ASEAN Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 139 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 ASEAN Cyber Security Market size is estimated at USD 5.51 billion in 2025, and is expected to reach USD 12.20 billion by 2030, at a CAGR of 17.24% during the forecast period (2025-2030).

Key Highlights
- Organizations, employees, and assets in the ASEAN region are increasingly threatened by cyberattacks. As these attacks become more frequent and sophisticated, and as corporate networks grow more complex, the demand for a variety of cybersecurity solutions has surged.
- Mobile internet usage is on the rise in ASEAN nations. With more people accessing digital services via mobile devices, the urgency to secure these applications and networks has heightened. According to GSMA, Indonesia's subscriber penetration is projected to jump from 66% in 2023 to 77% by 2030.
- As cyberattacks, including ransomware, phishing, and data breaches, evolve in sophistication, organizations are heightening their vigilance. The Indonesian government, through regulations like Presidential Regulation No. 47 of 2023, is emphasizing a National Cyber Security Strategy and Cyber Crisis Management. This aims to strengthen the nation's cybersecurity and adeptly handle cyber crises. With regional industries prioritizing compliance and customer data protection, the demand for cybersecurity services in Indonesia has become paramount.
- The ASEAN region is witnessing a boom in IT investments alongside a surge in smartphone and internet adoption. Yet, the region grapples with significant cybersecurity challenges, leaving it vulnerable to hacker exploits. As the Internet of Things (IoT) proliferates, the demand for robust cybersecurity measures intensifies. However, the shortage of cybersecurity professionals threatens to stifle the market's growth. With high internet penetration and comparatively low cybersecurity spending, the region stands out as a prime target for cybercriminals.
- Geopolitical tensions, notably the Russia-Ukraine conflict, ripple through ASEAN's cybersecurity realm. With global unrest

escalating, the shadow of state-sponsored cyberattacks looms, endangering the digital framework. Confronted with this intensified threat landscape, regional organizations are driven to strengthen their cybersecurity defenses against potential assaults and geopolitical cyber challenges.

ASEAN Cybersecurity Market Trends

Cloud Expected to Witness Major Growth

- Cloud-based cybersecurity solutions are experiencing increased adoption due to their scalability, flexibility, platform centralization, accessibility, and cost-effectiveness. The growing reliance of the global workforce on remote and mobile capabilities further drives the demand for these solutions. Cloud-based systems enable secure access and monitoring from any location, meeting the requirements of modern, flexible work environments.
- Key trends influencing cloud adoption include the rise of multi-cloud and hybrid strategies, the prominence of cloud-native security, integration with DevOps practices, increased automation and orchestration, cloud analytics, and threat intelligence. For example, US investments in Malaysia's cloud infrastructure are steadily growing. A recent USD 6.5 billion investment by a US company aims to establish a new public cloud region, providing Malaysian businesses with access to advanced AI infrastructure. This includes patented generative AI agents and high-performance AI supercomputers powered by US-manufactured GPUs. These developments align with Malaysia's national cloud policy, which seeks to position the country as a hub for digital innovation.
- In May 2024, Microsoft Corporation announced a USD 2.2 billion investment to enhance Malaysia's cloud and AI capabilities. This initiative includes building digital infrastructure, launching AI training programs, establishing a national AI Centre of Excellence, and strengthening cybersecurity measures. Microsoft's commitment reflects its vision of transforming Malaysia into a central hub for cloud computing and generative AI while boosting the nation's productivity and economic growth.
- In Thailand, industries ranging from large corporations to small and medium-sized enterprises (SMEs) are increasingly adopting cloud-based cybersecurity solutions. This trend is driven by the solutions' scalability, flexibility, platform centralization, accessibility, and cost-effectiveness. Leading global players such as Google, Microsoft, AWS, and Alibaba Cloud have made significant investments in Thailand's cloud infrastructure market.
- The growth of the SMEs and their prefer cloud deployment as it allows them to focus on their core competencies rather than invest their capital in security infrastructure since they have limited cybersecurity budgets. For instance, In Thailand, the entrepreneurial sentiment index for micro, small, and medium enterprises (MSMEs) stood at approximately 53 points in the second quarter of 2024, as reported by the Office of Small and Medium Enterprises Promotion.

BFSI Sector to be the Largest End User

- Financial institutions are increasingly digitizing their operations and services, necessitating robust cybersecurity measures. The BFSI sector, managing high-value transactions and sensitive customer data, remains a prime target for cybercriminals.
- Driven by digital transformation, cloud adoption, and the integration of technologies like blockchain and Artificial Intelligence (AI), the industry is witnessing a significant shift in its security measures. With the rise of fintech innovations, the need for agile cybersecurity strategies becomes paramount to safeguard transactions and customer information in this interconnected landscape.
- The surge in digital technologies and online financial services has broadened the attack surface of cyber threats in the BFSI sector. As mobile banking, digital payment platforms, and Online transactions expand, they introduce challenges that demand advanced cybersecurity solutions to combat fraud, data breaches, and other cyber risks. Bank Indonesia reported that Indonesia's e-money transaction volume reached around USD 0.470 million in 2023.

- Banking businesses embracing new technologies for enhanced customer service inadvertently become prime targets for cyberattacks, fueling the demand for diverse cybersecurity solutions. For example, in June 2024, OCBC Indonesia, a publicly listed bank, partnered with Cloudera in its journey to becoming a digital-first bank, aiming to elevate customer banking experiences. Through this collaboration, OCBC Indonesia plans to harness Cloudera's hybrid platform, emphasizing generative AI solutions alongside data management, analytics, and AI capabilities.

ASEAN Cybersecurity Industry Overview

The ASEAN cybersecurity market is fragmented and has some major players who have adopted various growth strategies, such as mergers and acquisitions, new product launches, expansions, joint ventures, partnerships, and others, to strengthen their position in this market. The major players in the market are IBM Corporation, Cisco Systems Inc, Fujitsu Thailand Co. Ltd, Red Sky Digital Ventures Ltd, Info Security Consultant Co. Ltd, among others.

In the competitive landscape of cybersecurity, global and regional players jostle for prominence. Despite the market's steep entry barriers, a wave of new entrants has successfully carved out their niche.

Characterized by moderate to high product differentiation and intense competition, the market sees solutions often bundled, blurring the lines between product and service.

To manage costs, many users are leaning towards annual contracts. Recently, there's been a noticeable shift towards services that promise quicker security updates, driving a surge in demand for cloud-based solutions that offer real-time updates. This trend is particularly favored in the service-oriented sector.

Innovation stands as a key pillar for sustainable competitive advantage. Emerging domains like Big Data and IoT are redefining security paradigms. As software firms eye the market's lucrative potential, a notable uptick in the firm concentration ratio is anticipated during the forecast period.

Additional Benefits:

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

Table of Contents:

ASEAN Cyber Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 139 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	2025-05-06
		Signature