

Healthcare Cybersecurity Market Surges as Global Health Systems Brace for Digital Threats | DataM Intelligence

Healthcare cybersecurity market is expected to reach a value of approximately US\$ 82.9 billion by 2033, which is equivalent to an 18.5% CAGR between 2025-2033

AUSTIN, TX, UNITED STATES, June 2, 2025 /EINPresswire.com/ -- The global [healthcare cybersecurity industry](#) is experiencing accelerated growth as a result of the increasing number of cyber threats and the stringent regulatory requirements. The market is expected to reach a value of approximately US\$ 82.9 billion by 2033, which is equivalent to an 18.5% compound annual growth rate (CAGR) between 2025 and 2033, as per projections.



Market Overview

There have been approximately 400 documented instances of cyberattacks in the United States alone over the past year, and healthcare businesses worldwide are becoming increasingly susceptible to these attacks. These breaches have resulted in substantial financial losses, interrupted services, and compromised sensitive patient information. The average cost of a severe cyberattack on a healthcare provider is estimated to be \$4.7 million.

Get Detailed Premium Sample PDF: <https://www.datamintelligence.com/download-sample/healthcare-cybersecurity-market>

Healthcare providers are responding by investing in sophisticated cybersecurity solutions, including secure cloud infrastructures, endpoint protection, and intrusion detection systems. The detection and response capabilities of peril are enhanced by the integration of AI and machine learning technology.

Regional Outlook

North America

By 2024, North America will account for over 43.9% of global revenue in the healthcare cybersecurity sector. Effective regulatory measures, a robust healthcare infrastructure, and a high incidence of cybercrime all contribute to the region's expansion. The US government's proposed updates to the Health Insurance Portability and Accountability Act (HIPAA) include mandatory multifactor authentication, data encryption, and regular security audits, all of which are intended to enhance the security of sensitive healthcare data.

Asia-Pacific

The Asia-Pacific region is currently experiencing a significant increase in healthcare cybersecurity due to the increased use of electronic health records (EHRs), telemedicine services, and cyber threat awareness. In 2024, the healthcare cybersecurity industry in Japan is anticipated to grow from \$1.8 billion to \$6.1 billion by 2033, with a compound annual growth rate (CAGR) of 20.4% between 2025 and 2033. Major drivers of this expansion are government initiatives and investments in digital health infrastructure.

Industry Developments

The healthcare cybersecurity landscape is marked by strategic partnerships and mergers aimed at enhancing security capabilities.

- Palo Alto Networks and Accenture Partnership: In early 2025, Palo Alto Networks and Accenture announced a partnership to enhance the cyber resilience of healthcare businesses, with a particular focus on advanced threat detection and response strategies.
- Datadog's Expansion: Datadog, a cybersecurity company based in the United States, has pledged to establish local data center capacity in Australia in order to comply with stringent data sovereignty regulations. This action is indicative of a broader trend toward regional data protection measures.

Latest News from USA

In 2025, the healthcare industry in the United States experienced a substantial increase in intrusions, which resulted in the implementation of new government regulations and increased cybersecurity expenditures. Healthcare providers are now required to implement more stringent data protection measures, including encryption, multi-factor authentication, and frequent security assessments, as a result of the Department of Health and Human Services (HHS)'s proposal to amend HIPAA regulations. The purpose of these measures is to enhance the security of patient data in the wake of three significant intrusions, one of which directly impacted the information of over one million patients.

The market is expected to advance as hospitals and clinics invest in advanced security solutions, including AI-powered threat detection and secure cloud systems, as a result of the increased emphasis on cybersecurity. It is anticipated that the new restrictions will result in a rise in demand for cybersecurity products and services, which presents new opportunities for technology companies. Although these criteria may be challenging to meet, particularly for smaller firms, they will ultimately strengthen the industry's digital defenses and stimulate robust growth in the healthcare cybersecurity market.

Latest News from Japan

The healthcare cybersecurity industry in Japan is anticipated to experience a remarkable 20.4% compound annual growth rate (CAGR) from over US\$1.3 billion in 2024 to approximately US\$6.1 billion by 2033. This growth is attributed to the increased use of electronic health records and telemedicine, as well as improved public-private collaborations that increase security awareness. The government announced new AI-friendly policies in early 2025, as well as planned updates to the Act on the Protection of Personal Information. These changes will facilitate the safe use of patient data for research and diagnostics. Additionally, the Active Cyberdefense Law now mandates that major hospitals report breaches promptly and provides authorities with additional tools to combat foreign cyberattacks. Collectively, these enhancements will motivate healthcare providers to allocate resources toward secure cloud platforms, multi-factor authentication, and real-time threat detection, which will accelerate the implementation of advanced cybersecurity solutions in Japan's healthcare sector, which is rapidly evolving.

Industry News:

Palo Alto Networks & Accenture (January 2025): Formed a strategic alliance to develop customized cybersecurity frameworks for healthcare institutions, blending AI-driven threat detection with incident response consulting.

Northrop Grumman Collaboration (June 2025): Entered into a public-private initiative with U.S. government health agencies to fortify digital defense systems in critical healthcare infrastructure.

CrowdStrike Holdings Acquisition (March 2024): Acquired Bionic, a security posture management firm, to enhance visibility across cloud-native healthcare applications and tighten defense mechanisms.

Broadcom's Integration of Symantec (ongoing through 2024): Continued to merge and optimize Symantec's cybersecurity services with a focus on endpoint protection and data loss prevention specifically for healthcare clients.

CloudWave & Sensato (Q4 2024): Jointly launched a comprehensive Managed Detection and Response (MDR) service tailored to small-to-mid-size hospitals in North America, addressing

staffing shortages in IT security.

Market Players: Checkpoint Software Technologies Inc., Intel Corporation, Juniper Networks Inc., Cloudwave Sensato Cybersecurity, Crowdstrike Holdings, Kaspersky Labs, Northrop Grumman, Palo Alto Networks, Broadcom, Sophos Ltd., among others.

Future Outlook

In order to safeguard sensitive patient data and ensure uninterrupted services, the healthcare industry must prioritize robust cybersecurity policies as cyber threats continue to escalate. A robust healthcare cybersecurity system necessitates investments in contemporary technology, regulatory compliance, and personnel training.

Gain expert insights on market trends, challenges, and future outlook. Buy the Full Report Now and strengthen your strategy with DataM Intelligence.

<https://www.datamintelligence.com/buy-now-page?report=healthcare-cybersecurity-market>

Stay informed with the latest industry insights-start your subscription now:

<https://www.datamintelligence.com/reports-subscription>

Related Reports:

[Medical Device Cybersecurity Solutions Market- CAGR of 8.5% by 2031](#)

[Healthcare Services market to exhibit a CAGR of 6.6 % by 2031](#)

Sai Kumar

DataM Intelligence 4market Research LLP

+1 877-441-4866

sai.k@datamintelligence.com

Visit us on social media:

[LinkedIn](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/818268837>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.