Malaysia Cybersecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 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 Malaysia Cybersecurity Market is anticipated to grow with a CAGR of 6.2% during the forecast period. A major concern for national security is cybersecurity. Whether through terrorism, criminal activity, or state and industrial espionage, it impacts the public and commercial sectors and covers a broad spectrum of concerns relating to national security. The danger landscape is always changing due to the expanding IT technological advancement and the capabilities of cyber weapons that threaten national security.

Key Highlights
In Malaysia, the vast majority of industries place high importance on cybersecurity. With an allocation of USD 434 million, the Government of Malaysia (GOM) developed the Malaysia Cyber Security Strategy (MCSS) 2020-2024 to improve the nation'snation's cybersecurity preparedness.
Furthermore, During the following five years, the MCSS identifies five strategic pillars as guiding principles for enhancing the nation'snation's cybersecurity management. The first pillar aims to strengthen Malaysia'sMalaysia's vital ICT infrastructure while improving national governance and cybersecurity management. By examining pertinent legislation and creating new cybersecurity regulations, the second pillar seeks to improve existing cybersecurity laws. The remaining pillars include fostering innovation, developing Malaysia'sMalaysia's cybersecurity workforce, and utilizing local, regional, and global collaboration to safeguard cyberspace.
In April this year, The majority of Malaysian organizations anticipate becoming the target of cyberattacks in the upcoming year, with 22% saying it is "extremely likely" to occur. According to cybersecurity company Trend Micro'sMicro's most recent worldwide Cyber Risk Index (CRI) for the second half of last year, 87% of Malaysians reported having been the victim of one or more successful cyberattacks in the previous year. This is anticipated to offer lucrative opportunities for the growth of the studied market.

Further, owing to the COVID-19 pandemic, nation-state cyber activity has witnessed a surge in intensity and an escalation in severity because the traditional tactics to gather intelligence and knowledge were no longer feasible due to the social distancing norms. Additionally, amid the coronavirus-led lockdown, cyber-attacks targeted toward organizations have increased considerably, primarily resulting in a growing demand for skilled cybersecurity professionals and robust solutions.

Organizations rely on diverse professionals to safeguard their systems, employees, and data. Organizations in Malaysia are still looking for talented professionals who can support them against these risks when cyber threats are increasing faster than at any other time in history. A cybersecurity workforce shortage continues to be a problem for businesses of all sizes and industries. The increasing importance of a broader mix of technical and non-technical skills underscores today'stoday's cybersecurity roles are multi-dimensional and increasingly varied across specializations, organizations, and industries.

Malaysia Cybersecurity Market Trends

Identity Access Management will Drive the Market

The rise in cloud services, social and mobile, has reduced the traditional firewall to increasingly outmoded. Digital identity has become crucial to enforcing access controls. As a result, identity and access management are expected to become a priority for modern enterprises.

IAM, which was once viewed as an operational back-office issue, has been gaining board-level visibility following multiple high-level breaches due to the failure of organizations to manage and control user access effectively. The prominence of IAM has been further elevated by an evolving regulatory landscape and trends such as Bring Your Device (BYOD) and cloud adoption. The risks related to access to information and data have also increased.

The impact of an identity-related cybersecurity breach from organized crime, state-sponsored militaries, and others is packed with implications that can impact staff productivity and morale apart from substantial financial and potential life losses and further damage the IT network and company reputation. These risks demand a new level of identity and access management solutions.

The changing business processes brought millions of new devices into the network, demanding effective access management solutions to protect IP and sensitive data from breaches. In the past years, companies have been investing significantly in IAM solutions to perform job that is out of reach for humans since hackers and malicious employees are primarily unknown and can inflict massive damage to the inside of an organization.

As IAM centralizes authorization and authentication, it is a prime candidate to track all access securely for Blockchain platforms. This is often needed for compliance reasons and helps the enterprise detect and prevent fraud. An audit trail entry is logged each time a user logs in or requests specific permissions in a particular context. According to the Ministry of Communication and Multimedia Malaysia, last year, The number of fraud incidents that occurred in the region was more, with 7,098 reported incidents, followed by intrusion with 1,410 reported incidents and Malicious Codes with 648 incidents.

Manufacturing is One of the Sector Driving the Market

To improve overall operational efficiency and lower production costs, every manufacturing industry sector, including automotive, numerous engineering disciplines, power systems, consumer goods, and chemicals, have embraced digital technologies. Due to the sectors' efforts to collect data and use it for analytics to prevent downtime and keep the manufacturing sector functioning 24/7, M2M communication and networking have increased.

Industrial equipment is built to last, with machinery being expensive, cumbersome, and costly to replace. Although IoT offers several positive facets to the industry, these innovations are often incorporated gradually within existing assembly lines, as gaps between legacy and modern industrial devices are prime targets for hackers.

The workplace shift caused by COVID-19 has altered how work is carried out. With assembly lines managed on the cloud or remotely, Internet usage increased exponentially. This transition, albeit necessary, was rushed due to the pace and intensity of the pandemic, leaving several companies needing to establish security guidelines for their machine operations.
The convergence of operational and information technology impacts industrial control systems (ICS) security, supervisory control, and data acquisition (SCADA) systems. The designs are exposed to increasing threats and targets for hackers involved in terrorism, cyber warfare, and espionage. According to the department of statistics, Malaysia's manufacturing production increased by 52% from March to June.
Increasingly connected and automated industrial devices with wider networks of industry 4.0 offer broader surfaces for attack. Reliable industry 4.0 cybersecurity, smart manufacturing, and other industrial operations can help prevent the pipeline from stalling during a procedure. Legacy devices need to have proactive real-time prevention. They can be a foothold for attackers to propagate throughout the network, as older equipment augmented with connectivity generally lacks on-device monitoring capabilities to ensure IoT network security.

Malaysia Cybersecurity Market Competitor Analysis

The Malaysian cybersecurity market is moderately consolidated, with the presence of a few major companies. The companies continuously invest in strategic partnerships and product developments to gain market share. Some of the recent developments in the market are:

In April 2022, A partnership between IBM Malaysia Sdn Bhd and Tech Mahindra was finalized to increase the cybersecurity services available to Malaysian businesses, including managing security compliance and enhancing commercial information systems. Tech Mahindra and IBM will co-develop cutting-edge goods and services and improve current ones as part of this collaboration. These solutions include Guardium, Cloud Pak for Security, and QRadar XDR (threat detection and response).

In February 2022, To raise awareness among Malaysian businesses about the value of protecting mobile applications and Internet of Things systems, SecIron and Cybersecurity Malaysia (CSM) have formed a strategic partnership. Section and CSM will collaborate closely to promote industry best practices for businesses to lessen the effects of cyberattacks and raise awareness about mobile application security and data protection.

Additional Benefits:

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

Table of Contents:

Malaysia Cybersecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2023 - 2028)

Market Report | 2023-01-23 | 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