

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

<https://marketpublishers.com/r/HD5DBE71B24FEN.html>

Date: June 2026

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: HD5DBE71B24FEN

Abstracts

According to Statistics MRC, the Global Healthcare Cybersecurity Market is accounted for \$21.3 billion in 2026 and is expected to reach \$67.5 billion by 2034, growing at a CAGR of 15.6% during the forecast period. Healthcare Cybersecurity encompasses a comprehensive suite of technologies, solutions, and practices designed to safeguard sensitive medical information, connected devices, and healthcare IT infrastructure from cyber threats. It protects electronic health records, medical devices, and clinical networks against unauthorized access, ransomware, and data breaches. By enabling regulatory compliance and ensuring continuous availability of critical health systems, healthcare cybersecurity plays a pivotal role in maintaining patient safety and the operational integrity of healthcare organizations worldwide.

Market Dynamics:

Driver:

Escalating volume and sophistication of cyberattacks on healthcare systems

Healthcare organizations have emerged as prime targets for cybercriminals due to the highly sensitive nature of patient data and the critical urgency of uninterrupted care delivery. Ransomware campaigns have disrupted hospital operations globally, compelling administrators to invest heavily in advanced threat detection, endpoint protection, and security information management systems. Regulatory mandates such as HIPAA and GDPR further intensify the need for robust cybersecurity frameworks. As

electronic health records, connected medical devices, and telehealth platforms proliferate, the attack surface expands, making sustained investment in cybersecurity solutions a non-negotiable organizational priority.

Restraint:

Shortage of skilled cybersecurity professionals in the healthcare sector

The healthcare industry faces a pronounced deficit of qualified cybersecurity specialists who possess both technical expertise and an understanding of clinical workflows. Recruiting and retaining such talent requires substantial compensation packages that many healthcare providers, particularly smaller hospitals and rural clinics, cannot sustain. This workforce gap limits the effectiveness of deployed security tools, delays incident response, and leaves organizations vulnerable to evolving threats. The complexity of healthcare IT environments comprising legacy systems, medical IoT devices, and cloud platforms further amplifies the challenge, constraining organizations' ability to maintain comprehensive, proactive cyber defenses.

Opportunity:

Rapid expansion of AI-driven threat intelligence and automated security platforms

Artificial intelligence and machine learning are transforming healthcare cybersecurity by enabling real-time anomaly detection, predictive threat modeling, and automated incident remediation at speeds no human team can match. AI-powered security platforms can analyze vast streams of network activity data, identify behavioral deviations, and neutralize threats before they escalate. This capability is especially vital in healthcare environments where continuous uptime is critical. Vendors integrating AI into next-generation security operations centers and offering managed detection and response services are well-positioned to capture significant market share as healthcare organizations seek scalable, cost-effective protection.

Threat:

Vulnerabilities inherent in legacy medical devices and outdated IT infrastructure

A substantial share of medical equipment in clinical use operates on end-of-life operating systems that no longer receive security patches, creating persistent entry points for attackers. Replacing these devices is prohibitively expensive and

operationally disruptive, leaving healthcare networks exposed. Interconnectivity between legacy clinical systems and modern digital health platforms further compounds the risk, as a single compromised endpoint can cascade across the entire organization. Addressing these vulnerabilities requires a sustained capital commitment and careful orchestration with clinical operations, presenting a formidable structural challenge that tempers the pace of security modernization across the healthcare industry.

Covid-19 Impact

The COVID-19 pandemic significantly accelerated digital transformation in healthcare, expanding telehealth services, remote monitoring, and cloud adoption at unprecedented speed. While these changes improved patient access, they dramatically broadened the cybersecurity attack surface. Cybercriminals exploited the crisis with a surge in phishing campaigns, ransomware attacks, and COVID-related fraud targeting overburdened health systems. Despite initial budget pressures, the pandemic ultimately elevated cybersecurity to a board-level priority, stimulating accelerated procurement of advanced security solutions and managed services, and positioning the market for robust post-pandemic growth.

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, underpinned by pervasive demand for identity and access management, firewall protection, and security information and event management tools. Healthcare organizations prioritize solution-based investments to address regulatory compliance mandates including HIPAA and GDPR, while protecting electronic health records from increasingly sophisticated threats. The comprehensive nature of cybersecurity solution suites spanning network, endpoint, and application protection—positions this segment as the foundational layer of healthcare security strategy, attracting consistent enterprise and hospital-level procurement across both developed and emerging markets.

The Cloud-Based segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the Cloud-Based segment is predicted to witness the highest growth rate throughout the forecast period, propelled by healthcare organizations' accelerating migration to cloud infrastructure for scalability, cost efficiency, and remote access capabilities. Cloud-native security architectures enable continuous threat

monitoring, seamless software updates, and centralized management across distributed care environments. The proliferation of telehealth and cloud-hosted electronic health record platforms intensifies demand for cloud-native security tools. Vendors offering security-as-a-service models with subscription-based pricing are attracting growing adoption, particularly among mid-sized healthcare providers seeking enterprise-grade protection without substantial upfront capital expenditure.

Region with largest share:

During the forecast period, the North America holds the dominant regional share in the healthcare cybersecurity market, anchored by the United States' advanced healthcare IT infrastructure, stringent regulatory environment, and high density of leading cybersecurity vendors. Federal mandates such as HIPAA compel widespread security investment, while frequent high-profile healthcare data breaches sustain executive-level attention to cyber risk. The presence of large health systems, insurance conglomerates, and pharmaceutical enterprises with substantial IT budgets supports robust market demand. Additionally, strong government cybersecurity initiatives and public-private partnerships reinforce the region's leadership position throughout the forecast period.

Region with highest CAGR:

Over the forecast period, the Asia Pacific is set to register the highest CAGR during the forecast period, driven by rapid digitization of healthcare systems in China, India, and Southeast Asian economies. Government-led e-health initiatives, expanding hospital networks, and growing telemedicine adoption are generating significant volumes of sensitive health data requiring protection. Rising awareness of cyber threats following several high-profile regional breaches is prompting accelerated security investment. Local regulators are also tightening data protection frameworks, compelling healthcare organizations to upgrade their cybersecurity postures, thereby creating substantial market expansion opportunities across the region.

Key Players:

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

Key Developments:

In February 2026, CrowdStrike Holdings expanded its Falcon platform with dedicated healthcare modules, offering specialized ransomware prevention and HIPAA-aligned threat intelligence feeds, enabling healthcare institutions to streamline compliance reporting while maintaining comprehensive endpoint protection across their clinical and administrative IT infrastructure.

In January 2026, Palo Alto Networks announced the general availability of its AI-powered Cortex XSIAM platform tailored specifically for healthcare environments, incorporating automated threat response capabilities and native medical device security integrations designed to reduce mean time to remediation across hospital networks.

Components Covered:

Solutions

Services

Threat Types Covered:

Malware

Ransomware

Phishing & Social Engineering

Distributed Denial of Service (DDoS)

Advanced Persistent Threats (APT)

Spyware

Insider Threats

Lost or Stolen Devices

Deployment Modes Covered:

On-Premises

Cloud-Based

Hybrid

Security Types Covered:

Network Security

Endpoint Security

Cloud Security

Application Security

IoT & Medical Device Security

Database Security

Applications Covered:

Electronic Health Records (EHR) Protection

Medical Device Security

Telemedicine Security

Health Information Exchange Security

Pharmacy Information Systems Security

Remote Patient Monitoring Security

Claims & Billing Fraud Prevention

Cloud Data Protection

Other Applications

End Users Covered:

Hospitals & Clinics

Pharmaceutical & Biotechnology Companies

Health Insurance Providers/Payers

Medical Device Manufacturers

Clinical Laboratories

Government Healthcare Agencies

Research Institutions

Telehealth & Digital Health Providers

Ambulatory Surgical Centers

Regions Covered:

North America

United States

Canada

Mexico

Europe

United Kingdom

Germany

France

Italy

Spain

Netherlands

Belgium

Sweden

Switzerland

Poland

Rest of Europe

Asia Pacific

China

Japan

India

South Korea

Australia

Indonesia

Thailand

Malaysia

Singapore

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, 3032 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

Contents

1 EXECUTIVE SUMMARY

- 1.1 Market Snapshot and Key Highlights
- 1.2 Growth Drivers, Challenges, and Opportunities
- 1.3 Competitive Landscape Overview
- 1.4 Strategic Insights and Recommendations

2 RESEARCH FRAMEWORK

- 2.1 Study Objectives and Scope
- 2.2 Stakeholder Analysis
- 2.3 Research Assumptions and Limitations
- 2.4 Research Methodology
 - 2.4.1 Data Collection (Primary and Secondary)
 - 2.4.2 Data Modeling and Estimation Techniques
 - 2.4.3 Data Validation and Triangulation
 - 2.4.4 Analytical and Forecasting Approach

3 MARKET DYNAMICS AND TREND ANALYSIS

- 3.1 Market Definition and Structure
- 3.2 Key Market Drivers
- 3.3 Market Restraints and Challenges
- 3.4 Growth Opportunities and Investment Hotspots
- 3.5 Industry Threats and Risk Assessment
- 3.6 Technology and Innovation Landscape
- 3.7 Emerging and High-Growth Markets
- 3.8 Regulatory and Policy Environment
- 3.9 Impact of COVID-19 and Recovery Outlook

4 COMPETITIVE AND STRATEGIC ASSESSMENT

- 4.1 Porter's Five Forces Analysis
 - 4.1.1 Supplier Bargaining Power
 - 4.1.2 Buyer Bargaining Power
 - 4.1.3 Threat of Substitutes
 - 4.1.4 Threat of New Entrants

- 4.1.5 Competitive Rivalry
- 4.2 Market Share Analysis of Key Players
- 4.3 Product Benchmarking and Performance Comparison

5 GLOBAL HEALTHCARE CYBERSECURITY MARKET, BY COMPONENT

- 5.1 Solutions
 - 5.1.1 Identity & Access Management (IAM)
 - 5.1.2 Antivirus & Antimalware
 - 5.1.3 Encryption & Tokenization
 - 5.1.4 Firewall
 - 5.1.5 Security Information & Event Management (SIEM)
 - 5.1.6 Intrusion Detection & Prevention Systems (IDS/IPS)
 - 5.1.7 Data Loss Prevention (DLP)
 - 5.1.8 Risk & Compliance Management
- 5.2 Services
 - 5.2.1 Professional Services
 - 5.2.2 Managed Security Services
 - 5.2.3 Consulting Services
 - 5.2.4 Training & Support Services

6 GLOBAL HEALTHCARE CYBERSECURITY MARKET, BY THREAT TYPE

- 6.1 Malware
- 6.2 Ransomware
- 6.3 Phishing & Social Engineering
- 6.4 Distributed Denial of Service (DDoS)
- 6.5 Advanced Persistent Threats (APT)
- 6.6 Spyware
- 6.7 Insider Threats
- 6.8 Lost or Stolen Devices

7 GLOBAL HEALTHCARE CYBERSECURITY MARKET, BY DEPLOYMENT MODE

- 7.1 On-Premises
- 7.2 Cloud-Based
- 7.3 Hybrid

8 GLOBAL HEALTHCARE CYBERSECURITY MARKET, BY SECURITY TYPE

- 8.1 Network Security
- 8.2 Endpoint Security
- 8.3 Cloud Security
- 8.4 Application Security
- 8.5 IoT & Medical Device Security
- 8.6 Database Security

9 GLOBAL HEALTHCARE CYBERSECURITY MARKET, BY APPLICATION

- 9.1 Electronic Health Records (EHR) Protection
- 9.2 Medical Device Security
- 9.3 Telemedicine Security
- 9.4 Health Information Exchange Security
- 9.5 Pharmacy Information Systems Security
- 9.6 Remote Patient Monitoring Security
- 9.7 Claims & Billing Fraud Prevention
- 9.8 Cloud Data Protection
- 9.9 Other Applications

10 GLOBAL HEALTHCARE CYBERSECURITY MARKET, BY END USER

- 10.1 Hospitals & Clinics
- 10.2 Pharmaceutical & Biotechnology Companies
- 10.3 Health Insurance Providers/Payers
- 10.4 Medical Device Manufacturers
- 10.5 Clinical Laboratories
- 10.6 Government Healthcare Agencies
- 10.7 Research Institutions
- 10.8 Telehealth & Digital Health Providers
- 10.9 Ambulatory Surgical Centers

11 GLOBAL HEALTHCARE CYBERSECURITY MARKET, BY GEOGRAPHY

- 11.1 North America
 - 11.1.1 United States
 - 11.1.2 Canada
 - 11.1.3 Mexico
- 11.2 Europe

- 11.2.1 United Kingdom
- 11.2.2 Germany
- 11.2.3 France
- 11.2.4 Italy
- 11.2.5 Spain
- 11.2.6 Netherlands
- 11.2.7 Belgium
- 11.2.8 Sweden
- 11.2.9 Switzerland
- 11.2.10 Poland
- 11.2.11 Rest of Europe
- 11.3 Asia Pacific
 - 11.3.1 China
 - 11.3.2 Japan
 - 11.3.3 India
 - 11.3.4 South Korea
 - 11.3.5 Australia
 - 11.3.6 Indonesia
 - 11.3.7 Thailand
 - 11.3.8 Malaysia
 - 11.3.9 Singapore
 - 11.3.10 Vietnam
 - 11.3.11 Rest of Asia Pacific
- 11.4 South America
 - 11.4.1 Brazil
 - 11.4.2 Argentina
 - 11.4.3 Colombia
 - 11.4.4 Chile
 - 11.4.5 Peru
 - 11.4.6 Rest of South America
- 11.5 Rest of the World (RoW)
 - 11.5.1 Middle East
 - 11.5.1.1 Saudi Arabia
 - 11.5.1.2 United Arab Emirates
 - 11.5.1.3 Qatar
 - 11.5.1.4 Israel
 - 11.5.1.5 Rest of Middle East
 - 11.5.2 Africa
 - 11.5.2.1 South Africa

11.5.2.2 Egypt

11.5.2.3 Morocco

11.5.2.4 Rest of Africa

12 STRATEGIC MARKET INTELLIGENCE

12.1 Industry Value Network and Supply Chain Assessment

12.2 White-Space and Opportunity Mapping

12.3 Product Evolution and Market Life Cycle Analysis

12.4 Channel, Distributor, and Go-to-Market Assessment

13 INDUSTRY DEVELOPMENTS AND STRATEGIC INITIATIVES

13.1 Mergers and Acquisitions

13.2 Partnerships, Alliances, and Joint Ventures

13.3 New Product Launches and Certifications

13.4 Capacity Expansion and Investments

13.5 Other Strategic Initiatives

14 COMPANY PROFILES

14.1 IBM Corporation

14.2 Cisco Systems, Inc.

14.3 Palo Alto Networks

14.4 Fortinet, Inc.

14.5 CrowdStrike Holdings, Inc.

14.6 Check Point Software Technologies Ltd.

14.7 Trend Micro Incorporated

14.8 Broadcom Inc.

14.9 CyberArk Software Ltd.

14.10 Claroty Ltd.

14.11 Armis, Inc.

14.12 McAfee, LLC

14.13 Kaspersky Lab

14.14 Imperva, Inc.

14.15 Symantec Corporation

List Of Tables

LIST OF TABLES

Table 1 Global Healthcare Cybersecurity Market Outlook, By Region (2023-2034) (\$MN)

Table 2 Global Healthcare Cybersecurity Market Outlook, By Component (2023-2034) (\$MN)

Table 3 Global Healthcare Cybersecurity Market Outlook, By Solutions (2023-2034) (\$MN)

Table 4 Global Healthcare Cybersecurity Market Outlook, By Identity & Access Management (IAM) (2023-2034) (\$MN)

Table 5 Global Healthcare Cybersecurity Market Outlook, By Antivirus & Antimalware (2023-2034) (\$MN)

Table 6 Global Healthcare Cybersecurity Market Outlook, By Encryption & Tokenization (2023-2034) (\$MN)

Table 7 Global Healthcare Cybersecurity Market Outlook, By Firewall (2023-2034) (\$MN)

Table 8 Global Healthcare Cybersecurity Market Outlook, By Security Information & Event Management (SIEM) (2023-2034) (\$MN)

Table 9 Global Healthcare Cybersecurity Market Outlook, By Intrusion Detection & Prevention Systems (IDS/IPS) (2023-2034) (\$MN)

Table 10 Global Healthcare Cybersecurity Market Outlook, By Data Loss Prevention (DLP) (2023-2034) (\$MN)

Table 11 Global Healthcare Cybersecurity Market Outlook, By Risk & Compliance Management (2023-2034) (\$MN)

Table 12 Global Healthcare Cybersecurity Market Outlook, By Services (2023-2034) (\$MN)

Table 13 Global Healthcare Cybersecurity Market Outlook, By Professional Services (2023-2034) (\$MN)

Table 14 Global Healthcare Cybersecurity Market Outlook, By Managed Security Services (2023-2034) (\$MN)

Table 15 Global Healthcare Cybersecurity Market Outlook, By Consulting Services (2023-2034) (\$MN)

Table 16 Global Healthcare Cybersecurity Market Outlook, By Training & Support Services (2023-2034) (\$MN)

Table 17 Global Healthcare Cybersecurity Market Outlook, By Threat Type (2023-2034) (\$MN)

Table 18 Global Healthcare Cybersecurity Market Outlook, By Malware (2023-2034)

(\$MN)

Table 19 Global Healthcare Cybersecurity Market Outlook, By Ransomware
(2023-2034) (\$MN)

Table 20 Global Healthcare Cybersecurity Market Outlook, By Phishing & Social
Engineering (2023-2034) (\$MN)

Table 21 Global Healthcare Cybersecurity Market Outlook, By Distributed Denial of
Service (DDoS) (2023-2034) (\$MN)

Table 22 Global Healthcare Cybersecurity Market Outlook, By Advanced Persistent
Threats (APT) (2023-2034) (\$MN)

Table 23 Global Healthcare Cybersecurity Market Outlook, By Spyware (2023-2034)
(\$MN)

Table 24 Global Healthcare Cybersecurity Market Outlook, By Insider Threats
(2023-2034) (\$MN)

Table 25 Global Healthcare Cybersecurity Market Outlook, By Lost or Stolen Devices
(2023-2034) (\$MN)

Table 26 Global Healthcare Cybersecurity Market Outlook, By Deployment Mode
(2023-2034) (\$MN)

Table 27 Global Healthcare Cybersecurity Market Outlook, By On-Premises
(2023-2034) (\$MN)

Table 28 Global Healthcare Cybersecurity Market Outlook, By Cloud-Based
(2023-2034) (\$MN)

Table 29 Global Healthcare Cybersecurity Market Outlook, By Hybrid (2023-2034)
(\$MN)

Table 30 Global Healthcare Cybersecurity Market Outlook, By Security Type
(2023-2034) (\$MN)

Table 31 Global Healthcare Cybersecurity Market Outlook, By Network Security
(2023-2034) (\$MN)

Table 32 Global Healthcare Cybersecurity Market Outlook, By Endpoint Security
(2023-2034) (\$MN)

Table 33 Global Healthcare Cybersecurity Market Outlook, By Cloud Security
(2023-2034) (\$MN)

Table 34 Global Healthcare Cybersecurity Market Outlook, By Application Security
(2023-2034) (\$MN)

Table 35 Global Healthcare Cybersecurity Market Outlook, By IoT & Medical Device
Security (2023-2034) (\$MN)

Table 36 Global Healthcare Cybersecurity Market Outlook, By Database Security
(2023-2034) (\$MN)

Table 37 Global Healthcare Cybersecurity Market Outlook, By Application (2023-2034)
(\$MN)

Table 38 Global Healthcare Cybersecurity Market Outlook, By Electronic Health Records (EHR) Protection (2023-2034) (\$MN)

Table 39 Global Healthcare Cybersecurity Market Outlook, By Medical Device Security (2023-2034) (\$MN)

Table 40 Global Healthcare Cybersecurity Market Outlook, By Telemedicine Security (2023-2034) (\$MN)

Table 41 Global Healthcare Cybersecurity Market Outlook, By Health Information Exchange Security (2023-2034) (\$MN)

Table 42 Global Healthcare Cybersecurity Market Outlook, By Pharmacy Information Systems Security (2023-2034) (\$MN)

Table 43 Global Healthcare Cybersecurity Market Outlook, By Remote Patient Monitoring Security (2023-2034) (\$MN)

Table 44 Global Healthcare Cybersecurity Market Outlook, By Claims & Billing Fraud Prevention (2023-2034) (\$MN)

Table 45 Global Healthcare Cybersecurity Market Outlook, By Cloud Data Protection (2023-2034) (\$MN)

Table 46 Global Healthcare Cybersecurity Market Outlook, By Other Applications (2023-2034) (\$MN)

Table 47 Global Healthcare Cybersecurity Market Outlook, By End User (2023-2034) (\$MN)

Table 48 Global Healthcare Cybersecurity Market Outlook, By Hospitals & Clinics (2023-2034) (\$MN)

Table 49 Global Healthcare Cybersecurity Market Outlook, By Pharmaceutical & Biotechnology Companies (2023-2034) (\$MN)

Table 50 Global Healthcare Cybersecurity Market Outlook, By Health Insurance Providers/Payers (2023-2034) (\$MN)

Table 51 Global Healthcare Cybersecurity Market Outlook, By Medical Device Manufacturers (2023-2034) (\$MN)

Table 52 Global Healthcare Cybersecurity Market Outlook, By Clinical Laboratories (2023-2034) (\$MN)

Table 53 Global Healthcare Cybersecurity Market Outlook, By Government Healthcare Agencies (2023-2034) (\$MN)

Table 54 Global Healthcare Cybersecurity Market Outlook, By Research Institutions (2023-2034) (\$MN)

Table 55 Global Healthcare Cybersecurity Market Outlook, By Telehealth & Digital Health Providers (2023-2034) (\$MN)

Table 56 Global Healthcare Cybersecurity Market Outlook, By Ambulatory Surgical Centers (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.

I would like to order

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

Product link: <https://marketpublishers.com/r/HD5DBE71B24FEN.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/HD5DBE71B24FEN.html>