+357 96 030922
info@marketpublishers.com

Healthcare Cyber Security Market Size, Share, Trends and Forecast by Type of Threat, Type of Solution, End User, and Region, 2026-2034

https://marketpublishers.com/r/H9D4309AC955EN.html
Date: April 2026
Pages: 143
Price: US$ 3,999.00 (Single User License)
ID: H9D4309AC955EN

Abstracts

The global healthcare cyber security market size was valued at USD 22.5 Billion in 2025. Looking forward, it is estimated that the market to reach USD 71.5 Billion by 2034, exhibiting a CAGR of 13.27% during 2026-2034. North America currently dominates the market, holding a significant market share of over 38.9% in 2025. The rising prevalence and sophistication of cyber threats, the expanding use of electronic health records (EHRs) and telemedicine services, along with the increasing recognition of the harm caused by data breaches and cyber-attacks, are among the major factors propelling the market in this area.

Healthcare cyber security involves ensuring that electronic medical records, healthcare devices, and the data of patients remain free from unauthorized access, theft, or alteration. Several technologies, policies, and practices will be involved, making certain that sensitive health care information remains confidential and safe with integrity and availability in their aspects. It works based on some security controls installed within computer systems to prevent possible cyber- attacks and data breach. It helps in protecting the data of the patient, keeps medical devices from hacking, and ensures the compliance with all regulatory requirements. The benefits of healthcare cyber security are increased patient privacy, lesser identity theft, and frauds, and trust in the healthcare system.

Increasing complexity and frequency of threats targeting healthcare organizations represent one of the key drivers providing considerable thrust to the market. With digitization of medical records as well as interconnection of healthcare systems, the requirement for protection of highly sensitive patient data has significantly increased, which also boosts market growth. Also, increasing the usage of electronic health

+357 96 030922
info@marketpublishers.com

records and telemedicine services coupled with strict regulatory requirements and data protection laws imposed by governments and other regulatory authorities are contributing to a bright prospect of the market. Increasingly healthcare organizations are now aware of potential damage both to their reputation and finances due to data breaches and cyber-attacks are helping propel growth in this market. Apart from that, the fast growth of technologies such as integration of Internet of Things devices into the health care infrastructure and need for security over the critical medical devices such as pacemakers and insulin pumps are accelerating the growth in this market. The increasing adoption of artificial intelligence (AI) and machine learning (ML) technologies in cybersecurity solutions, as well as the ever-increasing number of partnerships and collaborations between healthcare organizations and cybersecurity firms, are driving the market. Healthcare expenditure is also growing, and the recent outbreak of COVID-19 and the increase in the adoption of digital healthcare technologies are boosting the global healthcare cyber security market growth.

An increase in the frequency and sophistication of cyberattacks targeting healthcare organizations handling critical patient information and vital infrastructure has propelled this global healthcare cybersecurity industry. A higher utilization of telemedicine, IoMT devices, and EHRs escalates the attack surface. Such situations demand robust cyber strategies. Organizations need to invest in robust security measures for compliance and to avoid costly fines under the General Data Protection Regulation in Europe and the Health Insurance Portability and Accountability Act in the United States. Healthcare organizations are also compelled to place a focus on cybersecurity given the increasing monetary and reputational damage wrought by breaches.

The United States has emerged as a market disruptor, motivated by the continuous rise in cyber threats concerning critical healthcare information and key systems. The uptake of EHRs, telehealth services, and connected devices has significantly expanded the attack surface, heightening demands for improved security measures. The HIPAA standards have made it mandatory to ensure data protection, and such a requirement has compelled the healthcare providers to invest more in cybersecurity initiatives. The growing cases of ransomware attacks and data breaches have identified areas of weakness, hence there is increased investment and emphasis on the strength of cybersecurity infrastructure.

HEALTHCARE CYBER SECURITY MARKET TRENDS:

Rising cyberattacks and data breaches

+357 96 030922
info@marketpublishers.com

The global healthcare cybersecurity market has significant growth drivers with the increase in cyberattacks and data breaches. Healthcare organizations have started adopting digital technologies such as electronic health records, telemedicine, and connected medical devices at a significant rate, making them more vulnerable to cybercriminals. According to Health Insurance Portability and Accountability Act (HIPAA), between 2009 and 2023, 5,887 healthcare data breaches involving more than 500 records were reported and compromised over 519 million healthcare records. These breaches often involved sensitive patient data, hence making the healthcare institutions the most attractive targets for ransomware attacks and theft of data. The increased frequency and sophistication of these attacks thus make this a pressing need for advanced cybersecurity solutions. Thus, healthcare organizations have been spending lavishly on cybersecurity measures to protect patient data, adhere to regulatory requirements, and maintain continuity of operations. This increasingly hostile environment for threat is what fuels the demand for strong cybersecurity technologies and services across the health sector.

Increasing utilization of electronic health records (EHRs) and telemedicine

The adoption of EHRs and growth in telemedicine services are the major drivers of the global healthcare cybersecurity market. According to the American Hospital Association, as of 2021, nearly 4 in 5 office-based physicians (78%) and nearly all non-federal acute care hospitals (96%) had adopted a certified EHR. This massive digitalization has brought in a significant improvement in healthcare efficiency though increases the volume of sensitive health data that is stored and transmitted electronically. Moreover, the global telemedicine market was USD 83.5 Billion in 2022, as per an industry report and will expand rapidly in the coming years based on increased adoption, especially after the pandemic. This increasing number of digital healthcare services does come with an increased vulnerability for cyberthieves to exploit. And so, healthcare institutions heavily invest in advanced security against cyber threats, such as intrusion detection systems, multi-factor authentication, and encryption solutions, to prevent breach incidences, hacking, etc. This increased threat posed a significant rise in demands for strong cybersecurity measures that provide protection for sensitive patient data.

Regulatory compliance and data privacy laws

Governments worldwide are strengthening data protection regulations, which is driving the healthcare cybersecurity market growth considerably. Two instances are the European Union's General Data Protection Regulation and the U.S. Health Insurance Portability and Accountability Act, which enforce strict security protocols on healthcare

+357 96 030922
info@marketpublishers.com

providers. The GDPR was enforced since May 2018, which mandates data privacy and security with stringent measures. Failure to comply would result in penalties up to Euro 20 Million (USD 21 Million) or 4% of the annual global turnover. In the U.S., civil monetary penalties for HIPAA violations are based on the offense level, ranging from USD 141 to USD 2.13 Million per violation. These regulations have forced healthcare organizations to deploy sophisticated cybersecurity technologies to be in compliance with the regulations, to protect the privacy of their patients, and avoid hefty fines. This is further fueling the demand for strong cybersecurity solutions, such as encryption, secure communication, and access controls, hence propelling market growth.

HEALTHCARE CYBER SECURITY INDUSTRY SEGMENTATION:

IMARC Group provides an analysis of the key trends in each sub-segment of the global healthcare cyber security market report, along with forecasts at the global, regional and country levels from 2026-2034. Our report has categorized the market based on type of threat, type of solution and end user.

Analysis by Type of Threat:

- Malware
- Distributed Denial of Service (DDoS)
- Advanced Persistent Threats (APT)
- Spyware
- Others

Malware leads the market with around 25.9% of healthcare cyber security market share in 2025, on account of its adaptability and prevalent use in cyberattacks. Healthcare institutions are key targets for malware, such as ransomware, spyware, and trojans, since they manage large volumes of sensitive patient information and essential systems. Ransomware, specifically, is extremely common, frequently disrupting operations and compelling organizations to pay large amounts to restore access. The interlinked structure of contemporary healthcare systems, encompassing Internet of Medical Things (IoMT) devices and electronic health records (EHRs), heightens susceptibility to malware. Its capacity to take advantage of human and system

+357 96 030922
info@marketpublishers.com

weaknesses renders malware a leading threat category.

Analysis by Type of Solution:

- Identity and Access Management
- Risk and Compliance Management
- Antivirus and Antimalware
- DDoS Mitigation
- Security Information and Event Management
- Intrusion Detection System and Intrusion Prevention System
- Others

Antivirus and antimalware lead the market with around 22.9% of market share in 2025, as they are crucial in safeguarding healthcare systems from various cyber threats, such as viruses, worms, ransomware, and spyware. These remedies are essential for protecting endpoints, which rank as some of the most susceptible elements within healthcare networks. As the use of connected devices and electronic health records (EHRs) grows, the likelihood of malware attacks has escalated considerably, prompting higher demand for these solutions. Furthermore, antivirus and antimalware solutions are economical, commonly used, and consistently updated to tackle emerging threats, rendering them essential for thorough healthcare cybersecurity plans.

Analysis by End User:

- Hospitals
- Pharmaceutical Companies
- Medical Device Companies
- Health Insurance Companies

+357 96 030922
info@marketpublishers.com

Others

Hospitals lead the market with around 63.7% of market share in 2025, on account of their heavy dependence on digital systems and the significant volume of confidential patient information they manage. Hospitals, serving as primary healthcare providers, utilize electronic health records (EHRs), linked medical devices, and telehealth services, which makes them key targets for cyberattacks. The essential role of hospital functions and patient treatment heightens the risk and possible consequences of data breaches or ransomware incidents, requiring substantial investment in cybersecurity. Additionally, compliance with regulations such as HIPAA compels hospitals to implement enhanced cybersecurity strategies to safeguard their systems.

Regional Analysis:

North America

United States

Canada

Europe

Germany

France

United Kingdom

Italy

Spain

Russia

Others

Asia Pacific

+357 96 030922
info@marketpublishers.com

China

Japan

India

South Korea

Australia

Indonesia

Others

Latin America

Brazil

Mexico

Others

Middle East and Africa

In 2025, North America accounted for the largest market share of over 38.9%. The market is propelled by its sophisticated health care infrastructure, widespread digital technology adoption, and regulatory compliance requirements such as HIPAA. Cyberattacks occur more frequently in this region, hence investment in advanced cybersecurity solutions is increased. Widespread usage of EHRs, telemedicine, and networked medical devices add a significant need for effective security. North America also boasts key market players, government initiatives in strengthening cybersecurity, and growing awareness among healthcare organizations, leading to dominance. Its mature technology ecosystem, innovation focus, and all of these contribute to its dominance.

KEY REGIONAL TAKEAWAYS:

UNITED STATES HEALTHCARE CYBER SECURITY MARKET ANALYSIS:

+357 96 030922
info@marketpublishers.com

In 2025, the United States accounts for over 82.80% of the healthcare cyber security market in North America. The United States healthcare cybersecurity market will grow significantly with the increasing cyberattacks on the healthcare sector. The American Hospital Association (AHA) has reported 386 healthcare cyberattacks in 2024, and it is reported that data theft crimes and ransomware attacks are at the same elevated rate as 2023, which had been the worst year ever recorded for healthcare breaches. These attacks undermine the integrity and security of sensitive patient information, besides disrupting crucial healthcare functions and those of other vital third-party service providers whose mission-critical services could be compromised.

The department of HHS, on account of increasing attacks, has developed voluntary Cybersecurity Performance Goals in cooperation with the HPH sector. It intends to promote strong effects cybersecurity practice within health organizations while also enhancing the former's capacity for preparation against cyber risk as well as mitigation of that cyber risk. In partnership with the growing urgency toward good digital defenses, this level of regulatory and collaborative impetus is driving increased investment into advanced cybersecurity solutions, increasing the growth of the market for healthcare cybersecurity in the U.S.

EUROPE HEALTHCARE CYBER SECURITY MARKET ANALYSIS

The Europe healthcare cybersecurity market is experiencing significant growth due to increased instances of cyberattacks targeting healthcare organizations. According to European Union Agency for Cybersecurity (ENISA) analysis, 54% of the reported cyber incidents in the healthcare sector involved ransomware, and 46% were related to breaches of patient data. These threats compromise the safety of patients, undermine data integrity, and disrupt the continuity of operation of essential health care services, making it a high priority for healthcare providers.

The rise in cyberattacks coincides with the rapid digitization of healthcare across Europe, where electronic health records (EHRs), telemedicine platforms, and connected medical devices are being widely adopted. Additionally, regulatory frameworks such as the General Data Protection Regulation (GDPR) and the NIS2 Directive impose stringent data protection and cybersecurity standards, compelling healthcare organizations to implement advanced security measures. The growing concern over safeguarding sensitive patient information, combined with increased government investments in digital health programs, is driving the demand for innovative cybersecurity solutions. This collective push to protect healthcare infrastructure and

+357 96 030922
info@marketpublishers.com

ensure compliance with regulatory requirements is propelling the growth of the healthcare cybersecurity market in Europe.

ASIA PACIFIC HEALTHCARE CYBER SECURITY MARKET ANALYSIS

The Asia-Pacific region is reporting huge growth in the healthcare cybersecurity market in view of an alarming cyberattack trend against the healthcare segment. According to research paper published in 2023 by The HIPAA Journal, in the year, 725 hacking incidents involved the leakage of more than 124 million health records worldwide that were reported as the worst on record against the cybersecurity sector in healthcare. Access to 69% of the compromised data was performed via network servers and indicates breaches in digitalized healthcare solutions.

As the Asia-Pacific region accelerates its digitization of healthcare infrastructure through the use of EHRs, telemedicine, and IoT-enabled medical devices, it has expanded the attack surface for cybercriminals. Therefore, there is a growing need for robust cybersecurity solutions to protect sensitive patient data, prevent ransomware attacks, and ensure operational continuity. Governments in the region are implementing strict data protection legislations, such as India's Digital Personal Data Protection Act and China's Cybersecurity Law, thereby fuelling investments in advanced cybersecurity technologies, which is a key growth driver for the market.

LATIN AMERICA HEALTHCARE CYBER SECURITY MARKET ANALYSIS

The Latin America healthcare cybersecurity market is growing rapidly since cyberattacks are becoming highly frequent and impactful on the regional healthcare systems. According to an industrial report, in Brazil, the average cost of a cyberattack increased by 10.5% between the years 2019 to 2020, proving that the financial burden against organizations is increasing. For instance, 80 percent of compromised data in these breaches have personal information, which makes them vulnerable in the healthcare sector. It is very alarming that in Latin America, the detection of a data breach takes 329 days on average, which is one of the highest detection times globally, making it even worse in relation to patient safety and integrity.

The region has suffered several high-profile cases: sensitive data leaks in Mexico, Chile, and Argentina, among others, which point to the need for strengthening cybersecurity solutions. This growing threat landscape, coupled with greater adoption of digital technologies within the healthcare system, propels demand for advanced cybersecurity solutions protecting sensitive patient information while assuring continuity

+357 96 030922
info@marketpublishers.com

of operations. These factors make cybersecurity one of the most vital drivers of growth in Latin American healthcare.

MIDDLE EAST AND AFRICA HEALTHCARE CYBER SECURITY MARKET ANALYSIS

The Middle East and Africa (MEA) cybersecurity market is growing at a high rate, primarily due to the increasing rate and severity of cyberattacks, especially in the healthcare sector. In 2023, the number of healthcare cybersecurity incidents worldwide skyrocketed to 550 breaches that compromised the protected health information (PHI) of 108 million individuals, which is a significant increase from previous years. This drastic increase, particularly in ransomware-attacks, that have hiked by almost 300 percent in the recent past speaks volumes about how vulnerable regional healthcare organizations have become.

The MEA region is becoming a prime target for cybercriminals with the healthcare sector's increasing digitalization and reliance on electronic health records (EHRs). High-profile incidents in Saudi Arabia, UAE, and South Africa further underscore the region's cybersecurity challenges. Governments are responding to these challenges by implementing stronger regulatory frameworks, such as the UAE's National Cybersecurity Strategy and South Africa's POPIA, thereby driving demand for advanced cybersecurity solutions to protect sensitive data and maintain operational continuity.

COMPETITIVE LANDSCAPE:

Major players in the healthcare cybersecurity sector are implementing diverse strategies to promote growth and tackle emerging threats. They are significantly investing in research and development (R&D) to develop cutting-edge solutions, such as AI-driven threat detection systems and machine learning algorithms for real-time observation. Collaborations and partnerships represent a typical strategy, as players collaborate with healthcare providers, tech companies, and governments to improve security systems. Cloud security measures are a key focus since the use of cloud computing is increasing in healthcare. Businesses are also broadening their portfolios to provide cohesive cybersecurity solutions that tackle network, endpoint, and data protection.

The report provides a comprehensive analysis of the competitive landscape in the healthcare cyber security market with detailed profiles of all major companies, including:

AO Kaspersky Lab

+357 96 030922
info@marketpublishers.com

Check Point Software Technologies Ltd.

Cisco Systems, Inc.

Claroty

CrowdStrike

CyberArk Software Ltd.

Cynerio (Axonius)

Forcepoint

Forescout Technologies Inc.

International Business Machines Corporation

Palo Alto Networks

Trellix

Trend Micro Incorporated

KEY QUESTIONS ANSWERED IN THIS REPORT

1. What is healthcare cyber security?
2. How big is the healthcare cyber security market?
3. What is the expected growth rate of the global healthcare cyber security market during 2026-2034?
4. What are the key factors driving the global healthcare cyber security market?
5. What is the leading segment of the global healthcare cyber security market based on the type of threat?
6. What is the leading segment of the global healthcare cyber security market based on type of solution?
7. What is the leading segment of the global healthcare cyber security market based on end user?
8. What are the key regions in the global healthcare cyber security market?
9. Who are the key players/companies in the global healthcare cyber security market?

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

7 MARKET BREAKUP BY TYPE OF SOLUTION

8 MARKET BREAKUP BY END USER

+357 96 030922
info@marketpublishers.com

9 MARKET BREAKUP BY REGION

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+357 96 030922
info@marketpublishers.com

List Of Figures

LIST OF FIGURES

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Healthcare Cyber Security Market Size, Share, Trends and Forecast by Type of Threat, Type of Solution, End User, and Region, 2026-2034

Product link: https://marketpublishers.com/r/H9D4309AC955EN.html

Price: US$ 3,999.00 (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/H9D4309AC955EN.html