

Japan 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 Japan Cybersecurity Market size is estimated at USD 2.27 billion in 2025, and is expected to reach USD 3.98 billion by 2030, at a CAGR of 11.89% during the forecast period (2025-2030).

Key Highlights

- The increasing usage of software solutions, the Internet, and connected devices across end-user industries in Japan, in line with the country's priority on developing a digital economy, infrastructural development for high-speed Internet, growth of online banking services, and the demand for cloud-based software, are raising the risk of cyberattacks. This is driving the demand for cybersecurity solutions in the country, which is expected to fuel market growth.
- Cybersecurity is rapidly gaining attention from the government and enterprises in Japan. The increase in the number of cyberattacks on Japanese organizations across a wide range of industries has prompted the country to establish new legislation, strategies, and facilities.
- The rapid growth of scalable IT infrastructure is another significant factor driving Japan's increased need for cybersecurity. Adopting scalable and flexible IT architectures, driven by cloud services and data storage solutions, is becoming increasingly prevalent among organizations.
- The need for qualified and experienced cybersecurity specialists has increased as the digital landscape evolves and cyber threats get more complex. The scarcity of skilled professionals in this field hinders the effective implementation and management of cybersecurity solutions, creating a bottleneck that impacts the overall cybersecurity market in the region.
- The pandemic-driven shift toward remote work and the increased reliance on digital platforms have significantly amplified businesses' exposure to cyber threats. This heightened vulnerability has, in turn, fueled a substantial rise in the demand for advanced cybersecurity solutions. Organizations are prioritizing these solutions to safeguard sensitive information, mitigate risks, and ensure seamless business continuity in an increasingly digital and interconnected environment.

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

Japan Cyber Security Market Trends

Network Security to Witness the Growth

- The growing demand for the protection of integrity, confidentiality, and availability of network infrastructure within organizations is leading to increased demand for cybersecurity solutions in the Japanese cybersecurity market. Due to the government's Cloud First policy, there has been a strong demand for networking infrastructure security as many end users are increasingly taking advantage of virtual environments.
- In addition, the need for robust network security measures has been highlighted by constantly developing cyber threats targeting networks in countries' end-user sectors, predominantly healthcare, IT and telecommunications, and production.
- Secure networks are important for IT systems and their proper functioning because the majority of applications work in a networking environment, which is highly dependent on their performance, security, or reliability. Networks are becoming decentralized, and hybrid networks with existing network resources from cloud data centers across end-user countries drive the market. This has driven the adoption of network security solutions to protect networking infrastructure from unauthorized access, data theft, and manipulation.
- Moreover, the country's end users have witnessed growth in adopting multi-cloud environments, largely driven by the growth in data centers and cloud region launches by IT vendors such as Microsoft, Google, and AWS. This has increased the complexity, making it difficult for Japanese businesses to secure a network.

BFSI Expected to Witness Significant Market Share

- In particular, factors such as the digital transformation of financial services, the adoption of cloud computing, and the integration of advanced technologies such as machine learning and artificial intelligence to enhance banking and finance operations have led to a significant change in the security measures of the BFSI industry in Japan. In addition, growing data breaches and cyberattacks in financial firms further necessitate adopting cybersecurity solutions in the country's BFSI sector.
- Further, with the growing technological penetration and digital channels, such as mobile banking and internet banking, in the country's financial sector, the attack surface for cyber threats in the BFSI sector has expanded.
- The expansion of mobile banking, digital payment platforms, and online transactions in the country's BFSI sector has created new challenges for cybersecurity, thus driving the demand for advanced cybersecurity solutions to protect against fraud, data breaches, and other cyber risks.
- Moreover, the growth in cyberattacks in banks and financial firms has witnessed a significant rise in the past few years, necessitating the demand for robust cybersecurity measures to protect customer data.

Japan Cyber Security Industry Overview

The Japanese cybersecurity market is semi-consolidated, with a considerable number of regional and global players. Key players include IBM Corporation, Cisco Systems Inc., Dell Inc., and Intel Security (Intel Corporation).

- April 2024: Fortinet announced the latest version of its FortiOS operating system and other major enhancements to the company's cybersecurity platform, the Fortinet security fabric, where FortiOS 7.6 empowers customers to better mitigate risk,

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

reduce complexity, and realize a superior user experience across their entire network

- October 2023: IBM announced its managed detection and response service offerings with new AI technologies, including the ability to escalate or close up to 85% of alerts automatically and new threat detection and response services. The new threat detection and response service (TDR) provides 24x7 monitoring, investigation, and automated removal of security alerts from all available technologies in a client's hybrid cloud environment, including the current safety tools and investments, as well as on-premise, on-virtuous, or operating technologies.

Additional Benefits:

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

Table of Contents:

1 INTRODUCTION

1.1 Study Assumption and Market Definition

1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHTS

4.1 Market Overview

4.2 Value Chain Analysis

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 COVID-19 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 Increasingly Leveraging AI to Enhance Their Cyber Security 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

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

- 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
 - 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 Inc.
 - 7.1.4 Fortinet Inc.
 - 7.1.5 F5 Inc.
 - 7.1.6 AVG Technologies
 - 7.1.7 FireEye Inc.
 - 7.1.8 Fujitsu
 - 7.1.9 Intel Security (Intel Corporation)

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

Japan 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



Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com