

Germany Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 100 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 Germany Cybersecurity Market size is estimated at USD 14.02 billion in 2025, and is expected to reach USD 23.89 billion by 2030, at a CAGR of 11.25% during the forecast period (2025-2030).

The rising number of cyberattacks with the emergence of e-commerce platforms, the proliferation of smart devices, and the deployment of cloud solutions are some factors driving the market's growth. Cyber threats are expected to evolve with the increase in the usage of devices with intelligent and IoT technologies. As such, firms are expected to adopt and deploy progressive cyber security solutions to detect, minimize, and mitigate the risk of cyber-attacks, thereby driving the market's growth.

Key Highlights

- Various government initiatives and strategies adopted by major players are expected to drive the market. Germany has a strong and diversified cybersecurity ecosystem, with a wide spectrum of established enterprises, startups, research organizations, and universities dedicated to cybersecurity. The country's government policy is particularly supportive, with efforts such as the National Cybersecurity Strategy and the Cybersecurity Act.
- The rise in the number of cyberattacks in the region is expected to drive the demand for cybersecurity solutions. For instance, the State of IT Security in Germany in 2022 by the Federal Office of Information Security states that consumers' general level of concern has recently risen slightly compared to the past three years. About 29% of the respondents stated that they had already been victims of crime on the internet. In previous years, the figure was 25%.
- In each case, a quarter of the respondents had experienced fraud when shopping online (25%), third-party access to an online account (25%), and infection with malware (24%). In contrast to online shopping fraud (2021: 19%), the figures for being affected by third-party access to an online account (2021: 31%) or infection with malware (2021: 29%) have decreased compared to the

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

previous year. Only 19% of respondents were affected by phishing in the last year.

- Addressing risks associated with trends like third-party vendor risks, changes in managed security service providers (MSSPs), and a shift toward a cloud-first strategy is pivotal in the cybersecurity market. As businesses increasingly rely on external vendors for various services and technologies, the associated risks also rise.
- Over the past few years, security systems have made it difficult for an attacker to reach critical data. As a result, ordinary users are increasingly wary of the security of the internet. Solutions that may have worked a few years ago are irrelevant now. To identify and recover from cyberattacks, organizations need several resources and must be highly prepared. In many cases, to recover from a breach or attack, the organization may need to shut down its operations for days altogether. In case of poor planning and inadequate infrastructure, the time to recover from an incident may be considerably high.

Germany Cyber Security Market Trends

Data Security Segment is Expected to Hold Significant Market Share

- The growth of Germany's data protection law has forced enterprises to adopt data security solutions to become operational in the country, which shows the increasing importance of data security awareness.
- Industrial automation and data monetization trends in Germany's enterprise segments are fueling the risk of data privacy breaches and financial losses for end-users, which is driving the demand for data security solutions in the country.
- For instance, in November 2023, the German Federal Office for Information Security published a report stating that Germany has been experiencing a significant increase in cyber threats, with the risk of ransomware attacks considered exceptionally high among SMEs, which account for approximately 80% of the German economy.
- Therefore, organizations are expected to actively invest in data security solutions in the coming years largely due to the need to protect and safeguard their sensitive information across multiple environments, meet regulatory compliance, and simplify operational complexity. According to DLA Piper, the maximum number of personal data breaches as of January 2023 were reported in the Netherlands, a total of approximately 117,434. Germany ranked next, with more than 76,000 personal data breach notifications.
- The emergence of the digital economy in European initiatives for digital transformations of the business landscape of the region, including the Digital Decade targets for 2030, has raised the number of electronic data in the area, which has raised the risk of data breaching.
- For instance, in October 2023, the European Commission published the first report on the State of the Digital Decade, showing the progress toward achieving the digital transformation to empower a digitally sovereign, resilient, and competitive European Union, supporting the demand for data security solutions to protect the digital infrastructures from cyberattacks in Germany.

IT and Telecommunication End-user Segment is Expected to Hold Significant Market Share

- Information technology (IT) and telecommunications are vital in businesses, government agencies, and organizations. The need for robust cybersecurity measures has become crucial with the increasing reliance on interconnected networks, cloud computing, and digital communication. IT and telecom end-users form a substantial portion of the global cybersecurity market as they seek to protect their sensitive data, networks, and communications from evolving cyber threats.
- Germany is a developed economy with significant connectivity through mobile phones. For instance, Deutsche Telekom, one of the prominent players in the telecom industry, recently noted that 99% of Germans have access to LTE service. In comparison, 92% of homes can now access the carrier's 5G network. Deutsche Telekom said it offers 5G services in over 2,000 places across Germany using 3.6 GHz frequencies.

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- In December 2023, Whalebone and O2 Telefonica entered a new partnership in Germany. It will give O2 Telefonica customers a cybersecurity solution called Aura. This move will strengthen Whalebone as a leader in the telecommunications industry's cybersecurity space and an ally of its customers.
- According to the European 5G Observatory, as of 2023, Germany had the most 5G base stations among EU (European Union) member states, with approximately 90,000 base stations installed.
- The IT and telecom end-user segment in the cybersecurity market significantly contributed to the market's growth, owing to the rising frequency and complexity of cyber threats posing significant risks to IT and telecom infrastructures, gaining prominence in cloud deployment, corporate partnerships, and acquisitions. Furthermore, IT and telecom end-users in the global cybersecurity market are expected to continue investing in innovative solutions. As technology advances, the proactive adoption of advanced cybersecurity measures is expected to be essential for maintaining the integrity and security of global IT and telecom operations.

Germany Cyber Security Industry Overview

The German cybersecurity market is semi-consolidated with the presence of major players like IBM Corporation, Cisco Systems Inc., Dell Technologies Inc., Fortinet Inc., and Intel Security (Intel Corporation). Players in the market are adopting strategies such as partnerships and acquisitions to enhance their product offerings and gain sustainable competitive advantage.

- October 2023: IBM launched the managed detection and response service offerings with new AI technologies, including the ability to automatically escalate or close up to 85% of alerts, assisting in accelerating security response timelines for clients. The new Threat Detection and Response Services (TDR) provide 24x7 investigation, monitoring, and automated remediation of security alerts from all relevant technologies across the client's hybrid cloud environments, including existing security tools and investments, and cloud, on-premise, and operational technologies (OT).
- October 2023: McAfee Corp. launched a product lineup with AI-powered protection and new features to help consumers safeguard their privacy and identity online. McAfee's portfolio of products includes innovative safety features, such as McAfee Next-gen Threat Protection and McAfee Scam Protection, that utilize advanced AI to combat the rise in AI threats and provide automated layers of security for consumers and their families.

Additional Benefits:

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

Table of 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 Value Chain Analysis

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

4.3 Industry Attractiveness - Porter's Five Forces Analysis

4.3.1 Threat of New Entrants

4.3.2 Bargaining Power of Buyers

4.3.3 Bargaining Power of Suppliers

4.3.4 Threat of Substitutes

4.3.5 Intensity of Competitive Rivalry

4.4 Impact of Macroeconomic Factors on the Market

5 MARKET DYNAMICS

5.1 Market Drivers

5.1.1 Increasing Demand for Digitalization and Scalable IT Infrastructure

5.1.2 Need to Tackle Risks from Various Trends, such as Third-party Vendor Risks, the Evolution of MSSPs, and Adoption of Cloud-first Strategy

5.2 Market Restraints

5.2.1 Lack of Cybersecurity Professionals

5.2.2 High Reliance on Traditional Authentication Methods and Low Preparedness

5.3 Trends Analysis

5.3.1 Organizations Leveraging AI to Enhance their Cybersecurity Strategy

5.3.2 Exponential Growth to be Witnessed in Cloud Security owing to Shift toward Cloud-based Delivery Model

6 MARKET SEGMENTATION

6.1 By Offering

6.1.1 Solutions

6.1.1.1 Application Security

6.1.1.2 Cloud Security

6.1.1.3 Data Security

6.1.1.4 Identity and Access Management

6.1.1.5 Infrastructure Protection

6.1.1.6 Integrated Risk Management

6.1.1.7 Network Security Equipment

6.1.1.8 End point Security

6.1.1.9 Other Solutions

6.1.2 Services

6.1.2.1 Professional Services

6.1.2.2 Managed Services

6.2 By Deployment Mode

6.2.1 Cloud

6.2.2 On-Premise

6.3 By Organization Size

6.3.1 SMEs

6.3.2 Large Enterprises

6.4 By End User

6.4.1 BFSI

6.4.2 Healthcare

6.4.3 IT and Telecom

6.4.4 Industrial & Defense

6.4.5 Retail

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 6.4.6 Energy and Utilities
- 6.4.7 Manufacturing
- 6.4.8 Others

7 COMPETITIVE LANDSCAPE

- 7.1 Company Profiles
 - 7.1.1 IBM Corporation
 - 7.1.2 Cisco Systems Inc.
 - 7.1.3 Dell Technologies Inc.
 - 7.1.4 Fortinet Inc.
 - 7.1.5 Intel Security (Intel Corporation)
 - 7.1.6 F5 Networks Inc.
 - 7.1.7 AVG Technologies
 - 7.1.8 FireEye Inc.
 - 7.1.9 Fujitsu

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Germany Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 100 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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	<input type="text" value="2026-03-05"/>
		Signature	

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

