Japan Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-01-16 | 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:

Japan Cybersecurity Market Analysis

The Japan cybersecurity market was valued at USD 10.34 billion in 2025 and estimated to grow from USD 11.43 billion in 2026 to reach USD 18.9 billion by 2031, at a CAGR of 10.60% during the forecast period (2026-2031). The uplift rests on public-private spending that prioritizes sovereign security capabilities, zero-trust adoption timelines, and rapid cloud migration. Mandatory cyber-risk disclosures on the Tokyo Stock Exchange, AI-driven threat escalation, and 5G-enabled smart-factory rollouts add further momentum. Heightened government capital expenditure channeled through the Digital Agency, coupled with region-specific projects such as the Osaka-Kansai Expo 2025, enlarges the demand pool for advanced threat-detection platforms and managed services. Competitive intensity remains moderate as domestic champions defend share against global suppliers by bundling compliance knowledge with integrated platforms.

Japan Cybersecurity Market Trends and Insights

Japanese Government CAPEX Surge Post-Digital Agency Formation

The 2021 launch of the Digital Agency signalled an inflection point. National defence outlays climbed to 8.5 trillion yen in 2025, and explicit earmarks for cybersecurity infrastructure moved well beyond military projects into cloud platforms, electronic signature systems, and supply-chain security criteria.Procurement rules now require compliance with stringent encryption and incident-response benchmarks, stimulating enterprise demand for sovereign solutions that can reside on forthcoming government

clouds.

Mandatory Zero-Trust Guidelines for Critical Infrastructure by 2026

The Financial Services Agency issued a 177-point rule set in October 2024 that forces banks, insurers, and payment operators to harden identity controls, third-party risk oversight, and continuous monitoring regimes. Parallel grading frameworks from METI extend the obligation to supply-chain partners, accelerating zero-trust pilots in manufacturing and energy corridors. Early adopters report shorter containment times and audit cost reductions, reinforcing the adoption cycle.

Acute Cyber-Talent Shortage Inflating SOC Service Costs

METI estimates a gap of roughly 110,000 practitioners, forcing providers to raise hourly SOC tariffs and elongate onboarding queues. Language barriers and seniority-based hiring norms hinder quick relief from overseas recruitment. Planned training programs aim to lift the pool of certified experts to 50,000 by 2030, yet wage inflation is likely to persist into the next decade.

Other drivers and restraints analyzed in the detailed report include:

Generative-AI-Driven Attack Surface Expansion Across Enterprises5G Private-Network Roll-outs in Smart Factories, Especially ChubuConservative Corporate Culture Slows Zero-Trust Adoption

For complete list of drivers and restraints, kindly check the Table Of Contents.

Segment Analysis

Solutions retained 59.27% of Japan cybersecurity market share in 2025 thanks to integrated suites that bundle endpoint, cloud, and identity safeguards. Large buyers gravitate to unified consoles that alleviate head-count constraints and simplify compliance audits. Network firewalls and intrusion-prevention systems still occupy sizeable allocations, yet growth tilts toward software-defined controls and AI-powered analytics. Identity and access management tools saw a sharp uptake as zero-trust milestones came into view, with domestic vendor FFRI reporting 64.1% operating-profit growth on sovereign software demand.

Managed security lines, particularly MDR and SOC-as-a-service, post the fastest 13.62% CAGR through 2031. Buyers cite the talent deficit and round-the-clock monitoring needs as catalysts. Professional services, risk assessments, penetration testing, and compliance mapping-ride the same wave. Domestic system integrators partner with hyperscalers for incident-response retainers that embed cloud forensics. The overarching shift pivots from one-off licences to recurring service revenue, deepening stickiness and data-sharing depth.

Cloud options captured 54.90% of the Japan cybersecurity market size in 2025 on the strength of subscription economics and elastic scaling. Federated ID services and continual patch pipelines answer the speed-of-change demanded by AI-enhanced threats. Government cloud directives, including a 72.5 billion-yen domestic facility programme, reinforce migration urgency. Financial operators align with FSA guidance that permits cloud use under risk-based controls, prompting institutions to shift vault applications to hardened virtual private clouds.

On-premise installations persist where data-residency or ultra-low-latency requirements prevail, notably in defence and critical infrastructure. Hybrid estates grow as a pragmatic bridge, with sensitive data fenced in private clusters while analytic workloads sit in public clouds. Vendors respond by offering single policy engines that span Kubernetes, virtual machines, and legacy servers. Customers report lower dwell times and quicker rollback after adopting unified asset inventories across environments.

The Japan Cybersecurity Market Report is Segmented by Offering (Solutions, and Services), Deployment Mode (On-Premise, and Cloud), End-User Vertical (BFSI, Healthcare, IT and Telecom, Industrial and Defense, Manufacturing, Retail and E-Commerce, Energy and Utilities, Manufacturing, and Others), and End-User Enterprise Size (SMEs, and Large Enterprises). The Market Forecasts are Provided in Terms of Value (USD).

List of Companies Covered in this Report:

Trend Micro Inc. NEC Corporation NTT Security Holdings Fujitsu Ltd. Cisco Systems Inc. IBM Corporation Dell Technologies Inc. Fortinet Inc. Palo Alto Networks Check Point Software Tech. CrowdStrike Holdings Rapid7 Inc. Secure Brain Corporation Macnica Networks Corp LAC Co., Ltd. FFRI Security, Inc Cyberreason Inc. (JP) SoftBank Technology Corp. NS Solutions Corp. Hitachi Systems Ltd.

Additional Benefits:

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

Table of Contents:

Japan Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2026 - 2031)

Market Report | 2026-01-16 | 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*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-04
		Signature