+357 96 030922
info@marketpublishers.com

Global Cybersecurity Market Assessment, By Component [Hardware, Software, Services], By Security Type [Network Security, Cloud Security, Endpoint Security, Mobile Security, IoT Security], By Deployment [Cloud, On-Premises], By Solution [Identity & Access Management, Infrastructure Security, Governance Risk & Compliance, Data Security & Privacy Service Offering, Cloud Storage, Others], By Enterprise Size [Large Enterprise, Small and Medium Sized Enterprises (SME's)], By Industry Vertical [IT and Telecommunication, Automotive, Government, BFSI, Retail, Healthcare, Manufacturing, Others], By Region, Opportunities and Forecast, 2016-2030F

https://marketpublishers.com/r/GD31E1EE9C1BEN.html
Date: February 2025
Pages: 224
Price: US$ 4,500.00 (Single User License)
ID: GD31E1EE9C1BEN

Abstracts

Global Cybersecurity Market size was valued at USD 193.26 billion in 2022 which is expected to reach USD 478.85 billion in 2030 growing at 12.01% CAGR for the forecast period between 2023 and 2030. The global cybersecurity market is a rapidly growing and focuses on protecting computer systems, networks, and digital assets from unauthized access, attacks, and theft. Cybersecurity has become a critical concern for businesses, governments, and individuals as more sensitive information is being stored and shared online. The market for cybersecurity products and services includes a wide range of offerings such as antivirus and anti-malware software, firewalls, intrusion

+357 96 030922
info@marketpublishers.com

detection and prevention systems, encryption tools, and security information and event management (SIEM) solutions. It also encompasses managed security services, consulting, training, and other professional services.

The demand for cybersecurity solutions is being driven by the increasing frequency and sophistication of cyber-attacks, as well as the growing awareness among businesses and consumers of the risks posed by data breaches and other security incidents. In addition, regulatory requirements such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are also driving organizations to invest in cybersecurity measures to protect sensitive data.

Since data breaches remain a persistent threat to organizations which have their respective customer data stored onto the servers, the need for cybersecurity is stronger in today's scenario than ever. There had been many prominent cases reported in 2022 related to data breach and server hacking, for instance, in October 2022, 9.7 million Australian Citizen's information was stolen in Medibank data leak due to ransomware hack. Hence, data breaches like these had been compromising sensitive information, damaging reputations, and imposing substantial financial and legal consequences. Hence, to improve the cybersecurity throughout the globe, research and development is going on to provide the enhanced security for consumers data. Moreover, the need for cybersecurity among companies and government organizing to protect sensitive data is driving the market growth.

Growing Technological Advancement

Artificial Intelligence (AI) and Machine Learning (ML) have become essential components of the global cybersecurity market, providing advanced and automated solutions for identifying and preventing cyber-attacks. AI and ML algorithms can analyze vast amounts of data from multiple sources to detect potential security threats, respond to incidents more quickly and effectively, detect fraudulent activities, and manage vulnerabilities. They can also automate routine security tasks, allowing security professionals to focus on more strategic activities. As the threat landscape continues to evolve, AI and ML are expected to play an increasingly important role in helping organizations stay ahead of cyber threats and protect their data and infrastructure more effectively. Therefore, this trend is expected to create positive shift in the demand for cybersecurity, thereby fuelling the market growth in the coming years.

For example, in 2023, the IBM launched Safety QRadar Suite, which was created with the needs of hybrid clouds in mind. It has a single, updated user interface for all

+357 96 030922
info@marketpublishers.com

products that is integrated with cutting-edge AI and automation to enable analysts to work more quickly, effectively, and precisely across their main toolkits.

Rise in Cloud-Based Security Solutions

Cloud-based security solutions have become increasingly popular in the global cybersecurity market, providing organizations with flexible and scalable solutions for protecting their data and infrastructure. Cloud Access Security Broker (CASB), Cloud Identity and Access Management (IAM), Cloud Security Information and Event Management (SIEM), Cloud Data Loss Prevention (DLP), Cloud Encryption, and Cloud Firewall are some of the top cloud-based security solutions that can help organizations secure their cloud environments. These solutions provide visibility and control over cloud applications used by employees, centralize control over user access to cloud resources, monitor and analyze security events across an organization's cloud infrastructure, prevent sensitive data from being leaked or stolen in cloud environments, protect data in transit and at rest, and protect cloud infrastructure from external threats. Overall, cloud-based security solutions are expected to play a crucial role in helping organizations meet the security challenges of the rapidly changing threat landscape.

BFSI Segment Growing at the Fastest Pace

Adequate cybersecurity measures are now essential given the financial sector's fast digitalization and growing dependence on technology. Cyberattacks on financial institutions, such as ransomware attacks, data breaches and server hacking are a persistent concern. As a result, these institutions are making significant investments in cutting-edge cybersecurity solutions to protect their sensitive data, preserve consumer information, and guarantee continuous operations. Additionally, the BFSI sector demands comprehensive cybersecurity solutions that encompass network security, data protection, identity and access management, and threat intelligence. As a result, the global cybersecurity market is witnessing significant growth, driven by the increasing cybersecurity spending by the BFSI sector to stay ahead of evolving cyber threats and maintain customer trust.

For example, in 2023, IBM has launched Trusteer, a comprehensive fraud protection platform specifically designed for the BFSI sector. Trusteer combines advanced analytics, machine learning, and behavioural biometrics to detect and prevent fraudulent activities such as account takeover, phishing, and malware-based attacks.

The Identity and Access Management Segment Strengthens the Market

+357 96 030922
info@marketpublishers.com

The growth of digital products and the increasing complexity of IT infrastructures, organisations are recognising the critical need of effectively controlling user identities and limiting the usage of sensitive resources. IAM solutions offer strong capabilities for authorization, verification, and identity lifecycle management, assisting organisations in making sure that only authorised users have access to the appropriate data at the appropriate time. Moreover, IAM solutions play a vital role in addressing compliance requirements and mitigating the risks associated with insider threats and unauthorised access. As a result, the demand for IAM solutions is growing significantly, driving the overall growth of the global cybersecurity market as organisations prioritise identity and access management to enhance their security posture and protect valuable assets.

Government Regulations

Government regulations are playing a crucial role in global cybersecurity. They aim to establish standards and frameworks that organizations must follow to ensure the protection of sensitive data and mitigate cyber threats. These regulations often include requirements for data privacy, breach notification, secure infrastructure, and industry-specific compliance. By enforcing such regulations, governments contribute to raising the overall cybersecurity posture, fostering trust, and minimizing the impact of cyber incidents on individuals, businesses, and national security. For instance, California Consumer Privacy Act (CCPA) - in June 2018, the CCPA was passed within the state of California with the intention of enhancing people' rights to privacy and data protection. It gives people more power over their personal knowledge and requires corporations to have security measures in place. Hence owing to these measures taken by government, the market witnessed up-surge in the market for cybersecurity.

Impact of COVID-19

The COVID-19 pandemic has had a significant impact on the global cybersecurity market. As businesses and individuals have increasingly moved online to work, learn, and communicate, the need for cybersecurity solutions has grown. However, the pandemic has also created new challenges and risks that have affected the cybersecurity market in various ways. One impact of the pandemic has been an increase in cyber threats and attacks. With more people working remotely and using digital tools and platforms, cyber criminals have found new opportunities to exploit vulnerabilities in digital systems. Another impact of the pandemic has been a shift in the cybersecurity market towards cloud-based solutions.

+357 96 030922
info@marketpublishers.com

For example, Palo Alto Networks has introduced new features and updates to their cybersecurity offerings to address the increased cyber risks during the pandemic. They have emphasized the importance of securing remote workforces and have enhanced their threat intelligence capabilities to detect and respond to COVID-19-themed phishing attacks and other pandemic-related threats.

Impact of Russia-Ukraine War on Global Cybersecurity Market

The conflict has led to a rise in state-sponsored cyber-attacks, as both Russia and Ukraine have been accused of carrying out cyber espionage and sabotage against each other. These attacks have included the theft of sensitive data, the disruption of critical infrastructure, and the spreading of disinformation and propaganda. The conflict has also highlighted the importance of cybersecurity for governments and critical infrastructure providers. As the conflict has shown, cyber-attacks can have serious consequences for national security and the functioning of essential services such as energy, transportation, and healthcare. As a result, governments and critical infrastructure providers have had to invest more in cybersecurity solutions to protect themselves from these risks.

Key Player Landscape and Outlook

The market is witnessing the emergence of innovative startups and niche players offering specialized cybersecurity solutions. Companies operating in this market are coming up with new cybersecurity solutions for different security needs according to the organization’s nature. For instance, in 2023, Cisco is developing Extended Detection and Response (XDR) with a SaaS-delivered merged system of endpoint, the network, firewall, email, and identity software geared at protecting organisational resources. With Cisco's XDR service, regulating network access, examining events, eliminating risks, and automating reaction all through a single cloud-based platform would increase feasibility. Similarly, competitors are coming up with cybersecurity solutions in order to differentiate themselves and gain market share.

+357 96 030922
info@marketpublishers.com

Contents

+357 96 030922
info@marketpublishers.com

8. GLOBAL CYBERSECURITY MARKET OUTLOOK, BY REGION, 2016-2030F

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

+357 96 030922
info@marketpublishers.com

9. MARKET MAPPING, 2022

10. MACRO ENVIRONMENT AND INDUSTRY STRUCTURE

+357 96 030922
info@marketpublishers.com

*Companies mentioned above DO NOT hold any order as per market share and can be

+357 96 030922
info@marketpublishers.com

changed as per information available during research work

16. STRATEGIC RECOMMENDATIONS

17. ABOUT US & DISCLAIMER

+357 96 030922
info@marketpublishers.com

I would like to order

Product name: Global Cybersecurity Market Assessment, By Component [Hardware, Software, Services], By Security Type [Network Security, Cloud Security, Endpoint Security, Mobile Security, IoT Security], By Deployment [Cloud, On-Premises], By Solution [Identity & Access Management, Infrastructure Security, Governance Risk & Compliance, Data Security & Privacy Service Offering, Cloud Storage, Others], By Enterprise Size [Large Enterprise, Small and Medium Sized Enterprises (SME's)], By Industry Vertical [IT and Telecommunication, Automotive, Government, BFSI, Retail, Healthcare, Manufacturing, Others], By Region, Opportunities and Forecast, 2016-2030F

Product link: https://marketpublishers.com/r/GD31E1EE9C1BEN.html

Price: US$ 4,500.00 (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/GD31E1EE9C1BEN.html