APAC IoT Security - 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 APAC IoT Security Market is expected to register a CAGR of 38.67% during the forecast period.

Key Highlights
- The Asia-Pacific region has surfaced as a manufacturing hub, owing to the low production costs in emerging countries such as India and China, which remain a significant market in Asia Pacific's IoT security market. Investments are being planned for the quality of growth, addressing environmental concerns, and reducing overcapacity. The region's automotive industry has emerged as one of the world's largest and is expected to grow further over the next five years.
- India is the fastest-growing economy in the world, and generating enough energy is the key to achieving developmental ambitions that support expansion. The country is regarded as a newly industrialized landscape, becoming a preferred manufacturing hub. India is far superior to many nations in manufacturing medical drugs and products.
- Cyber attackers took advantage of the conditions created by the COVID-19 pandemic in the region and targeted sectors like hospitals, medical and pharmaceutical manufacturers, and other companies. According to the latest IBM X-Force Threat Intelligence Index report, Asia saw a high volume of attacks on finance and insurance organizations last year, accounting for 34% of all attacks on this industry.
- APAC is one of the fastest-growing regions in digital transformation and internet penetration and has experienced exponential growth in financial technology and e-commerce, resulting in a rising demand for Internet and broadband services. This change has brought many benefits and has a lot of potential for the future, but it has also opened the door to a large number of cybersecurity threats, which is driving the growth of the market.
- The rise in connectivity between companies in the region has exposed vulnerabilities in hardware and software environments, giving cybercriminals greater attack surfaces to exploit. This includes employees' smaller, personal IoT devices, which can provide a potential backdoor into more well-protected systems. Further, several countries have attempted to impose data protection and

breach notification laws. However, as a whole, cybersecurity regulation in Asia-Pacific is still in the early phases of development and tends to focus mainly on critical infrastructure and regulated industries.

APAC IoT Security Market Trends

Emergence of Smart City and Smart Home Developments to Drive the Market Growth

Increasing government focus on smart cities, smart buildings, and Industry 4.0 initiatives is driving the demand for digital IoT solutions in the Asia-Pacific region, such as in public transportation, eGovernment, smart traffic management systems, and smart power grids. The integration of edge-computing networks with IoT systems and narrow-band (NB) IoT deployments, along with rising investments in 4G/LTE and 5G, reduced IoT sensor costs, and governmental support, are fueling the growth of the market in the region.

- 5G is expected to accelerate the adoption of smart home IoT devices in the region. Companies such as China Mobile International (CMI) are supporting the transition to 5G with a global digital infrastructure encompassing more than 70 international cables, including various self-built submarine cables and invested terrestrial cables, with a total network capacity of over 98 terabits per second. It also has more than 180 overseas points of presence on key continents, 340 data centers in China, and four data centers that it owns in key centers outside of China.
- Government investment in smart cities accounts for almost one-third of the region's combined spending, followed by logistics, transportation, and manufacturing. Various governments in the region are promoting the adoption of "smart cities." According to the Government Technology Agency, a statutory board of the Singapore government, in the last year, the Singapore government planned to spend 13% of their ICT spending on accelerating the adoption and deployment of Artificial Intelligence (AI) for the public sector and 70% on transforming, integrating, and streamlining digital services. The planned ICT spending for the last year was USD 2.8 billion.
- However, the resource-constrained nature of various IoT devices in a smart home environment, such as meters, thermostats, and entertainment units, does not permit the implementation of standardized security solutions. Therefore, smart homes are currently vulnerable to security threats.

Also, the rise of high-tech smart devices that store and share personal information poses a serious threat to people's privacy in the region. Existing privacy laws don't do enough to deal with this problem, which could slow the growth of the smart home market in the region as a whole.

China Witnesses Significant Growth Opportunities in the Market

- The significant factors for the growth of the IoT security market in China are the high adoption of advanced technologies, increasing cyberattacks, and a growing number of connected devices in the country. The country is one of the dominant regions for IoT deployment. Other factors include the growth of digitalization and IoT security spending in the region.
- The Chinese Ministry of Industry and Information Technology published guidelines for creating a security standard system for the Internet of Things. The guidance seeks to outline a framework that will promote public network security risk mitigation and prevention, along with developing and implementing standards for the IoT. MIIT has a list of standard requirements that includes things like software security, access authentication, and data security.
- Companies such as China Mobile International (CMI) are also building an ecosystem to help industry partners capitalize on the flourishing market for smart solutions, with an initial focus on elevating the smart home experience for consumers. CMI develops

and delivers international data services and solutions that lay the foundation for the rapid growth of IoT across key markets. CMI has provided IoT solutions to over 100 enterprises in 20 countries and regions, primarily in Asia Pacific, as of October last year. This can promote IoT connectivity and eSIM platform integration, enhancing IoT network capabilities around the world.
- The Chinese government informed companies last September about increased cyber-data security oversight on connected vehicles. According to the Ministry of Industry and Information Technology, the companies were asked to establish data security management systems and regularly assess risks from network attacks.

APAC IoT Security Industry Overview

The Asia-Pacific Internet of Things (IoT) Security Market is fragmented with a few major players, such as Symantec Corporation, IBM Corporation, FireEye Inc., Intel Corporation, and Infineon Technologies, as well as various established international brands, domestic brands, and new entrants that form a competitive landscape. Some major players are increasingly seeking market expansion through strategic mergers and acquisitions, innovation, and increased investments in research and development.

In November 2022, Truvisor announced a partnership with Vectra AI, a security AI-driven hybrid cloud threat detection and response solution provider. The Vectra platform and services include public cloud, SaaS applications, identity systems, and on-premises and cloud-based network infrastructure. Through the partnership, the company would be able to sell its products and services through the resellers of Truvisor in Singapore, Indonesia, and Thailand.

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 Value Chain Analysis
4.3 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 Assessment of the Impact of COVID-19 on the Market

5 MARKET DYNAMICS
5.1 Market Drivers

5.1.1 Increasing Number of Data Breaches
5.1.2 Emergence of Smart Cities
5.2 Market Restraints
5.2.1 Growing Complexity among Devices, coupled with the Lack of Ubiquitous Legislation

6 MARKET SEGMENTATION
6.1 Type of Security
6.1.1 Network Security
6.1.2 Endpoint Security
6.1.3 Application Security
6.1.4 Cloud Security
6.1.5 Other types of security
6.2 Solutions
6.2.1 Identity Access Management (IAM)
6.2.2 Intrusion Prevention System (IPS)
6.2.3 Data Loss Protection (DLP)
6.2.4 Unified Threat Management (UTM)
6.2.5 Security & Vulnerability Management (SVM)
6.2.6 Network Security Forensics (NSF)
6.2.7 Other solutions
6.3 Applications
6.3.1 Home Automation
6.3.2 Wearables
6.3.3 Manufacturing Process Management
6.3.4 Patient Information Management
6.3.5 Supply Chain Operation
6.3.6 Customer Information Security
6.3.7 Other applications
6.4 End-User Verticals
6.4.1 Healthcare
6.4.2 Manufacturing
6.4.3 Utilities
6.4.4 BFSI
6.4.5 Retail
6.4.6 Government
6.4.7 Other end-user verticals
6.5 Geography
6.5.1 China
6.5.2 India
6.5.3 Japan
6.5.4 Other countries

7 COMPETITIVE LANDSCAPE
7.1 Company Profiles
7.1.1 Symantec Corporation (NortonLifeLock Inc)
7.1.2 IBM Corporation
7.1.3 FireEye Inc.

7.1.4 Intel Corporation
7.1.5 Infineon Technologies
7.1.6 Trend Micro Inc.
7.1.7 Sophos Group PLC
7.1.8 ARM Holdings PLC
7.1.9 Wurldtech Security Technologies Inc.
7.1.10 Gemalto NV

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

SCOTTS INTERNATIONAL

APAC IoT Security - 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*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-28
		Signature