Indonesia Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 138 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 Indonesia Cybersecurity Market size is estimated at USD 1.35 billion in 2025, and is expected to reach USD 3.48 billion by 2030, at a CAGR of 20.79% during the forecast period (2025-2030).

Key Highlights
- Cybersecurity encompasses the strategies and measures implemented to shield organizations, their personnel, and assets from cyber threats. As cyberattacks become more frequent and sophisticated, and as corporate networks grow increasingly intricate, the demand for varied cybersecurity solutions to effectively counter these risks has surged.
- Digitalization and the need for scalable IT infrastructure are major drivers of the cybersecurity market. With a significant portion of the population online, both businesses and the government in Indonesia are turning to digital platforms to boost efficiency and enhance customer service. This uptick in internet engagement, combined with the rapid expansion of the nation's digital economy, underscores the need for a robust IT infrastructure to manage the vast data being generated.
- In the realm of the Internet of Things (IoT), cybersecurity is paramount. A single breach can jeopardize the entire network or, more concerning, provide cybercriminals with unfettered access. Sectors such as government and defense, which handle highly sensitive data through IoT, are particularly vulnerable. An exploited weak entry point or a compromised device could allow hackers to extract crucial intelligence or even cause physical harm. Thus, IoT cybersecurity emphasizes protecting both devices and networks, as well as the data they transmit.
- Indonesia is home to four technology unicorns, each boasting revenues surpassing USD 1 billion. These startups harness the public cloud, reaping benefits like expedited market entry and the smooth integration of AI and machine learning, facilitating rapid expansion.
- While Indonesian organizations are tapping into the advantages of cloud computing, they're grappling with heightened challenges in threat detection and prevention, demanding more time and resources. A 2024 report from Palo Alto Networks

reveals that a staggering 98% of organizations are storing sensitive data in varied locales, from on-premises servers and public clouds to SaaS applications with local storage, third-party hosted private clouds, and multiple endpoints. This diversity underscores the substantial security challenges at hand.
- Indonesia, a rapidly growing economy, is witnessing heightened investments in IT infrastructure alongside a boom in smartphone and internet usage. Yet, the nation grapples with significant cybersecurity challenges, often falling prey to hackers. This vulnerability is further magnified by the expanding number of IoT connections, driving the demand for stringent cybersecurity measures. However, a looming shortage of cybersecurity professionals could stifle the market's growth. With high internet penetration and relatively modest cybersecurity spending, Indonesia stands out as a prime target for cybercriminals.

Indonesia Cyber Security Market Trends

Cloud Segment Sees Significant Expansion in Indonesia

- In Indonesia, cloud technology is becoming a cornerstone of enterprise networks and technological infrastructure, propelling a swift expansion in the nation's IT sector. As Indonesian entities transition their operations to the cloud, they encounter heightened vulnerabilities. These include potential security breaches, inadvertent misconfigurations on cloud platforms, and uneven coverage in identity access management (IAM) and privileged access management (PAM) across various hyperscalers and cloud services.
- Indonesian enterprises are grappling with unprecedented cyber threats and ransomware assaults. These challenges jeopardize organizational integrity and can lead to dire repercussions, such as significant data loss and exposure of sensitive information. Data from Badan Siber dan Sandi Negara highlights the severity: August 2023 marked a peak for Indonesia, with cyber attack-related traffic anomalies hitting approximately 78.46 million.
- Given the escalating risks, combating this digital threat is urgent. Such mounting challenges are poised to attract heightened investments from leading cloud providers and regional cybersecurity firms.
- As reliance on cloud services deepens, the demand for robust cybersecurity measures has surged. Reports from CBN Cloud IT indicate that Indonesia's cloud sector has witnessed a staggering compounded annual growth rate (CAGR) of over 45% over the past five years, outpacing the global average. This explosive growth not only highlights the cloud's ascent in Indonesia but also signals a burgeoning market for cybersecurity solutions. With an increasing number of organizations migrating to the cloud, the imperative for advanced security protocols to shield sensitive data becomes paramount. This trend accentuates the necessity of bolstering cybersecurity infrastructure to fend off potential threats.
- As hybrid and multi-cloud environments gain traction in Indonesia, the intricacies of managing security have intensified. Organizations are diversifying their cloud platform choices, turning to giants like AWS, Google Cloud, and Microsoft Azure, each introducing its own set of security challenges. This complex scenario amplifies the demand for comprehensive cloud security solutions, which include encryption, access control, and monitoring tools to ensure data protection across diverse platforms.

Government and Defense Sectors Lead in Cybersecurity Adoption

- Alongside IT, telecommunications, BFSI, and retail, the government and defense sectors are increasingly adopting advanced cybersecurity solutions. This trend is spurred by government digitalization initiatives and a swiftly evolving threat landscape, propelling market growth.
- As the government rolls out digital technologies for public services, the demand for cybersecurity solutions is set to surge. With a growing number of services transitioning online, there's an escalating need for robust data protection and secure digital infrastructures. Data from Indonesia's Anti-Phishing Data Exchange highlights this urgency: in Q4 2023, government institutions constituted 0.65% of phishing attack targets. This emphasizes the heightened demand for security solutions-be it cloud security,

data protection, or identity access management-all crucial for safeguarding sensitive government data and citizen information from cyber threats.
- In a significant move, the Indonesian government, in January 2024, unveiled plans for nine super-apps, set to launch by Q3 2024. These super-apps will encompass vital public services, including digital IDs, healthcare, education, and social assistance. Such initiatives underscore the government's commitment to its digital strategy, further amplifying the demand for cybersecurity solutions to counter threats and safeguard sensitive data.
- Recognizing this urgency, there's a pronounced emphasis on robust security investments, which not only bolster individual agencies but also catalyze overall market growth. The defense sector mirrors this trend, seeking diverse cybersecurity solutions to shield critical infrastructure and sensitive data. Tools in demand include intrusion detection systems, VPNs for enhanced network security, and advanced endpoint detection and response mechanisms.

Indonesia Cyber Security Industry Overview

The Indonesian cybersecurity market is competitive and fragmented, featuring a mix of international and regional players. These firms can achieve a sustainable competitive edge through innovation. Emerging domains like big data and IoT influence security trends, and we anticipate a rise in the firm concentration ratio during the forecast period. Some of the major players include IBM Corporation, Cisco Systems Inc., Dell Technologies Inc., FUJITSU Limited, and Intel Corporation.

While the market presents significant entry barriers for newcomers, several have successfully carved out a niche. The market is characterized by moderate to high product differentiation and intense competition. Solutions are often bundled, appearing as integral services.

Many users are leaning towards annual contracts to manage costs. Recently, there's been a noticeable shift towards services that promise quicker security updates. This trend has spurred a surge in demand for cloud-based services that enable real-time updates, a preference echoed by the service-based industry.

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 Industry Value Chain Analysis
4.3 Industry Attractiveness - Porter's Five Forces Analysis
4.3.1 Bargaining Power of Suppliers
4.3.2 Bargaining Power of Consumers

4.3.3 Threat of New Entrants
4.3.4 Threat of Substitute Products
4.3.5 Intensity of Competitive Rivalry
4.4 Impact of Macroeconomic Factors on the Market

5 MARKET DYNAMICS
5.1 Market Drivers
5.1.1 Increasing Demand for Digitalization and Scalable IT Infrastructure
5.1.2 Growing M2M/IoT Connections Demanding Strengthened Cybersecurity in Enterprises
5.2 Market Restraints
5.2.1 Lack of Cybersecurity Professionals

6 MARKET SEGMENTATION
6.1 By Offering
6.1.1 Solutions
6.1.1.1 Application Security
6.1.1.2 Cloud Security
6.1.1.3 Data Security
6.1.1.4 Identity and Access Management
6.1.1.5 Infrastructure Protection
6.1.1.6 Integrated Risk Management
6.1.1.7 Network Security Equipment
6.1.1.8 End point Security
6.1.1.9 Other Solutions
6.1.2 Services
6.1.2.1 Professional Services
6.1.2.2 Managed Services
6.2 By Deployment Mode
6.2.1 Cloud
6.2.2 On-Premise
6.3 By Organization Size
6.3.1 SMEs
6.3.2 Large Enterprises
6.4 By End User
6.4.1 BFSI
6.4.2 Healthcare
6.4.3 IT and Telecom
6.4.4 Industrial & Defense
6.4.5 Retail
6.4.6 Energy and Utilities
6.4.7 Manufacturing
6.4.8 Others

7 COMPETITIVE LANDSCAPE
7.1 Company Profiles
7.1.1 IBM Corporation
7.1.2 Cisco Systems Inc.

7.1.3 FUJITSU Limited
7.1.4 Dell Technologies Inc.
7.1.5 Intel Corporation
7.1.6 Fortinet Inc.
7.1.7 AVG Technologies (Avast Software SRO)
7.1.8 Trend Micro Incorporated
7.1.9 Palo Alto Networks Inc.
7.1.10 Xynexis International

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

Indonesia Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2025 - 2030)

Market Report | 2025-04-28 | 138 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	2025-05-08
		Signature	