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

Market Report | 2024-02-17 | 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 Cybersecurity Market size is estimated at USD 65.28 billion in 2024, and is expected to reach USD 124.05 billion by 2029, growing at a CAGR of 13.70% during the forecast period (2024-2029).

Due to the advent of IoT and the growing speed and scope of digital transformation in this region, the current network infrastructure is becoming more exposed to cyberattacks. Internet, social media, and mobile users have all seen significant increases in recent years, contributing to the region's strong rise in cybersecurity. The Asia-Pacific cybersecurity industry is expected to expand even more due to the increasing severity of these attacks and strict government laws.

Key Highlights
-The growing internet usage in both developed and developing countries increases the adoption of cybersecurity solutions. Additionally, due to increased data susceptibility brought on by the expansion of the wireless network for mobile devices, cybersecurity has become a crucial component of every organization.
-Many emerging countries, such as India, China, Singapore, and Japan, face increasing cybersecurity-related issues. India ranks third in the number of DNS hijacks, indicating a sharp rise in cybercrime registration. Additionally, Asia received 26% of all worldwide attacks in 2021, according to IBM X-Force Threat Intelligence Index 2022, making it the most attacked area globally. India tops the list of the most frequently attacked country in Asia. Recent research by the Australian Cyber Security Growth Network entitled the cybersecurity sector might triple in size over the next ten years.
-Although there have been several cybersecurity events in recent years, most of them have remained hidden. Recent high-profile incidents that significantly impacted many common persons have brought public conversation and government and regulatory body attention to the forefront. For Instance, CERT-In, India's official cybersecurity organization, issued a direction relating to Information security practices, procedures, prevention, response, and reporting of cyber incidents for safe and trusted internet to

impose stringent cybersecurity reporting requirements. It stated that India had recorded over 2.12 lakh cybersecurity incidents as of February 2022.

-The industry is being driven by new business models and applications as well as reducing device costs, such as an increasing number of connected devices, including consumer electronics, connected cars, factories, etc., which is driving the adoption of IoT and strengthening cybersecurity in enterprises. So, The adoption of M2M/IoT connections drives the cybersecurity market.

-Low preparedness and a high reliance on conventional authentication techniques are challenging. In a market environment where security professionals advise identity-management solutions like facial recognition and biometric identification, more than 80% of organizations still rely solely on usernames and passwords for login, which could challenge growth.

-The APAC cybersecurity market is anticipated to grow significantly as a result of the recent COVID-19 outbreak because of the rising trend of cyberattacks involving malware and ransomware in the context of COVID-19, which is forcing the organizations to adopt cybersecurity solutions as many of them have switched to remote work environments amid lockdown in various countries.

-As more people use cloud-based services during this pandemic and operate in unfamiliar, less secure environments, this is becoming a hotspot for cyberattacks. According to Barracuda Sentinel, email threats linked to COVID-19 have grown by 67%. As a result, cloud-based cybersecurity solutions are essential during this pandemic and are predicted to develop.

Asia Pacific Cyber Security Market Trends

Cloud Deployment Drives Market Growth

- The increasing realization among companies about the importance of saving money and resources by moving their data to the cloud rather than building and maintaining new data storage drives the demand for cloud-based solutions, hence increasing the adoption of on-demand security services.
- Owing to these benefits, large enterprises and SMEs in the region are increasingly adopting cloud-based solutions. Over the next few years, cloud platforms and ecosystems are expected to serve as the launch pad for an explosion in the pace and scale of digital innovation.
- Countries in the Asia-Pacific tend to have higher percentages of their infrastructures hosted in the cloud rather than on-premise, according to the CISCO Cybersecurity report. Additionally, in March 2023, during the Cisco India Summit 2023, the company announced that it has been growing its cyber security capabilities to support Indian businesses in strengthening their security resilience and utilizing digitalization as a competitive advantage and to provide its clients with better security options, Cisco has been establishing a new data center in Chennai and modernizing the one that already exists in Mumbai.
- With the rising adoption of cloud services, like Google Drive, Dropbox, and Microsoft Azure, and with these tools emerging as an integral part of business processes, enterprises must deal with security issues, such as losing control over sensitive data. This gives rise to the increased incorporation of on-demand cyber-security solutions.
- The company, such as Microsoft in the region, offers Cloud-based endpoint protection technology that enables employees to work when, where, and how they need to function and can allow them to use the devices and apps they find most beneficial to get their work done.

China to Occupy the Largest Market Share

- Growing cyber-attacks in the country have propelled China to strengthen its defensive capabilities. The government is also a major source of cyberattacks in other parts of the world. According to the statistics provided by Cloudflare, in March 2022, China accounted for 45% of the world's cyberattack incidents.
- The increasing initiatives by the government and the related regulatory bodies to strengthen cloud security are expected to fuel

the adoption of cyber security-based solutions over the forecast period.
- The Cyberspace Administration of China issued new measures for cybersecurity review in January 2022 for critical information infrastructure operators (CIIO) purchasing network products and services, which may influence national security. Under this measure, Important communications products, high-performance computers or servers, mass storage equipment, large database or application, cloud computing service, or any other network product or service that has an important influence on the security of any critical information infrastructure, CIIO should apply to Cybersecurity Review Office (CRO) for cybersecurity review.
- Moreover, encryption has met greater resistance in China. The government's encryption regulations and implementation are among the most restrictive in the world, giving the government full access to all encrypted content within its domestic territory. Article 31 of China's Cryptography Law allows the State Cryptography Administration to inspect and access encrypted systems. Since conversations are not end-to-end encrypted, this rule applies to all industries, including social media platforms like WeChat, which are required (and able) to turn over all user data.
- Owing to technological advancements, there is an increase in the number of connected devices in China. It is the world's largest Internet of Things (IoT) market. Furthermore, 5G and 5G enabled devices will exponentially increase the devices' interconnectivity. As a result, it increases connected devices, directly augmenting the market's need for security products.

Asia Pacific Cyber Security Industry Overview

The Asia-Pacific cybersecurity market is moderately fragmented. Players in the market adopt strategic initiatives such as mergers and acquisitions, partnerships, and new product offerings due to increasing awareness regarding mobility security among enterprises.

- February 2022: The IBM Security Command Center in India, for which investments were made on the aforementioned date, represents a sizeable investment in security incident response and training for organizations throughout the Asia-Pacific. It is designed to prepare everyone from the C-Suite to technical staff by training cybersecurity response techniques through highly realistic, simulated cyberattacks. The investment also includes a brand-new Security Operation Center (SOC), which would be added to IBM's extensive worldwide network of SOCs and would offer clients all over the world round-the-clock security response services.

Additional Benefits:

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

Table of Contents:

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

Market Report | 2024-02-17 | 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	