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

Market Report | 2024-02-17 | 120 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 11.40 billion in 2024, and is expected to reach USD 19.53 billion by 2029, growing at a CAGR of 11.36% during the forecast period (2024-2029).

In the current market scenario, Cybersecurity clusters can grow organically or develop through intentional, often top-down actions taken by local governments, and government regulations and policies play a significant role in their development. However, several market failures require government attention and action, beginning with concerns about imperfect markets. In Japan, for example, the cybersecurity industry has grown slowly due to dependence on large firms with strong ties to government ministries and the practice of top-down policymaking.

Key Highlights
-In terms of cybersecurity, Germany is pushing itself as a technologically independent country like the United States and China. In August 2020, the country's government announced the launch of a federal agency dedicated to handling cyberattacks and strengthening the country's digital security. The agency is also slated to receive total funding of USD 412 million by 2023, aimed toward continuous innovation and solutions to cyber-attacks.
-According to statistics in the Cost of Data Breach Report published by IBM in 2022, Germany was among the top five nations with the highest average total cost of a data breach. The country's average cost of data breaches stood at USD 4.89 million in 2021, increasing from USD 4.45 million in 2020.
-Kaspersky's study on spam and phishing highlighted the prevalence of malicious correspondence across different geographies. It was discovered that Germany was previously the most popular target for several years until 2020 and was the sixth most frequently targeted nation by malicious emails in 2021. A 4.83% proportion of fraudulent email campaigns were sent to it.
-As more government and commercial personnel work remotely, the coronavirus pandemic has accelerated the trend of rising

cybercrime. Information technology makes it evident that cyberattacks have increased in cost and frequency. Blackmail and system failure losses, according to Bitkom a Germany based IT industry association, have increased 358 % from 2019-2021.
-Over the past few years, the security systems have focused on making it difficult for attackers to reach critical data. Some would say that even this has not happened. As a result, the ordinary user is increasingly wary of the security of the Internet. Solutions that may have worked a few years ago are irrelevant now. Organizations need several resources to identify and recover from cyberattacks and be highly prepared. In many cases, the organization might need to shut down its operations for days to recover from a breach or attack. With poor planning and inadequate infrastructure, the time to recover from an incident may be considerably high.

Germany Cybersecurity Market Trends

Cloud Adoption is one of the Factor Driving the Market

- The increasing realization among enterprises about the importance of saving money and resources by moving their data to the cloud instead of building and maintaining new data storage is driving the demand for cloud-based solutions, and hence, the adoption of on-demand security services in the region.
- Owing to multiple benefits, cloud platforms and ecosystems are anticipated to serve as a launchpad for an explosion in the pace and scale of digital innovation over the next few years.Security has been critical at each step of the cloud adoption cycle, as IT provision has moved from on-premise to outside company walls. SMEs prefer cloud deployment as it allows them to focus on their core competencies rather than invest their capital in security infrastructure since they have limited cybersecurity budgets.
- Furthermore, deploying public cloud service extends the boundary of trust beyond the organization, making security a vital part of the cloud infrastructure. However, the increasing usage of cloud-based solutions has significantly simplified enterprises' adoption of cybersecurity practices.
- With the increased adoption of cloud services, such as Google Drive, Dropbox, and Microsoft Azure, among others, and with these tools emerging as an integral part of business processes, enterprises must deal with security issues, such as loss of control over sensitive data. This gives rise to the increased incorporation of on-demand cybersecurity solutions.
- Furthermore, In June 2021, IBM announced the launch of the IBM Center for Government Cybersecurity, a collaborative environment to assist federal agencies in addressing existing and future cyber threats. The center will include events and learning opportunities, leveraging IBM's cybersecurity knowledge gained by providing software and managed services to more than 17,500 security customers worldwide. The center will leverage IBM technology and host workshops focused on priorities such as zero-trust frameworks and cloud security by access to IBM Research labs to collaborate around the future of encryption, working with a group of internal IBM experts and external advisors, including former government officials with decades of cybersecurity experience.

Healthcare is One of the Prominent End-User Boosting Growth of Cybersecurity Market

- As more commercial and government employees work remotely, the coronavirus epidemic has accelerated the trend of increasing cyber criminality. Cyber-attacks have not only gotten more common but also more expensive, according to the survey. According to the BSI federal cyber security office president, since the COVID-19 pandemic, German clinics have been the subject of a series of assaults. For example, in 2021, CyberEdge reported that a woman from Dusseldorf was taken to a hospital in Wuppertal, 19 miles away after her local hospital in Dusseldorf was hit by a ransomware attack.
- As a result of the attack, 30 of the hospital's servers were compromised, preventing new patients from being processed. Germany is pushing itself as a technically self-governing nation like China and the United States regarding cybersecurity. For

instance, Germany announced the launch of a federal agency dedicated to handling cyberattacks and strengthening the country's digital security in the previous year. Moreover, the agency is slated to receive total funding of USD 412 million by 2023 to continue innovation and solutions to cyber-attacks.
- Modern IAM solutions developed by the healthcare cybersecurity vendors are designed with security top of mind while ensuring flexibility in accessing patient records by medical professionals and staff members. Automated provisioning and de-provisioning of accounts, management of access entitlements, audit and governance, and granular access controls are all essential IAM capabilities for modern healthcare IT. IAM solutions can also add additional layers of protection to sensitive data and systems with Multi-Factor Authentication (MFA). With rise in medical devices in the region will drive the studied market.
- Electronic prescription of controlled substances (EPCS) regulatory requirements require secure, two-factor authentication (2FA) for prescribing controlled substances. Using flexible authentication methods, such as fingerprint biometrics and one-time passwords (OTPS), clinician identities can be quickly verified while enhancing patient safety.
- Advanced Persistent threats are about stealing data through malware placed on computer networks. APTs are usually the work of organized crime, high-skilled hackers, or nation-states. Throughout the pandemic, hospitals worldwide have been hit with surging ransomware levels as highly organized groups use advanced persistent threat (APT)-style tactics to take lifesaving services offline. For instance, in January 2022, German intelligence said that the hacker group APT 27 had started targeting German companies in sectors including pharmaceuticals and technology.

Germany Cybersecurity Industry Overview

The germany cybersecurity market is moderately consolidated, with the presence of a few major companies. The companies are continuously investing in making strategic partnerships and product developments to gain more market share. Some of the recent developments in the market are:

- June 2022 - Fortinet, a provider of comprehensive, integrated, and automated cybersecurity solutions, unveiled FortiRecon, a full Digital Risk Protection Service (DRPS) offering that manages a company's risk posture and provides actionable advice to safeguard its brand reputation, corporate assets, and data using a potent combination of machine learning, automation capabilities, and cybersecurity experts from FortiGuard Labs.
- March 2022 - Vodafone and Accenture are teaming to provide managed security services to small to medium-sized enterprises (SMEs) in Germany. The services will give enterprises that lack the capacity, time, or resources to keep up with this quickly expanding field access to top cybersecurity talent and industry expertise, enabling SMEs to be more robust to cyber threats.

Additional Benefits:

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

Table of Contents:

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

Market Report | 2024-02-17 | 120 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	2025-05-08
		Signature