Healthcare Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 120 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 34.05 billion in 2025, and is expected to reach USD 69.45 billion by 2030, at a CAGR of 15.32% during the forecast period (2025-2030).

Key Highlights
- Escalating Cyber Threats Drive Healthcare Security Market: The Healthcare Cyber Security Market is experiencing significant growth, driven by an escalating wave of cyberattacks targeting the healthcare sector. Healthcare organizations face unprecedented risks, with ransomware attacks increasing by 755% in 2021. This surge in threats is forcing healthcare providers to bolster their cybersecurity infrastructure, safeguarding critical patient data and ensuring operational continuity.
- Cyberattack Impact: According to the IBM Cost of a Data Breach Report, healthcare had the highest average data breach cost, reaching $7.13 million in 2020.
- Widespread Incidents: The CyberPeace Institute recorded over 235 cyberattacks on healthcare organizations in 33 countries, resulting in the theft of more than 10 million patient records.
- High-Profile Attack: The ransomware attack on Ireland's Health Service Executive (HSE) in May 2021 highlights the sector's vulnerability and urgent need for advanced protection.
- Cloud Adoption Accelerates Cybersecurity Demand: The rapid adoption of cloud services in healthcare is creating both challenges and opportunities in cybersecurity. Hybrid cloud solutions, which enhance operational efficiency and data analytics, are being embraced to manage costs. However, this shift increases the need for robust cybersecurity measures to protect sensitive patient information across diverse cloud platforms.
- Cloud Integration Growth: Nutanix projects that healthcare organizations will increase hybrid cloud deployments by 32 percentage points over the next five years.
- Strategic Partnerships: Major institutions like Cleveland Clinic are collaborating with tech companies such as IBM to harness

hybrid cloud, AI, and quantum computing technologies.
- Guidelines for Cloud Security: The European Union Agency for Cybersecurity (ENISA) has released cloud security guidelines specifically for healthcare, underscoring the growing need for secure cloud infrastructures.
- Inadequate Security Infrastructure Poses Risks: A significant gap in healthcare information security infrastructure presents both risks and opportunities. Many healthcare organizations have limited cybersecurity training and outdated infrastructure, leaving them vulnerable to breaches. This gap is fueling demand for customized cybersecurity solutions designed to meet healthcare providers' unique needs.
- Training Gaps: NordLocker's survey revealed that 56% of healthcare employees have not received any cybersecurity training from their current employers.
- Regional Disparities: In India, the adoption of Healthcare Information Technology (HIT) remains low compared to developed nations due to underfunding and limited IT expertise.
- Growing mHealth Market: The rapid growth of the mHealth market in India signals a pressing need for mobile-specific cybersecurity solutions as healthcare organizations adopt mobile technologies.
- Market Dynamics Shaped by Regulatory Pressures: Regulatory frameworks such as HIPAA in the U.S. are playing a pivotal role in driving the Healthcare Cyber Security Market. These regulations require strict data protection measures, compelling healthcare organizations to invest in compliant cybersecurity solutions.
- Data Breach Incidents: The U.S. Department of Health and Human Services reported that hacking incidents accounted for most data breaches involving 500+ patient records in 2021.
- EHR Systems: The increasing adoption of electronic health records (EHR) mandates robust security protocols to protect patient data.
- ROI-Driven Adoption: Vendors are focusing on demonstrating a return on investment (ROI) by improving the efficiency of cybersecurity systems, which is crucial for overcoming implementation barriers.
- Emerging Technologies Reshape Security Landscape: The rise of Internet of Things (IoT) devices and artificial intelligence (AI) in healthcare is introducing new cybersecurity challenges. These technologies increase the attack surface and demand specialized security solutions, prompting vendors to develop AI-powered tools and IoT-specific protection.
- IoT Device Risks: A 2022 report revealed that one-third of bedside IoT devices in healthcare have critical vulnerabilities that could be exploited by cybercriminals.
- AI Integration: The U.S. Department of Health and Human Services is using AI-powered SaaS tools for tasks such as grant application analysis, showing the growing role of AI in healthcare operations.
- Medical Device Security: Cybersecurity companies are creating solutions that safeguard the increasingly interconnected ecosystem of medical devices and data systems, addressing the evolving healthcare threat landscape.

Healthcare Cyber Security Market Trends

Risk and Compliance Management Largest Solution Segment

Risk and compliance management is the largest solution segment in the Healthcare Cyber Security Market, driven by increasing regulatory pressures and the need to protect sensitive patient data. In 2021, this segment accounted for 28.97% of the market share, underscoring its dominance.

- Revenue Generation: The risk and compliance management segment generated USD 5.41 billion in 2021, capturing 28.95% of the market. This figure is expected to rise to USD 15.27 billion by 2027, with a projected CAGR of 18.88%.
- Regulatory Pressure: The complexity of evolving cyber threats and compliance with regulations such as HIPAA are key drivers for the segment's growth. Healthcare's high data breach costs, highlighted by IBM's report, further emphasize the need for robust compliance frameworks.

- Growing Awareness: The importance of risk and compliance management solutions is growing among healthcare organizations, exemplified by partnerships like that between SailPoint and Canadian healthcare providers, which address data residency and streamline identity management.
- Compliance Solutions: As cyber threats evolve and regulations tighten, the demand for comprehensive risk and compliance management solutions will continue to grow, securing the segment's leading position in the market.

Asia-Pacific: Fastest-Growing Regional Segment

The Asia-Pacific region has emerged as the fastest-growing segment in the Healthcare Cyber Security Market, driven by rapid healthcare digitization, rising cyber threats, and increasing data protection awareness.

- Market Value: In 2021, the Asia-Pacific healthcare cybersecurity market was valued at USD 3.92 billion, representing 20.97% of the global market. The region is projected to reach USD 12.08 billion by 2027, with a CAGR of 20.63%.
- Technology Adoption: The region's rapid adoption of digital health technologies, such as telehealth and AI-driven healthcare solutions, necessitates more robust cybersecurity infrastructure. For instance, Singapore's Woodlands Health Campus will heavily rely on telehealth, robotics, and AI.
- Cyber Threats: High-profile breaches like the 2018 SingHealth data breach, which affected 1.5 million patients, and the 2021 attack on Eye & Retina Surgeons have fueled investments in cybersecurity across the region.
- Cloud-Based Solutions: The adoption of cloud platforms for managing patient information is simplifying the implementation of cybersecurity protocols in the Asia-Pacific healthcare sector, accelerating market growth.

Healthcare Cyber Security Industry Overview

Healthcare Cyber Security Market Competitive Landscape Analysis: The Healthcare Cyber Security Market is dominated by global players, with the competitive landscape characterized by high barriers to entry due to stringent regulations and advanced technological demands. The market remains fairly consolidated, with a few key players holding significant market share.

Market Leaders: Major companies such as Cisco Systems Inc., IBM Corporation, Kaspersky Labs Inc., and FireEye Inc. dominate the market. These leaders offer comprehensive solutions that address threat detection, prevention, and response needs specific to healthcare.

Research & Development: Continuous investment in research and development helps market leaders stay ahead of evolving threats. For example, CloudMD Software & Services Inc. enhanced its capabilities by acquiring IDYA4 to provide integrated cybersecurity and healthcare solutions.

Acquisitions & Partnerships: Partnerships with healthcare providers and strategic acquisitions are critical for expanding product portfolios and market reach. These collaborations help cybersecurity firms tailor their offerings to the complex needs of the healthcare sector.

Innovation and Compliance Drive Market Success: Market leaders must focus on continuous innovation, particularly in threat detection, prevention, and compliance, to stay competitive. Addressing challenges posed by IoT and AI applications will be essential.

AI-Driven Solutions: Companies that develop AI-driven cybersecurity tools capable of protecting against sophisticated cyberattacks will gain a competitive edge.

Regulatory Adherence: Solutions that meet the latest healthcare regulations, such as HIPAA and GDPR, while addressing the growing challenges of data protection, will likely dominate the market.

Custom Solutions: Firms that offer tailored cybersecurity systems, particularly through managed security service providers (MSSPs), are expected to see increased adoption in healthcare settings. These solutions focus on protecting medical workflows and patient care from emerging cyber threats.

Additional Benefits:

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

Table of Contents:

Healthcare Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 120 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	