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

https://marketpublishers.com/r/E721C8A667B7EN.html
Date: July 2024
Pages: 136
Price: US$ 4,750.00 (Single User License)
ID: E721C8A667B7EN

Abstracts

The Europe Cybersecurity Market size is estimated at USD 56.96 billion in 2024, and is expected to reach USD 95.17 billion by 2029, growing at a CAGR of 10.81% during the forecast period (2024-2029).

The key drivers contributing to the increase in the adoption of data-intensive approaches and decisions with the growth include the rise in the number of cyber-attacks regionally 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.

Key Highlights

The pandemic raised the demand for cybersecurity solutions to protect businesses and countries from malicious cyber attacks supported by increasing digitalization. Additionally, the Bank for International Settlements stated that, during the pandemic, financial institutions faced an increasing risk of cyber attacks, which were accelerated by remote working conditions. The need for cyber security majors in enterprises and government entities of various countries increased in the post-pandemic time due to the trend of online and data-driven businesses, fueling the implementation of cybersecurity solutions.

According to a European DIGITAL SME Alliance report released in October 2023, a marked increase in ransomware attacks was reported, followed by phishing campaigns carried out over the same period each year, mainly targeting France, Germany, Italy, and Spain. In all four quarters, there was a consistent peak in attacks during the first quarter of 2023, with 7,772 new Common Vulnerabilities and Exposures being released, highlighting yet again the constantly changing and dynamic nature of cyber vulnerability.

Digital connectivity has become a fundamental aspect of life in today's constantly evolving world. It is the key to communication, commerce, and access to information in this age. To ensure equal opportunities for all individuals and communities, it is therefore essential to prioritize investments in digital connectivity. According to new research by the UK government, superfast broadband is available to 98% of households in urban areas, compared to 86% in rural areas.

The increasing integration of digital technologies into critical infrastructure, such as energy grids, transportation systems, and healthcare facilities, has significantly intensified the potential damages 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.

However, the increasing demand for cyber security solutions in a shorter period has raised the skill gap in the cyber security market among the workforce, restricting the market adoption during the forecast period because, without a presence of professional cyber security professionals, companies cannot implement the cyber security solution in their systems effectively.

With the outbreak of COVID-19, the cloud market gained significant traction as cloud-based services and tools are increasingly adopted due to organizations deploying remote work access amid lockdowns in various countries, as indicated in the graph. With the growing trends of cloud adoption and ongoing migration of on-premise to cloud solutions, cyberattacks and threats have also increased considerably, fueling the market growth rate. The end-user cloud adoption scope expanded by the COVID-19 outbreak also fueled investment in the market. Many start-ups in the market have gained investments in recent months, which is also expected to fuel innovation in the coming years.

Europe Cybersecurity Market Trends

Cloud Security to Witness Rapid Growth

The growth of cloud computing services and the emergence of cloud-based solutions adoptions by end-users in European countries are fueling the risk of cloud security breaches, including Distributed denial of service (DDoS), Hypervisor DoS Attacks, Hypercall Attacks, among others, in the cloud environments, fueling the adoption of cloud security solutions among the enterprise segment of Europe, which would drive the market growth in the future.

Additionally, in December 2023, the European Commission has planned to provide USD 1.29 in funding for cloud computing and Edge development in France, Germany, Hungary, Italy, the Netherlands, Poland, and Spain. This fund would include 19 projects from 19 companies and 90 indirect partners to build a healthier European cloud community with European requirements for interoperability, data privacy, sustainability, and cybersecurity, showing the region's demand for cloud security solutions during the forecast period.

The growth of digital services in European countries to benefit the citizens, public administrations, and businesses is fueling the growth of cloud-based IaaS, PaaS, and SaaS business models in the region, which is raising the vulnerability of the digital infrastructure to cloud-based cyber-attacks and fueling the need for cloud cyber security solutions in the region.

For instance, in December 2023, the European Commission amended the Digital Europe work programs for 2024, assigning EUR 762.7 million (USD 818.54 million) in funding for digital solutions, including cloud services. Additionally, the commission has stated that EUR 214 million (USD 229.67 million) for 2024 would be used for cybersecurity to enhance the European Union's collective resilience against cyber threats, showing the demand for cloud security in the market.

Additionally, in November 2023, the European Commission adopted the proposed EU Cybersecurity Certification Scheme for Cloud Services, which the EU cybersecurity agency has developed, as an implementing act in Q1 2024. It would support adopting cloud security solutions for all the end users in Europe because EU- and non-EU-based cloud service providers must comply with the cyber security regulations to offer their cloud services in the European region during the forecast period.

United Kingdom Holds a Significant Market Share

The United Kingdom is constantly confronted with new cyber threats. The country has become a target for nation-state hacking groups worldwide, which have targeted various government and defense agencies. In September 2023, Darkbeam, a London-based company, revealed that over 3.8 billion records had been exposed after the company left an interface containing the exposed records unprotected.

Moreover, the country faces diverse cyber threats in the public and private sectors, including ransomware, phishing attacks, and nation-state-sponsored cyber espionage. For instance, as of 2023, the UK Government estimated that, on average, the most disruptive breach for each business resulted in a loss of around EUR 1,100 (USD 1193.41). Breaking that down further, the average charity cost for the most severe breach was estimated to be approximately EUR 530 (USD 575). This resulted in a loss of approximately EUR 4,960 (USD 5381.18) for medium and large businesses.

According to money.co.uk, cyberdependent crime indicates different forms of hacking and cybercrime, followed by over 8100 reported cases. With the increasing cyber threat, the United Kingdom has established a regulatory framework for cybersecurity, including the General Data Protection Regulation (GDPR), which strongly emphasizes protecting personal data. Compliance with GDPR and other regulations drives the adoption of cybersecurity solutions. As the market grows, government agencies and private companies in the country establish partnerships and launch new products.

Moreover, more than 50% of employees in the United Kingdom work from home and use different devices. Due to this, cybercriminals have more entry points to target, including home networks and personal devices. Cybercriminals often leverage phishing attacks, and remote workers can be more susceptible to falling victim to these scams when outside the corporate network. Phishing emails may trick employees into revealing sensitive information or login credentials. Hence, adopting cyber security for every company has become mandatory in the country.

In addition, by the end-user industry, the demand for cyber security in the IT and Telecom sectors is growing. With the ever-increasing 5G and total fiber broadband networks in the country, the government, in collaboration with telecommunication companies, is taking initiatives to tackle cyberattacks and improve security standards and practices across the United Kingdom's telecoms sector. For instance, in October 2023, BT Group PLC announced its collaboration with Google, focusing on an enhanced commitment to cybersecurity innovation. As part of the partnership, BT will become a managed services delivery partner for Google's Autonomic Security Operations (ASO) offering based on Google Chronicle.

Due to these factors, the cybersecurity market in the United Kingdom is characterized by a complex threat landscape, regulatory imperatives, and a proactive approach to addressing cybersecurity challenges. Organizations across sectors invest in advanced cybersecurity solutions and services to mitigate risks and protect against cyber threats.

Europe Cybersecurity Industry Overview

The European cybersecurity market is highly competitive, owing to several global players. Some of the major players in the market are IBM Corporation, Cisco Systems, Inc., Fujitsu, Fujitsu Limited (Fujitsu Group), Dell Technologies Inc., and Broadcom. The market players are indulging in strategic partnerships, product launches, and acquisitions as lucrative paths toward expanding their market share. Several global cybersecurity providers are also expanding their presence and strengthening their foothold in the European region.

In December 2023, IBM Corporation announced that the company had signed an agreement with the NATO Communications and Information Agency (NCI Agency) to help strengthen the Alliance’s cybersecurity posture with improved security visibility and asset management across all NATO enterprise networks.

In December 2023, Palo Alto Networks Inc. completed its acquisition of Dig Security, a provider of Data Security Posture Management, to integrate its data security solutions into the Palo Alto Networks Prisma Cloud platform, which would enable organizations with real-time data protection across the entire cloud environment and can fuel its market adoption in Europe, supported by the increasing trend of cloud migrations in the European region.

Additional Benefits:

The market estimate (ME) sheet in Excel format

3 months of analyst support

Contents

I would like to order

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

Product link: https://marketpublishers.com/r/E721C8A667B7EN.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/E721C8A667B7EN.html