilities
 predictive, 108, 117, 122, 125, 127
 telehealth, 57, 210, 247
Carbon Black, 69, 77, 111, 220, 236, 271
Carbonite Endpoint Encryption, 72, 173, 228
CareClix, 92, 111, 220
care teams, 133, 178, 191, 198, 207, 215, 240
CASBs (cloud access security brokers), 27, 31, 259–60
Cellebrite, 89, 111, 220, 246
Censys, 82, 111–12, 220
Centrify, 68, 112, 220



Centrify Privileged Access Service, 83, 112, 220
 Cerner Secure Messaging, 78, 112, 220
 Chainalysis, 86, 113, 220
 Change Healthcare, 15
 Check Point CloudGuard, 75, 113, 220
 Check Point Email Security, 85, 113–14, 220
 Check Point Harmony Endpoint, 69, 77, 114, 220
 Check Point IoT Protect, 76, 114, 220
 Check Point Software, 43, 70, 114, 220, 237
 Check Point ThreatCloud, 79, 115, 220
 Chiron Health, 92, 115, 220
 Chronicled, 86, 115, 220
 Cisco, 42, 68, 74, 84, 116, 129–30, 222, 243, 282
 Cisco IoT Threat Defense, 76, 115, 220, 272
 Cisco Meraki Systems Manager, 81, 116, 220
 Cisco Secure Email, 85, 116, 220, 244
 Cisco Talos, 79, 117, 220, 241
 Cisco Webex, 92, 117, 221, 267
 Cisco Zero Trust, 74, 239
 Citrix Endpoint Management, 81, 118, 221
 claims platforms, 160–61, 169–70, 172, 174–75, 185, 188, 190, 192, 194, 197, 208, 212–13, 216
 targeting, 149, 183, 198, 200
 claims processing platforms, 94, 108, 122–23, 131–32, 137, 140–41, 151–53, 159, 171, 177, 184
 claims processing workflows, 123, 130, 145, 150, 164, 178, 181, 205
 Claroty, 76, 162, 227, 240, 272, 280
 clinician devices, 109, 139, 160, 168, 189, 193, 197, 199, 203, 211
 clinicians, 52–53, 94, 145–46, 153, 155–56, 158, 187, 191, 195–96, 204, 207, 213, 215
 cloud, 27, 42, 44–45, 95, 97, 104, 120, 149, 174, 210, 216
 cloud applications, 119, 145, 147, 169, 180, 239, 271
 Cloudflare, 75, 85, 100, 119, 218, 221
 cloud migration, 27–28, 39
 Code42, 71, 119, 221
 Codeproof Enterprise MDM, 81, 119, 221
 Cofense, 88, 178, 229
 Cohesity DataProtect, 77, 120, 221
 Commvault Complete Backup, 77, 120, 221, 254, 274
 compliance, 31, 38–39, 94–101, 110–12, 115–17, 133–36, 139–41, 145–47, 156–58, 164–73, 176–77, 179–88, 203–5, 211–12, 215–16, 236–37, 244–47, 253–56, 259–65, 273–75
 compliance features, 39, 43, 129
 compliance standards, 177, 180, 190
 ConnectWise Automate, 90, 120, 221
 Coral Health, 86, 121, 221
 credentials, targeting EHR, 100, 114, 152
 CrowdStrike, 41, 69, 121–22, 221, 236, 270, 279
 CrowdStrike Falcon, 77, 240, 250, 273
 CrowdStrike Falcon Cloud, 75, 121, 221
 CrowdStrike Falcon Forensics, 89, 121, 221
 CrowdStrike Falcon Fusion, 87, 122, 221
 CrowdStrike Falcon Spotlight, 82, 122, 221
 CrowdStrike Threat Intelligence, 79, 122, 221
 CRQ (Cyber Risk Quantification), 264

Curricula Security Awareness Training, 88, 122, 221

CyberArk, 46, 68, 83, 123, 221, 243, 270, 281

CyberArk Zero Trust, 74, 123, 221

cyberattacks, 6–7, 21, 30, 95–96, 101, 164, 166, 176, 183, 189–90, 193–98, 208, 216, 254–55, 276

Cybereason Defense Platform, 80, 125, 222

Cybereason Threat Analysis, 79, 125, 222

CyberGRX, 91, 124, 221

CyberMDX, 76, 124, 221, 240

Cyber Risk Quantification (CRQ), 264

cyber risks, 11, 99, 163, 264

cybersecurity measures, robust, 7, 15, 32

cybersecurity posture of vendors, 124, 156, 173, 183, 189

Cybersecurity Tool, 160, 235, 270, 276, 284

CyberSponse, 87, 124, 221

cyber threats, advanced, 150, 188, 282

CyFIR Investigator, 89, 123, 221

Cynerio, 76, 126, 222

Cynet, 80, 126, 222, 253, 265

D

Darktrace, 80, 126–27, 222, 241, 250, 257, 265

databases, patient, 105, 125

data encryption, 17, 34, 130, 154, 179, 260

data exchanges, 31, 35, 43, 97, 100, 110, 113, 163, 166, 196, 247

data integrity, 95, 114, 127, 132, 143, 147, 154, 162, 196, 238

data masking, 212, 257

data privacy, 44, 46, 178

data privacy regulations, 192, 203, 205, 212

Data Protection Encryption, 72, 127, 222

data recovery, 105–6, 108, 111, 123, 135

DDoS protection, 104, 118–19, 150

Delinea, 83, 112, 243

desktops, 109, 116, 249

detection capabilities, advanced threat, 64, 116, 203

deviations, 33, 94, 241

device authentication, 32, 188

device health, 10, 30, 39, 129, 169, 238

Devolutions PAM, 83, 128, 222

Digital Guardian, 71, 128, 222, 237, 272

disaster recovery, 27, 48, 99, 120, 218, 221, 225, 230, 254–55, 274

DLP (data loss prevention), 38, 43, 51, 71, 119, 128, 137, 142, 161, 165, 169, 180, 199, 221–25, 227–33, 237, 272

Doc.ai, 86, 129, 222

downtime, 27, 96, 105, 109, 120, 126, 149, 240, 254, 276

Doxy.me, 92, 129, 222, 247, 267

Dragos, 76, 129, 222

Duo Security, 68, 74, 84, 129–30, 222, 243

E

EclecticIQ, 79, 131, 222

EcoVadis, 91, 131, 222



EDR (Endpoint Detection and Response), 30, 38, 51, 69, 111, 121, 125, 130, 137, 139, 175, 189, 218–28, 230–32, 236, 270

Egress Protect, 85, 131–32, 222

EHR platforms, 26, 30, 33, 125, 137, 142, 152, 242

EHR systems, 32–34, 102–3, 111–12, 117–24, 126–27, 134–36, 142–43, 145–47, 149–51, 159–60, 165, 172–77, 182–87, 190–94, 196–98, 200–202, 204–9, 211–14, 242–43, 251–53

Elastic Security, 73, 87, 132, 223, 250, 257

email gateways, 48, 54, 85, 140, 244

EncrypGen, 86, 132, 223

encryption, 26–27, 34–35, 43, 52–53, 142–43, 147, 161, 193, 205, 212, 219–20, 222–26, 228–29, 231–33, 238–39, 244, 261

EncryptRIGHT, 72, 133, 179, 223

endpoint detection and response, 30, 38, 51, 69, 111, 121, 125, 218–28, 230–32, 236, 270

endpoint management, unified, 148, 210, 219–21, 233, 242

endpoint protection, 44–46, 48, 96, 101, 116, 127–28, 166, 193, 201, 249, 265

endpoints, 103–4, 119–20, 152–53, 175, 181–82, 195–97, 203–4, 209, 237, 242–43, 246, 254, 256, 264–65, 271–72

endpoint security, 43, 46, 114, 137, 152, 154, 161, 255, 271, 279

End-to-End Healthcare Cybersecurity Vendors, 38–39, 41, 43, 45, 47, 49

Enterprise Security Manager (ESM), 73, 161, 227

Entrust Identity MFA, 84, 133, 223

Epic Secure Chat, 78, 133, 223

Epic Telehealth Integration, 92, 133, 223

ESET, 80, 130, 222

ESET Cybersecurity Awareness, 88, 130, 222

ESET Endpoint Security, 69, 130, 222

ESET Secure Authentication, 84, 131, 222

ESM (Enterprise Security Manager), 73, 161, 227

Exabeam DLP, 71, 134, 223

Exterro, 89, 95, 135, 218, 223

Extreme Networks, 70, 134, 223

F

Factom, 86, 135, 223

FarmaTrust, 86, 135–36, 223

Fidelis Cybersecurity, 71, 136, 223

financial platforms, 125, 152, 166–68, 182–83, 187, 193, 205–7

Financial Viability, 41–42, 44–46

FireEye Cloud Security, 75, 136, 223

FireEye Email Security, 85, 136, 223

FireEye Endpoint Security, 69, 77, 89, 137, 223

FireEye Threat Intelligence, 79, 137, 223, 241

firewalls, 51, 114, 139, 153, 174, 196, 208, 213, 237, 260, 281

Flexera Software Vulnerability Manager, 90, 137, 223

Forcepoint, 70–71, 137–38, 223, 237

Forensic Analysis Tools, 55, 89, 108, 139, 218–21, 223, 226, 228–30, 233, 246

forensic capabilities, 105, 135, 157, 160, 177, 250

Forensic Toolkit, 89, 135, 223, 246

Forescout, 76, 138, 223, 272

ForgeRock, 68, 138, 223

Fortanix, 72, 139, 223

FortiEDR, 69, 139, 224

Fortinet, 43, 47, 69–70, 76, 139, 224, 237, 271, 280

Fortinet FortiInsight, 80, 140, 224

Fortinet FortiMail, 85, 140, 224

Fortinet FortiSOAR, 87, 141, 224, 249

Forward Advantage, 78, 141, 224

Foxpass PAM, 83, 141, 224

fraud, 115, 143–45, 152, 154, 160–62, 166, 177, 183, 186, 191, 198–99, 213–14, 244

F-Secure Countercept, 79, 134, 223

F-Secure Radar, 82, 135, 223, 248

FTK, 89, 135, 223, 246

Fudo Security PAM, 83, 142, 224

G

GDPR, 94, 97, 103, 106, 127–28, 151, 156, 161–62, 205, 236–37, 248, 276

GFI LanGuard, 82, 90, 142, 224

Google Authenticator, 84, 142–43, 224, 243

Google Chronicle, 87, 191, 230

Google Cloud Security, 75, 143, 224, 239

Graylog, 73, 143, 224

Greatest Buyer Demand, 269, 271, 273, 275, 277

GTB Technologies, 71, 142, 224

Guardtime, 86, 143, 224, 244

Guardtime Health, 86, 144, 224

Gurukul Behavioral Analytics, 80, 144, 224

H

Habitu8, 88, 145, 224, 267

Halo Health, 78, 145, 224

Hashed Health, 86, 145, 224, 244

HashiCorp Vault, 83, 145, 224

healthcare costs, 115, 146, 162–63, 191, 204

Healthcare Cybersecurity Vendors, 39, 62, 65–66, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199, 201, 203, 205, 207, 209, 211, 213, 215

healthcare regulations, 96–98, 145–47, 149–54, 159, 161–62, 164–66, 170, 176, 180–83, 192–94, 211–12

HealthCombix, 86, 146, 224

health plans, 7, 11

health systems, 10, 22, 95, 97, 100–101, 126, 144, 146

HealthTap, 92, 146, 224

Hexnode MDM, 81, 146, 225

HID Global, 68, 144, 224

HID Global ActivID, 84, 144, 224

HIE (health information exchanges), 38, 41, 57, 110

High Demand Vendors, 270–74



HIPAA, 94–98, 109–12, 127–28, 131–35, 139–40, 142–47, 150–51, 155–56, 161–62, 168–72, 178–79, 182–83, 186, 198–99, 201, 203–5, 207–9, 212–16, 236–37

HIPAA compliance, maintaining, 181, 257

HIPAA-compliant features, 118, 151, 162–63, 168, 178, 191

HIPAA-compliant platform, 163, 181, 204, 207

Hitachi ID PAM, 83, 146–47, 225

HIT Cyberattacks, 14–15, 17, 19, 21, 23

HITECH, 39, 41, 57, 94

I

IBM Blockchain, 86, 147, 225

IBM Cloud Security, 75, 147, 225

IBM Guardium, 72, 147, 225

IBM MaaS360, 81, 148, 225

IBM Security QRadar, 73, 148, 225

IBM Security QRadar UEBA, 80, 148, 225

IBM Security Resilient, 87, 148, 225, 245

IBM Security Secret Server, 83, 149, 225

IBM Security Verify, 68, 149, 225

IBM Spectrum Protect, 77, 149, 225

IBM X-Force Exchange, 79, 149, 225

identity and access management, 38, 51, 68, 97, 102, 138, 149, 165, 185, 187, 218–30, 236, 270

Identity Governance and Administration (IGA), 186, 253

Identity Safeguard, 83, 172, 228, 261

IGA (Identity Governance and Administration), 186, 253

Imperva, 70, 150, 225, 281

incident response, 20, 95–96, 106, 115, 136, 182, 190, 198, 202, 204, 249–50, 255, 265

Incident Response Platforms, 54, 87, 148, 218, 220–26, 228–33, 245

incidents, 6, 15–16, 109–10, 121–23, 125, 149, 156, 159, 174–75, 177, 198, 214

information exchanges, health, 38, 41, 110

Infosec IQ, 88, 150, 225

infusion pumps, 114, 116, 124, 126–27, 154, 176, 188–89, 202, 205, 216, 239

Innovation & Product Usability, 41–48

insider threats, 38, 106–7, 110, 119, 126, 140, 148, 165, 170, 196–97, 209, 248, 261

InsightVM, 82, 151, 225

integration, 10, 27, 30–31, 57, 98–99, 115–16, 130, 165–67, 172–74, 184–85, 191, 276

InTouch Health, 92, 151, 225

IoMT (Internet of Medical Things), 19, 22, 28, 239, 280

IoT/IoMT Security, 28, 52, 76, 218–23, 226–28, 230, 232, 234, 239, 272, 275

IoT networks, 114–15, 124, 136

IoT Security, 44, 127, 218, 224

IoT systems, 109, 176, 189, 205, 216

IPS (intrusion prevention system), 197, 271, 281

Ironscales, 85, 151–52, 225

Ivanti, 46, 81, 152, 168, 227

Ivanti Endpoint Security, 69, 152, 225

Ivanti Neurons for Vulnerability Management, 82, 152, 225

J

Jamf Pro, 81, 152–53, 225, 242

Juniper Networks, 70, 153, 225

K

Kandji, 81, 153, 225

Kaseya VSA, 90, 153, 225

Kaspersky Anti-Ransomware, 77, 154, 226

Kaspersky Endpoint Security, 69, 154, 226

Keycloak, 84, 155, 226

Klara, 78, 155–56, 226

KnowBe4, 88, 155, 226, 245

Knox, 81, 155, 226

KPIs (Key Performance Indicators), 57, 59, 62, 65–66, 283

KY3P, 91, 156, 226

L

Lacework, 75, 156, 226

laptops, 51, 107, 154, 161, 195, 203, 236, 242, 249

LastPass MFA, 84, 157, 226

leverages, 98, 113, 116, 158, 236

LogicGate Risk Cloud, 91, 158, 226

LogRhythm, 73, 157, 226, 238, 274

LogRhythm Forensic, 89, 157, 226

LogRhythm SOAR, 87, 157–58, 226

M

machine learning, 38, 136–37, 158, 165–66, 170, 188–89, 196–97, 199–200, 236, 240–41, 244, 250, 265

Magnet AXIOM, 89, 159–60, 226, 246

Malwarebytes, 77, 160, 226

Malwarebytes Endpoint Protection, 69, 160, 226

MAM (mobile application management), 167–68

ManageEngine, 48, 68, 158, 226

ManageEngine Mobile Device Manager, 81, 159, 226

ManageEngine PAM360, 83, 159, 226, 243

ManageEngine Patch Manager, 90, 159, 226, 246

McAfee Advanced Threat Defense, 79, 160, 226

McAfee Complete Data Protection, 72, 161, 226

McAfee Enterprise Security Manager, 73, 161, 227

McAfee Total Protection for DLP, 71, 161, 227, 237

MDM (mobile device management), 53, 81, 118, 148, 152, 155, 167–68, 187, 195, 199, 218–19, 221, 225–27, 230–33, 242

MDR (Managed Detection and Response), 27, 134, 190, 253

medical devices, 7, 54–55, 100–101, 103, 106, 108, 110, 112, 114, 116, 120–21, 123–28, 130–32, 134–45, 149–54, 156–62, 165–80, 182–209, 211–14, 216, 251–52

Medici Telehealth, 92, 162, 227

Medigate, 28, 76, 162, 227, 240, 272

MEDITECH Expanse Secure Messaging, 78, 163, 227



member portals, 98–99, 127–28, 130–31, 133–34, 138–39, 141, 143–44, 149, 151, 154–55, 165, 172, 174, 178–79, 196

Mend VIP Telehealth, 92, 163, 227

messaging, encrypted, 112, 145, 155, 198, 201, 204

Messaging Platforms, 53, 78, 191, 240

MetaCompliance, 88, 163–64, 227, 267

MFA (multi-factor authentication), 26, 54, 84, 102, 138, 141–42, 149, 155, 157–58, 171–73, 179, 185, 187, 218, 222–24, 226, 228–30, 232–33, 236, 243

Micro Focus, 73, 99, 218

Microsoft, 42, 71–72, 107, 165, 219, 227, 272

Microsoft Advanced Threat Analytics, 80, 165, 227

Microsoft Azure Blockchain, 86, 165, 227

Microsoft Azure Security, 75, 166, 227, 239, 273

Microsoft Defender, 85, 167, 227, 256

Microsoft Defender ATP, 77, 166, 227

Microsoft Defender Vulnerability Management, 82, 167, 227

Microsoft Intune, 81, 167, 227, 242

Microsoft SCCM, 90, 167, 227

Microsoft Teams, 92, 168, 227, 247, 267

Mimecast Awareness Training, 88, 164, 227, 245

Mimecast Secure Email Gateway, 85, 164, 227, 244

misconfigurations, 94, 96, 111, 239, 252

mitigation, 38, 43, 47, 141, 180, 271, 276

mobile application management (MAM), 167–68

mobile devices, 94, 107–9, 120, 122, 146, 148, 152, 155, 167–68, 187, 195, 203, 242–43

MobileIron, 81, 168, 227

N

Netskope, 70, 169, 227

Netskope Cloud Security, 75, 169, 228, 273

Netskope Zero Trust, 74, 169, 228

Netsurion EventTracker, 73, 169, 228

NetWitness UEBA, 80, 170, 228

Netwrix Auditor, 71, 170, 228, 253

Nexpose, 82, 171, 228

Ninite Pro, 90, 171, 228

O

Office, 85, 165, 167, 180, 227, 260

Okta, 68, 74, 102, 171–72, 228, 236, 239, 270–71

Okta MFA, 84, 172, 228, 243

OneLogin, 68, 172, 228

OneTrust Vendorpedia, 91, 173, 228, 247

OpenVAS, 82, 173–74, 228

Oracle Cloud Security, 75, 174, 228

outsourcing partners, 173, 180, 184

Oxygen Forensics, 89, 174, 228

P

Palo Alto Networks, 41, 70, 74, 174, 176, 228, 237, 271, 279

Palo Alto Networks Cortex XDR, 69, 77, 175, 228

Palo Alto Networks Cortex XDR Forensics, 89, 175, 228

Palo Alto Networks Cortex XSOAR, 87, 175, 228

Palo Alto Networks IoT Security, 76, 175–76, 228

Palo Alto Networks Prisma, 75, 176, 228

Palo Alto Networks Prisma Cloud, 82, 176, 228, 256, 273

PAM (Privileged Access Management), 46, 54, 83, 94, 106, 110, 112, 128, 170, 172, 212, 219–26, 228–30, 233, 243

Panorays, 91, 177, 229, 263

Paraben E3 Platform, 89, 177, 229

Patch, 90, 177, 229

patching, 102, 171, 177, 182, 203, 205

patch management, 46, 48, 96, 104, 120, 137, 152–53, 177, 193, 203–4, 242, 246, 264

Patch Management Systems, 55, 90, 218–19, 221, 224–26, 228–29, 231, 246, 248, 264

patient portals, 102, 105, 112–13, 118–19, 147, 150, 156, 166, 169, 176, 180, 211, 243, 247, 252

payers, 10–11, 27–28, 41–42, 51–57, 94–96, 98–100, 102–10, 112–14, 116–21, 123, 127–28, 130–70, 172–216, 244–45, 276, 282–83

Perception Point, 85, 178, 229

PerfectServe, 78, 177–78, 204, 229, 232

pharmaceutical companies, 10, 12, 94–96, 98, 100, 102, 106, 109, 112–15, 136, 276

pharmacies, 15, 51–54

PHI (protected health information), 10–11, 21, 38, 103, 249, 272

phishing, 38, 150–51, 164, 178, 181, 188, 213–14, 237, 241, 244–45, 258, 266–67

phishing simulations, 145, 150, 163–64, 181, 186, 206, 213–14, 258

PhishMe, 88, 178, 229

Ping Identity, 68, 178, 229, 236

Ping Identity MFA, 84, 179, 229

Ping Identity Zero Trust, 74, 179, 229

PKWARE, 72, 133, 223

privacy regulations, 187, 195, 199, 201, 207–8, 212–16, 240

Privileged Access Manager, 83, 110, 220

privileged accounts, 106, 123, 128, 146, 172, 186, 212, 243, 248, 261, 281

Privileged Identity Management (PIM), 248

Proofpoint, 71, 80, 88, 180, 214, 229, 233, 250, 267, 280

Proofpoint Email Protection, 85, 181, 229, 244

Proofpoint Security Awareness Training, 88, 181, 229, 245

PSM (Privileged Session Management), 261

Pulsara, 78, 181, 229

Q

Qualys, 82, 181–82, 229, 242, 248

R

ransomware protection, 48, 53, 77, 99, 107, 120, 125, 149, 218–19, 230, 240, 273, 275

Rapid7, 82, 151, 171, 182, 225, 228–29

Rapid7 InsightConnect, 87, 182, 229

Rapid7 InsightIDR, 73, 80, 183, 229



real-time threat detection, 96, 109, 111, 121, 126, 148, 151, 157, 161–62, 169, 184, 193, 196, 200, 202

Remediant SecureONE, 83, 183, 229

Return on Investment (ROI), 60, 64, 264

risk assessments, 124, 135, 147, 154, 162, 179, 253, 264, 280

RiskRecon, 91, 183–84, 229, 247, 263

risks, 12–13, 32–36, 94–95, 98–100, 112–14, 150–52, 158, 164, 175–77, 179–85, 197–98, 202–3, 205, 207–9, 213–14, 242–43, 246–48, 250–51, 253–54, 258–61

RiskWatch, 91, 184, 229

ROI (Return on Investment), 60, 64, 264

Role-based access control (RBAC), 28, 32, 155, 236

RSA Archer Third-Party Risk Management, 91, 184, 230

RSA NetWitness, 73, 184, 230

RSA SecurID, 68, 84, 185, 230, 243

RSA Zero Trust, 74, 185, 230

Rubrik, 77, 185, 230, 240, 254, 273–74

S

Samsung, 81, 155, 226

SASE (Secure Access Service Edge), 259, 282

Saviynt, 68, 186, 230

Saviynt Privileged Access Management, 83, 186, 230

scalability, 39, 57, 101–2, 104, 107, 110, 120–21, 134, 138–39, 143, 166, 188, 200

scalable solutions, 30, 47, 97, 105, 116, 123

Scalefusion MDM, 81, 187, 230

Scores, 62–65, 263

Sectigo IoT Manager, 76, 188, 230

Secure Access Service Edge (SASE), 259, 282

SecureAuth MFA, 84, 187, 230

Secure File Transfer Protocol (SFTP), 261

SecureTrust DLP, 71, 187–88, 230

SecureWorks Taegis, 69, 188, 230, 253

security awareness, 13, 36, 88, 181, 186, 188, 205, 230, 245

Security Awareness Training, 55, 88, 122, 214, 218–19, 221–22, 224–27, 229–30, 232–33, 245, 267

SecurityScorecard, 91, 189, 230, 263

SentinelOne Singularity, 77, 189, 230, 240, 273

SFTP (Secure File Transfer Protocol), 261

SIEM (security information event management), 52, 73, 97, 99, 140, 166, 183–84, 200, 218–20, 222–33, 238, 249, 274

SIEM tools, 238, 250, 274

SIFT (SANS Investigative Forensics Toolkit), 89, 185–86, 230

SimplePractice Telehealth, 92, 191, 230

Skybox Security, 82, 191, 230

SOAR (Security Orchestration, Automation, and Response), 124, 126, 141, 157, 175, 182, 191, 198–200, 249

SolarWinds Access Rights Manager, 83, 192, 230

SolarWinds Mail Assure, 85, 192, 231

SolarWinds Security Event Manager, 73, 193, 231

Solve.Care, 86, 196, 231, 244

SonicWall, 70, 196, 231

Sophos, 44, 69, 193, 231, 236, 271, 279

Sophos Behavioral Analytics, 197–98, 231

Sophos Cloud Optix, 75, 193–94, 231

Sophos Encryption, 72, 194, 231, 238, 249

Sophos Endpoint Security Mobile, 197, 231

Sophos Firewall, 70, 194, 231

Sophos Intercept X, 77, 195, 231, 240, 273

SophosLabs, 79, 195, 231

SophosLabs Behavioral Analytics, 196, 231

Sophos Mobile Security, 81, 195, 231

Sophos Vision, 197, 231

Sophos Worry-Free, 195, 231

spam, 104, 192, 194, 201, 207, 244

S&P Global, 91, 156, 226

Spirion, 71, 199, 231

Splunk, 45, 73, 198, 231, 238, 274

Splunk Behavioral Analytics, 80, 199, 231

Splunk Phantom, 87, 198, 231, 245, 249

Spok, 78, 198, 231, 241

SSO, 102, 138, 149, 155, 165, 171–72, 178, 187, 236, 270

Sumo Logic, 73, 200, 232

Sumo Logic SOAR, 87, 200, 232

SureMDM, 81, 94, 218

Swimlane, 87, 199–200, 232

Symantec, 71, 201, 232, 281

Symantec Email Security, 85, 201, 232

Symantec Endpoint Management, 90, 203, 232

Symantec Endpoint Protection, 69, 203, 232

Symantec IoT Security, 76, 202, 232

Symantec Managed Security Services, 87, 202, 232

Symantec VIP Access, 84, 202, 232

T

Tanium, 69, 204, 232

Teladoc, 92, 151, 204, 225

Teladoc Health, 92, 151, 204, 232, 247

Telehealth Security, 55, 92, 218, 220–25, 227, 230, 232–33, 247

Telmediq, 78, 204, 232

Tenable, 82, 204–5, 232, 242, 248

Terranova Security, 88, 205, 232

Thales Group, 72, 205, 232, 238

Thales IoT Solutions, 76, 205, 232

Thales SafeNet MFA, 84, 206, 232

third-party risk management platform, 124, 173, 177, 179–80

ThreatConnect, 79, 206, 232

threat detection, 43–44, 124, 126, 140, 143, 152–54, 156–58, 160–61, 166, 169–70, 182–83, 188–90, 198–200, 238–39, 249–50, 255

threat intelligence, 95, 97–98, 114, 116, 131, 136, 167, 176, 178, 183, 190–91, 201, 206, 249–50, 263–64

Threat Intelligence Platforms, 45, 53, 79, 149, 183, 206, 218–27, 229, 231–32, 241

threat protection, 117, 169, 180, 239

ThreatQuotient, 79, 206, 232

threats, advanced, 97–98, 102, 111, 114, 117, 121, 125–27, 130, 139, 150, 195

ThreatSim, 88, 206–7, 232

TigerConnect, 78, 207, 232, 240



TitanHQ SpamTitan, 85, 207, 233

Top AI-Driven, 278–79, 281, 283, 285

Trellix, 47, 79, 85, 87, 89, 136–37, 223, 241, 250, 257, 280

Tripwire IP360, 82, 207

Trustwave, 68, 208, 233

U

UBA (user behavior analytics), 126, 134, 137, 241

UEM (Unified Endpoint Management), 109, 148, 210, 219–21, 233, 242

Untangle, 70, 208, 233

UpGuard, 91, 208–9, 233

usability, 44, 48, 58, 63, 65

UTMs (Unified Threat Management), 260

V

Varonis, 71, 80, 209, 233, 241, 250

VBC (value-based care), 38, 41–42, 57

VidyoConnect, 92, 210, 233

Vigilance, 21, 29, 31, 33, 35, 190

Virtru, 72, 210, 233, 238, 255

VMware, 69, 77, 111, 220, 271

VMware Workspace, 81, 90, 210, 233, 242

VMware Zero Trust Solutions, 74, 211, 233

Voalte, 78, 212, 233

Vocalcom, 211, 233

Vocera Communications, 78, 211, 233, 241

Vormetric, 72, 212, 233

VPNs (virtual private networks), 196, 208, 213, 237, 251, 260

W

WAFs (web application firewalls), 119, 150

Wallix Bastion, 83, 212, 233, 261

WatchGuard, 70, 213, 233

Webroot Security Awareness Training, 88, 213, 233

Wickr, 78, 213, 233

WinMagic SecureDoc, 72, 213, 233

Wombat Security, 88, 214, 233, 267

workflows, automated, 94, 103, 116, 184, 243, 245, 248, 253

X

X-Ways Forensics, 89, 214, 233

Z

Zero Trust, 32, 63, 256, 259, 271, 275

Zero Trust Architecture (ZTA), 52, 74, 218–19, 221–25, 227–30, 232–34, 238, 271

Zero Trust Frameworks, 22, 32, 35, 279

Zinc Secure Messaging, 78, 215, 233

Zix Email Encryption, 85, 215, 233

Zscaler, 44, 70, 72, 74, 215, 234, 239, 271, 281

Zscaler Cloud Security, 75, 216, 234

Zscaler IoT Security, 216, 234

ZTNA (zero trust network access), 251, 259