

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

<https://marketpublishers.com/r/E1BC259CA78BEN.html>

Date: July 2024

Pages: 120

Price: US\$ 4,750.00 (Single User License)

ID: E1BC259CA78BEN

Abstracts

The Europe Security Services Market size is estimated at USD 17.84 billion in 2024, and is expected to reach USD 23.64 billion by 2029, growing at a CAGR of 5.80% during the forecast period (2024-2029).

Key Highlights

The demand for security services in Europe is rising due to various factors, such as regulatory requirements, an ever-changing threat environment, heightened awareness of cybersecurity threats, and the digital revolution. In addition, European organizations must adhere to industry-specific and international regulations, necessitating the provision of security services to ensure and sustain compliance. People increasingly recognize the value of SaaS (software-as-a-service) solutions, and integrating the physical and digital realms is leading to the development of increasingly sophisticated security systems, particularly in more developed markets.

Cloud adoption has fundamentally altered how organizations store and exchange data, thus necessitating the demand for security services. As a result, cloud computing is enabling more efficient multi-site administration, integration of security technology solutions, and the ability to conduct security operations remotely. For instance, Flexera Software has identified cost savings and the migration of more workloads into the cloud as the most essential cloud initiatives in 2023 for European organizations, with 62% of respondents citing this as their top priority.

Cyber threats are rising in Europe, as in any region worldwide. The prevalence of cyberattacks, ransomware attacks, data breaches, and other malicious activities is

increasing, prompting organizations to invest in comprehensive cybersecurity strategies. For instance, according to ANSSI (National Information Systems Security Agency), in 2023, there were 110 major ransomware attacks in Europe. Additionally, in 2023, SMEs (small and medium enterprises) continued to be the primary victims of ransomware attacks. Hence, European organizations are exploring cybersecurity strategies to safeguard digital resources in a rapidly digitalizing environment.

Organizations in the public sector may be subject to budgetary restrictions and administrative obstacles that may prevent them from utilizing security services. Many European organizations still use legacy IT infrastructure and technology that may need to be equipped with the most up-to-date security capabilities. The upkeep of these systems can prove to be laborious and expensive. In addition, as technology progresses, new vulnerabilities and threats are created. As a result, security services must be continually adjusted to address these new threats effectively. This factor can result in a need for more security service options, which can impede the market's growth.

Furthermore, as the COVID-19 aftereffects highlighted the need for security services to respond to public health crises, the healthcare industry adopted telehealth and digitized health records to meet patients' needs, driving the demand for security services. These services were crucial in protecting patient data and ensuring regulatory compliance.

Moreover, in the current scenario, the macroeconomic situation remains volatile, and players continue to see macro trends such as high interest rates, inflation, fear of recession, and geopolitical tensions increasing in some parts of the world. For instance, the macroeconomic situation did not improve in 2023, with inflation rates and interest rates staying relatively high, and the fear of recession amid geopolitical conflicts remained. The continued macroeconomic uncertainty means customers in different market segments have remained cautious. A later recovery of markets is expected, and the timing and shape of the recovery slope remain unclear.

Europe Security Services Market Trends

Cloud Adoption to Hold Significant Market Share

Multiple European organizations are increasingly transitioning their data and applications into the cloud. Compliance with stringent data protection regulations, such as the General Data Protection Regulation (GDPR), necessitates providing security and privacy services to protect sensitive data and ensure compliance. Organizations

increasingly recognize the cost and resource savings that can be achieved by transitioning their data into the cloud instead of constructing and sustaining new data storage. Due to their numerous advantages, cloud-based solutions are expected to be a significant driver of digital innovation.

Cloud services offer users the advantage of accessing data from any location. However, this also raises the risk of cybercriminals being able to access the data. According to CESIN, as of January 2023, the number of cyberattacks detected by companies in France varied across different ranges. Approximately 32% of companies reported detecting between one and three cyberattacks, while 7% experienced between four and nine attacks.

Cyber-attacks are becoming increasingly frequent and sophisticated, necessitating the development of cybersecurity solutions. Furthermore, the increasing regulatory requirements in the European Union, such as the GDPR (General Data Protection Regulation), are leading many organizations to invest in and adopt cybersecurity solutions. The development of cloud-native technologies and architectures necessitates providing specialized security services to address the specific security threats they pose.

Cloud providers operate on the principle of shared responsibility, meaning they are responsible for infrastructure security and customers for protecting data and applications. As a result, security services are necessary to fulfill the role of the customer. Cloud services are most commonly employed in Europe's information and communication industry and the professional, technical, and scientific sectors.

Organizations across Europe that utilize a cloud-based infrastructure gain access to advanced technologies that are secure, expandable, and highly productive. This step eliminates the need to allocate resources, transforms investment costs into operational costs, and increases operational flexibility.

United Kingdom to Witness Significant Growth

The UK government has established various cybersecurity regulations and benchmarks, including NIS regulations and cyber essentials certification. These regulations require that organizations invest in security services to meet the necessary requirements. The proposed changes will increase security standards and enhance the reporting of

significant cyber incidents to reduce the likelihood of attacks causing disruption. Laws may be amended to include new organizations or sectors when they become essential for essential services.

The United Kingdom is experiencing a period of digital transition across various industries, such as healthcare, finance, and government. As businesses transition to digital operations and embrace new technologies, the need for security services to safeguard digital resources and data has significantly increased. One of the primary reasons for the rise in cyberattacks is a need for more qualified cybersecurity personnel in each sector. The number of skilled cybersecurity professionals, particularly in Europe, is low compared to the demand for security professionals to address cyber threats for financial institutions, government entities, and private sector/industrial enterprises.

Organizations in Europe are increasingly turning to managed security services due to the growing threats to their cybersecurity, such as IT ransomware attacks and data exfiltration. Furthermore, the increased media coverage of significant cyberattacks is driving conventional industries' adoption of MSS (managed security services). As a result, the demand for Internet center services is also rising, further contributing to the market's growth.

The recent breaches in the United Kingdom have highlighted the importance of safeguarding confidential data. Several companies are investing in security measures to protect the information and prevent unauthorized access.

For instance, according to the UK government, by January 2023, approximately 20% of organizations in the country reported a data breach incident occurring monthly. Additionally, 29% of organizations reported a data breach event occurring less than once per month in the preceding 12 months. On the other hand, 11% of organizations reported weekly data breach incidents.

Europe Security Services Industry Overview

The European security services market is fragmented, with many players serving the market at the regional and global levels. Almost all industries are transitioning from on-premises to cloud platforms for corporate activity. This factor has sped up the development of cloud-based security solutions as the volume of data and processing requirements from cloud services also supports the further growth of AI and ML. These

security services providers launch enhanced products, collaborate with various companies for market expansion, and gain leadership. Some significant players offering their services in this market include Fortra LLC, G4S Limited, Fujitsu, Wipro Ltd, Palo Alto Networks, Allied Universal, and IBM Corporation, among many others.

July 2023: Netskope partnered with Wipro Limited, enabling Netskope to provide comprehensive cloud-native SASE (secure access service edge) and zero trust network access (ZTNA) services to Wipro's global enterprise client base. Through its CyberTransform platform, Wipro provides clients with cyber resilience through comprehensive strategy-aligned advisory and implementation solutions for specific business needs. This partnership will combine Wipro's extensive cybersecurity managed services experience with Netskope's advanced, fully integrated secure access service edge platform to enable customers to secure and expedite digital transformation initiatives.

June 2023: L&T Technology Services partnered with Palo Alto to offer security services and solutions to 5G and OT enterprises. As part of the agreement, L&T partners with Palo Alto Networks' managed security services provider (MSSP), providing a comprehensive suite of security solutions to end customers across industrial verticals. The security solutions offered by L&T Technologies include 5G, OT, and IT/OT Converged SOC Services. The MSSP agreement offers a managed service for implementing the Palo Alto Networks zero trust OT Security solution, allowing customers to outsource the management of their operational technology security to L&T.

Additional Benefits:

The market estimate (ME) sheet in Excel format

3 months of analyst support

Contents

1 INTRODUCTION

- 1.1 Study Assumptions and Market Definition
- 1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHTS

- 4.1 Market Overview
- 4.2 Industry Attractiveness - Porter's Five Forces Analysis
 - 4.2.1 Bargaining Power of Suppliers
 - 4.2.2 Bargaining Power of Consumers
 - 4.2.3 Threat of New Entrants
 - 4.2.4 Threat of Substitutes
 - 4.2.5 Intensity of Competitive Rivalry
- 4.3 Impact of COVID-19 Aftereffects and Other Macroeconomic Factors on the Market

5 MARKET DYNAMICS

- 5.1 Market Drivers
 - 5.1.1 The Increasing Proliferation of Internet of Things (IoT) Devices
 - 5.1.2 The Integration of Artificial Intelligence (AI) and Automation in Security Services
 - 5.1.3 Increasing Investments by Organizations to Protect Against Country-sponsored Attacks
- 5.2 Market Challenges
 - 5.2.1 Lack of Awareness of Security Services
 - 5.2.2 Shortage of Skilled Personnel
 - 5.2.3 Rising Concerns about Data Privacy and Potential Misuse of Security Services

6 MARKET SEGMENTATION

- 6.1 By Service Type
 - 6.1.1 Managed Security Services
 - 6.1.2 Professional Security Services

- 6.1.3 Consulting Services
- 6.1.4 Threat Intelligence Security Services
- 6.2 By Mode of Deployment
 - 6.2.1 On-premise
 - 6.2.2 Cloud
- 6.3 By End-user Industry
 - 6.3.1 IT and Infrastructure
 - 6.3.2 Government
 - 6.3.3 Industrial
 - 6.3.4 Healthcare
 - 6.3.5 Transportation and Logistics
 - 6.3.6 Banking
 - 6.3.7 Other End-User Industries
- 6.4 By Country***
 - 6.4.1 United Kingdom
 - 6.4.2 Germany
 - 6.4.3 France
 - 6.4.4 Italy
 - 6.4.5 Spain

7 COMPETITIVE LANDSCAPE

- 7.1 Company Profiles*
 - 7.1.1 Fortra LLC
 - 7.1.2 SecurityHQ
 - 7.1.3 Allied Universal
 - 7.1.4 Trustwave Holdings Inc.
 - 7.1.5 Broadcom Inc.
 - 7.1.6 G4S Limited
 - 7.1.7 Fujitsu Ltd
 - 7.1.8 Wipro Ltd
 - 7.1.9 Palo Alto Networks
 - 7.1.10 Securitas Inc.
 - 7.1.11 IBM Corporation
 - 7.1.12 Cybaverse Ltd
 - 7.1.13 Digital Pathways Ltd
 - 7.1.14 Thales Group

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

I would like to order

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

Product link: <https://marketpublishers.com/r/E1BC259CA78BEN.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/E1BC259CA78BEN.html>