State of the Healthcare Cybersecurity Industry

Top Healthcare Industry Technology Security Solutions

Q4 2020 User Survey Results

End-to-End Vendor Analysis

Top Cybersecurity Advisors and Consultants

Client-Ranked Vendor Performance by Function

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 the client experience. Independent and unbiased from vendor influence, more than 617,000 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

Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Black Book disclaims all warranties as to the accuracy, completeness or adequacy of such information. Black Book shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice. Black Book's unrivaled objectivity and credibility is perhaps your greatest assurance. At a time when alliances between major consultancies and suppliers have clouded the landscape, Black Book Market Research LLC and Black Book Rankings remain resolutely independent. We have no incentive to recommend specific software vendors. Our only allegiance is to help you achieve the results you want with the best possible solution.

For more information, visit www.blackbookmarketresearch.com or Lead Researcher Brian Locastro at
brian.locastro@blackbookmarketresearch.com

Executive Summary

Black Book Market Research LLC surveyed nearly 3000 security professionals from 890 provider organizations to identify gaps, vulnerabilities and deficiencies that persist in keeping hospitals and physicians proverbial sitting ducks for data breaches and cyber-attacks. The good news is that 94% of surveyed professionals understand the risks tacked by cybersecurity but only 19% of surveyed healthcare organizations say that security is a top IT concern, down from 82% in 2019. The not-so-great news is that most of these organizations still have a long way to go.

A fragmented mix of 447 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 2020. 89% 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. 87% of those in the healthcare industry believe they are at great risk for a data breach than other industries as compared to 69% when surveyed in 2019.

The number of cyber-attacks 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.

In 2019, over 41 million patient records were breached and 23 million of those records were the result of one stand alone breach. This was from one massive security breach at the American Medical Collection Agency (AMCA) a third-party billing agency and this breach spread out to include popular clinical labs such as Quest Diagnostics and LabCorp. These particular breaches are estimated to cost an average of more than $6.6M.

This Q4 2020 analysis revealed the average healthcare data breach costs $612 per record - the highest of any industry for nine straight years. At more than four times the cross-industry average of $150 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.

With nine of ten healthcare organizations experiencing some level of cyber assault and many seeing multiple attacks each year, the need for increased security is clear, but what is it going to cost?

The global healthcare cybersecurity market was valued at $10.6 billion in Q3 2020 and is expected to reach $36 billion dollars by the year 2023 globally at an estimated CAGR of 20%.

The U.S. is a prime target for these attacks, so it is expected to spend more than most countries. A full 48% of U.S. healthcare firms do not have cyber risk insurance and 29% of U.S. executives say their firms have no plans to take out cyber insurance, even though 81% of them expect cyber breaches to increase in the next year, up from 61% in 2019. Even among those that have insurance, only 14% said they have enough cybersecurity insurance that covers all risks.

The dilemma with cybersecurity budgeting and forecasting is the lack of reliable historical data. Cybersecurity is a newer line item for hospitals and physician enterprises and budgets have not evolved to cover the true scope of human capital and technology requirements yet.

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 by offering healthcare providers and hospitals with a growing portfolio of services yet to be perfected.

The key place to start when choosing a cybersecurity vendor is to understand the threat landscape, understanding the type of services vendors offer and comparing that to your organization's risk framework to select your best suited vendor. Healthcare organizations are also more prone to attacks than other industries because they persist at managing through breaches reactively and not proactively.

In 2019, there was an actual drop in national cybersecurity standards in the healthcare market as only 44% of hospital networks met these standards (this is slightly less than the standard from 2018). Cybersecurity is more important than ever in the healthcare industry because of the emerging importance of telehealth, remote monitoring of patients, remote workers, and wearable devices.

66% of IT management respondents report their operation teams are not aware of the full variety of cybersecurity solution sets that exist particularly mobile security environments, intrusion detection, attack prevention, forensics and testing. Providers are at a severe disadvantage when they are forced to hastily retain a cybersecurity firm in the midst of an ongoing incident as the ability to conduct the necessary due diligence is especially limited.

11% 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.

44% 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 2020, 22% of providers still do not carry out measurable assessments of their cybersecurity status. Of those that did, 13% used an objective third-party service to benchmark their cybersecurity status, 19% used an objective software solution to benchmark their cybersecurity status, and 65% self-assessed with own criteria.

17% of CIO respondents currently report they do not have an adequate cybersecurity solution to instantly detect and respond to an organizational attack.

70% 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. 72% 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 2020

The global healthcare cybersecurity market was valued at $9.8 billion in Q3 2020 and is expected to reach $35.0 billion by 2027, at a CAGR 19.3% Healthcare cybersecurity is a growing concern. 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 the 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.

Cyber-attacks 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.

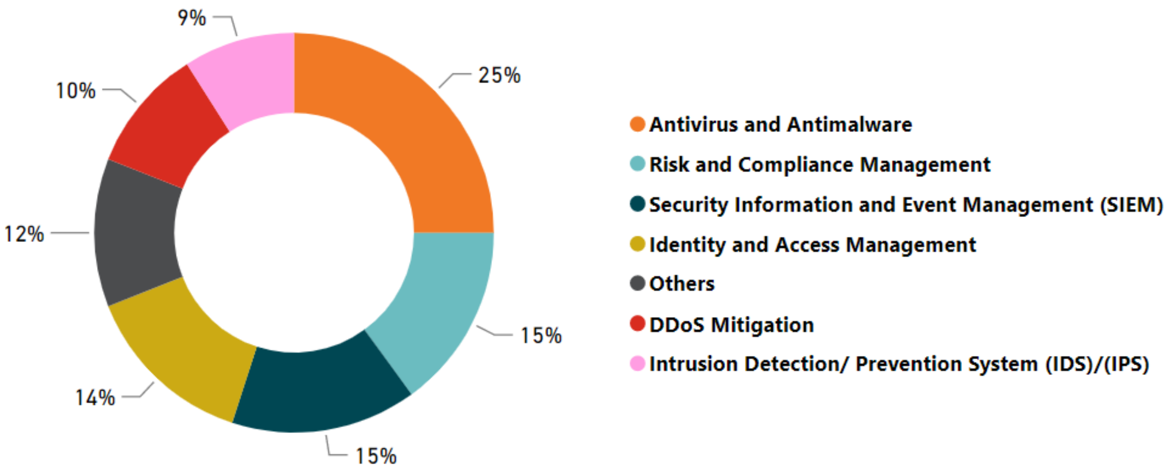
Technological advancements have led to advanced cyber warfare using SQL injections, advanced persistent threats, zero-day attacks, and advanced malware. The rise in the prevalence of cyber-attacks on the confidential data of patients, their transactions and other personal details are anticipated to fuel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

There were 510 reported healthcare data breaches in 2019, a 37% increase over 2018.

From Q1 through Q3 2020, the largest healthcare industry data breaches reported include:

1. HEALTH SHARE OF OREGON: 654,000 PATIENTS
2. FLORIDA ORTHOPAEDIC INSTITUTE: 640,000 PATIENTS
3. ELITE EMERGENCY PHYSICIANS (FORMERLY KNOWN AS ELKHART EMERGENCY PHYSICIANS): 550,000 PATIENTS
4. MAGELLAN HEALTH: 365,000 PATIENTS
5. BJC HEALTH SYSTEM: 287,876 PATIENTS
6. BENEFIT RECOVERY SPECIALISTS: 274,837 PATIENTS
7. AMBRY GENETICS: 232,772 PATIENTS
8. PIH HEALTH: 199,548 PATIENTS
9. BST & CO. CPAS: 170,000 PATIENTS
10. AVEANNA HEALTHCARE: 166,077 PATIENTS

Prioritized Demand for Healthcare Security Solutions in 2019, as reported by surveyed CIOs / CISOs



Source: Black Book™ 2019

For 2021, one of the boards' top priorities will be cybersecurity. Due to the potential financial impact of data breaches, the leadership is shifting to CFOs. Nearly 84% of executives expressed concern in their readiness to tackle data breaches when cybersecurity is solely under their CIOs responsibility.

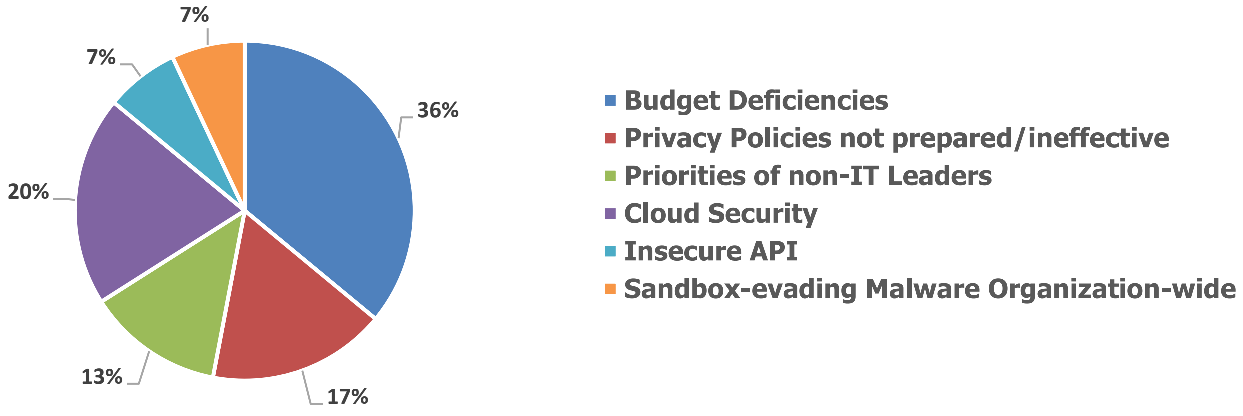
Lack of adequate IT spending by healthcare organizations and lack of awareness about cybercrime have exposed the vulnerabilities of healthcare organizations. The overall impact of cyber-attacks on the hospitals and healthcare systems is estimated to be nearly six billion per year.

88% providers revealed that lack of budget was the major obstacles to properly securing and protecting health information, up from 68% in 2019.

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

In 2020, 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.

CIO/CISO Reported Challenges to Healthcare Security in Q4 2019

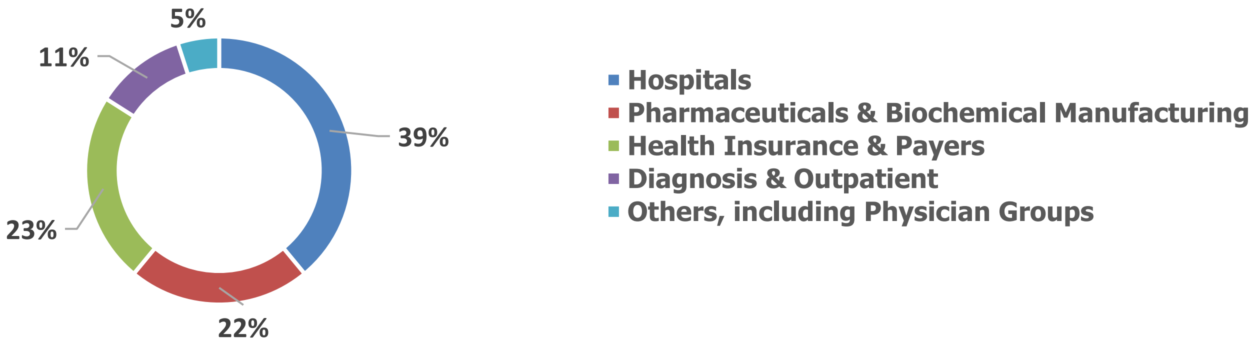


Source: Black Book$_{TM}$ 2019

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.

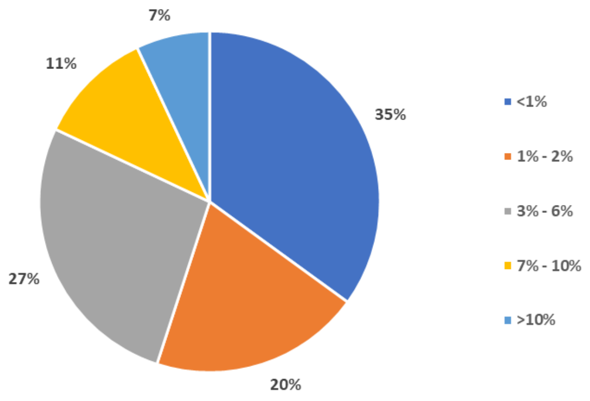
Segmented Expenditure in Healthcare Security Market in Q4 2019



Source: Black Book^{TM} 2019

Most (82%) healthcare vendors admit 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 58% of breaches are attributed to smaller companies.

Healthcare Organizations'
Total IT Budget Allocation Projections for Cybersecurity 2020

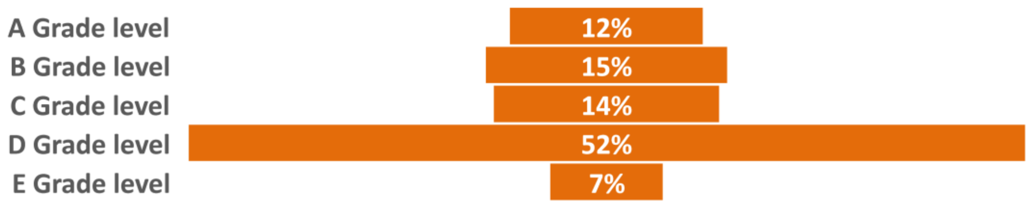


Source: Black Book^{TM} 2019

Buyers of Healthcare IT still give their vendors poor performance ratings on security measures & integration. Even after thousands of efforts approximately half of security vendors fail to protect healthcare data. This variation is more or less no different than that of 2018-2019.

In 2019, medical devices continue to be a major vulnerability, cyberattacks are usually targeted to midsized or less known healthcare organizations. However, this is changing and evolving as cyberattacks are becoming more sophisticated and medical devices are five times more likely to be breaches than attacks in other mechanical instruments.

Healthcare Client Scores on Vendor Corporate Cybersecurity Culture in 2019



Source: Black Book^{TM} 2019

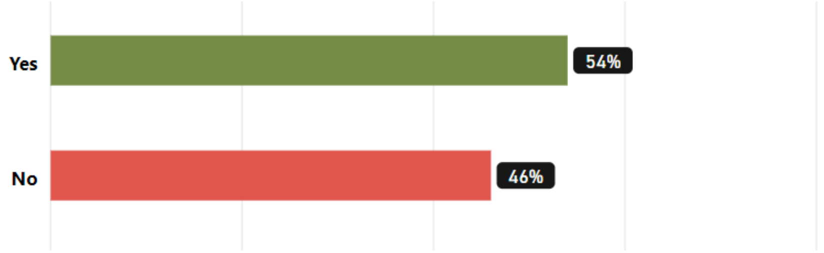
KEY for above score definitions for vendors defined as:

A Grade Level - High confidence that vendor demonstrates a strong culture of security
B Grade Level - Moderate confidence that vendor demonstrates a culture of security
C Grade Level - Indeterminate confidence that vendor demonstrates a culture of security
D Grade Level - Lack of confidence based on demonstrated weaknesses with vendor's culture of security
F Grade Level - No confidence in vendor's ability to protect information

The variation is more than 2019 as nearly 46% of buyers of healthcare IT software and services continue to give vendors poor performance ratings. A growing area of concern is the lack of education for IT users.

Black Book Research found that only 56% healthcare organizations hold the competitive security certification. 46% of the organizations are not holding vendors accountable for meeting minimum acceptable security standards. Security certifications provide third party validation of security practices. Examples for the industries include: HITRUST, AICPA SOC 2 and 3 reports, ISO 27001, and FedRAMP. It is important for organizations to understand the scope and baseline criteria used for certifications to boost the security arena.

Healthcare Vendors with at least one Product Security Certification in 2020



Source: Black Book^{TM} 2019

In 2019, the healthcare sector saw over 41.2 million patient records compromised in 510 healthcare data breaches which was a 38.4% increase over the previous year survey period. By the end of Q2 2020 the number had dropped to near that of the previous year, however, the cyberattacks were just as significant. Healthcare continues to be the most frequent victim of these breaches because of the amount of information that a can be obtained. In addition to banking health information management data contains date of birth, social security numbers, and other significant privileged information, in 2019, it was the worse year in relation to cyberattacks and the compromise of critical information in healthcare. The breaches thus far in 2020 have been limited. Surprisingly, COVID does play a part, however, actual statistics are expected to show a growing number because of the successful attacks so far this year.

In 2018, the healthcare sector saw 13.3 million patient records compromised in 365 breaches, three times the amount seen in 2017. By the end of Q2 2019, the number of data breaches dramatically rose with potentially more than 25 million patient records breached. Healthcare has been plagued with massive data breaches, with each of the 10 largest seeing more than 200,000 records breached at a time. Third-party vendors and phishing attacks were behind most of these security incidents, and the investigations into the largest vendor breach is still ongoing. it stands, 2019 is proving to be the worst seen for healthcare cybersecurity and it can be seen in the figures of top 10 healthcare security data breaches, to date, in 2019 so far, with the number of patients effected below per breach:

1. Optum360 (on behalf of Quest Diagnostics): 11.5 million
2. LabCorp: 10.3 million
3. Dominion National: 3 million
4. Clinical Pathology Laboratories: 1.7 million
5. Inmediata Health Group: 1.6 million
6. UW Medicine: 970,000
7. CareCentrix: 468,000
8. BioReference Laboratories: 426,000
9. Bayamon Medical Center: 423,000
10. American Esoteric Laboratories: 410,000

Notable 2020 Survey Findings

Black Book Market Research LLC surveyed 2,464 security professionals from 705 provider organizations to identify gaps, vulnerabilities and deficiencies that persist in keeping hospitals and physicians proverbial sitting ducks for data breaches and cyber-attacks. Ninety-six percent of IT professionals agreed with the sentiments that data attackers are outpacing their medical enterprises, holding providers at a disadvantage in responding to vulnerabilities.

With the healthcare industry estimated to spend $134 billion on cybersecurity from 2021 to 2026, $18 billion in 2021, increasing 20% each year to nearly $37 billion in 2026, 82% of CIOs and CISOs in health systems in Q3 2020 agree that the dollars spent currently have not been allocated prior to their tenure effectively, often only spent after breaches, and without a full gap assessment of capabilities led by senior management outside of IT.

Key findings include:

1. Talent Shortage for Cybersecurity Professionals Continues, Far Exceeds Demand by Health Systems

Additionally, Black Book surveyed 291 healthcare industry human resources executives to determine the organizational supply and demand of experienced cybersecurity candidates. On average, cybersecurity roles in health systems take 70% longer to fill than other IT jobs.

Health systems are struggling to find workers that request cybersecurity-related skills as vacancy duration as reported by survey HR respondents average about 118 days to fill positions, nearly three times as high as the national average for other industries.

"The talent shortage for cybersecurity experts with healthcare expertise is nearing a very perilous position," said Brian Locastro, lead researcher on the 2020 State of the Healthcare Cybersecurity Industry study by Black Book Research.

Seventy-five percent of the sixty-six-health system CISOs responding agreed that experienced cybersecurity professionals are unlikely to choose a healthcare industry career path because of one main reason. More than in other industries, healthcare CISOs are ultimately held responsible for a data breach and the financial and reputation impacts to the provider organization despite having extremely limited decision-making technology or policy making authority.

2. COVID-19 Has Greatly Increased Risk of Data Breaches from Remote Work & Cloud-Based Business Operations

Healthcare cybersecurity has become more complicated as providers are forced to deal with the COVID-19 pandemic. Understaffed and underfunded IT security departments are scrambling to accommodate the surge in demand of remote services from patients and physicians while simultaneously responding to the surge in security risks.

Black Book surveying found 90% of health systems and hospital employees who shifted to a work-at-Home assignment due to the pandemic, did not receive any updated guidelines or training on the increasing risk of accessing sensitive patient data compromising systems

"Despite the rising threat, the vast majority of hospitals and physicians are unprepared to handle cybersecurity threats, even though they pose a major public health problem," said Locastro.

Forty percent of all clinical hospital employees receive little or no cybersecurity awareness training still in 2020, beyond initial education on log in access. Fifty-nine percent of health system CIOs surveyed are shifting security strategies to address user authentication and access as malicious incidents and hackers are the 2020 attacker's go-to entry point of choice for health systems. Stolen and compromised credentials were ongoing issues for 53% of health systems surveyed as hackers are increasingly using cloud misconfigurations to breach networks.

3. Cybersecurity Consulting and Advisory services are in high demand

Sixty-nine percent of 219 C-Suite Respondents state their health system's budget for Cybersecurity consulting is increasing in 2021 to assess gaps, secure network operations, and user security on-premises and in the cloud.

"In today's highly competitive cybersecurity market there isn't enough talent to staff hospitals and health systems," said Locastro. "As provider organizations struggle with recruit, hire and retain in house staff, the plausible choice is retaining an experienced advisory firm that is capable of identifying and remediating hidden security vulnerabilities, which appeals to the strategic and economic sense of boards and CEOs."

4. Healthcare Cybersecurity Challenges find resolutions from Outsourced Services

"The dilemma with cybersecurity budgeting and forecasting is the lack of reliable historical data," said Locastro. "Cybersecurity is a newer line item for hospitals and physician enterprises and budgets have not evolved to cover the true scope of human capital and technology requirements yet."

That shortage of healthcare cybersecurity professionals and a lack of appropriate technology solutions implemented is forcing a rush to acquire services and outsourcing at a pace five times more than the acquisition of cybersecurity products and software solutions. Cybersecurity companies are responding to the labor crunch by offering healthcare providers and hospitals with a growing portfolio of managed services.

"The key place to start when choosing a cybersecurity services vendor is to understand your threat landscape, understanding the type of services vendors offer and comparing that to your organization's risk framework to select your best-suited vendor," said Locastro. "Healthcare organizations are also more prone to attacks than other industries because they persist at managing through breaches reactively."

Fifty-one percent of in-house IT management respondents with purchasing authority report their group is e not aware of the full variety of cybersecurity solution sets that exist, particularly mobile security environments, intrusion detection, attack prevention, forensics and testing in various healthcare settings.

5. Cybersecurity in healthcare provider organizations remains underfunded

The amount of dollars that are actually spent on healthcare industry cybersecurity products and services are increasing, averaging 21% year over year since 2017. Extended estimates have estimated nearly $140 Billion will be spent by health systems and health insurers by 2026. However, 82% of hospital CIOs in inpatient facilities under 150 staffed beds and 90% of practice administrators collectively state they are not even close to spending an adequate amount on protecting patient records from a data breach.

"Outdated IT systems, fewer cybersecurity protocols, untrained IT staff on evolving security skills, and data-rich patient files are making healthcare the current target of hacker attacks," said Locastro. "And the willingness of hospitals and physician practices to pay high ransoms to regain their data quickly motivates hackers to focus on patient records."

"Threats are now four times more likely to be centered on healthcare than any other industry, and ransomware attacks are increasing in popularity because of the amount of privileged information the hacker can obtain," said Locastro. "Providers at the point-of-care haven't kept pace with the cybersecurity progress and tools that manufacturers, IT software vendors, and the FDA have made either."

6. Majority of Healthcare consumers are willing to change providers if they feel their medical records are not secure

Eighty percent of healthcare organization have not had a cybersecurity drill with an incident response process, despite the skyrocketing cases of data breaches in the healthcare industry in 2020.

Only 14 percent of hospitals and six percent of physician organizations believe that a 2021 assessment of their cybersecurity will show improvement from 2020. Twenty-six percent of provider organizations believe their cybersecurity position has worsened, as compared to three percent in other industries, year-to-year.

"Medical and financial leaders have wielded more influence over organizational budgets and made it difficult for IT management to implement needed cybersecurity practices despite the existing environment, but now consumers are beginning to react negatively to the provider's lack of protection solutions."

A poll of 3,500 healthcare consumers that used medical or hospital services in the last eighteen months revealed 93% would leave their provider if their patient privacy was comprised in an attack that could have been prevented.

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.

2020 SOLUTIONS RATING RESULTS

HEALTHCARE CYBERSECURITY SOLUTIONS

Survey Overview

From Q3 2019 through Q4 2020, the Black Book Research healthcare cybersecurity solutions client/user survey investigated 404 IT security functional category vendors utilized by over 3,000 validated client users for the solutions vendor ratings.

491 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 622,000 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 2019 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 three hundred cybersecurity (190 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, 1103 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.

2019 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

2020 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

FORTINET

TOP VENDOR: HOSPITALS 101-300 BEDS

FIREEYE

TOP VENDOR: HEALTH SYSTEMS & CORPORATIONS

FORTINET

TOP VENDOR: PHYSICIAN PRACTICES & GROUPS

BLACKBERRY

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

Black Book raw score scales

1 = Deal breaking dissatisfaction ◄ ► 10 = Exceeds all expectations

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
10	FORTINET	1
4	FIREEYE	2
1	JUNIPER NETWORKS	3
1	BLACKBERRY	4
1	IMPERVA	5
1	IBM	7

Source: Black Book Research

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	FORTINET	1
2	Innovation & Optimization	IBM	7
3	Training & Education	FORTINET	4
4	Client relationships and cultural fit	FIREEYE	2
5	Trust, Accountability, Transparency, Ethics	FORTINET	1
6	Breadth of offerings, client types, delivery excellence	FORTINET	1
7	Deployment and services implementation	JUNIPER NETWORKS	3
8	Customization	BLACKBERRY	4
9	Integration and interfaces	FORTINET	1
10	Scalability, client adaptability, flexible pricing	FORTINET	1
11	Compensation and employee performance	IMPERVA	5
12	Reliability	FORTINET	1
13	Brand image and marketing communications	FORTINET	1
14	Marginal value adds and modules	FIREEYE	2
15	Financial & Managerial Viability	FORTINET	1
16	Data security and backup services	FORTINET	1
17	Support and customer care	FIREEYE	2
18	Best of breed technology and process improvement	FIREEYE	2

TOP HEALTHCARE ENTERPRISE (END-TO-END) CYBERSECURITY SOLUTIONS RATED SOLUTIONS

AGGREGATE KEY PERFORMANCE INDICATOR SCORES AND RANKED BY OVERALL MEAN

Rank	Vendor	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Mean
1	**FORTINET**	9.55	9.41	9.66	8.99	9.37	9.59	9.41	9.34	9.49	9.34	9.24	9.54	9.42	9.17	9.26	9.50	9.44	9.16	**9.38**
2	**FIREEYE**	9.39	8.59	9.24	9.46	9.32	9.56	9.12	9.37	9.11	9.00	8.75	8.68	9.08	9.29	8.97	8.81	9.47	9.36	**9.14**
3	**JUNIPER NETWORKS**	9.18	9.25	8.69	9.22	8.87	8.45	9.57	9.58	8.51	9.28	8.65	9.21	8.33	8.90	8.17	9.34	8.48	8.98	**8.93**
4	**BLACKBERRY**	9.45	8.92	9.42	9.00	9.12	8.89	8.53	9.90	8.99	9.19	8.49	7.01	8.23	7.10	8.93	8.83	8.23	8.61	**8.71**
5	**IMPERVA**	8.89	8.93	8.34	8.97	9.13	9.23	8.36	8.71	8.57	9.08	9.31	8.19	7.66	8.14	7.07	8.46	8.65	8.78	**8.58**
6	**NORTHROP GRUMMAN**	8.24	9.03	9.07	9.38	8.42	8.62	9.29	7.86	7.76	7.11	7.39	8.46	8.53	7.02	8.19	8.95	9.30	8.21	**8.38**
7	**IBM**	8.30	9.57	8.36	6.86	8.79	8.76	8.20	7.90	8.87	7.20	9.01	8.69	7.80	8.71	9.07	7.12	8.53	8.28	**8.33**
8	**MICROSOFT**	8.99	7.55	8.27	8.44	6.54	9.27	8.63	8.15	7.61	8.06	8.96	8.30	8.38	8.62	6.58	7.98	8.57	8.19	**8.17**
9	**PALO ALTO**	8.41	8.53	9.13	8.52	7.36	8.06	7.52	8.77	8.69	8.87	7.83	6.87	8.47	5.90	8.41	8.57	8.67	8.74	**8.18**
10	**CISCO**	8.27	8.84	7.44	9.04	8.39	5.78	8.47	7.44	7.51	7.54	8.94	8.68	8.10	7.92	7.71	8.71	9.12	8.54	**8.14**
11	**SENSATO**	7.29	6.85	8.60	8.49	8.87	8.05	6.99	7.08	7.83	8.01	8.61	7.02	5.75	7.01	7.52	8.58	7.78	8.22	**7.70**
12	**SYMANTEC**	8.65	8.77	8.80	8.20	6.99	7.01	8.02	8.08	7.55	7.03	5.69	8.57	8.08	8.17	6.28	7.13	7.34	7.87	**7.68**
13	**INTEL**	7.92	8.41	8.15	7.32	8.26	8.11	6.94	8.23	8.39	6.95	6.71	7.21	8.52	8.61	5.56	7.99	7.11	7.02	**7.63**
14	**MCAFEE**	8.78	5.56	7.88	7.92	7.83	7.72	8.87	7.24	5.70	8.17	6.64	7.36	6.89	8.77	7.11	7.39	4.74	8.58	**7.40**
15	**AT&T**	7.87	7.19	8.27	7.93	7.30	8.02	7.80	8.61	6.01	6.92	5.77	6.29	6.54	8.33	6.05	8.59	8.76	7.00	**7.40**
16	**CROWDSTRIKE**	7.99	8.53	9.02	6.88	7.38	6.43	6.40	7.70	8.78	7.18	5.66	5.44	6.25	5.61	7.00	6.45	5.75	7.43	**6.99**
17	**LOGRHYTHM**	6.99	5.70	7.20	7.35	5.66	8.90	6.42	5.77	7.12	8.45	5.77	6.22	7.59	6.54	5.71	7.77	7.19	7.05	**6.86**
18	**SAVIYNT**	7.50	9.22	7.43	5.77	7.08	6.55	5.56	6.83	6.88	6.46	6.92	5.45	7.40	8.79	6.26	4.97	7.11	6.25	**6.80**
19	**SOPHOS**	7.28	7.17	5.65	7.11	5.74	6.22	7.04	5.70	6.2	7.04	7.22	4.98	6.94	6.69	7.19	5.73	5.44	7.08	**6.47**
20	**TREND MICRO**	5.70	5.75	5.77	6.77	5.72	5.29	6.22	6.09	6.65	5.65	6.41	5.95	7.00	8.37	6.44	6.03	5.70	6.12	**6.20**

RELEVANT. ACCURATE

BLACK BOOK

2020

UNBIASED SOURCE

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.

2020 Top Healthcare Cybersecurity Vendors

Product or Service: Access & Identity Management

Access & Identity Management

1. IMPRIVATA
2. CLEARDATA
3. SAILPOINT
4. RSA
5. AVATIER
6. OPTIMAL
7. AUTH0
8. CYBERARK
9. SAVIYNT
10. ORACLE
11. WATCH GUARD
12. BETA SYSTEMS
13. LAST PASS
14. IBM
15. IATRIC SYSTEMS
16. VARONIS
17. OKTA
18. WORLD WIDE TECHNOLOGY
19. SYSTEM FRONTIER
20. INTELLITRUST

Product or Service: Application Security Testing

Application Security Testing

1. RAPID7
2. QUALITEST
3. CAPGEMINI
4. AUDACIX
5. TESTBYTES
6. WHITEHAT SECURITY
7. QA MENTOR
8. KIWIQA
9. VERACODE
10. IMPACTQA
11. MICROFOCUS
12. IBM
13. ANGLER
14. SYNOPSYS
15. AVYAAN
16. CONTRAST SECURITY
17. QUALYS
18. CHECKMARX
19. CONTRAST SCURITY
20. COGNIZANT

Product or Service: Attack Detection Protection & Predictive Protection

Attack Detection Protection & Predictive Protection DDOS

1. BLACKBERRY CYLANCE
2. IMPERVA
3. HUNTERS.AI
4. CLOUDFLARE
5. F5 NETWORKS
6. FORTINET
7. JVION
8. ARBOR NETWORKS
9. NEXUSGUARD
10. MCAFEE
11. AKAMAI TECHNOLOGIES
12. ROOT 9B
13. CODE DX
14. A10 NETWORKS
15. RADWARE
16. LINK11
17. VERISIGN
18. VIPRE
19. CENTURY LINK
20. LEVEL3 COMMUNICATIONS

Product or Service: Authorization Solutions

Authorization / Authentication & Single Sign-on Solutions

1. FIREEYE
2. IMPRIVATA
3. SAILPOINT
4. IDAPTIVE
5. SECUREAUTH
6. AUTH0
7. CENTRIFY
8. OKTA
9. IDENTITY AUTOMATION
10. AVATIER
11. ONE IDENTITY
12. HEALTHCAST
13. OPTIMAL IDM
14. CROSSMATCH
15. ONELOGIN
16. PING IDENTITY
17. JANRAIN
18. ZEBRA
19. JUMPCLOUD
20. IDM WORKS

Product or Service: Blockchain Development Solutions

Blockchain Development Solutions

1. HASHED HEALTH
2. IBM BLOCKCHAIN
3. BLOCKCHAIN HEALTH
4. AMAZON WEB SERVICES
5. MICROSOFT AZURE
6. MEDBLOX
7. SIMPLYVITAL HEALTH
8. GOOGLE
9. MEDIBLOC
10. HUMANSCAPE
11. HEALTHCOMBIX
12. ALPHACON
13. MEDCHAIN
14. ORACLE
15. SHIVOM
16. GAINFY
17. ALIBABA CLOUD
18. OPEN HEALTH
19. SOLVECARE
20. ETHEAL

Product or Service: Cloud Solutions

Cloud Solutions

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

Product or Service: Compliance & Risk Management Solutions

Compliance & Risk Management Solutions
1. CLEARWATER COMPLIANCE
2. HEALTHICITY COMPLIANCE MANAGER
3. COMPLIANCY GROUP
4. CYNERGISTEK
5. FAIRWARNING
6. DELOITTE
7. SERA-BRYNN
8. KPMG
9. COALFIRE
10. NAVIGATE
11. CHANGE HEALTHCARE
12. CONVERGEPOINT
13. DIGITAL DEFENSE
14. ACCENTURE
15. CIMCOR
16. EY
17. CONTINUUM GRC
18. LOCKPATH
19. PWC
20. BT GLOBAL

Product or Service: Cybersecurity Awareness & Training

Cybersecurity Awareness, Training & Education
1. KNOWBE4
2. PROOFPOINT
3. ESET TRAINING
4. THE SANS INSTITUTE
5. INFOSEC INSTITUTE
6. COFENSE
7. TERRANOVA
8. INSPIRED ELEARNING
9. DIGITAL DEFENSE
10. BARRACUDA
11. (ISC)2
12. OPTIV
13. FIREEYE
14. SECURE NINJA
15. SECURITY INNOVATION
16. GLOBAL LEARNING
17. CYBRARY
18. VANGUARD
19. CIRCADENCE
20. INFOSIGHT

2020 Top Healthcare Cybersecurity Vendors

Product or Service: Data Encryption

Data Encryption

1. IBM GUARDIUM DATA ENCRYPTION
2. BLACKBERRY CYLANCE
3. CHECK POINT ENCRYPTION
4. ESET
5. CRYTOMOVE
6. SYMANTEC ENCRYPTION
7. MICROSOFT BITLOCKER
8. IRONCLAD ENCRYPTION
9. MICRO FOCS SECUREDATA
10. BITDEFENDER GRAVITY ZONE
11. SOPHOS SAFEGUARD
12. DELL ENCRYPTION ENTERPRISE
13. MCAFEE COMPLETE DATA PROTECTION
14. TREND MICRO ENCRYPTION
15. DISKCRYPTOR
16. APPLE FILEVALT
17. ONPAGE
18. SENETAS
19. THALES
20. DATA LOCKER

Product or Service: End Point Security

End Point Security Solutions

1. MICROSOFT
2. BLACKBERRY CYLANCE
3. SYMANTEC
4. PALO ALTO
5. TREND MICRO
6. PANDA SECURITY
7. ABSOLUTE SOFTWARE
8. CROWDSTRIKE
9. IBM
10. CARBON BLACK
11. ESET
12. INTEL SECURITY
13. SOPHOS
14. MCAFEE
15. FORTINET
16. CHECK POINT SOFTWARE
17. VMWARE
18. LANDESK
19. F-SECURE
20. MALWAREBYTES

Product or Service: Firewall Network Solutions

Firewall Network Solutions

1. CHECKPOINT SOFTWARE SOLUTIONS
2. JUNIPER NETWORKS
3. PALO ALTO NETWORKS
4. FORTINET
5. CISCO
6. MICROSOFT
7. HUAWEI
8. FORCEPOINT
9. VENUSTECH
10. SOPHOS
11. WATCHGUARD
12. BARRACUDA NETWORKS
13. H3C
14. STORMSHIELD
15. VMWARE

Product or Service: GDPR Compliance Solutions

GDPR Compliance Solutions

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

Product or Service: Intrusion Detection & Threat Prevention

Intrusion Detection & Threat Prevention

1. CROWDSTRIKE
2. DIGITALGUARDIAN
3. VERIZON
4. BLACKBERRY CYLANCE
5. SYMANTEC
6. PALO ALTO NETWORKS
7. FORTINET
8. IMPERVA
9. FORCEPOINT
10. CARBON BLACK
11. CISCO
12. MCAFEE
13. FIREEYE
14. KOUNT
15. SUMOLOGIC

Product or Service: Mobile & Medical Device Security

Mobile Device Management / EDM

1. MEDIGATE
2. MEDCRYPT
3. ZINGBOX
4. ARMIS
5. CYBEATS
6. VMWARE
7. CITRIX MOBILE
8. IDATPIVE
9. IBM
10. COALFIRE
11. BLACKBERRY
12. CYBERMDX
13. CYNERIO
14. BATTELLE
15. VELETIUM
16. CYLERA
17. SENRIO
18. XAGE SECURITY
19. STERNUM
20. STERLING

Product or Service: Patient Privacy Monitoring

Patient Privacy Monitoring

1. FAIRWARNING
2. PROTENUS
3. AT&T HEALTHCARE
4. CONVERGEPOINT
5. INTRUNO
6. FOGHORN
7. MAIZE ANALYTICS
8. BLUE FIN
9. IDEXPERTS MIDAS
10. IDENTITYFORCE
11. SEDARA SECURITY
12. GTB TECHNOLOGIES
13. HITACHI
14. ZETTASET
15. IATRIC SYSTEMS
16. UNIVERSAL PATIENTKEY
17. LIFELOCK
18. JERICHO SYSTEMS
19. TRUE VAULT
20. EXPERIAN

Product or Service: Ransomware Protection

Ransomware Protection

1. ACRONIS
2. SYMANTEC
3. SOPHOS
4. FORTINET
5. ESET
6. IBOSS
7. TREND MICRO
8. KASPERSKY
9. WEBROOT
10. ARCSERVE
11. MICROSOFT SECURITY
12. MCAFEE
13. ZSCALER
14. RUBRIK
15. VIPRE
16. DIGITAL GUARDIAN
17. WEBSENSE
18. CISCO
19. ZIX CORPORATION
20. BARRACUDA NETWORKS

Product or Service: Secure Communications Platforms:

Physicians Practices

Secure Communication Platforms: Physicians Practices

1. TIGER CONNECT
2. VOCERA
3. TELEMEDIQ
4. PERFECTSERVE
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

2020 Top Healthcare Cybersecurity Vendors

Product or Service: Secure Communications Platforms: Hospitals & Health Systems

Secure Communications Platforms: Hospitals & Health Systems

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

Product or Service: Secure Web Gateways & Protection

Secure Web Gateways & Protection

1. PALO ALTO NETWORKS
2. ZSCALER
3. CLOUDFARE
4. CISCO
5. SYMANTEC
6. IBOSS
7. MCAFEE
8. FORCEPOINT
9. TREND MICRO
10. MICRO FOCUS
11. MENLO SECURITY
12. BARRACUDA
13. SANGFER

2020 Top Healthcare Cybersecurity Vendors

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

Security Information & Event Management Solutions (SIEM)
1. SPLUNK
2. BLUMIRA
3. FORTINET
4. NETSURION
5. FIREEYE
6. CONDUENT
7. DELL RSA
8. SENSEON
9. CYGILANT
10. IBM
11. COALFIRE
12. TRIPWIRE
13. LOGRHYTHM
14. SOLARWINDS
15. FORTIFIED
16. TRUSTWAVE
17. VENUSTECH
18. ALIENVAULT
19. LOGPOINT
20. MCAFEE

2020 Top Healthcare

Cybersecurity Advisors & Consultants

Healthcare Cybersecurity Consultants

1. CYNERGISTEK
2. IMPACT ADVISORS
3. DELOITTE
4. FORTIFIED HEALTH
5. ACCENTURE
6. GUIDEHOUSE (NAVIGANT)
7. THE HCI GROUP
8. TYLER CYBERSECURITY
9. KPMG
10. IBM
11. PONDURANCE
12. VERIZON
13. HURON
14. AT&T
15. EY
16. AGIO
17. ADVISORY BOARD
18. PROVITI
19. ATOS
20. CROWE

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

All Rights Reserved.
No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form Product or Service: any means (electronic, mechanical, photocopying, recording or otherwise), without the prior permission of the publisher, Black Book Market Research LLC. The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Black Book Research delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always able to guarantee. As such, Black Book Research can accept no liability whatever for actions taken based on any Information that may subsequently prove to be incorrect.

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 equipment 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