Healthcare Cyber Security Market Size Worth US$ 61.5 Billion by 2032 | CAGR: 15%: IMARC Group

In 2023, the global healthcare cybersecurity market was valued at US$ 17.1B. IMARC Group forecasts it to reach US$ 61.5B by 2032, with a 15% CAGR during 2024-32

SHERIDAN, WYOMING, UNITED STATES, February 3, 2024 /EINPresswire.com/ -- The latest report by IMARC Group, titled "[Healthcare Cyber Security Market](#) Report by Type of Threat (Malware, Distributed Denial of Service (DDoS), Advanced Persistent Threats (APT), Spyware, and Others), Type of

Healthcare Cyber Security

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, and Others), End User (Hospitals, Pharmaceutical Companies, Medical Device Companies, Health Insurance Companies, and Others), and Region 2024-2032", offers a comprehensive analysis of the industry, which comprises insights on the market. The global healthcare cyber security market size reached US$ 17.1 Billion in 2023. Looking forward, IMARC Group expects the market to reach US$ 61.5 Billion by 2032, exhibiting a growth rate (CAGR) of 15% during 2024-2032.

Factors Affecting the Growth of the Healthcare Cyber Security Industry:

• Rising Digitalization in Healthcare:

The healthcare industry's increasing digitalization is a significant factor propelling the growth of the cybersecurity sector. With the widespread adoption of electronic health records (EHRs), telemedicine, and IoT (Internet of Things) devices in healthcare, there is a heightened need for robust cybersecurity measures. This digital transformation, while enhancing efficiency and patient care, also opens numerous cyber vulnerabilities. The response of the industry has been to invest in advanced cybersecurity solutions to protect sensitive health data and ensure the

continuity of healthcare services, driving substantial growth in the healthcare cybersecurity market.

• Stringent Regulatory Compliance:

The stringent regulatory environment surrounding patient data protection acts as a catalyst for the healthcare cybersecurity growth of the industry. Regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the United States mandate strict standards for patient data confidentiality and security. This regulatory pressure compels healthcare organizations to adopt comprehensive cybersecurity solutions to comply with legal requirements, thus fueling the expansion of the industry. These regulations ensure the safety of patient information and standardize and elevate cybersecurity measures across the healthcare sector.

• Increasing Cyber Threats and Awareness:

The growth of the healthcare cybersecurity industry is also driven by the increasing awareness about cyber threats and their potential impact on healthcare operations. As cyberattacks become more sophisticated and frequent, healthcare organizations are recognizing the critical need to invest in cybersecurity. This awareness is about protecting data, and ensuring operational continuity and patient safety. As a result, there is a growing demand for advanced cybersecurity solutions, including threat intelligence, intrusion detection systems, and encryption technologies, further stimulating the growth and innovation of the industry.

For an in-depth analysis, you can request the sample copy of the report:
https://www.imarcgroup.com/healthcare-cyber-security-market/requestsample

Competitive Landscape:

The competitive landscape of the market has been studied in the report with the detailed profiles of the key players operating in the market.

• AO Kaspersky Lab
• Broadcom Inc.
• Cisco Systems Inc.
• Claroty Ltd.
• CyberMDX Technologies Inc. (Forescout Technologies Inc.)
• Cynerio Israel Ltd.
• FireEye, Inc. (Trellix)
• Forcepoint LLC
• International Business Machines Corporation
• McAfee LLC
• Palo Alto Networks Inc.

• Trend Micro Inc.

Healthcare Cyber Security Market Report Segmentation:

Type of Threat Insights:

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

Malware dominates the market due to its widespread and frequently evolving nature, posing a persistent and versatile threat to healthcare systems and data.

Type of Solution Insights:

• 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 accounts for the largest market share as they are fundamental and primary defense mechanisms against the most common and damaging forms of cyber threats in healthcare, providing essential protection for sensitive data and systems.

End User Insights:

• Hospitals
• Pharmaceutical Companies
• Medical Device Companies
• Health Insurance Companies
• Others

Hospitals emerged as the largest segment among end-users, as they are primary targets for cyberattacks due to their vast repositories of sensitive patient data and critical reliance on digital systems for patient care.

Regional Insights:

• North America
o United States

- o Canada
- • Asia-Pacific
- o China
- o Japan
- o India
- o South Korea
- o Australia
- o Indonesia
- o Others
- • Europe
- o Germany
- o France
- o United Kingdom
- o Italy
- o Spain
- o Russia
- o Others
- • Latin America
- o Brazil
- o Mexico
- o Others
- • Middle East and Africa

North America's dominance in the healthcare cyber security market is due to the region's advanced healthcare infrastructure, stringent regulatory requirements for data protection, and high awareness of cybersecurity risks, coupled with substantial investments in healthcare IT solutions.

Global Healthcare Cyber Security Market Trends:

The global healthcare cybersecurity market is rapidly expanding, driven by an increasing need to protect sensitive medical data and healthcare infrastructure from cyber threats. With the healthcare industry's growing reliance on digital technologies like electronic health records, telemedicine, and IoT devices, vulnerabilities to cyberattacks have risen significantly. This scenario has spurred demand for robust cybersecurity solutions. The trend toward integrating advanced technologies like artificial intelligence and blockchain for enhanced security is notable. Moreover, stringent regulatory requirements for data protection and privacy, especially with laws like HIPAA in the USA, are further propelling this market. Healthcare organizations are now prioritizing cybersecurity as a critical component of their operations to safeguard patient data and ensure uninterrupted medical services.

Ask Analyst for Customization:
https://www.imarcgroup.com/request?type=report&id=4989&flag=C

Note: If you need specific information that is not currently within the scope of the report, we will provide it to you as a part of the customization.

Browse other reports:

Industrial IoT market: https://www.imarcgroup.com/industrial-iot-market

Mobile and wireless backhaul market: https://www.imarcgroup.com/mobile-wireless-backhaul-market

Photovoltaic materials market: https://www.imarcgroup.com/photovoltaic-materials-market

Screenless display market: https://www.imarcgroup.com/screenless-display-market

Water cooler market: https://www.imarcgroup.com/water-cooler-market

Elena Anderson
IMARC Services Private Limited
+1 631-791-1145
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/685951140