2024 State of the Healthcare Cybersecurity Industry

- End-to-End Cybersecurity IT Vendor Analysis
- Client-Ranked Vendor Performance by Cyber Function
- Top Healthcare Cybersecurity Advisors & Consultants

Q4 2023 User Survey Results

Identifying the top vendors and advisors protecting critical areas of enterprise health system risk – endpoints, cloud processes, digital workloads, identity, and patient data.

Black Book Market Research LLC annually evaluates leading health care/medical software, information exchanges and service providers across 18 operational excellence key performance indicators completely from the perspective of client experience. Independent and unbiased from vendor influence, more than 1,300,000 health care IT users are invited to contribute. Suppliers also encourage their clients to participate in 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

For more information, visit www.blackbookmarketresearch.com

Executive Summary

Black Book Market Research LLC surveyed 2,779 security professionals from 2,404 health systems hospitals, medical practices and health plans to identify gaps, vulnerabilities and deficiencies that persist in keeping providers and payers proverbial sitting ducks for data breaches and cyber-attacks. The good news is that 95% of surveyed professionals understand the risks tackled by cybersecurity and 54% of surveyed healthcare organizations say that security is a top IT concern, up from 19% in post-Covid 2022.

A fragmented mix of 430 vendors offering data security services, core products and solutions, software, consulting, and outsourcing received user feedback including large IT companies, mid and small security vendors,and start-ups in the polling period Q1 to Q4 2023. 79% of healthcare organizations experienced a data breach in the past two years. Despite the sophisticated measures put in place by providers, data breaches are still common. 98% of those IT professionals responding in the healthcare industry believe they are at greater risk for a data breach than other industries as compared to 69% when surveyed in 2019.

The number of cyberattacks on healthcare has risen consistently year after year. In 2009, there were less than 50 attacks overall. By 2013, that number was up to over 300. In 2018, there were 477 breaches of healthcare data, compromising more than five million patient records. Between 2018 and 2019, the number of vulnerability submissions increased nearly 3.5 times, and roughly 30% were critical submissions. The dramatic rise in successful attacks still illustrates how attractive and vulnerable these healthcare enterprises are to exploitation. Despite these wake-up calls, the provider sector remains exceedingly susceptible to ongoing breaches. The striking surge in cyberattacks in the health care sector fueled the demand for cybersecurity services worldwide.

In 2021, 46.1 million users were affected due to healthcare cyberattacks compared to 13.6 million in 2014.

Healthcare executives are expected to invest $140 billion for cybersecurity software, services, outsourcing, advisors, and consulting in 2026. The global healthcare cybersecurity market was valued at $10.6 billion in Q3 2023 and is expected to reach $36 billion dollars by end of this year globally at an estimated CAGR of 20%.

Organizational spending for security risk management technology, managed services and outsourcing rose 18.7% in healthcare enterprises from 2022 to 2023, compared with all industry spends rising 12%.

Cybersecurity compliance in 44% hospitals and inpatient provider centers was compromised due to cyberattacks and attempts in 2022-2023.

The cost of ransomware attacks on US healthcare providers reached $28.2 billion in 2022. Security breaches alone cost healthcare companies $6.6 trillion by the end of 2022.

Data breaches in medical practices and groups increased 72% from 2019 to 2022 and increased 59% in hospitals and health systems during the same period.

Our Q4 2023 analysis revealed the average healthcare data breach costs $697 per record - the highest of any industry for ten straight years. At more than four times the cross-industry average of $170 per record, it is obvious that cyber and data security is one of the most critical concerns for the industry.

Budget constraints have encumbered the practice of replacing legacy software and devices leaving enterprises more susceptible to an attack. It is becoming increasingly difficult for hospitals to find the dollars to invest in an area that does not produce revenue. However, decision-makers must understand that this investment will prevent future losses in other critical business units.

The shortage of healthcare cybersecurity professionals is forcing a rush to acquire services and outsourcing at a pace five times more than cybersecurity products and software solutions. Cybersecurity companies are offering healthcare providers and hospitals with a growing portfolio of services yet to be perfected.

Cybersecurity professionals in the healthcare sector change jobs more frequently than in all other industries. In 2023, 58% of incumbent CISOs and cybersecurity support IT professionals reported an industry job change in the past eighteen months. Responses indicate that the work-related stressors within healthcare were the reason 89% of the job changers left the industry. Average tenure for a healthcare industry cybersecurity professional has decreased from 3.3 years to 1.5 years over the past 5 years.

The lack of qualified cybersecurity professionals entering the healthcare industry workforce is expected to be the cause of at least half of attacks in 2025 according to 97% of respondents.

More Survey Findings:

7% of healthcare organizations reported they felt intimidated by a vendor to retain services when the vendor identified a vulnerability or security flaw, down from 23% in 2019. While the intrinsic nature of cybersecurity radiates pressures and urgency, hospitals shouldn't let this dictate the vendor selection process.

20% of healthcare enterprises have not formally identified specific security objectives and requirements in a strategic and tactical plan, also down from 60% in 2019. Without a clear set of security goals, providers are operating in the dark and it is impossible to measure results. 77% of healthcare organizations have not had a cybersecurity drill with an incident response process despite the skyrocketing cases of data breaches in the healthcare industry.

As of Q4 2023, 15% of providers still do not carry out measurable assessments of their cybersecurity status. Of those that did, 21% used an objective third-party service to benchmark their cybersecurity status, 34% used an objective software solution to benchmark their cybersecurity status, and 26% self-assessed with own criteria.

11% of CIO respondents currently report they do not have an adequate cybersecurity solution to instantly detect and respond to an organizational attack.

67% of surveyed CIOs did not evaluate the total cost of ownership (TCO) before making a commitment to sign their current cybersecurity solution or service contract, only a slight improvement since last year. 77% reported they bought their cybersecurity solution to be compliant, not necessarily to reduce risk when the IT decision was made.

Assessment of Healthcare IT & Data Security Market in 2023

The health care industry progressively depends on the technology that's connected to the internet from patient records and lab results to radiology equipment and hospital elevators. It has proved to be lucrative for patient care, as predominantly it facilitates data integration, patient engagement, and clinical support. On the other hand, those technologies are often vulnerable to cyberattacks, which can siphon off patient data, hijack drug infusion devices, or shut down an entire hospital until a ransom is paid, in the most extreme cases. Cybersecurity fissures include stealing health information and ransomware attacks on hospitals and could also include attacks on implanted medical devices, also known as the "internet of things" devices.

The mounting need for progressive security cloud-based solutions, growing technological developments in cybersecurity, and the incidence of promising government regulations and laws to protect patient information from data breaches is inspiring the expansion of the healthcare cyber security market.

Cyberattacks are usually focused on stealing financial data, billing information and bank account numbers using stolen devices with un-encrypted data, phishing, and spam mails. Other forms of attack focus on physician identities in order to gather license information, insurance login data, or falsify insurance cards or prescriptions. Employee discipline lacking, studies show 84% know the corporate dangers of spam emails yet 29% of hospital staff claimed clicking on suspicious links.

Technological advancements have led to advanced cyber warfare using SQL injections, advanced persistent threats, zero-day attacks, and advanced malware. The rise in the prevalence of cyber-attacks on the confidential data of patients, their transactions and other personal details are anticipated to fuel the growth of the cyber security market.

United States Status

Healthcare companies are increasingly falling victim to sophisticated hacking efforts, insider threats, and basic security flaws despite the highly confidential nature of patient data. As digital health records and connected care continue growing, the healthcare sector struggles to keep pace with modern data protection standards.

According to the data presented by the Atlas VPN team, 87 million patients in the United States had their information breached in 2023. That is more than twice as much as last year when 37 million people had their data exposed.

The data is based on the U.S. Department of Health and Human Services Office for Civil Rights database. Health organizations must report any health data breaches that impact 500 or more people to the secretary, which makes them public.

In 2022, over 37 million patients in the U.S. had their personal information exposed by healthcare organizations. However, breaches have skyrocketed this year. Just in the first half of 2023, hackers stole the data of over 41 million people. The third quarter marked an even greater cause for alarm, with 45 million more patients impacted.

Overall, there have already been 480 reported data breaches across the healthcare sector in the first three quarters of 2023 alone. This compares to only 373 total breaches during the entirety of 2022, highlighting the alarming acceleration in attacks. Each new incident further erodes patient trust.

The largest data incident so far was the HCA Healthcare breach, which impacted 11 million people. The second most significant breach happened at Managed Care of North America. The company found that an unauthorized third party accessed certain systems and stole the data of 8.9 million individuals.

The sensitive nature of medical records makes them highly desirable targets for criminals, thus demanding the strongest security standards. Patients deserve to know their most personal information is safe, and providers must ensure that confidence.

At some point soon, healthcare must view data protection as being just as critical as patient care.

The US Healthcare system reports more data breaches resulting in consumer (patient) data leaks than all other countries combined with over two thousand organizations responsible for the exposures.

Healthcare continues to experience the highest data breach costs of all industries increasing from USD 10.1 Million in 2023 to $11.0 Million in Q4 2023. Over the past three years, the average cost of a data breach in healthcare has grown 55%. Increasing more than US$ 3 million compared to the average cost of $7.1 Million in 2020.

Healthcare faces high levels of industry regulation and is considered critical infrastructure by the US government.

The top cybersecurity challenges for the healthcare industry as identified by survey respondents in Q4 2023 are:

Ransomware attacks (92% strongly agree). Ransomware attacks disrupt hospitals' operations leading to potential interruptions in patient care delivery. Attackers demand large ransom to unlock critical data systems and placing a major financial burden for healthcare organizations.

Human error and Insider threats (80% strongly agree). Healthcare employees are typically overworked and inadvertently compromise security through actions like mishandling patient data or opening phishing emails. Whether intentional or accidental, hospital and medical staff pose a serious threat to data security and patient privacy.

Legacy systems and EHR/RCM software (77% strongly agree). Hospitals and physician practices still rely on legacy systems and outdated software that do not receive regular security updates making them vulnerable to attacks. The cost and compatibility issued of migrating to more secure cloud technologies is still implementing better solutions.

Internet of Medical Objects Device Vulnerabilities (84% agree), The proliferation of medical devices and wearables in healthcare has expanded the cyberattack surface because they lack proper security measures allowing unauthorized access.

For 2024, one of the health systems and hospital boards' top priorities will be cybersecurity. Due to the potential financial impact of data breaches, the leadership is shifting to CFOs. Nearly 85% of executives expressed concern in their readiness to tackle data breaches when cybersecurity is solely under their CIOs responsibility.

Lack of adequate IT spending by healthcare organizations and lack of awareness about cybercrime have exposed the vulnerabilities of healthcare organizations. The overall impact of cyberattacks on the hospitals, physicians, payers and healthcare systems is estimated to be nearly six billion per year.

79% of providers revealed that lack of budget was the major obstacle to properly securing and protecting health information, down from 88% in 2022.

Cyberattacks in the healthcare market have become more sophisticated as phishing and vendors contribute to most of these attacks.

In 2024, these attacks will continue to evolve effecting sectors including cloud vulnerability, AI-enhanced cyber-threats, AI fuzzing, machine learning, smart contract hacking and social engineering attacks.

Roughly 10% of gross domestic product (GDP) of most developed nations is invested yearly in healthcare, making it one of the world's largest and fastest-growing industries, as well as an enormous part of a country's economy.

The Global Industry Classification Standard and the Industry Classification Benchmark further distinguish the healthcare industry as several sectors, and the need of security in each. This vertical is highly diverse, which gives an opportunity to build a strong and growing business that specializes in healthcare. Today, there are four key healthcare segments that can benefit greatly from physical security technologies: Hospitals (including everything from large, enterprise healthcare large networks to small stand-alone facilities); Pharmaceuticals; Health Insurance Firms; Outpatient Diagnostics & Physicians, Facilities.

Most (80%) healthcare vendors admit to lacking minimum security practices, well short of HIPAA standards. Healthcare organizations are often unaware of how many of their vendors have access to protected health information. Furthermore, with a growing number of small and niche healthcare vendors, organizations often struggle to manage their data safety. Healthcare organizations do little to gain assurances or enforce security requirements for vendors. Most healthcare organizations focus due diligence on their largest vendors, but data breach reports and investigations show that over 61% of breaches are attributed to smaller companies.

Buyers of healthcare IT still give their vendors poor performance ratings on security measures & integration. Even after thousands of efforts approximately half of EHR, RCM and other industry software vendors fail to protect healthcare data. This variation is no different than that of 2018.

As the trend line indicates escalations in healthcare data breaches, the approach to understanding cybersecurity must be multi-dimensional to clearly address the risks and find corrective measures in order to minimize the impact of data breaches or cyberattacks proactively.

Essential Functions of IT & Data Security Products and Services

*Functions (also) specific to healthcare security are highlighted in bold red.

Function	Definition
Access Control Mechanism	Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Active Security Testing	Security testing that involves direct interaction with a target, such as sending packets to a target.
Address	Addresses (Cryptocurrency addresses) are used to receive and send transactions on the network. An address is a string of alphanumeric characters, but can also be represented as a scannable QR code.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard specifies a U.S. government approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.
Advanced Key Processor - (AKP)	A cryptographic device that performs all cryptographic functions for a management client node and contains the interfaces to 1) exchange information with a client platform, 2) interact with fill devices, and 3) connect a client platform securely to the primary services node (PRSN).
Altcoin	Altcoin is simply any digital currency alternative to Bitcoin. Many altcoins are forks of Bitcoin with minor changes (e.g. Litecoin).
Anomaly-Based Detection	The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.
Anti-Jam	Countermeasures ensuring that transmitted information can be received despite deliberate jamming attempts.
Anti-Spoof	Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker.
Antispyware Software	A program that specializes in detecting both malware and non-malware forms of spyware.
Anti-Virus Software	Software designed to detect and potentially eliminate viruses before they have had a chance to wreak havoc within the system. Anti-virus software can also repair or quarantine files that have already been infected by virus activity.

API	Application Programming Interface, a software intermediary that helps two separate applications communicate with one another. They define methods of communication between various components.
Approved Security Function	A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either a) specified in an Approved Standard; b) adopted in an Approved Standard and specified either in an appendix of the Approved Standard or in a document referenced by the Approved Standard; or c) specified in the list of Approved security functions.
Attack Sensing and Warning (AS&W)	Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed.
Attack Signature	A specific sequence of events indicative of an unauthorized access attempt. A characteristic byte pattern used in malicious code or an indicator or set of indicators that allows the identification of malicious network activities.
Authentication	Confirming the correctness of the claimed identity of an individual user, machine, software component or any other entity.
Authorization	The approval, permission or empowerment for someone or something to do something.
Authorized Vendor Program (AVP)	Program in which a vendor, producing an information systems security (INFOSEC) product under contract to NSA, is authorized to produce that product in numbers exceeding the contracted requirements for direct marketing and sale to eligible buyers. Eligible buyers are typically U.S. government organizations or U.S. government contractors. Products approved for marketing and sale through the AVP are placed on the Endorsed Cryptographic Products List (ECPL).
Backup	File copies that are saved as protection against loss, damage or unavailability of the primary data. Saving methods include high-capacity tape, separate disk sub- systems or on the Internet. Off-site backup storage is ideal, sufficiently far away to reduce the risk of environmental damage such as flood, which might destroy both the primary and the backup if kept nearby.
Bastion Host	A special-purpose computer on a network specifically designed and configured to withstand attacks.
Blacklisting Software	A form of filtering that blocks only websites specified as harmful. Parents and employers sometimes use such software to prevent children and employees from visiting certain websites. You can add and remove sites from the "not permitted" list. This method of filtering allows for more full use of the Internet but is less efficient at preventing access to any harmful material that is not on the list.
Block Cipher	A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block.
Blockchain	A blockchain is a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Bulk Encryption	Simultaneous encryption of all channels of a multichannel telecommunications link.
Canister	Type of protective package used to contain and dispense keying material in punched or printed tape form.
Capstone Policies	Those policies that are developed by governing or coordinating institutions of Health Information Exchanges (HIEs). They provide overall requirements and guidance for protecting health information within those HIEs. Capstone Policies must address the requirements imposed by: (1) all laws, regulations, and guidelines at the federal, state, and local levels; (2) business needs; and (3) policies at the institutional and HIE levels.
Clear Desk Policy	A policy that directs all personnel to clear their desks at the end of each working day, and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of the "in" and "out" trays —not simply for cleanliness, but also to ensure that sensitive papers and documents are not exposed to unauthorized persons outside of working hours.
Clear Screen Policy	A policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. Typically, the easiest means of compliance is to use a screen saver that engages either on request or after a specified short period of time.
Chain of Custody	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.
Chain of Evidence	A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner.
Challenge and Reply Authentication	Prearranged procedure in which a subject requests authentication of another and the latter establishes validity with a correct reply.
Challenge-Response Protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (often by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret.
Check Word	Cipher text generated by cryptographic logic to detect failures in cryptography.
Checksum	Value computed on data to detect error or manipulation.
Cipher Block Chaining-Message Authentication Code (CBC-MAC)	A secret-key block-cipher algorithm used to encrypt data and to generate a Message Authentication Code (MAC) to provide assurance that the payload and the associated data are authentic.
Cipher Text Auto-Key (CTAK)	Cryptographic logic that uses previous cipher text to generate a key stream.

Ciphony	Process of enciphering audio information, resulting in encrypted speech.
Clearance	Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: confidential, secret, and top secret. A top-secret clearance permits access to top secret, secret, and confidential material; a secret clearance, to secret and confidential material; and a confidential clearance, to confidential material.
Cold Start	Procedure for initially keying crypto equipment
Common Configuration Enumeration (CCE)	A SCAP specification that provides unique, common identifiers for configuration settings found in a wide variety of hardware and software products.
Common Platform Enumeration (CPE)	A SCAP specification that provides a standard naming convention for operating systems, hardware, and applications for the purpose of providing consistent, easily parsed names that can be shared by multiple parties and solutions to refer to the same specific platform type.
Common Vulnerability Scoring System (CVSS)	An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity.
Communications Cover	Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.
Communications Security (COMSEC)	A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.
Compartmentalization	A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone.
Compensating Security Control	A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.
Comprehensive Testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment. Also known as white box Testing
Computer Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
Computer Network Defense (CND)	Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.
Configuration Control	Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.
Cross Certificate	Certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs.
Content Filtering	The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.

Controlled Cryptographic Item (CCI)	Secure telecommunications or information system, or associated cryptographic component, that is unclassified and handled through the COMSEC Material Control System (CMCS), an equivalent material control system, or a combination of the two that provides accountability and visibility. Such items are marked "Controlled Cryptographic Item," or, where space is limited, "CCI".
Cooperative Key Generation	Electronically exchanging functions of locally generated, random components, from which both terminals of a secure circuit construct traffic encryption key or key encryption key for use on that circuit.
Cover-Coding	A technique to reduce the risks of eavesdropping by obscuring the information that is transmitted.
Covert Channel Analysis	Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information.
Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
Cryptographic Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1) (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and 2) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
Cryptographic Logic	The embodiment of one (or more) cryptographic algorithm(s) along with alarms, checks, and other processes essential to effective and secure performance of the cryptographic processes.
Cyclical Redundancy Check (CRC)	A method to ensure data has not been altered after being sent through a communication channel.
Data Origin Authentication	The process of verifying that the source of the data is as claimed, and that the data has not been modified.
Decentralized Application (DApp)	An open source, trustless software application with the backend code running on a decentralized peer-to-peer network rather than a centralized server.
Defense-in-Breadth	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).
Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
Device Distribution Profile	An approval-based Access Control List (ACL) for a specific product that 1) names the user devices in a specific key management infrastructure (KMI) Operating Account (KOA) to which PRSNs distribute product, and 2) states conditions of distribution for each device.
Digital Certificate	The electronic equivalent of an ID card that establishes your credentials when doing business or other transactions on the Web. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Digital Signature	Generated by public key encryption, a digital signature is a code attached to an electronically transmitted document to verify its contents.
Distributed Ledger	Distributed ledgers are a type of database that are spread across multiple sites, countries or institutions. Records are stored one after the other in a continuous ledger. Distributed ledger data can be either "permissioned" or "unpermissioned" to control who can view it.
Electronic Authentication (E- authentication)	The process of establishing confidence in user identities electronically presented to an information system.
Electronic Key Entry	The entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator of the key may have no knowledge of the value of the key being entered.)
Emanations Security (EMSEC)	Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emissions from crypto-equipment or an information system.
Enclave	Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.
Encryption	A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.
Encryption Certificate	Certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing, protecting, and escrowing the private component of the key pair associated with the encryption certificate.
Entrapment	Deliberate planting of apparent flaws in an IS for the purpose of detecting attempted penetrations.
Error Detection Code	A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.
Fail Safe	Automatic protection of programs and/or processing systems when hardware or software failure is detected.
Fail Soft	Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent.
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.
False Acceptance	When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.
Firewall	A hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side.
Firewall Control Proxy	The component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call and direct the firewall to close these ports at call termination.

Firmware	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
Flaw Hypothesis Methodology	System analysis and penetration technique in which the specification and documentation for an information system are analyzed to produce a list of hypothetical flaws. This list is prioritized on the basis of the estimated probability that a flaw exists, on the ease of exploiting it, and on the extent of control or compromise it would provide. The prioritized list is used to perform penetration testing of a system.
Focused Testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing.
Formal Access Approval	A formalization of the security determination for authorizing access to a specific type of classified or sensitive information, based on specified access requirements, a determination of the individual's security eligibility and a determination that the individual's official duties require the individual be provided access to the information.
Full Disk Encryption (FDE)	The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product.
Functional Testing	Segment of security testing in which advertised security mechanisms of an information system are tested under operational conditions.
Graduated Security	A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.
Handshaking Procedures	Dialogue between two information systems for synchronizing, identifying, and authenticating themselves to one another.
Hash-based Message Authentication Code (HMAC)	Hash-based Message Authentication Code – (HMAC) A message authentication code that uses a cryptographic key in conjunction with a hash function.
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Hot Site	A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption.
Hybrid Security Control	A security control that is implemented in an information system in part as a common control and in part as a system-specific control.
Identity Certificate	Certificate that provides authentication of the identity claimed. Within the National Security Systems (NSS) PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures.
Immutable	An inability to be altered or changed over time. This refers to a ledger's inability to be changed by a single administrator, all data once written onto a blockchain can be altered.
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization's information system(s).

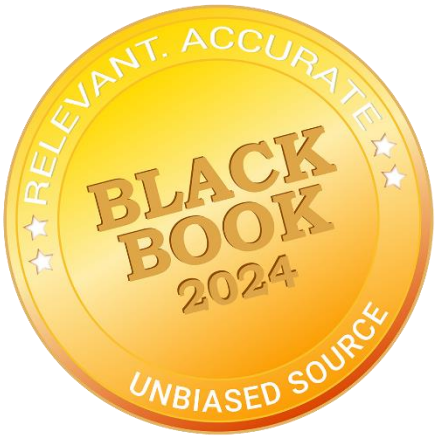
Information Security Continuous Monitoring (ISCM)	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Information Assurance Vulnerability Alert (IAVA)	Notification that is generated when an Information Assurance vulnerability may result in an immediate and potentially severe threat to DoD systems and information; this alert requires corrective action because of the severity of the vulnerability risk.
Internal Security Testing	Security testing conducted from inside the organization's security perimeter.
Interoperability	For the purposes of this standard, interoperability allows any government facility or information system, regardless of the PIV Issuer, to verify a cardholder's identity using the credentials on the PIV Card.
Intrusion Detection Systems (IDS)	Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)
Intrusion Prevention System (IPS)	System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
Kerberos	A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users.
Key Escrow System	A system that entrusts the two components comprising a cryptographic key (e.g., a device unique key) to two key component holders (also called "escrow agents").
Link Encryption	Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line). Since link encryption also encrypts routing data.
Manual Cryptosystem	Cryptosystem in which the cryptographic processes are performed without the use of crypto-equipment or auto-manual devices.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Memory Scavenging	The collection of residual information from data storage.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection.
Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Multi Signature	Multi-signature (multisig) addresses allow multiple parties to require more than one key to authorize a transaction. The needed number of signatures is agreed at the creation of the address. Multi signature addresses have a much greater resistance to theft.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other.
Network Sniffing	A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.
Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Off-line Cryptosystem	Cryptographic system in which encryption and decryption are performed independently of the transmission and reception functions.
Operating System (OS) Fingerprinting	Analyzing characteristics of packets sent by a target, such as packet headers or listening ports, to identify the operating system in use on the target.
Patch	A patch is a small security update released by a software manufacturer to fix bugs in existing programs. Your computer's software programs and/or operating system may be configured to check automatically for patches, or you may need to periodically visit the manufacturers' websites to see if there have been any updates.
Peer Entity Authentication	The process of verifying that a peer entity in an association is as claimed.
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Periods Processing	The processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be purged of all information from one processing period before transitioning to the next.
Permissioned Ledger	A permissioned ledger is a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors — government departments or banks, for example — which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than an unpermissioned ledger.
Print Suppression	Eliminating the display of characters in order to preserve their secrecy.
Profiling	Measuring the characteristics of expected activity so that changes to it can be more easily identified.
Public Key Cryptography	Encryption system that uses a public-private key pair for encryption and/or digital signature.
Public Key Enabling (PKE)	The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation.

Quarantine	Store files containing malware in isolation for future disinfection or examination.
Remediation	The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application.
Resilience	The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.
Resource Encapsulation	Method by which the reference monitor mediates accesses to an information system resource. Resource is protected and not directly accessible by a subject. Satisfies requirement for accurate auditing of resource usage.
Risk Analysis	The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
Root Cause Analysis	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.
Sandboxing	A method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to system resources can also be controlled through a unique identifier associated with each domain.
Scoping Guidance	A part of tailoring guidance providing organizations with specific policy/regulatory- related, technology-related, system component allocation-related, operational/environmental-related, physical infrastructure-related, public access- related, scalability-related, common control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the security control baseline.
Secure Erase	An overwrite technology using firmware-based process to overwrite a hard drive. Is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware? It completes in about 1/8 the time of 5220 block erasure.
SSL (Secure Socket Layer)	An encryption system that protects the privacy of data exchanged by a website and the individual user. Used by websites whose URLs begin with https instead of http.
Security Fault Analysis (SFA)	An assessment, usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered.
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Information & Event Management (SIEM) Tool	Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.
Signature Validation	The (mathematical) verification of the digital signature and obtaining the appropriate assurances (e.g., public key validity, private key possession, etc.).
Signature Verification	The use of a digital signature algorithm and a public key to verify a digital signature on data.

Spam Filtering Software	A program that analyzes emails to look for characteristics of spam, and typically places messages that appear to be spam in a separate email folder
Strong Authentication	The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity.
Super Encryption	Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, online circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted.
Suppression Measure	Action, procedure, modification, or device that reduces the level of, or inhibits the generation of, compromising emanations in an information system.
Tabletop Exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
Tailoring	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.
Threat Analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
Trusted Identification Forwarding	Identification method used in information system networks whereby the sending host can verify an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host.
Tunneling	Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.
Two-Factor Authentication	An extra level of security achieved using a security token device; users have a personal identification number (PIN) that identifies them as the owner of a particular token. The token displays a number which is entered following the PIN number to uniquely identify the owner to a particular network service. The identification number for each user is changed frequently, usually every few minutes.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system.
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome)
Web Content Filtering Software	A program that prevents access to undesirable Web sites, typically by comparing a requested Web site address to a list of known bad Web sites.

Whitelisting Software	A form of filtering that only allows connections to a pre-approved list of sites that are considered useful and appropriate for children. Parents sometimes use such software to prevent children from visiting all but certain websites. You can add and remove sites from the "permitted" list. This method is extremely safe but allows for only extremely limited use of the Internet.
Worm	A program that makes copies of itself and can spread outside your operating system worms can damage computer data and security in much the same way as viruses.
WPA	Wi-Fi Protected Access; a standard designed to improve on the security features of WEP.
Zeroization	A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.
Zero-Day	zero-day (or zero-hour or day zero) attack, threat or virus is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or the software developer, also called zero-day vulnerabilities. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability.



SOLUTIONS RATING RESULTS

HEALTHCARE CYBERSECURITY SOLUTIONS

Survey Overview

From Q3 2019 through Q4 2023, the Black Book Research healthcare cybersecurity solutions client/user survey investigated 404 IT security functional category vendors utilized by 2,779 validated client users for the solutions vendor ratings.

510 healthcare cybersecurity solutions' user respondents qualified in this year's CISO/CIO and healthcare IT leadership provider survey subsets including ad hoc polls to identify trends and industry challenges of CEOS, CFOs & Boards.

Black Book Methodology

How the data sets are collected

Black Book collects ballot results on 18 performance areas of operational excellence to rank vendors by electronic medical and health record product lines. The gathered data are subjected immediately to an internal and external audit to verify completeness and accuracy and to make sure the respondent is valid while ensuring that the anonymity of the client company is maintained. During the audit, each data set is reviewed by a Black Book executive and at least two other people. In this way, Black Book's clients can clearly see how a vendor is truly performing. The 18 criteria on operational excellence are subdivided by the client's industry, market size, geography and function outsourced and reported accordingly.

Situational and market studies are conducted on areas of high interest such as e-Prescribing, Health Information Exchange, Accountable Care organization, hospital software, services providers, educational providers in e-health, bench markers and advisors. These specific survey areas range from four to 20 questions or criteria each.

Understanding the statistical confidence of Black Book data Statistical confidence for each performance rating is based upon the number of organizations scoring the cybersecurity solutions. Black Book identifies data confidence by one of several means:

Top 10 ranked vendors must have a minimum of ten unique clients represented. Broad categories require a minimum of 20 unique client ballots. Data that are asterisked (*) represent a sample size below required limits and are intended to be used for tracking purposes only, not ranking purposes. Performance data for an asterisked vendor's services can vary widely until a larger sample size is achieved.

The margin of error can be very large, and the reader is responsible for considering the possible current and future variation (margin of error) in the Black Book performance score reported.

Vendors with over 20 unique client votes are eligible for top 10 rankings and are assured to have highest confidence and lowest variation. Confidence increases as more organizations report on their outsourcing vendor. Data reported in this form are shown with a 95% confidence level (within a margin of 0.25, 0.20 or 0.15, respectively).

Raw numbers include the quantity of completed surveys and the number of unique organizations contributing the data for the survey pool of interest.

Who participates in the Black Book Ranking process

Over 1,900,000 total provider solutions and services users ranking from hospital and medical practice executives, clinicians, IT specialists and front-line implementation veterans are invited to participate in the 2024 annual Black Book satisfaction surveying. Non-invitation receiving participants must complete a verifiable profile, utilize valid corporate email address, and are then included as well. The Black Book survey web instrument is open to respondents and new participants each year at http://blackbookrankings.com and mobile applications from iTunes and Google Play. Only one ballot per corporate email address is permitted and changes of ballots during the open polling period require a formal email request process to ensure integrity.

The members of 22 professional healthcare associations, 9 media outlets and returning participants with previous identification verifications are among those invited to surveys. Individuals and provider management can register as new participants on mobile applications and online polling instruments. Ballots are validated through two independent survey verification services software companies before being included in the scoring process.

Externally validate users of systems with validated corporate/valid email addresses ranked over four hundred cybersecurity (309 receiving ten or more qualified, unique client site ballots) offering individual or bundled arrangements as part of the Black Book annual survey, conducted via web survey instruments.

Additionally, 1,782 about-to-be users and those in the replacement phases to a non-original cybersecurity system answered questions about budgeting, vendor familiarity and vendor selection processes but current non-user ballots are not counted in the vendor ranking process of client satisfaction.

BLACK BOOK™ RESEARCH

Q4 2023 Healthcare End-to-End/Enterprise Cybersecurity Solutions (Products & Services)

The 7 Subsets of Healthcare End-to-End Cybersecurity Solutions as measured by Black Book™
Data Loss Prevention
Privacy Breach Audits
Network Access Control
Intrusion & Attack Protection
Encryption
Email/Web Filter & Firewalls
Analytics, Predictive AI

2024 TOP END-TO-END HEALTHCARE CYBERSECURITY VENDORS

BLACK BOOK RESEARCH

FUNCTIONAL SUBSET HONORS: END-TO-END CYBERSECURITY PRODUCTS & SERVICES

TOP VENDOR: HOSPITALS UNDER 100 BEDS

CROWDSTRIKE

TOP VENDOR: HOSPITALS 101-300 BEDS

PROOFPOINT

TOP VENDOR: HEALTH SYSTEMS & CORPORATIONS

CROWDSTRIKE

TOP VENDOR: PHYSICIAN PRACTICES & GROUPS

CLEARWATER

Stop Light Scoring Key

FIGURE 1A/B: COMPREHENSIVE END-TO-END VENDORS ARE DEFINED AS BEING COMPRISED OF FOUR SURVEYED FUNCTIONS			
SMALL HOSPITALS	COMMUNITY HOSPITALS	HEALTH SYSTEMS	PHYSICIAN ORGANIZATIONS

Source: Black Book Research

FIGURE 2: KEY TO RAW SCORES			
0.00 – 5.79 ►	◄ 5.80 – 7.32 ►	◄ 7.33 – 8.70 ►	◄ 8.71 – 10.00
Deal breaking dissatisfaction	**Neutral**	**Satisfactory performance**	**Overwhelming satisfaction**
Does not meet expectations	**Meets/does not meet expectations consistently**	**Meets expectations**	**Exceeds expectations**
CANNOT RECOMMEND VENDOR	**WOULD NOT LIKELY RECOMMEND VENDOR**	**RECOMMENDS VENDOR**	**HIGHLY RECOMMENDED VENDOR**

Source: Black Book Research

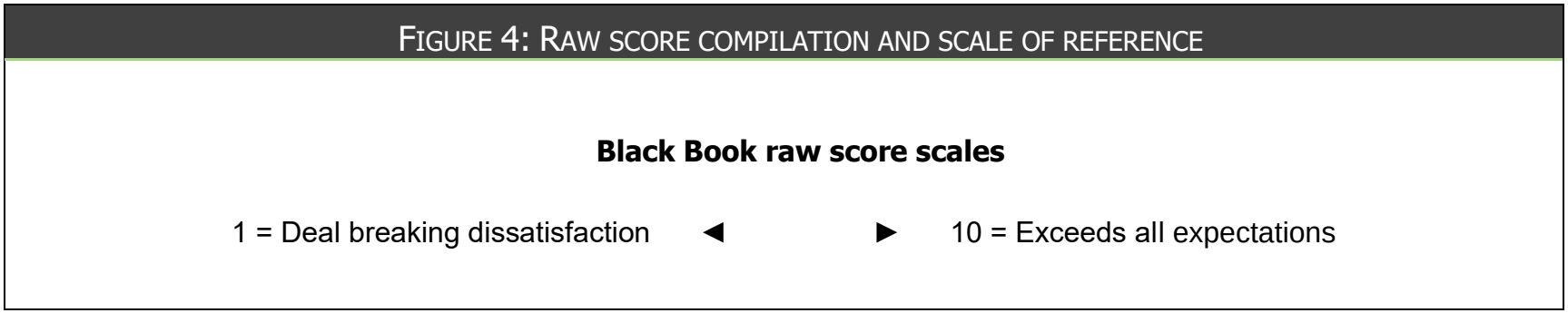
STOP LIGHT SCORING KEY

FIGURE 3: COLOR-CODED STOP LIGHT DASHBOARD SCORING KEY	
Green 8.71 +	**(Top 10%) scores better than 90% of PATIENT PRIVACY MONITORING SOLUTIONS vendors. Green coded vendors have received constantly highest client satisfaction scores.**
Clear **7.33 to 8.70**	**(Top 33%) scores better than 67% of vendors. Well-scored vendor which have middle of the pack results.**
Yellow **5.80 to 7.32**	**Scores better than half of vendors. Cautionary performance scores, areas of improvement required.**
Red **Less than 5.79**	**Scores worse than 66% of vendors. Poor performances reported potential cause for contract.**

Source: Black Book Research

STOP LIGHT SCORING KEY

FIGURE 4: RAW SCORE COMPILATION AND SCALE OF REFERENCE



Source: Black Book Research

Individual vendors can be examined by specific indicators on each of the main functions of vendors as well as grouped and summarized subsets. Details of each subset are contained so that each vendor may be analyzed by function and end-to-end cybersecurity solutions & services collectively.

STOP LIGHT SCORING KEY

FIGURE 5: SCORING KEY							
OVERALL RANK	Q1 CRITERIA RANK	COMPANY	SMALL HOSPITALS	COMMUNITY HOSPITALS	HEALTH SYSTEMS	PHYSICIAN ORGANIZATIONS	MEAN
5	1	VENDOR NAME	8.49	8.63	8.50	8.01	8.66

Source: Black Book Research

- **Overall rank** – this rank references the final position of all 18 criteria averaged by the mean score collectively. This vendor ranked fifth of the 20 competitors.
- **Criteria rank** – refers to the number of the question or criteria surveyed. This is the sixth question of the 18 criteria of which this vendor ranked first of the 20 vendors analyzed positioned only on this particular criteria or question. Each vendor required ten unique client ballots validated to be included in the top ten ranks.
- **Company** – name of the vendor.
- **Subsections** – each subset comprises one-sixth of the total vendor mean at the end of this row and includes all buyers and users who indicate that they contract each respective functional subsection with the supplier, specific to their healthcare enterprise.
- **Mean** – congruent with the criteria rank, the mean is a calculation of all three subsets of functions surveyed. As a final ranking reference, it includes all market sizes, specialties, delivery sites and geographies.

OVERALL KPI LEADERS: END-TO-END HEALTHCARE CYBERSECURITY SOLUTIONS

Summary of criteria outcomes

TABLE 1: SUMMARY OF CRITERIA OUTCOMES		
Total number one criteria ranks	**Vendor**	**Overall rank**
9	**CROWDSTRIKE**	1
4	**INTRAPRISE HEALTH**	2
1	**PROOFPOINT**	3
1	**AT&T CYBERSECURITY**	5
3	**THREATLOCKER**	6

Source: Black Book™ 2023, 2024

OVERALL KPI LEADERS: END-TO-END HEALTHCARE CYBERSECURITY SOLUTIONS

Top score per individual criteria

TABLE 2: TOP SCORE PER INDIVIDUAL CRITERIA

Question	Criteria	Vendor	Overall
1	Strategic Alignment of Client Goals MU VBC MACRA, Breaches	CROWDSTRIKE	1
2	Innovation & Optimization	PROOFPOINT	3
3	Training & Education	CROWDSTRIKE	1
4	Client relationships and cultural fit	INTRAPRISE HEALTH	2
5	Trust, Accountability, Transparency, Ethics	CROWDSTRIKE	1
6	Breadth of offerings, client types, delivery excellence	INTRAPRISE HEALTH	2
7	Deployment and services implementation	INTRAPRISE HEALTH	2
8	Customization	AT&T CYBERSECURITY	5
9	Integration and interfaces	THREATLOCKER	6
10	Scalability, client adaptability, flexible pricing	THREATLOCKER	6
11	Compensation and employee performance	INTRAPRISE HEALTH	2
12	Reliability	CROWDSTRIKE	1
13	Brand image and marketing communications	CROWDSTRIKE	1
14	Marginal value adds and modules	CROWDSTRIKE	1
15	Financial & Managerial Viability	THREATLOCKER	6
16	Data security and backup services	CROWDSTRIKE	1
17	Support and customer care	CROWDSTRIKE	1
18	Best of breed technology and process improvement	CROWDSTRIKE	1

Source: Black Book™ 2023, 2024

TOP HEALTHCARE ENTERPRISE CYBERSECURITY SOLUTIONS RATED SOLUTIONS VENDOR

AGGREGATE KEY PERFORMANCE INDICATOR SCORES AND RANKED BY OVERALL MEAN																				
Rank	**Enterprise Cybersecurity Vendor**	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	**Q17**	**Q18**	**Mean**
1	CROWDSTRIKE	9.60	9.53	9.61	9.38	9.68	9.50	9.30	9.34	9.48	9.42	9.61	9.71	9.72	9.56	9.63	9.56	9.78	9.56	**9.55**
2	INTRAPRISE HEALTH	8.98	8.77	8.85	9.40	9.05	9.57	9.37	9.38	9.42	9.45	9.79	9.40	9.48	9.25	9.62	9.53	9.41	9.20	**9.33**
3	PROOFPOINT	8.51	9.55	9.06	8.86	9.24	9.31	8.74	9.29	9.23	9.16	9.08	9.43	8.87	9.14	8.84	9.16	9.19	9.06	**9.10**
4	CLEARWATER	9.24	8.80	8.86	9.32	8.37	8.27	9.07	9.05	9.30	9.28	8.94	8.56	9.25	8.67	9.21	9.33	9.39	9.13	**9.00**
5	AT&T	8.99	7.77	9.08	8.83	7.90	9.12	9.22	9.44	8.89	8.70	9.73	9.33	9.22	8.30	9.46	8.93	9.23	9.45	**8.98**
6	THREATLOCKER	8.45	8.92	8.77	9.01	9.20	6.37	9.35	8.87	9.49	9.53	8.47	9.28	9.11	8.98	9.50	8.92	9.20	8.89	**8.91**
7	FORTINET	8.54	8.78	8.33	9.30	8.43	6.31	9.02	9.02	8.78	9.02	8.99	8.76	8.00	9.04	8.77	9.28	9.07	8.55	**8.67**
8	TREND MICRO	8.02	9.00	9.40	7.40	7.75	9.10	9.11	8.50	8.95	8.66	7.18	9.20	8.79	8.69	9.83	9.27	8.08	9.11	**8.67**
9	COALFIRE	7.60	9.31	9.03	7.57	6.89	9.39	8.83	8.81	9.49	7.87	9.32	8.96	9.07	8.09	9.05	8.70	9.10	8.22	**8.63**
10	PALO ALTO	8.45	9.09	7.99	7.86	7.69	9.25	9.23	7.10	8.19	7.53	8.64	8.71	8.06	9.16	9.41	9.34	8.17	8.74	**8.48**
11	RAPID7	7.74	9.28	8.38	8.52	8.88	7.16	7.77	8.65	7.51	7.64	8.55	8.04	6.12	8.25	8.93	8.60	8.93	8.66	**8.20**
12	RADWARE	8.11	7.92	8.54	7.76	7.52	9.08	8.74	7.14	6.82	6.21	8.66	8.40	9.36	8.50	9.21	8.64	8.45	8.37	**8.19**
13	IBM	7.20	8.99	7.75	7.45	8.75	8.04	8.42	7.05	6.94	9.49	8.83	7.74	9.26	7.33	8.83	8.14	7.72	8.24	**8.12**
14	FIREEYE	7.40	7.68	7.55	8.57	8.70	7.71	7.39	8.57	8.47	6.00	7.86	8.83	8.12	9.23	8.84	8.58	9.13	7.26	**8.11**
15	IMPRIVATA	6.18	7.20	7.97	7.56	8.71	8.26	7.14	8.13	8.52	9.25	8.98	7.65	5.59	8.91	7.26	8.75	8.43	8.51	**7.94**
16	ORACLE	6.90	6.87	8.23	8.58	8.05	6.83	6.39	8.55	5.77	9.36	8.76	6.68	9.03	7.17	8.97	8.49	9.08	8.35	**7.89**
17	IMPERVA	7.07	7.59	6,86	7.67	6.72	9.00	8.17	7.76	9.10	8.31	8.00	7.69	6.54	7.81	9.76	9.47	7.34	7.21	**7.51**
18	CISCO	6.65	5.90	7.58	8.58	6.60	8.41	8.16	8.02	7.65	8.08	8.97	8.13	5.24	5.17	7.66	8.04	9.18	7.15	**7.51**
19	CHECKPOINT	6.29	5.93	7.99	7.83	6.76	8.59	7.77	6.22	8.39	5.46	7.77	6.05	7.16	4.88	7.99	8.14	5.98	6.09	**6.96**
20	GAVS	5.65	5.94	5.96	6.75	5.62	6.03	5.99	5.56	7.64	6.22	7.54	7.10	5.79	6.02	5.46	8.02	7.79	6.04	**6.40**

HEALTHCARE CYBERSECURITY VENDOR KEY PERFORMANCE INDICATORS:

1. Strategic Alignment of Vendor Offerings to Customer Goals & Client'3s Mission (MACRA, MU, ONC, HIE, Breaches, RCM)

Table 5: Organizational structure meets the needs of stakeholders or customers and stakeholder satisfaction is the most important priority. Financial digital transformation solutions client is likely to recommend the vendor to similar sized provider organizations within the same geography, specialty or delivery setting.

Overall Rank	Q1 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
1	1	CROWDSTRIKE	9.63	9.40	9.53	9.83	9.60
4	2	CLEARWATER	9.47	9.18	8.44	9.98	9.24
5	3	AT&T	9.01	8.94	9.58	8.41	8.99
2	4	INTRAPRISE HEALTH	8.84	8.79	9.25	9.02	8.98
7	5	FORTINET	8.90	8.43	8.51	8.32	8.54
3	6	PROOFPOINT	8.58	7.76	9.68	8.00	8.51
6	7	THREATLOCKER	9.24	8.72	8.47	7.36	8.45
11	8	RAPID7	8.50	7.81	7.72	6.92	7.74
9	9	COALFIRE	7.06	7.52	7.71	8.11	7.60
10	10	PALO ALTO	7.95	7.24	6.57	8.02	7.45

Source: Black Book™ 2023, 2024

HEALTHCARE CYBERSECURITY VENDOR KEY PERFORMANCE INDICATORS:

2. Innovation and Optimization

Table 6: Customers are also continuing to push the envelope for further enhancements to which the vendor is responsive. Cybersecurity solutions clients also believe that their vendors' technology is helping them manage business and care units more effectively, generate accurate records and reimbursement billings and cut their overhead in ways that were difficult or impossible to accomplish before electronic medical records were implemented. Vendor is responsive to make client recommendations with cutting edge improvements.

Overall Rank	Q2 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
3	1	PROOFPOINT	9.70	9.30	9.70	9.48	9.55
1	2	CROWDSTRIKE	9.55	9.66	9.72	9.18	9.53
9	3	COALFIRE	9.13	9.39	9.50	9.21	9.31
11	4	RAPID7	9.11	8.87	9.58	9.55	9.28
10	5	PALO ALTO	8.68	9.31	9.41	8.96	9.09
8	6	TREND MICRO	8.54	8.98	9.20	9.26	9.00
13	7	IBM	8.88	9.20	9.09	8.78	8.99
6	8	THREATLOCKER	9.04	9.18	8.91	8.55	8.92
4	9	CLEARWATER	8.61	8.70	8.78	9.10	8.80
7	10	FORTINET	8.70	8.66	8.65	9.10	8.78

Source: Black Book™ 2023, 2024

HEALTHCARE CYBERSECURITY VENDOR KEY PERFORMANCE INDICATORS:

3. Training

Table 7: Cybersecurity vendor leadership provides significant and meaningful training opportunities for internal employees and client staff. Leadership strives to develop technology staff, client service and customer servicing consultant employees. Training modules are effective and practical so that minimal post-implementation training is required on or off site. Regular updates are timely and require minimal additional training to implement.

Overall Rank	Q3 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
1	1	CROWDSTRIKE	9.71	9.82	9.55	9.36	9.61
8	2	TREND MICRO	9.37	9.34	9.41	9.46	9.40
5	3	AT&T	9.17	8.97	9.04	9.15	9.08
3	4	PROOFPOINT	9.02	9.24	9.69	8.27	9.06
9	5	COALFIRE	9.22	9.02	8.63	9.26	9.03
4	6	CLEARWATER	8.67	9.04	8.25	9.46	8.86
2	7	INTRAPRISE HEALTH	8.60	8.72	9.25	8.83	8.85
6	8	THREATLOCKER	9.51	8.17	8.90	8.50	8.77
11	9	RAPID7	7.64	7.77	8.85	9.06	8.33
7	10	FORTINET	8.16	8.22	8.52	8.40	8.33

Source: Black Book™ 2023, 2024

4. Client relationships and cultural fit

Table 8: Cybersecurity solutions vendor leadership honors customer relationships highly. The relationship with the vendor elevates the customer reputation. Improving practice and healthcare delivery efficiency and effectiveness is a priority of the supplier. Governance of engagement is neither complex for buyer nor does it require vendor management attention regularly. There is no regular transparency or quality issue. There are no culture clashes or misfits that threaten relationship's success or client's satisfaction.

Overall Rank	Q4 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
2	1	INTRAPRISE HEALTH	9.42	9.51	9.39	9.28	9.40
1	2	CROWDSTRIKE	9.02	9.44	9.58	9.48	9.38
4	3	CLEARWATER	9.00	9.14	9.48	9.64	9.32
7	4	FORTINET	9.19	9.45	9.30	9.24	9.30
6	5	THREATLOCKER	9.03	9.19	9.14	8.67	9.01
3	6	PROOFPOINT	8.57	9.14	9.67	8.05	8.86
5	7	AT&T	8.35	8.82	8.94	9.21	8.83
16	8	ORACLE	8.89	9.30	8.50	7.63	8.58
18	9	CISCO	8.84	9.05	8.65	7.79	8.58
14	10	FIREEYE	7.92	8.65	8.69	9.00	8.57

Source: Black Book™ 2023, 2024

5. Trust, Accountability, Ethics and Transparency

Table 9: Trust in enterprise reputation is important to cybersecurity solutions clients as well as prospects. Client possesses an understanding that its vendor organization has the people, processes, and resources to effectively deliver the desired business and clinical results, based on its industry reputation and past performance. There are no disconnects between promises and delivery.

Overall Rank	Q5 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
1	1	CROWDSTRIKE	9.77	9.57	9.59	9.77	9.68
3	2	PROOFPOINT	9.23	8.59	9.51	9.36	9.24
6	3	THREATLOCKER	9.55	9.12	9.09	9.05	9.20
2	4	INTRAPRISE HEALTH	8.99	9.13	9.07	9.01	9.05
11	5	RAPID7	9.14	8.59	9.04	8.76	8.88
13	6	IBM	9.00	9.10	8.62	8.26	8.75
15	7	IMPRIVATA	8.74	8.32	9.05	8.73	8.71
14	8	FIREEYE	8.69	8.06	8.67	8.82	8.56
7	9	FORTINET	8.20	8.52	8.08	8.91	8.43
4	10	CLEARWATER	8.62	7.89	7.87	9.10	8.37

Source: Black Book™ 2023, 2024

6. Breadth of offerings, varied client settings, delivery excellence across all user types

Table 10: Cybersecurity solutions vendor offers industry recognized horizontal functionality and vertical industry applications and manage bundled services and developing new healthcare technology initiatives. Vendor routinely drives operational performance improvements and results in the areas they affect. Comprehensive offerings are constructed to meet the unique needs of the client's IT initiatives. Breadth of vendor modules offers comprehensive system services and broad modules.

Overall Rank	Q6 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
2	1	INTRAPRISE HEALTH	9.57	9.63	9.54	9.54	9.57
1	2	CROWDSTRIKE	9.42	9.29	9.65	9.65	9.50
9	3	COALFIRE	9.48	9.40	9.15	9.53	9.39
3	4	PROOFPOINT	9.35	9.38	9.53	8.97	9.31
10	5	PALO ALTO	9.50	9.45	9.25	8.79	9.25
5	6	AT&T	9.58	9.21	8.99	8.71	9.12
8	7	TREND MICRO	9.31	8.98	8.73	9.38	9.10
12	8	RADWARE	8.68	9.31	9.19	9.15	9.08
17	9	IMPERVA	9.09	8.52	9.25	9.14	9.00
19	10	CHECKPOINT	8.54	8.27	9.02	8.54	8.59

Source: Black Book™ 2023, 2024

7. Deployment and solutions implementation

Table 11: Cybersecurity solutions client deploys at a pace acceptable to the client. Cyber technology solutions eliminate excessive supervision over vendor implementations. Vendor overcomes client implementation obstacles and challenges effectively. Technical, organizational and cultural implementation obstacles are handled professionally and punctually. Software implementation time meets standard expectations. Implementations are efficient and sensitive to users' specific situations which may cause delays.

Overall Rank	Q7 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
2	1	INTRAPRISE HEALTH	9.37	9.65	9.50	8.97	9.37
6	2	THREATLOCKER	9.42	9.58	9.43	8.95	9.35
1	3	CROWDSTRIKE	9.06	8.80	9.69	9.65	9.30
10	4	PALO ALTO	9.30	9.10	9.37	9.15	9.23
5	5	AT&T	9.27	9.19	9.09	9.31	9.22
8	6	TREND MICRO	8.70	9.03	9.24	9.48	9.11
4	7	CLEARWATER	8.63	9.07	8.66	9.93	9.07
7	8	FORTINET	9.03	8.89	9.13	9.03	9.02
9	9	COALFIRE	9.19	8.70	8.73	8.68	8.83
3	10	PROOFPOINT	8.73	8.76	8.90	8.57	8.74

Source: Black Book™ 2023, 2024

8. Customization

Table 12: Cybersecurity products and process services are customized to meet the unique needs of specific provider client purpose, processes and care delivery models. Little resistance is encountered when changing performance measurements as clients' needs vary. Extraordinary efforts are made to adapt and convert client special needs into workable solutions with efficient cost and time considerations. Cybersecurity software and services allows for modifications that are not costly or complex.

Overall Rank	Q8 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
5	1	AT&T	9.51	9.49	9.42	9.33	9.44
2	2	INTRAPRISE HEALTH	9.47	9.46	9.41	9.18	9.38
1	3	CROWDSTRIKE	9.07	8.91	9.69	9.69	9.34
3	4	PROOFPOINT	9.24	9.01	9.71	9.21	9.29
4	5	CLEARWATER	9.17	8.79	8.54	9.71	9.05
7	6	FORTINET	8.48	9.58	9.32	8.69	9.02
6	7	THREATLOCKER	8.05	9.00	9.23	9.21	8.87
9	8	COALFIRE	8.97	8.84	9.27	8.14	8.81
11	9	RAPID7	8.89	9.51	7.97	8.23	8.65
14	10	FIREEYE	8.77	9.24	8.62	7.65	8.57

Source: Black Book™ 2023, 2024

9. Integration and interfaces

Table 13: Cybersecurity solutions vendor supports interfaces so information can be shared between necessary applications. Solutions are easily integrated to existing backend systems as needed and HIE feasible. Seamless interfaces to legacy applications are performed as required for optimal functioning. Human integration and interface activities are administered precisely. Systems communicate effectively among provider groups and ancillaries. True interoperability with other healthcare organizations is factored into implementation.

Overall Rank	Q9 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
6	1	THREATLOCKER	9.61	9.65	9.30	9.40	9.49
1	2	CROWDSTRIKE	9.72	9.55	9.24	9.41	9.48
9	3	COALFIRE	9.55	9.00	9.70	9.67	9.48
2	4	INTRAPRISE HEALTH	9.48	9.55	9.30	9.34	9.42
4	5	CLEARWATER	8.90	9.21	9.24	9.86	9.30
3	6	PROOFPOINT	9.00	9.27	9.62	9.03	9.23
17	7	IMPERVA	9.12	9.45	9.05	8.77	9.10
8	8	TREND MICRO	9.26	9.32	8.72	8.49	8.95
5	9	AT&T	8.92	8.93	8.67	9.05	8.89
7	10	FORTINET	8.54	9.16	9.46	7.96	8.78

Source: Black Book™ 2023, 2024

10. Scalability, client adaptability, flexible pricing

Table 14: Cybersecurity solutions vendor provides flexible pricing allowing the client to choose and pay for the precise functionality and services needed. Vendor Invests in significant infrastructure and has the ability to provide services to enterprise organizations. IT products and services meet the changing and varied needs of the respective customer. Pricing is not rigid or shifting and meets needs of client.

Overall Rank	Q10 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
6	1	THREATLOCKER	9.35	9.76	9.60	9.39	9.53
13	2	SIMUND AURA	9.70	9.82	9.37	9.06	9.49
2	3	INTRAPRISE HEALTH	9.55	9.62	9.52	9.10	9.45
1	4	CROWDSTRIKE	8.83	9.29	9.74	9.82	9.42
16	5	ORACLE	9.64	9.82	8.85	9.11	9.36
4	6	CLEARWATER	9.00	9.04	9.12	9.95	9.28
15	7	IMPRIVATA	9.47	9.66	9.39	8.46	9.25
3	8	PROOFPOINT	9.19	9.10	9.62	8.71	9.16
7	9	FORTINET	9.19	9.47	8.65	8.75	9.02
5	10	AT&T	8.82	8.99	8.92	8.06	8.70

Source: Black Book™ 2023, 2024

11. Vendor staff expertise, compensation and employee performance

Table 15: Cybersecurity solutions vendor team of employees is considered top in industry for professionalism and skill. Vendor attracts and retains high performing staff. Vendor is focused on building and developing a strong employee team of producers. Employees act like owners/leaders. Company is moving towards leveraged pay at all levels. Vendor is using effective tools to tie performance metrics to compensation policy and compensating top leaders. Human resources-related criteria are scored from the client perspective on this indicator.

Overall Rank	Q11 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
2	1	INTRAPRISE HEALTH	9.86	9.86	9.75	9.69	9.79
5	2	AT&T	9.85	9.79	9.71	9.56	9.73
1	3	CROWDSTRIKE	9.29	9.55	9.86	9.75	9.61
9	4	COALFIRE	9.29	9.63	9.39	8.96	9.32
3	5	PROOFPOINT	8.75	9.21	9.59	8.76	9.08
7	6	FORTINET	9.43	9.14	8.89	8.48	8.99
15	7	IMPRIVATA	9.50	9.35	9.01	8.07	8.98
18	8	CISCO	8.93	9.40	8.87	8.68	8.97
4	9	CLEARWATER	8.28	8.94	8.79	9.74	8.94
13	10	IBM	9.31	8.19	9.26	8.55	8.83

Source: Black Book™ 2023, 2024

12. Reliability

Table 16: Cybersecurity solutions supplier meets agreed terms as evidenced by routine, acceptable service level reporting and industry expectations. Depth and breadth of applications/solutions are acceptable in meeting client needs. Online reliability meets expectations, and outages/downtimes are minimized. Solid product and service capacities are demonstrated consistently. Service levels are consistently met as agreed. Services and support response is expedient and provided with appropriate resources by vendor team.

Overall Rank	Q12 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
1	1	CROWDSTRIKE	9.70	9.72	9.82	9.61	9.71
3	2	PROOFPOINT	9.07	9.19	9.76	9.68	9.43
2	3	INTRAPRISE HEALTH	9.59	9.64	9.05	9.31	9.40
5	4	AT&T	9.45	9.42	9.13	9.30	9.33
6	5	THREATLOCKER	9.56	9.72	8.76	9.08	9.28
8	6	TREND MICRO	9.49	9.66	9.00	8.66	9.20
9	7	COALFIRE	8.97	8.72	8.75	9.39	8.96
14	8	FIREEYE	9.06	8.79	8.72	8.74	8.83
7	9	FORTINET	9.30	9.42	8.26	8.04	8.76
10	10	PALO ALTO	8.65	9.15	8.77	8.25	8.71

Source: Black Book™ 2023, 2024

13. Brand image and marketing communications

Table 17: Cybersecurity solutions vendor's marketing and sales statements/pitches are accurately and appropriately represented by actual product and service deliverables. The image is consistent with top software and services rankings. Sales presentations and proposals are delivered upon and corporate integrity/honesty in marketing and business development are highly valued. Company image and integrity are values upheld top-down consistently. An elevated level of relevant client communications enhances the vendor – customer/user relationship.

Overall Rank	Q13 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
1	1	CROWDSTRIKE	9.43	9.70	9.88	9.86	9.72
2	2	INTRAPRISE HEALTH	9.71	9.75	9.45	8.99	9.48
12	3	RADWARE	9.50	9.55	9.36	9.02	9.36
13	4	IBM	9.69	9.44	9.07	8.85	9.26
4	5	CLEARWATER	9.12	9.57	9.33	8.99	9.25
5	6	AT&T	9.66	9.63	8.93	8.67	9.22
6	7	THREATLOCKER	9.28	9.46	8.95	8.76	9.11
9	8	COALFIRE	9.23	9.26	9.11	8.69	9.07
16	9	ORACLE	9.20	9.22	8.90	8.80	9.03
3	10	PROOFPOINT	8.42	8.08	9.66	9.31	8.87

Source: Black Book™ 2023, 2024

14. Marginal value adds

Table 18: Beyond stimulus achievement, the vendors' cost savings are realized as generally estimated and not over-positioned or over/underestimated in ways that affect major client satisfaction or costs. Vendor offers value-adds as a cybersecurity management partner in cost savings and avoidance initiatives and creative programs through bundled product design. Provides true business transformation opportunities to physician practices, hospitals and other healthcare delivery settings utilizing digital transformation solutions.

Overall Rank	Q14 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
1	1	CROWDSTRIKE	9.31	9.79	9.40	9.74	9.56
2	2	INTRAPRISE HEALTH	9.37	9.42	9.16	9.04	9.25
14	3	FIREEYE	9.73	9.54	8.50	9.15	9.23
10	4	PALO ALTO	9.52	9.69	8.72	8.71	9.16
3	5	PROOFPOINT	9.43	8.52	9.53	9.08	9.14
7	6	FORTINET	9.23	9.41	8.79	8.71	9.04
6	7	THREATLOCKER	9.47	8.87	8.21	9.37	8.98
15	8	IMPRIVATA	9.36	9.39	8.94	7.96	8.91
8	9	TREND MICRO	9.40	8.86	8.40	8.08	8.69
4	10	CLEARWATER	8.72	9.45	8.69	7.83	8.67

Source: Black Book™ 2023, 2024

15. Viability and managerial stability

Table 19: Vendor's viability, employee turnover, data security stability and/or cultural mismatches do not threaten relationship. Senior management and the board exemplify strong leadership principals to steward appropriate resources that impact buyers. Client is confident of long term industry viability for this vendor based on investments, client adoption, exceptional outcomes and service levels. Field management is notably competent, stable and supportive of clients. The vendor demonstrates and provides evidence of competent fiscal management and leadership.

Overall Rank	Q15 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
6	1	THREATLOCKER	9.87	9.87	9.82	9.77	9.83
17	2	IMPERVA	9.81	9.82	9.68	9.72	9.76
1	3	CROWDSTRIKE	9.52	9.31	9.87	9.82	9.63
2	4	INTRAPRISE HEALTH	9.74	9.68	9.49	9.56	9.62
4	5	CLEARWATER	9.65	9.64	9.60	9.10	9.50
5	6	AT&T	9.54	9.66	9.31	9.32	9.46
10	7	PALO ALTO	9.57	9.51	9.29	9.26	9.41
8	8	TREND MICRO	9.42	9.70	8.89	8.84	9.21
12	9	RADWARE	9.70	9.67	9.19	8.29	9.21
9	10	COALFIRE	9.15	8.61	9.41	9.01	9.05

Source: Black Book™ 2023, 2024

16. Data security and backup services

Table 20: In order to provide secure and constantly dependable service offerings for affiliated business units and provider entities, a vendor has to provide the highest level of security and data back-up services. The vendor's service in these two areas is superior to the security and back-up system of past internal systems of the provider organization, Cybersecurity practices and protections meet or exceed industry standards and regulations.

Overall Rank	Q16 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
1	1	CROWDSTRIKE	9.68	9.70	9.34	9.51	**9.56**
2	2	INTRAPRISE HEALTH	9.68	9.57	9.59	9.29	**9.53**
17	3	IMPERVA	9.46	9.55	9.51	9.35	**9.47**
10	4	PALO ALTO	9.02	8.98	9.65	9.70	**9.34**
4	5	CLEARWATER	9.65	9.52	8.98	9.18	**9.33**
7	6	FORTINET	9.50	9.68	9.03	8.89	**9.28**
8	7	TREND MICRO	8.98	9.50	9.18	9.42	**9.27**
3	8	PROOFPOINT	9.10	9.36	9.46	8.70	**9.16**
5	9	AT&T	9.55	9.04	8.70	8.42	**8.93**
6	10	THREATLOCKERF	8.63	9.59	8.82	8.62	**8.92**

Source: Black Book™ 2023, 2024

17. Support and customer care

Table 21: Account management provides an adequate amount of onsite administration and support to clients. There exists a formal account management program that meets client needs. Media and clients reference this vendor as an Cybersecurity solutions and services leader and top vendor correctly. Customer services and relationship satisfaction is manifested through significant flagship clients as well as smaller and newest customers similarly. Vendor provides appropriate number of accessible support and customer care personnel.

Overall Rank	Q17 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
1	1	CROWDSTRIKE	9.63	9.89	9.76	9.83	**9.78**
2	2	INTRAPRISE HEALTH	9.75	9.40	9.15	9.43	**9.41**
4	3	CLEARWATER	9.56	9.37	9.60	9.02	**9.39**
5	4	AT&T	9.39	9.68	8.93	8.93	**9.23**
6	5	THREATLOCKER	9.65	9.44	8.91	8.81	**9.20**
3	6	PROOFPOINT	9.11	9.21	9.82	8.63	**9.19**
18	7	CISCO	9.57	9.04	9.45	8.67	**9.18**
14	8	FIREEYE	9.48	9.57	8.87	8.60	**9.13**
9	9	COALFIRE	9.33	9.60	9.39	8.06	**9.10**
16	10	ORACLE	9.20	9.69	8.89	8.54	**9.08**

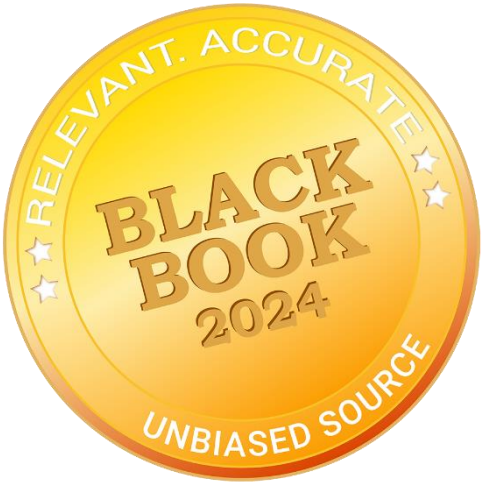
Source: Black Book™ 2023, 2024

18. Best of breed technology and process improvement developments

Table 22: Vendor management and related technology services are considered best of breed. The vendor technology elevates customers via capabilities, equipment, processes, deliverables, professional staff, leadership, quality assurance and innovative initiatives. Vendor services are delivered at or above current/former in-house service levels. Technology is current and relevant to protecting and securing all health information as prescribed and required by client. Vendor efforts continue to constantly update and improve the product and service.

Overall Rank	Q18 Criteria Rank	Cybersecurity Vendor	Small Hospitals	Community Hospitals	Health Systems	Physician Organizations	Mean
1	1	CROWDSTRIKE	9.68	9.21	9.85	9.50	**9.56**
5	2	AT&T	9.50	9.53	8.96	9.82	**9.45**
2	3	INTRAPRISE HEALTH	9.30	9.15	9.10	9.26	**9.20**
4	4	CLEARWATER	9.42	8.97	9.44	8.68	**9.13**
8	5	TREND MICRO	8.95	9.00	9.19	9.30	**9.11**
3	6	PROOFPOINT	8.73	9.26	8.27	8.99	**9.06**
6	7	THREATLOCKER	9.08	8.81	8.39	9.29	**8.89**
10	8	PALO ALTO	8.98	9.19	8.71	8.09	**8.74**
11	9	RAPID7	8.49	8.81	8.61	8.73	**8.66**
7	10	FORTINET	8.04	8.99	8.63	8.52	**8.55**

Source: Black Book™ 2023, 2024



Top Healthcare Cybersecurity Solutions Client Ratings

PRODUCTS
SOFTWARE
SERVICES
OUTSOURCING
CONSULTING

Contact Black Book Research for complete score cards of client ratings by category or for more information on each solution report.

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Cybersecurity Assessment & Advisory

Cybersecurity Consultants
1. CLEARWATER
2. MEDITOLOGY
3. ACCENTURE
4. PIVOT POINT
5. CHARTIS
6. FORTIFIED HEALTH SECURITY
7. CHECKPOINT
8. DELOITTE
9. AT&T CYBERSECURITY
10. ATOS
11. HURON
12. TRUENORTH
13. VC3
14. OPTIV
15. PROTIVITI

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Identity Governance & Administration

Identity Governance
1. CYBERARK
2. LEXIS NEXIS RISK SOLUTIONS
3. ONE LOGIN
4. NET IQ
5. RSA
6. OKTA
7. SAILPOINT
8. IBM SECURE VERIFY
9. SAVIYNT
10. IMPRIVATA
11. FORGEROCK
12. AVATIER
13. TENFOLD
14. OMADA IDENTITY
15. OPTIMAL

Product or Service: Patient Privacy Monitoring

Patient Privacy & HIPAA Solutions
1. IATRIC SYSTEMS HAYSTACK SOLUTIONS
2. CLEARWATER SECURITY
3. INTRUNO
4. PROTENUS
5. SECURELINK
6. IMPRIVATA (FORMERLY MAIZE ANALYTICS) PRIVACY MONITOR
7. IDEXPERTS MIDAS
8. IMPRIVATA (FORMERLY FAIRWARNING) PATIENT PRIVACY INTELLIGENCE
9. AT&T HEALTHCARE
10. EXPERIAN
11. CONVERGEPOINT
12. FOGHORN
13. BLUE FIN
14. IDENTITYFORCE
15. SEDARA SECURITY

2024 Top Healthcare Cybersecurity Vendors

Product or Service: End-to-End Enterprise Cybersecurity Suite

Enterprise Cybersecurity Suite & Comprehensive Organizational Solutions
1. CROWDSTRIKE
2. INTRAPRISE HEALTH
3. PROOFPOINT
4. CLEARWATER
5. AT&T CYBERSECURITY
6. THREATLOCKER
7. FORTINET
8. TREND MICRO
9. SONICWALL
10. PALO ALTO NETWORKS
11. RAPID7
12. RADWARE
13. IBM
14. FIREEYE
15. IMPRIVATA
16. ORACLE
17. IMPERVA
18. CISCO
19. CHECK POINT
20. GAVS

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Application Testing Security Solutions

Application Testing Solutions
1. HEALTHASYST
2. SCIENCESOFT
3. QUALTEST
4. VERACODE
5. VENTION
6. SYNOPSYS
7. STACKHAWK
8. RAPID7
9. CIGNITI
10. RHINO SECURITY LABS
11. QUALITEST
12. CAPGEMINI
13. AUDACIX
14. TESTBYTES
15. QA MENTOR

Product or Service: DDOS

DDOS Solutions
1. RADWARE
2. FORTINET
3. NETSCOUT
4. BLACKBERRY CYLANCE
5. SOPHOS
6. IMPERVA
7. HUNTERS.AI
8. CLOUDFLARE
9. GAVS NETWORKS
10. ARBOR NETWORKS
11. NEXUSGUARD
12. MCAFEE
13. ROOT 9B
14. CODE DX
15. A10 NETWORKS

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Authentication and Authorization

Authentication & Authorization Solutions
1. IMPERVA
2. NETSCOUT
3. RADWARE
4. CLOUDFLARE
5. AMAZON WEB SERVICES
6. VERIZON
7. GAVS AZURE
8. IMPRIVATA
9. SECUREAUTH
10. FIREEYE
11. SAILPOINT
12. IDAPTIVE
13. AUTH0
14. CENTRIFY
15. OKTA

Product or Service: Blockchain-Enabled Secure Digital Collaboration Platforms

Secure Data Collaboration Solutions
1. AVANEER HEALTH
2. BURSTIQ
3. SOLULAB
4. HASHED HEALTH
5. EMBLEEMA
6. MEDICAL CHAIN
7. PATIENTORY
8. CORAL HEALTH
9. AKIRI
10. IBM BLOCKCHAIN
11. GUARDTIME
12. SHARECARE
13. ORACLE
14. VELVETECH
15. TIERION

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Secure Cloud Solutions

Cloud Solutions
1. CLEARDATA
2. AMAZON WEB SERVICES (AWS)
3. GAVS AZURE
4. GOOGLE
5. NETSKOPE
6. QUALYS
7. SYMANTEC
8. REDLOCK BY PALO ALTO
9. DELOITTE
10. CHECKPOINT
11. CLOUD PASSAGE HALO
12. LACEWORK
13. TREND MICRO
14. THREAT STACK
15. CLOUDGUARD

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Compliance & Risk Management Solutions

Compliance & Risk Management Solutions
1. CLEARWATER
2. COALFIRE
3. HEALTHICITY COMPLIANCE MANAGER
4. COMPLIANCY GROUP
5. SERA-BRYNN
6. ACCENTURE
7. IMPRIVATA FAIRWARNING
8. EY
9. DELOITTE
10. KPMG
11. NAVIGATE
12. CHANGE HEALTHCARE
13. CONVERGEPOINT
14. DIGITAL DEFENSE
15. CIMCOR

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Cyber Threat Awareness & Training

Staff Awareness & Training Solutions
1. FORTIFIED HEALTH SECURITY
2. PHISHLABS
3. PROOFPOINT/WOMBAT
4. MEDPRO GROUP
5. ESET TRAINING
6. GREYCASTLE SECURITY
7. KNOWBE4
8. THE SANS INSTITUTE
9. INFOSEC INSTITUTE
10. COFENSE
11. TERRANOVA
12. INSPIRED ELEARNING
13. DIGITAL DEFENSE
14. BARRACUDA
15. (ISC)2

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Data Encryption

Data Encryption Solutions
1. IBM GUARDIUM DATA ENCRYPTION
2. VIRTRU
3. CHECK POINT ENCRYPTION
4. BLACKBERRY CYLANCE
5. ESET
6. CRYTOMOVE
7. SYMANTEC ENCRYPTION
8. GAVS BITLOCKER
9. IRONCLAD ENCRYPTION
10. TREND MICRO ENCRYPTION
11. DISKCRYPTOR
12. APPLE FILEVALT
13. ONPAGE
14. SENETAS
15. THALES

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Unified Endpoint Security

Endpoint Security Solutions
1. SYMANTEC ENDPOINT SECURITY
2. CYLANCE
3. CHECK POINT
4. CISCO
5. CROWDSTRIKE
6. PALO ALTO NETWORKS
7. FORTINET
8. BITDEFENDER
9. FORCEPOINT
10. BLUERIDGE NETWORKS
11. GAVS DEFENDER
12. CARBON BLACK
13. AO KASPERSKY
14. MALWAREBYTES
15. TREND MICRO

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Enterprise Network Firewall Solutions

Network Firewall Solutions
1. FORTINET FORTIGATE
2. SOPHOS
3. CISCO ASA
4. FORCEPOINT
5. SONICWALL TZ
6. UNTANGLE
7. CHECKPOINT SOFTWARE SOLUTIONS
8. PALO ALTO
9. PALO ALTO NETWORKS
10. GAVS
11. HUAWEI
12. VMWARE
13. WATCHGUARD
14. BARRACUDA NETWORKS
15. H3C

Product or Service: General Data Protection Regulation

GDPR Solutions US-Based
1. SAILPOINT (TEXAS)
2. TRUSTWAVE (ILLINOIS)
3. DATA443 RISK MITIGATION (NORTH CAROLINA)
4. IMPERVA (CALIFORNIA)
5. IBM (NEW YORK)
6. DXC TECHNOLOGY (VIRGINIA)
7. GAVS (WASHINGTON)
8. CIPHER (FLORIDA)
9. TRUSTARC (CALIFORNIA)
10. CASERTA (NEW YORK)
11. SYSARC (MARYLAND)
12. FTI CONSULTING (MARYLAND)
13. TEMPLAR SHIELD (CALIFORNIA)
14. TBG SECURITY (MASSACHUSETTS)
15. SECUREWORKS (TEXAS)

Product or Service: Intrusion Detection & Cyberattack Prevention

Threat Detection Solutions
1. CISCO UMBRELLA
2. THREATFUSION BY SOCRADAR
3. ZEROFOX
4. CROWDSTRIKE
5. NETSCOUT
6. PALO ALTO NETWORKS
7. DIGITALGUARDIAN
8. VERIZON
9. BLACKBERRY CYLANCE
10. SYMANTEC
11. FORTINET
12. GREYNOISE
13. IMPERVA
14. FORCEPOINT
15. CARBON BLACK

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Secure Medical Device & IOMT Solutions

Secure Medical Device Solutions
1. MEDIGATE CLAROTY
2. MEDCRYPT
3. GE CYBERSECURITY
4. ZINGBOX
5. ARMIS
6. CYBEATS
7. VMWARE
8. CITRIX MOBILE
9. IDATPIVE
10. IBM
11. COALFIRE
12. BLACKBERRY
13. CYBERMDX
14. CYNERIO
15. BATTELLE

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Secure Communications Platforms:

Hospitals & Health Systems

Secure Communications Platforms: Inpatient Providers
1. SPOK
2. TIGER CONNECT
3. PERFECTSERVE
4. QLIK
5. IMPRIVATA
6. HALO COMMUNICATIONS
7. TELEMEDIQ
8. AT&T
9. VOCERA
10. ONPAGE
11. PATIENT SAFE SOLUTIONS
12. VOALTE
13. CERNER CAREAWARE CONNECT
14. DIAMOND HEALTH COMMUNICATIONS
15. EPIC SECURE CHAT

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Secure Communications Platforms:

Physician Practices & Ambulatory Care Providers

Secure Communications Solutions Physicians
1. PERFECTSERVE
2. TIGER CONNECT
3. VOCERA
4. TELEMEDIQ
5. SPOK MOBILE
6. PATIENT SAFE SOLUTIONS
7. VOALTE
8. ONPAGE
9. ON MD
10. IMPRIVATA
11. QLIQ SOFT
12. HALO COMMUNICATIONS
13. DRFIRST
14. EPIC SECURE CHAT
15. UNIPHY

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Security Information & Event Management Solutions (SIEM)

Security Information & Event Management Solutions (SIEM)
1. AT&T CYBERSECURITY
2. CYBERSHARK
3. FORTIFIED HEALTH
4. IBM
5. LOGPOINT
6. TENABLE
7. MICROFOCUS
8. EXABEAM
9. TRUSTWAVE
10. LACEWORK
11. MCAFEE
12. SOPHOS
13. RSA NETWITNESS
14. RAPID 7
15. SECURONIX

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Secure Web Gateway Solutions

Secure Web Gateways
1. AT&T CYBERSECURITY
2. CYBERSHARK
3. FORTIFIED HEALTH
4. IBM
5. LOGPOINT
6. TENABLE
7. MICROFOCUS
8. EXABEAM
9. TRUSTWAVE
10. LACEWORK
11. MCAFEE
12. SOPHOS
13. RSA NETWITNESS
14. RAPID 7
15. SECURONIX

2024 Top Healthcare Cybersecurity Vendors

Product or Service: Outsourced Cybersecurity

Outsourced Cybersecurity Solutions & Managed Services
1. CLOUDWAVE
2. TRELLIX
3. LATITUDE INFORMATION SECURITY
4. FORTINET
5. CROWDSTRIKE
6. PALO ALTO NETWORKS
7. CLEARWATER
8. FORTIFIED HEALTH SECURITY
9. CLEARDATA
10. NTT SECURITY
11. ARMIS
12. CHECKPOINT
13. PIVOTPOINT
14. SAVIYNT
15. IMPRIVATA

APPENDIX

Black Book market research surveys & IT user polling

We hope that the data and analysis in this report will help you make informed and imaginative healthcare technology business decisions. If you have further requirements, the Black Book research team may be able to help you. For more information about Black Book's custom survey capabilities, please contact us directly at research@blackbookmarketresearch.com

DISCLAIMER

About Black Book ™

Black Book Market Research LLC, provides healthcare IT users, media, investors, analysts, quality minded vendors, and prospective software system buyers, pharmaceutical and equ ipment manufacturers, group purchasing organizations, and other interested sectors of the clinical and financial technology industry with comprehensive comparison data of the industry's top respected and competitively performing technology vendors.

The largest user opinion poll of its kind in healthcare IT, Black Book™ collects over a half million viewpoints on information technology and outsourced services vendor performance annually. Black Book was founded in 2003, is internationally recognized for over 15 years of customer satisfaction polling, particularly in technology, analytics, services, outsourcing and offshoring industries. Black Book™, its owners nor its employees holds any financial interest in the companies contained in this comparison performance report and is not incentivized to recommend any particular vendor.

Follow Black Book on Twitter at www.twitter.com/blackbookpolls

For methodology, auditing, resources, comprehensive research, and ranking data, see http://blackbookmarketresearch.com