Market Publishers
+357 96 030922
info@marketpublishers.com

Healthcare Cybersecurity Solutions Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Deployment Mode, Security Type, Threat Type, Application, End User and By Geography

https://marketpublishers.com/r/H2E56B6E9414EN.html
Date: June 2026
Pages: 200
Price: US$ 4,150.00 (Single User License)
ID: H2E56B6E9414EN

Abstracts

According to Stratistics MRC, the Global Healthcare Cybersecurity Solutions Market is accounted for $18.2 billion in 2026 and is expected to reach $62.7 billion by 2034, growing at a CAGR of 16.8% during the forecast period. Healthcare Cybersecurity Solutions encompass a comprehensive suite of software, hardware, and managed services designed to protect healthcare organizations' digital infrastructure, patient data, clinical networks, and connected medical devices from unauthorized access, ransomware attacks, data breaches, and operational disruptions. As healthcare systems undergo accelerating digital transformation integrating electronic health records, telehealth platforms, IoT medical devices, and cloud-based clinical applications the attack surface for malicious actors expands proportionally.

Market Dynamics:

Driver:

Escalating ransomware attacks and data breach incidents targeting healthcare institutions

Healthcare organizations have emerged as the most targeted sector for ransomware attacks and data breaches, driven by the high value of patient health records on dark web markets and the operational criticality of clinical systems that creates pressure for rapid ransom payment. High-profile attacks on hospitals have resulted in care diversions, surgical delays, and adverse patient outcomes, elevating cybersecurity

+357 96 030922
info@marketpublishers.com

investment from a compliance consideration to a patient safety imperative. Regulatory penalties for HIPAA violations and data breach notification requirements further incentivize proactive security investment. Healthcare boards and executives are allocating increasing capital to cybersecurity as operational risk management becomes inseparable from clinical risk management.

Restraint:

Legacy IT infrastructure and budget constraints at smaller health systems

A significant proportion of healthcare organizations particularly community hospitals, rural health systems, and physician practices operate on aging IT infrastructure with limited compatibility with modern cybersecurity solutions. Replacing or securing legacy systems requires substantial capital investment that competes with clinical priorities for limited budget allocations. Smaller organizations frequently lack dedicated cybersecurity personnel and rely on general IT staff without specialized security expertise. These structural constraints create persistent vulnerability gaps that sophisticated threat actors actively exploit, undermining overall healthcare sector security posture despite rising investment from larger institutions.

Opportunity:

Growth of IoMT device security and zero-trust architecture adoption

The proliferation of Internet of Medical Things (IoMT) devices including connected infusion pumps, patient monitors, imaging systems, and surgical robots creates a rapidly expanding and largely unprotected attack surface requiring specialized medical device security solutions. Vendors developing IoMT-specific security platforms that provide asset discovery, behavioral monitoring, and anomaly detection are addressing an urgent and underserved market need. Simultaneously, the adoption of zero-trust security architectures within healthcare environments is driving comprehensive security platform investments as organizations move beyond perimeter-based defenses toward continuous identity verification and micro-segmentation approaches.

Threat:

Sophisticated state-sponsored cyber threats and supply chain vulnerabilities

Nation-state cyber actors increasingly target healthcare systems for intelligence gathering, infrastructure disruption, and theft of pharmaceutical research data, employing sophisticated attack methodologies that frequently evade conventional detection systems. Supply chain attacks compromising healthcare software vendors and medical device manufacturers can simultaneously impact thousands of connected health institutions through a single breach point. The growing reliance on cloud service providers and third-party healthcare IT vendors introduces concentration risk that is difficult to monitor and mitigate through standard contractual security controls, requiring healthcare organizations to maintain continuous third-party risk assessments alongside their own internal security programs.

Covid-19 Impact:

The COVID-19 pandemic dramatically intensified healthcare cybersecurity challenges as organizations rapidly deployed remote access solutions, telehealth platforms, and cloud services to maintain care delivery frequently outpacing security controls. Cybercriminals exploited pandemic-related urgency, targeting vaccine distribution systems, clinical trial data repositories, and overwhelmed hospital networks with unprecedented attack volumes. The crisis revealed critical gaps in healthcare cybersecurity readiness while simultaneously accelerating technology adoption that expanded the long-term attack surface. Post-pandemic investment in cybersecurity infrastructure has accelerated significantly as health systems fortify defenses against increasingly sophisticated threat actor capabilities.

The Solutions segment is expected to be the largest during the forecast period

The solutions segment is expected to account for the largest market share during the forecast period, encompassing identity and access management, endpoint security, SIEM platforms, and network protection systems that form the foundational technical defense architecture for healthcare organizations. Increasing regulatory requirements mandating specific security control implementations are driving enterprise-wide solutions deployment across hospital networks. The critical need to protect electronic health record systems and clinical workflows from disruption ensures sustained solutions investment regardless of broader IT budget pressures throughout the forecast period.

The Cloud Security Solutions segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the Cloud Security Solutions segment is predicted to witness the highest growth rate, reflecting the accelerating migration of healthcare workloads to cloud environments and the corresponding need for specialized cloud-native security capabilities. As healthcare organizations adopt hybrid and multi-cloud architectures for clinical applications, data analytics, and telehealth delivery, demand for cloud access security brokers, cloud workload protection platforms, and data loss prevention solutions is expanding rapidly.

Region with largest share:

During the forecast period, the North America region is expected to hold the largest market share, driven by the world's highest concentration of high-value healthcare targets, mature regulatory enforcement under HIPAA, and the highest per-capita healthcare IT expenditure globally. The United States experiences the greatest volume of healthcare cyberattacks among all nations, creating commensurate demand for advanced security solutions. A dense ecosystem of specialized healthcare cybersecurity vendors, managed security service providers, and regulatory consultants supports comprehensive market development across the region.

Region with highest CAGR:

Over the forecast period, the Asia Pacific region is anticipated to exhibit the highest CAGR, driven by rapid healthcare digitalization, expanding telemedicine adoption, and escalating cyber threat activity targeting the region's growing health data repositories. China, India, and Australia are implementing new healthcare data protection regulations that mandate security investments from healthcare institutions of all sizes. The region's large and rapidly digitizing patient populations, combined with increasing cross-border health data flows requiring protection, position Asia Pacific as the highest-growth cybersecurity market within the global healthcare sector.

Key players in the market

Some of the key players in Healthcare Cybersecurity Solutions Market include IBM, Cisco Systems, Inc., Palo Alto Networks, Fortinet, Inc., Trend Micro Incorporated, McAfee, LLC, Broadcom, Check Point Software Technologies, CrowdStrike Holdings, Inc., Claroty, Armis, Inc., Imperva, Inc., Kaspersky Lab, Cylera, and Medigate by Claroty.

Key Developments:

+357 96 030922
info@marketpublishers.com

In March 2026, CrowdStrike announced the launch of a healthcare-specific module within its Falcon cybersecurity platform, delivering pre-configured threat detection rules, IoMT device behavior monitoring, and automated HIPAA compliance reporting tailored to the unique security requirements of hospitals and integrated health systems.

In February 2026, Claroty completed a significant strategic acquisition of a specialized medical device vulnerability assessment company, enhancing its healthcare extended IoT security platform with advanced clinical asset risk scoring and automated remediation workflow capabilities serving hospital network security operations teams globally.

Components Covered:

- Solutions
- Services

Deployment Modes Covered:

- On-Premise
- Cloud-Based
- Hybrid

Security Types Covered:

- Network Security
- Endpoint Security
- Application Security
- Cloud Security
- Wireless Security

IoT & Medical Device Security

Database & Data Security

Threat Types Covered:

Malware

Ransomware

Phishing Attacks

Distributed Denial of Service (DDoS)

Advanced Persistent Threats (APT)

Spyware

Insider Threats

Lost or Stolen Devices

Applications Covered:

Electronic Health Records (EHR) Protection

Telehealth & Remote Patient Monitoring Security

Medical Device & IoMT Security

Clinical Workflow Protection

Pharmacy Information Systems Security

Healthcare Cloud Infrastructure Protection

Revenue Cycle & Claims Security

+357 96 030922
info@marketpublishers.com

- Patient Data Protection & Privacy

End Users Covered:

- Hospitals & Clinics
- Diagnostic & Imaging Centers
- Pharmaceutical & Biotechnology Companies
- Medical Device Manufacturers
- Health Insurance Providers & Payers
- Ambulatory Surgical Centers
- Government Healthcare Organizations
- Research Institutes & Academic Medical Centers
- Other End Users

Regions Covered:

- North America
  - United States
  - Canada
  - Mexico
- Europe
  - United Kingdom

+357 96 030922
info@marketpublishers.com

- Germany
- France
- Italy
- Spain
- Netherlands
- Belgium
- Sweden
- Switzerland
- Poland
- Rest of Europe

Asia Pacific

- China
- Japan
- India
- South Korea
- Australia
- Indonesia
- Thailand
- Malaysia
- Singapore

+357 96 030922
info@marketpublishers.com

Vietnam

Rest of Asia Pacific

South America

Brazil

Argentina

Colombia

Chile

Peru

Rest of South America

Rest of the World (RoW)

Middle East

Saudi Arabia

United Arab Emirates

Qatar

Israel

Rest of Middle East

Africa

South Africa

Egypt

Morocco

Rest of Africa

What our report offers:

- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2023, 2024, 2025, 2026, 2027, 2028, 2030, 2032 and 2034
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

+357 96 030922
info@marketpublishers.com

Contents

5 GLOBAL HEALTHCARE CYBERSECURITY SOLUTIONS MARKET, BY COMPONENT

6 GLOBAL HEALTHCARE CYBERSECURITY SOLUTIONS MARKET, BY DEPLOYMENT MODE

7 GLOBAL HEALTHCARE CYBERSECURITY SOLUTIONS MARKET, BY SECURITY TYPE

+357 96 030922
info@marketpublishers.com

11 GLOBAL HEALTHCARE CYBERSECURITY SOLUTIONS MARKET, BY GEOGRAPHY

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

Institutes & Academic Medical Centers (2023-2034) ($MN)
Table 58 Global Healthcare Cybersecurity Solutions Market Outlook, By Other End Users (2023-2034) ($MN)
Note: Tables for North America, Europe, APAC, South America, and Rest of the World (RoW) are also represented in the same manner as above.

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Healthcare Cybersecurity Solutions Market Forecasts to 2034 – Global Analysis By Component (Solutions and Services), Deployment Mode, Security Type, Threat Type, Application, End User and By Geography

Product link: https://marketpublishers.com/r/H2E56B6E9414EN.html

Price: US$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/H2E56B6E9414EN.html