Healthcare Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 100 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Healthcare Cyber Security Market size is estimated at USD 29.53 billion in 2024, and is expected to reach USD 60.24 billion by 2029, growing at a CAGR of 15.32% during the forecast period (2024-2029).

While cyber-attacks are the principal factor among the drivers of growth in the healthcare cybersecurity market, data breaches might be in the run. An increasing number of healthcare institutions are expected to use these cybersecurity solutions to protect patient data. Due to digital transformation, the healthcare industry is witnessing a shift in the operational process of information security.

Key Highlights
-Cyber threats are expected to increase as connected technology becomes even more rooted in healthcare. So, this cyber threat is driving the market, along with other factors, such as increasing demand for cloud services and low penetration of information security systems in the healthcare sector. Smartphones are still the primary device for physician and patient communication. One of the primary reasons for healthcare mobile adoption is the standards and laws set by the US Centers for Medicare and Medicaid Services (CMS). Electronic health records are one of the prominent data sought by attackers.
-The latest developments in the healthcare sector, such as the Internet of Medical Things (IoMT) devices, not only opened the door for improved patient care but also increased potential threats. Embedded devices, such as pacemakers, threaten patient health by using radio or network technology. Moreover, the rise in patent infringement cases, business records, medical identity fraud, and loss of patient health records are expected to boost the healthcare cybersecurity market from 2015 to 2023. However, a lack of awareness about cybersecurity related to the healthcare industry would act as a restraining factor, thereby hampering the growth of the healthcare cybersecurity market.
-According to Cyber Peace Institute, over 10 million records have been stolen, including social security numbers, patient medical

records, financial data, HIV test results, and the private details of medical donors. On average, around 155,000 records are breached during attacks on the sector, and this number can be far higher, with some incidents reporting a breach of over 3 million records. Further, Palo Alto Networks analyzed over 200,000 medical infusions pumped on networks of hospitals and other healthcare organizations and discovered that around 75% are affected by known vulnerabilities that attackers could exploit.
-The lack of a cyber security policy framework in healthcare organizations harmed the market. For businesses that adhere to national, industry, and international cybersecurity regulations, cybersecurity frameworks are frequently required or, at the very least, strongly encouraged. For example, a business must pass an audit attesting to its compliance with the Payment Card Industry Data Security Standards (PCI DSS) framework to handle credit card transactions.
-COVID-19 had a favorable effect on the healthcare cyber security market. Due to the pandemic, cyberattacks on clinical testing databases, digital healthcare platforms and apps, medical diagnostic systems, and advanced healthcare devices have escalated. Because of the heightened risk of a data breach and the rising frequency of cyberattacks in the healthcare sector, this spread increased the adoption of cyber security services and solutions. Over the course of the year, 92 ransomware attacks affected over 600 hospitals, clinics, and other healthcare organizations. In addition, the COVID-19 phishing epidemic further increased the need for cyber security in the healthcare sector.

Healthcare Cybersecurity Market Trends

Hospitals to Drive the Healthcare Cyber Security Market

- Hospitals are vulnerable to cyber-attacks because the existing tech systems are becoming increasingly complicated. Hospital staff relies on mobile devices, along with monitoring equipment. They are also responsible for the collection of personal details of their patients, including social security numbers, medicines they are taking, and credit card information. This makes them a primary target of attackers.
- Over half of Internet of Things (IoT) devices in hospital settings were found to contain critical cybersecurity vulnerabilities, according to the 2022 State of Healthcare IoT Device Security report from Cynerio. According to a security report, one-third of bedside IoT healthcare devices contain critical cyber risks. Around 79% of hospital IoT devices are used at least monthly, which narrows the amount of time available to patch the vulnerability. Such instances are expected to cater to the demand for cybersecurity solutions.
- To address the issue of cybersecurity, contactless and RFID readers are being used for physical and logical control access applications. For instance, ELATEC readers are used for securing print management and other healthcare ecosystem applications. Nowadays, medical devices are connected to mobile devices, such as smartphones and laptops. They play a significant role in the delivery of care and operational efficiency, but on the other hand, each connected device also opens the door to a malicious cyberattack.
- In 2021, a Monongalia Health System in West Virginia suffered a data breach from a phishing attack, giving hackers access to several email accounts in the hospital. The hospital discovered the incident in July 2021. After investigations, it found that unauthorized individuals had accessed a contractor's email account and sent emails attempting to obtain funds from Mon Health via fraudulent wire transfers. Such incidents could be an example of a weak cybersecurity policy and enhance the need for healthcare cybersecurity in hospitals.
- The lack of dedicated IT professionals and a cybersecurity division in medical organizations drive several hospitals and healthcare organizations to prefer cloud-based cybersecurity solutions. Many healthcare organizations and hospitals globally lack the required IT infrastructure to establish an in-house cybersecurity division, and the demand for cloud-based cybersecurity services is expected to increase rapidly.

North America to Dominate the Market

- The North American region dominated the Healthcare Cybersecurity market. This is primarily due to the factors such as the presence of major players along with several emerging startups in the region, presence of highly developed medical and healthcare infrastructure, high spending on healthcare information technology, the proliferation of cloud-based solutions, increasing sophistication and frequency of cyberattacks, and emergence of disruptive digital technologies.
- The growing demand for cloud-based security solutions in the healthcare industry is driven by the fact that they lower data management costs and increase efficiency, as well as by a sharp increase in healthcare data breaches. Additionally, the sector's value will be stimulated by the expanding use of IoT devices and cloud-based security services for storage. The market demand will also be further fueled by growing government attempts to protect digital healthcare services in this region.
- The healthcare industry is one of the most regulated industries in the United States due to privacy and security concerns associated with digital patient records. Government regulations ensure steady growth in the penetration rates of cybersecurity solutions in the country's healthcare sector. For instance, the U.S. government established the Health Insurance Portability and Accountability Act (HIPAA) to encourage healthcare institutions to keep healthcare data private and secret. Such factors will contribute to the growth of the healthcare cyber security market in this region in the coming years.
- The growth of digital transformation of data, healthcare processes, awareness, and ease of usage of mobiles created a demand for health, thereby increasing online platforms' use builds up possibilities for data theft. Hundreds of healthcare facilities in the United States were attacked in 2020 and 2021. Sophos states that 66 percent of healthcare organizations were hit by ransomware attacks last year, which is 34 percent up to 2020. It increased the demand for the healthcare cybersecurity market in this region.

Healthcare Cybersecurity Industry Overview

The healthcare cyber security market is moderately competitive and consists of several major players. In terms of market share, few significant players currently dominate the market. Companies working in this space are spending abundantly on research and development. Business strategies such as collaboration, joint ventures, and mergers and acquisitions have allowed firms to stay competitive. Many organizations believe in upgrading their current portfolio to attract their customers. Firms are looking at the solutions offered by Healthcare Cyber Security companies to achieve a highly sought-after competitive advantage.

- In May 2022, Clearwater acquired CynergisTek, which provides cybersecurity, compliance, and IT services to help highly regulated industries tackle security and privacy issues, for $17.7 million. This partnership strengthens CynergisTek's people-centric approach to cybersecurity, privacy, and audit and its essential role in serving the healthcare industry and its clients.
- In November 2021, With its plan to purchase ReaQta, a Dutch cybersecurity threat detection and response company, IBM Security announced an extension of its cybersecurity threat detection and response capabilities. Endpoint security solutions from ReaQta use artificial intelligence (AI) to automatically identify and control threats while staying invisible to attackers. This deal will strengthen IBM's position in the extended detection and response (XDR) industry, consistent with the company's aim of providing security through an open approach that spans diverse technologies, data, and hybrid cloud settings.
- In November 2021, Fortinet, a global pioneer in comprehensive, integrated, and automated cybersecurity solutions, unveiled the industry's most comprehensive solution for securing and connecting work-from-anywhere environments. Fortinet delivers Protection, services, and threat intelligence by combining its broad range of zero trust, endpoint, and network security products into the Fortinet Security Fabric.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

SCOTTS INTERNATIONAL

Healthcare Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 100 pages | Mordor Intelligence

To place an Order with Scotts International:

□ - Print this form

□ - Complete the relevant blank fields and sign

□ - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

□** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email* Phone*

First Name* Last Name*

Job title*

Company Name* EU Vat / Tax ID / NIP number*

Address* City*

Zip Code* Country*

Date 2026-03-01

Signature