+44 20 8123 2220
info@marketpublishers.com

Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

https://marketpublishers.com/r/CBD6F1D81412EN.html
Date: July 2024
Pages: 226
Price: US$ 4,750.00 (Single User License)
ID: CBD6F1D81412EN

Abstracts

The Cybersecurity Market size is estimated at USD 182.84 billion in 2024, and is expected to reach USD 314.28 billion by 2029, growing at a CAGR of 11.44% during the forecast period (2024-2029).

Key Highlights

The key drivers contributing to the increase in the adoption of data-intensive approaches and decisions with the growth include the increase in the number of cyber-attacks globally with the growing digitalization has the potential to damage the internet-linked digital infrastructure of various government or private sector enterprises, thereby significantly driving the market growth rate.

IT advances, communications technologies, and the smart energy grid are changing the landscape of every country’s critical infrastructure and business networks. However, with rapidly evolving technology comes rapidly advancing threats. According to the Center for Strategic and International Studies (CSIS) and McAfee, cybercrimes cost the world almost USD 600 billion yearly, or 0.8% of global GDP. In addition, the average cost of data breaches has also increased in recent years, indicating a dire need to deploy cybersecurity solutions to mitigate the risks.

The cybersecurity landscape is increasing as companies worldwide adopt technologies like cloud computing, artificial intelligence (AI), the Internet of Things (IoT), and big data analytics as part of their digital transformation initiatives. This significant shift might present businesses that adopt digital transformation with the risk of encountering new and rapidly changing cybersecurity threats.

+44 20 8123 2220
info@marketpublishers.com

The increasing integration of digital technologies into critical infrastructure, such as energy grids, transportation systems, and healthcare facilities, has significantly intensified the potential damages resulting from cyber attacks. As these vital systems become more interconnected and reliant on digital platforms, they become more susceptible to malicious activities that can disrupt operations, compromise sensitive data, and even pose risks to public safety. This intensified vulnerability necessitates a robust and adaptive cybersecurity ecosystem to safeguard against potential consequences.

The expansion of data-intensive applications and technologies, fueled by the digital transformation period, has led to an exponential growth in the volume, rate, and variety of data generated and processed by businesses. As organizations utilize the power of big data, artificial intelligence, and machine learning, the need to strengthen the security of this valuable asset becomes essential. The increased use of data-intensive approaches necessitates managing large datasets that contain sensitive and vital information, which makes strong cybersecurity measures necessary for protecting against potential risks and vulnerabilities.

As organizations undergo digital transformation, the challenges associated with seamlessly integrating advanced cybersecurity solutions with existing legacy systems become increasingly evident. Legacy infrastructure, characterized by outdated hardware, software, and protocols, poses limitations to implementing modern cybersecurity measures. Combining these outdated systems with modern technology frequently results in an environment that makes it more challenging to implement and maintain strong cybersecurity frameworks.

COVID-19 caused significant disruption to businesses on a global scale and accelerated the growth of cybercriminal activities in private and government enterprises supported by digital transformation. The increase in cyber-attacks and frauds during the pandemic created an opportunity for cybersecurity solutions due to their application in minimizing cyber risks and fueled the market during and in the post-pandemic period.

Cybersecurity Market Trends

The Cloud Deployment Segment is Expected to Hold Significant Market Share

Various factors, including scalability, flexibility, platform centralization, ease of accessibility, and cost-effectiveness, drive the growing adoption of cloud-based cybersecurity solutions. According to IBM, in 2022, 33% of respondents said they were

using multi-cloud to guarantee availability. The global workforce's increasing reliance on remote and mobile capabilities contributes to the demand for cloud-based cybersecurity. Cloud solutions can facilitate secure access and monitoring of systems from any location, supporting the needs of modern, flexible work environments.

Furthermore, significant trends in cloud adoption in the market include the rise of multi-cloud and hybrid strategies, the prominence of cloud-native security, integration with DevOps practices, increased automation and orchestration, cloud-based analytics, and threat intelligence.

The rise of remote work and distributed workforces has further driven the adoption of cloud-based cybersecurity. Moreover, according to a Netwrix survey, 24% of businesses increased their cloud security and cybersecurity expenditures during the pandemic. Further, the IT security software firm stated that out of the organizations surveyed last year, 49% reported an increase in their cloud security spending for that year. Also, traditional network-centric security models are no longer sufficient in a landscape where endpoints extend beyond corporate networks. Cloud deployment facilitates centralized management, threat detection, and response capabilities, ensuring the security of remote devices and endpoints irrespective of their physical location.

North America is expected to be a significant player in adopting cloud-based cybersecurity solutions, owing to the significant adoption of cloud across numerous industries. For instance, in September 2023, Snowflake, the data cloud startup, and Lacework, the data-driven cloud security firm, announced an expanded partnership that will further automate cloud security at scale and advance the future of cloud architecture. With Snowflake's safe data sharing and the extended relationship, security teams may now have direct access to their Lacework cloud security data for unified visibility and personalized automation.

In conclusion, the growth of cloud deployment in the market is driven by its ability to address the evolving needs of organizations in an increasingly digital and interconnected environment. Cloud-based cybersecurity solutions are expected to gain prominence as organizations encounter the complexities of a dynamic threat landscape and undergo digital transformations.

North America is Expected to Hold Significant Market Share

+44 20 8123 2220
info@marketpublishers.com

The United States faces a continuously evolving and sophisticated cyber threat landscape. The United States is at the epicenter of cybercrime globally due to the high penetration of digital technologies and cloud computing in end-user industries compared to other countries. It is by far the most highly targeted nation, and American businesses face a higher volume of attacks and more costly consequences when an attack is successful.

The increasing frequency and sophistication of cyber-attacks drive the adoption of cybersecurity solutions in the United States. Also, the growing regulatory requirement leads many organizations to adopt and invest in cybersecurity solutions, as many industries in the United States are subject to regulations such as HIPPA, GDPR, and PCI DSS, which require the organization to implement. Due to this, companies are increasing their investments in cybersecurity.

For instance, in September 2023, the Open Commerce solution from Google Cloud and ONDC was accepted by over 20 e-commerce enterprises. This allows buyers, sellers, and logistical service providers to join the ONDC network seamlessly. With this, there will be an increase in the number of consumers and sellers who can use the generative AI tools offered by Google Cloud to transact on the network, particularly people who reside in smaller cities.

Additionally, the U.S. government plays a crucial role in promoting cybersecurity through initiatives, policies, and regulations. Also, the United States has invested significantly in cybersecurity research and development. For instance, in August 2023, The United States Department of Energy (DOE) opened USD 9 million in competitive federal funding for small and rural electric utilities to improve cybersecurity. With this, it will allow smaller and rural utilities and cooperatives in the electric sector to apply for chunks of funding to build more cyber resilience in their infrastructure that could defend against cyberattacks, ransomware actors, and other digital threats.

Moreover, cybercrime is rapidly gaining traction in Canada, and the impact is increasing alarmingly. As per the report published by The Communications Security Establishment (CSE) in August 2023, there were 70,878 reports of cyber fraud in Canada, with over USD 390 million stolen. The rising frequency and sophistication of cyber threats, including ransomware attacks and data breaches, have driven organizations in Canada to invest in cybersecurity solutions to protect against evolving threats.

Critical sectors like energy, finance, healthcare, and telecommunications in Canada

+44 20 8123 2220
info@marketpublishers.com

recognize the importance of cybersecurity in protecting critical infrastructure from cyber threats. For instance, in September 2023, the eHealth Centre of Excellence (eCE) announced the launch of the eCE shield in Canada, which addresses the pressing need for comprehensive cybersecurity and privacy education in healthcare, ultimately making healthcare organizations more resilient against cyber threats and privacy breaches.

Overall, the growing cybersecurity market in Canada is a response to the evolving threat landscape, increased digitization, and the recognition of cybersecurity as a strategic priority for organizations across various sectors. This trend will continue as cybersecurity remains critical to Canada's digital resilience and national security.

Cybersecurity Industry Overview

The cybersecurity market exhibited fragmentation, featuring major players such as IBM Corporation, NortonLifeLock Inc. (Gen Digital Inc.), Microsoft Corporation, Proofpoint Inc. (Thoma Bravo, L.P.), and McAfee LLC. These market participants embraced strategies like partnerships and acquisitions to bolster their solution offerings and attain a sustainable competitive advantage.

In October 2023, IBM announced the launch of its new managed detection and response service offerings, incorporating advanced AI technologies. The newly introduced Threat Detection and Response Services (TDR) offered 24-hour monitoring, investigation, and automated remediation of security alerts across the client's hybrid cloud environments.

In September 2023, Norton LifeLock Inc. unveiled Norton Small Business, an all-in-one cybersecurity solution designed to assist entrepreneurs and small business owners in safeguarding their financial futures. Norton Small Business provides triple-lock protection, making it accessible for small businesses to secure their team's online activities, devices, and customer data through a user-friendly, all-in-one cybersecurity solution.

Additional Benefits:

The market estimate (ME) sheet in Excel format

3 months of analyst support

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

7 COMPETITIVE LANDSCAPE

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

Product link: https://marketpublishers.com/r/CBD6F1D81412EN.html

Price: US$ 4,750.00 (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/CBD6F1D81412EN.html

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:
Last name:
Email:
Company:
Address:
City:
Zip code:
Country:
Tel:
Fax:
Your message:

**All fields are required

Custumer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at https://marketpublishers.com/docs/terms.html

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970

+44 20 8123 2220
info@marketpublishers.com