Europe Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 200 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Europe Cybersecurity Market size is estimated at USD 36.40 billion in 2024, and is expected to reach USD 64.81 billion by 2029, growing at a CAGR of 12.23% during the forecast period (2024-2029).

The adoption of cybersecurity solutions is expected to increase with the increasing penetration of the internet throughout Europe's major countries. Also, the expanding wireless network catering to mobile devices has enhanced data vulnerability.

Implementing EU legislation and actions stemming from the National Framework and the National Cybersecurity Plan is expected to facilitate the market's growth in the region. As part of its Digital Agenda, the Italian government plans to invest in digital identity protection to increase digital transactions' security levels and ground consumers' trust by protecting citizens' identities.

According to the European Council Union, the EU has committed to investing EUR 1.6 billion in cybersecurity capacity, and the widespread deployment of cybersecurity infrastructures and technologies across the EU for public administrations, enterprises, and individuals as part of the Digital Europe Programme for 2021-2027, and such investments boost the Europe cybersecurity market.

Connected devices, including machines, sensors, networks that comprise the Internet of Things (IoT), and cyber security, will play a key role in further shaping Europe's digital future.

The shortage of trained cybersecurity workers in many businesses is a key challenge facing cyberattacks. The number of experienced cybersecurity professionals, particularly in Europe, is low compared to the demand for security professionals to deal with cyber threats for financial institutions, government organizations, and private sector/industrial businesses.

The COVID-19 epidemic emphasized the need for greater digital security. People increased their online presence to preserve personal and professional relationships. In contrast, hackers took advantage of the situation, focusing on e-commerce, e-payment enterprises, and the healthcare system.

Europe Cyber Security Market Trends

Increasing Demand for Digitalization and Scalable IT Infrastructure drive the Europe Cybersecurity Market

The European External Action Service (EEAS) announced a new EU cybersecurity policy. This strategy aims to increase Europe's resilience to cyber-attacks while ensuring that all people and companies can fully benefit from trustworthy, dependable services and digital technologies. In May 2023, the Commission and the European Cybersecurity Competence Centre (ECCC) launched a new call for proposals under the Digital Europe Work Programme 2023-2024 for cybersecurity actions to strengthen operational cooperation and joint capacities with Member States at the EU level, totaling EUR 71 million.

The European cyber security market for connected devices and the Internet of Things (IoT) is expanding. Germany, the United Kingdom, France, and Italy are leading European countries adopting IoT and connected devices. According to ETNO, the number of active IoT smart city connections was 1.01 million in 2016, projected to increase to 53.63 million by 2025. However, many European customers increasingly understand the benefits of wearable devices.

Hackers have begun to attack banks that use the SWIFT network to transmit money-moving messages using malware such as Odinaff, Danabot, and Backswap, Camubot. The most important revenue sources for the Defence/Government cybersecurity industry are expanding government rules on data privacy, increased cyber threats, and a growing number of data centers.

Critical sectors such as transport, energy, health, and finance have increasingly depended on digital technologies to run their core business. While digitalization brings enormous opportunities and provides solutions for many of the challenges faced by Europe, the COVID-19 crisis also exposed the economy and society to cyber threats.

The risk to companies of cyber attacks is growing significantly, hence the increased investment in prevention. For instance, according to Hiscox Cyber Readiness Report 2022, companies in Belgium, France, Germany, Ireland, The Netherlands, Spain, and the United Kingdom increased their cybersecurity investment in 2022 compared to 2021.

United Kingdom Expected to Witness Significant Growth

With the growing 5G and full 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 example, the UK Cyber Security Council and ISACA announced a partnership for the Audit and Assurance program in February 2023 to bridge the gap between cybersecurity and audit professionals.

Furthermore, the proliferation of the internet and the adoption of payment-linked online services, which attract profit-seeking criminals, are the primary drivers for such attacks. For instance, according to data published by the National Crime Agency (NCA) of the United Kingdom, cybercrime has surpassed all different forms of conventional crimes.

Furthermore, as per a survey conducted by the UK government, nearly 39% of the businesses and more than a quarter (26%) of the charities surveyed suffered cybersecurity incidents at least once a week preceding the survey. With just under a fifth (19%) of businesses that suffered a breach consequently had material losses such as theft of money or data. Twice as many (35%) reported other negative impacts, such as costs from implementing better security, staff costs, and business disruption. Hence, following such instances, new government regulations came into effect and have been formulated.

For instance, in the United Kingdom, official statistics related to the most common type of data breaches are reported annually by the Department for Digital, Culture, Media, and Sport (DCMS) in a "cybersecurity breaches survey."

Moreover, more personnel and connected devices are accessing sensitive data from faraway places due to the transition to remote and hybrid working. As a result, businesses are finding it challenging to stay on top of appropriate cybersecurity measures as they need help managing complex security architectures while facing a scarcity of competent resources.

Europe Cyber Security Industry Overview

The European Cybersecurity Market is highly competitive, owing to several global players. The market players are indulging in strategic partnerships, product launches, and acquisitions as lucrative paths toward expanding their market share. Also, several global cybersecurity providers are expanding their presence and strengthening their foothold in the European region.

In May 2022, Cisco released the Cisco Cloud Controls Framework (CCF), accessible to the public. The Cisco CCF is a comprehensive framework aggregating international and national security compliance and certification standards. It empowers teams to ensure cloud products and services meet security and privacy standards.

In June 2022, IBM and Atos announced an expansion of their relationship centered on IBM Cloud for Financial Services to assist financial services firms in achieving optimal data and system security through "EU trusted third party cybersecurity monitoring" provided by Atos. This expansion will allow enterprises, such as operators of vital importance (OIV) and operators of essential services (OES), to advance their cloud technology use.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com

Europe Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 200 pages | Mordor Intelligence

To place an Order with Scotts International:
- Print this form
- Complete the relevant blank fields and sign
- Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.
** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-03
		Signature	

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com