

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

Market Report | 2026-02-09 | 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:

APAC Cybersecurity Market Analysis

The APAC cybersecurity market was valued at USD 74.22 billion in 2025 and estimated to grow from USD 84.25 billion in 2026 to reach USD 158.96 billion by 2031, at a CAGR of 13.52% during the forecast period (2026-2031). Heightened state-sponsored attacks, accelerating 5G roll-outs, surging digital-payment fraud, and chronic talent shortages are reshaping budget priorities, while local data-protection rules are recasting procurement in favor of regionally domiciled vendors. Competition now hinges less on product features and more on the ability to deliver sovereign-cloud architectures, AI-driven managed detection, and integrated IT-OT security across fragmented regulatory environments. Opportunities abound for providers that combine localized threat intelligence with scalable managed services, especially in mid-market segments underserved by in-house security expertise.

APAC Cybersecurity Market Trends and Insights

Government Data-Sovereignty Mandates Accelerating Domestic Cybersecurity Spend Across APAC

China's Network Data Security Management Regulations taking effect in 2025 require in-country data processing and create separate security stacks for multinationals operating inside China. Singapore's refreshed Cyber Essentials program ties government contracts to vendor certification, driving local provider demand. Australia's REDSPICE initiative allocates AUD 2 billion to a sovereign cloud for the intelligence community, illustrating how policy translates directly into cybersecurity outlays. Vendors now localize R&D centers and SOCs to preserve market access, while homegrown specialists gain a compliance-driven edge.

Scotts International. EU Vat number: PL 6772247784

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

www.scott-international.com

5G Roll-Outs Creating New Network Threat Surfaces for Telcos in Japan, South Korea and India

High-throughput 5G architectures introduce micro-slicing and edge-compute nodes that traditional perimeter tools cannot secure. Japan's Active Cyber Defense law authorizes pre-emptive disruption of cyber threats targeting telecom networks. South Korea logged 1.56 million hacking attempts on public networks in 2024, 80% aimed at 5G and IoT endpoints. India's operators report that 57% of breaches result in service slowdowns, highlighting the urgency for zero-trust and AI-driven analytics. Consequently, demand is rising for secure access service edge (SASE) platforms and virtualized firewalls optimized for carrier environments.

Acute Cybersecurity Talent Shortage Inflating Service Costs in Emerging APAC Economies

The region accounts for 2.8 million unfilled cyber roles, restricting managed-service scalability and pushing salaries beyond SME budgets. The Philippines counts only 200 certified specialists versus Singapore's 3,000, amplifying project delays. Vietnam earmarked USD 100 million for workforce programs to train 1,000 experts and 5,000 engineers by 2025. Scarcity is most severe in OT security and cloud architecture, forcing enterprises to outsource functions or postpone deployments, dampening addressable demand.

Other drivers and restraints analyzed in the detailed report include:

Surge in Digital-Payment and E-Commerce Fraud Driving Security Investments in Southeast Asia
Escalating State-Sponsored Attacks on APAC Critical Infrastructure Stimulating OT Security Adoption
Fragmented Regional Compliance Regimes Complicating Solution Standardization

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

Segment Analysis

Solutions retained 57.05% revenue in 2025, yet managed security services are projected to expand 20.86% CAGR through 2031 as enterprises confront staffing gaps. The APAC cybersecurity market favors providers that bundle 24/7 SOC monitoring, threat hunting, and incident response under outcome-based SLAs. Ensign InfoSecurity became the only APAC firm to reach the global top-10 MSSP list in 2024, signaling the region's ascent in managed-service maturity.

Rising wages for in-house analysts, coupled with board-level accountability for breaches, push even large enterprises to co-manage security tools with external SOCs. AI-assisted triage and automation enable MSSPs to serve mid-market clients profitably, widening adoption. As a result, investment in platform-based service delivery is accelerating, with providers embedding XDR, SOAR, and machine-learning analytics to differentiate.

On-premise installations held 61.88% of APAC cybersecurity market share in 2025 because regulated sectors still favor physical control over data. Cloud-native security, however, is growing at 22.8% CAGR, propelled by remote-work mandates and multi-cloud adoption. A HashiCorp survey showed 70% of regional firms hit business targets via multi-cloud, with 90% rating security the defining success factor.

Organizations are embracing zero-trust networking and container security to protect workloads that span CSPs and edge nodes. Skills shortages remain a headwind-31% cite limited cloud expertise-but vendors counter with low-code policy orchestration and managed SASE offerings. Consequently, cloud deployments increasingly win green-field projects, while hybrid architectures emerge as a transition path for legacy systems.

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

The APAC Cybersecurity Market Report Segments the Industry Into 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 (Small and Medium Enterprises (SMEs), and Large Enterprises), and Country.

List of Companies Covered in this Report:

Cisco Systems, Inc. IBM Corporation Huawei Technologies Co., Ltd. Palo Alto Networks, Inc. Check Point Software Technologies Ltd. Fortinet, Inc. Kaspersky Lab Broadcom, Inc. (Symantec Enterprise Division) BAE Systems plc NEC Corporation Infosys Limited Tata Consultancy Services Limited Darktrace plc Zscaler, Inc. CrowdStrike Holdings, Inc. F5, Inc. Sophos Ltd. Okta, Inc. SentinelOne, Inc. Rapid7, Inc. Imperva, Inc

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 LANDSCAPE

4.1 Market Overview

4.2 Market Drivers

4.2.1 Government Data-Sovereignty Mandates Accelerating Domestic Cybersecurity Spend Across APAC

4.2.2 5G Roll-Outs Creating New Network Threat Surfaces for Telcos in Japan, South Korea and India

4.2.3 Surge in Digital Payments and E-commerce Fraud Driving Security Investments in Southeast Asia

4.2.4 Escalating State-Sponsored Attacks on APAC Critical Infrastructure Stimulating OT Security Adoption

4.2.5 SME Cloud Migration Wave Necessitating Cloud Workload Protection in China and ASEAN

4.2.6 National Cybersecurity Incentive Programs (e.g., SG Cyber Safe, REDSPICE) Catalyzing Market Growth

4.3 Market Restraints

4.3.1 Acute Cybersecurity Talent Shortage Inflating Service Costs in Emerging APAC Economies

4.3.2 Fragmented Regional Compliance Regimes Complicating Solution Standardization

4.3.3 High Price Sensitivity Among APAC SMEs Limiting Adoption of Advanced Solutions

4.3.4 Supply-Chain Disruptions from Export Controls on Security Hardware Components

4.4 Evaluation of Critical Regulatory Framework

4.5 Value Chain Analysis

4.6 Technological Outlook

4.7 Porter's Five Forces

4.7.1 Bargaining Power of Suppliers

4.7.2 Bargaining Power of Buyers

4.7.3 Threat of New Entrants

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

- 4.7.4 Threat of Substitutes
- 4.7.5 Competitive Rivalry
- 4.8 Key Use Cases and Case Studies
- 4.9 Impact on Macroeconomic Factors of the Market
- 4.10 Investment Analysis

5 MARKET SEGMENTATION

- 5.1 By Offering
 - 5.1.1 Solutions
 - 5.1.1.1 Application Security
 - 5.1.1.2 Cloud Security
 - 5.1.1.3 Data Security
 - 5.1.1.4 Identity and Access Management
 - 5.1.1.5 Infrastructure Protection
 - 5.1.1.6 Integrated Risk Management
 - 5.1.1.7 Network Security Equipment
 - 5.1.1.8 Endpoint Security
 - 5.1.1.9 Other Services
 - 5.1.2 Services
 - 5.1.2.1 Professional Services
 - 5.1.2.2 Managed Services
- 5.2 By Deployment Mode
 - 5.2.1 On-Premise
 - 5.2.2 Cloud
- 5.3 By End-User Vertical
 - 5.3.1 BFSI
 - 5.3.2 Healthcare
 - 5.3.3 IT and Telecom
 - 5.3.4 Industrial and Defense
 - 5.3.5 Manufacturing
 - 5.3.6 Retail and E-commerce
 - 5.3.7 Energy and Utilities
 - 5.3.8 Manufacturing
 - 5.3.9 Others
- 5.4 By End-User Enterprise Size
 - 5.4.1 Small and Medium Enterprises (SMEs)
 - 5.4.2 Large Enterprises
- 5.5 By Country
 - 5.5.1 China
 - 5.5.2 Japan
 - 5.5.3 India
 - 5.5.4 South Korea
 - 5.5.5 Australia and New Zealand
 - 5.5.6 Singapore
 - 5.5.7 Rest of Asia Pacific

6 COMPETITIVE LANDSCAPE

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

6.1 Market Concentration

6.2 Strategic Moves

6.3 Market Share Analysis

6.4 Company Profiles {(includes Global level Overview, Market level overview, Core Segments, Financials as available, Strategic Information, Market Rank/Share for key companies, Products and Services, and Recent Developments)}

6.4.1 Cisco Systems, Inc.

6.4.2 IBM Corporation

6.4.3 Huawei Technologies Co., Ltd.

6.4.4 Palo Alto Networks, Inc.

6.4.5 Check Point Software Technologies Ltd.

6.4.6 Fortinet, Inc.

6.4.7 Kaspersky Lab

6.4.8 Broadcom, Inc. (Symantec Enterprise Division)

6.4.9 BAE Systems plc

6.4.10 NEC Corporation

6.4.11 Infosys Limited

6.4.12 Tata Consultancy Services Limited

6.4.13 Darktrace plc

6.4.14 Zscaler, Inc.

6.4.15 CrowdStrike Holdings, Inc.

6.4.16 F5, Inc.

6.4.17 Sophos Ltd.

6.4.18 Okta, Inc.

6.4.19 SentinelOne, Inc.

6.4.20 Rapid7, Inc.

6.4.21 Imperva, Inc

7 MARKET OPPORTUNITIES AND FUTURE OUTLOOK

7.1 White-space and Unmet-Need Assessment

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

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

Market Report | 2026-02-09 | 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="2026-02-26"/>
		Signature	

Scotts International. EU Vat number: PL 6772247784

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

www.scotts-international.com

