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

Market Report | 2025-06-01 | 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:

Healthcare Cyber Security Market Analysis

The healthcare cybersecurity market stands at USD 35.78 billion in 2025 and is forecast to expand to USD 89.93 billion by 2030, progressing at an 18.59% CAGR during 2025-2030. The spending surge reflects an industry-wide scramble to defend electronic protected health information against a record wave of intrusions. Healthcare providers reported 677 major breaches in 2024 that exposed 182.4 million patient records, underscoring the sector's high-value data and persistent threat landscape. Heightened federal oversight, notably the Food and Drug Administration's Section 524B requirements for all new connected medical devices, obliges manufacturers and providers to budget for life-cycle security programs. Parallel to device rules, the Office for Civil Rights' stiffer HIPAA enforcement and the Department of Health and Human Services' voluntary cybersecurity performance goals have pushed boards to elevate cyber risk to a top-three enterprise issue. Government funding amplifies the momentum: Washington's 2025 consolidated cyber budget earmarks USD 13 billion for civilian agencies, a portion of which flows to hospitals modernizing legacy systems. Simultaneously, the American Hospital Association's alert that nation-state actors targeted United States facilities in 2024 catalyzes the uptake of zero-trust frameworks and real-time monitoring solutions.

Global Healthcare Cyber Security Market Trends and Insights

Escalating Frequency and Sophistication of Cyber-Attacks

Security researchers confirmed that adversaries linked to Russia, China, North Korea, and Iran probed hospital infrastructure daily

in 2024, culminating in breaches that touched an estimated 259 million medical records. Health records command a premium on illicit markets because they enable insurance fraud, blackmail, and espionage. This dual utility fuels relentless reconnaissance, ransomware, and supply-chain attacks. Artificial-intelligence tooling now automates spear-phishing and voice deep-fake scams, eroding user-based defenses. Providers respond by prioritizing continuous monitoring, multi-factor authentication, and least-privilege policies across cloud workloads and connected devices.

Regulatory Mandates and Compliance Burden

Section 524B requires every new medical device submitted to the FDA after March 2023 to include a Software Bill of Materials, secure development attestations, and a plan for coordinated vulnerability disclosure. Beyond pre-market clearance, manufacturers must patch flaws for the product's commercial life. Hospitals integrating these devices, therefore, budget for integrated risk management platforms able to track firmware, security advisories, and patch status in real time. Simultaneously, the HHS Cybersecurity Performance Goals outline baseline safeguards-such as immutable backups and privileged access controls-that many boards treat as de facto standards. Identity, Credential, and Access Management frameworks endorsed by the Cybersecurity and Infrastructure Security Agency replace password-centric models with risk-based, certificate-driven authentication.

Budget Constraints in Small Providers

Smaller hospitals often run on operating margins below 2%, leaving inadequate reserves for layered security tooling and 24□7 monitoring. Investigations into recent closures show cyber incidents can trigger permanent shutdowns when ransom demands and downtime erode liquidity. The Healthcare Sector Coordinating Council recommends classifying cybersecurity as an allowable Medicare expense, yet reimbursement policy remains under review. Until sustainable funding emerges, adoption of subscription-based managed detection and response services is the primary avenue for risk reduction.

Other drivers and restraints analyzed in the detailed report include:

Rapid Cloud-Based EHR and Tele-Health Adoption / Low Security Penetration Among Smaller Providers / Shortage of Specialized Cyber-Security Talent /

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Identity and Access Management tools accounted for 26.2% of the healthcare cybersecurity market size in 2024 as organizations focused on controlling privileged credentials inside sprawling clinical ecosystems. However, demand is shifting toward Security Information and Event Management platforms, which are forecast to grow at 19.1% CAGR to 2030. The change reflects a consensus that continuous log correlation and behavioral analytics offer faster breach containment than perimeter controls alone. Over the forecast period, cybersecurity roadmaps show budget reallocation from stand-alone antivirus toward converged detection stacks that integrate SIEM, SOAR, and user-entity analytics.

Risk and compliance suites remain steady because they streamline documentation for HIPAA, GDPR, and device post-market surveillance audits. Encryption and data-loss-prevention modules gain traction within zero-trust architectures, especially where providers must share radiology images and lab data across multiple cloud tenants. Emerging behavioral analytics solutions built with machine learning sit in the "other solutions" bucket and are frequently piloted in research institutes experimenting with precision medicine workloads.

Network security retained 34.3% of the healthcare cybersecurity market share in 2024 because hospitals continue to segment VLANs connecting operating rooms, pharmaceutical automation, and picture-archiving systems. The pivot to cloud workloads is nonetheless reshaping priorities: cloud security tools are poised for an 18.9% CAGR, propelled by migrations of EHR instances to hyperscale providers.

Endpoint protection confronts proliferating device heterogeneity, from bedside infusion pumps to clinician smartphones. Application security rises as in-house development teams build patient-facing portals that integrate third-party APIs, necessitating runtime protection and software composition analysis. Medical-device and IoMT security, once an afterthought, is now a board-level issue because more than 14,000 healthcare IP addresses expose device telemetry to the public internet-a statistic that rallies funding for agentless network detection and regulated device patch orchestration.

Healthcare Cybersecurity Market is Segmented by Solution Type (Identity and Access Management, Risk and Compliance Management, and More), Security Type (Network Security, Endpoint Security, and More), Deployment Mode (On-Premises and Cloud), End User (Hospitals and Clinics, and More), Organization Size (Large Enterprises and Small and Medium Enterprises), and by Geography. The Market Forecasts are Provided in Terms of Value (USD).

Geography Analysis

North America maintained 34.5% healthcare cyber security market share in 2024, backed by the world's strictest PHI regulations, a mature insurance system, and high per-capita health IT budgets. Federal funding, including the 2025 civilian cyber allocation, underwrites modernization of electronic health records and cloud adoption. The United States also endured the largest known breach the 2024 Change Healthcare incident affecting 100 million individuals which solidified zero-trust roadmaps and third-party risk audits. Canada's Pan-Canadian Artificial Intelligence Strategy and Mexico's social-security digitization initiatives further enlarge regional demand for SIEM and endpoint detection tools.

Asia-Pacific is the fastest-growing territory at 19.7% CAGR. National e-health mandates in Japan, South Korea, and India integrate cloud-hosted patient registries with secure identity platforms, spurring local demand for data-masking and encryption-as-a-service offerings. China's Healthy China 2030 blueprint designates cybersecurity one of six enabling pillars for smart hospitals, boosting orders for domestic firewall and vulnerability-management vendors that meet cross-border data flow restrictions. Australia's federal budget anchors subsidies for rural tele-health, leading to a 92% jump in digital-health solicitation requests from 2022-2024.

Europe's privacy-centric regime ensures steady growth as GDPR fines crystallize board-level accountability. Germany allocates EUR 3 billion to hospital digitization with at least 15% reserved for IT security enhancements, stimulating procurement of identity orchestration and secure email gateways. France implements its "MaSante 2025" e-health strategy with a cybersecurity annex that mandates threat-intelligence sharing among regional health agencies. The United Kingdom's NHS "Data Saves Lives" program directs funds to modernize legacy paging and imaging platforms, contingent upon ISO 27001 certification.

The Middle East and Africa exhibit accelerating adoption as Gulf Cooperation Council states build smart-city hospitals and seek compliance with the National Cybersecurity Authority's Healthcare Sector Controls. South Africa and Kenya pilot cloud-based immunization registries accompanied by tokenization schemes that de-identify patient data. South America registers steady expansion led by Brazil's open-health initiatives and Argentina's electronic prescription rollout, both of which require encryption key management and secure API gateways.

List of Companies Covered in this Report:

Cisco Systems Inc. / IBM Corporation / AO Kaspersky Lab / McAfee LLC / Broadcom Inc. (Symantec) / Trend Micro Inc. / Palo

Alto Networks Inc. / Check Point Software Technologies Ltd. / Fortinet Inc. / CrowdStrike Holdings Inc. / FireEye Inc. (Trellix) / Imperva Inc. / Claroty Ltd. (Medigate) / Cynerio Ltd. / Sophos Group plc / Proofpoint Inc. / Rapid7 Inc. / CynergisTek Inc. / Clearwater Compliance LLC / Sensato Cybersecurity Solutions / SecureLink Inc. /

Additional Benefits:

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

Table of Contents:

5.6.5 Middle East and Africa
5.6.5.1 Middle East
5.6.5.1.1 Saudi Arabia
5.6.5.1.2 United Arab Emirates
5.6.5.1.3 Turkey
5.6.5.1.4 Rest of Middle East
5.6.5.2 Africa
5.6.5.2.1 South Africa
5.6.5.2.2 Egypt
5.6.5.2.3 Nigeria
5.6.5.2.4 Rest of Africa

6 COMPETITIVE LANDSCAPE
6.1 Market Concentration
6.2 Strategic Moves
6.3 Market Share Analysis
6.4 Company Profiles {(includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share for key companies, Products and Services, and Recent Developments)}
6.4.1 Cisco Systems Inc.
6.4.2 IBM Corporation
6.4.3 AO Kaspersky Lab
6.4.4 McAfee LLC
6.4.5 Broadcom Inc. (Symantec)
6.4.6 Trend Micro Inc.
6.4.7 Palo Alto Networks Inc.
6.4.8 Check Point Software Technologies Ltd.
6.4.9 Fortinet Inc.
6.4.10 CrowdStrike Holdings Inc.
6.4.11 FireEye Inc. (Trellix)
6.4.12 Imperva Inc.
6.4.13 Claroty Ltd. (Medigate)
6.4.14 Cynerio Ltd.
6.4.15 Sophos Group plc
6.4.16 Proofpoint Inc.
6.4.17 Rapid7 Inc.
6.4.18 CynergisTek Inc.
6.4.19 Clearwater Compliance LLC
6.4.20 Sensato Cybersecurity Solutions
6.4.21 SecureLink Inc.

7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK
7.1 White-space and Unmet-need Assessment

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

Market Report | 2025-06-01 | 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	2026-03-04
		Signature