

Thailand Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

Market Report | 2024-02-17 | 115 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 Thailand Cybersecurity Market size is estimated at USD 446.00 million in 2024, and is expected to reach USD 871.71 million by 2029, growing at a CAGR of 14.10% during the forecast period (2024-2029).

The increasing usage of software solutions, Internet, and connected devices across the end-user industries in Thailand, in line with the country's priority on developing a digital economy, infrastructural development for high-speed Internet, growth of online banking services, and the demand for cloud-based software, are raising the risk of cyber attacks in Thailand is driving the requirement of cyber security solutions in the country, which may fuel the market's growth.

The country has been prioritizing developing frameworks for making its digital economy cyber-resilient; however, the lack of skilled cyber security personnel makes it a challenge for the stakeholders of the cyber security market and may lower the market's growth during the forecast period. For instance, in September 2023, the Secretary General of the National Cyber Security Agency (NCSA) highlighted a significant talent gap in Thailand's cybersecurity workforce, mentioning that only 0.5% of Thai bureaucrats are in the IT field and an even more minor fraction work in cybersecurity, which may impact the country's objective in strengthening national cybersecurity. This lack of a cyber security workforce may affect the growth of cyber security solutions as, without skilled cyber security personnel, the market may witness a significant shortage in implementing cyber security solutions during the forecast period.

The widespread shift in multiple industries toward digital transformation has driven companies to reassess their cybersecurity measures. As the country adopts digital transformation across various sectors, organizations recognize the critical requirement to safeguard their digital assets against growing cyberattacks. This surge in demand may be attributed to the widespread adoption of digital technologies, including cloud computing, big data, and the Internet of Things (IoT), which has expanded the attack

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

surface and increased the complexity of safeguarding sensitive information.

The widespread adoption of a cloud-first strategy is driving the need for robust cybersecurity measures in Thailand. As organizations migrate their operations and data to cloud environments to enhance scalability and flexibility, they face distinctive security challenges. The inherent risks associated with cloud computing, including data breaches, unauthorized access, and compliance issues, have propelled the demand for specialized cloud security solutions. Adopting a cloud-first strategy necessitates cybersecurity measures that can secure data in transit, protect cloud infrastructure, and ensure robust identity and access management in the cloud. The cybersecurity market in Thailand is actively responding to these challenges by offering tailored solutions to address the complexities of cloud security, reflecting the industry's adaptability to evolving technology trends.

The need for qualified and experienced cybersecurity specialists has increased as the digital landscape evolves and cyber threats get more complex. The need for more skilled professionals in this field hinders the effective implementation and management of cybersecurity solutions, creating a bottleneck that impacts the overall cybersecurity market in Thailand.

The growth of digital payments in Southeast Asian countries, including Thailand, has emerged due to the growth of online banking services and the growth of online transactions, which has raised the risk of cyber attacks on the digital infrastructure of these payment activities in the country, increasing the demand for cyber security solutions during the forecast period.

In the post-pandemic period, the growth of online payments in the country and other online-based business activities has raised the risk of breaching network, infrastructure, cloud, and data security by the cyber attacks, fueling the demand for cyber security market in the country after the pandemic. For instance, in March 2023, Thailand's government introduced new Cybercrime Measures for Banks and other Service Providers to minimize cybercrimes in the country by providing legal measures applying to offenders, which shows the increasing governmental priority in the cybersecurity sector after the pandemic, supporting the market's growth in the future.

Thailand Cybersecurity Market Trends

Cloud Security to Register Major Growth

- The cloud security demand in the Thailand cybersecurity market is driven by the considerable presence of cloud regions and the evolving regulatory landscape, coupled with high growth in cloud migration among businesses, which requires new approaches to ensure that data remains secure across online infrastructure, applications, and platforms.
- Cloud computing has transformed how public and private sector organizations in the country use, share, and store data, applications, and workloads. However, it has also introduced new security threats and challenges to organizations. Moreover, significant data going into the cloud and public cloud services further increase the exposure, thus positively driving the demand for cloud security solutions. Moreover, as organizations across the country shift workloads to the cloud rapidly, data protection, loss of visibility, and control are emerging as major concerns, driving the demand for cloud security solutions.
- The country is at the forefront of cloud adoption, augmented by the end-user drive for digitalization and government initiatives such as cloud-first policy. The country's government is partnering with cloud vendors such as Google and Microsoft to facilitate governmental agencies using public cloud providers as part of the country's cloud-first policy. Such initiatives are further expected to bolster the adoption of cloud security solutions in government institutions as well as private end-user businesses of the country.
- Furthermore, cloud market vendors such as Google, Microsoft, and AWS have launched cloud regions in the country to bring the power and benefits of cloud services closer to businesses and organizations in Thailand, enabling them to leverage advanced cloud technologies for their digital transformation initiatives. However, as businesses in the country continue to migrate to the

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

cloud per the Thai government's cloud-first policy, understanding the security requirements for keeping data, applications, and platforms safe is becoming increasingly crucial. Thus, such developments are analyzed to result in significant demand for cloud security solutions in the country's end-user businesses during the forecast period.

- According to the Digital Economy Promotion Agency (DEPA), the market value of digital services in Thailand was reported to be THB 346.7 billion (USD 9.91 billion) in 2021. By 2024, this amount is anticipated to reach THB 700 billion (USD 20 billion). Moreover, in 2022, Thailand's digital market value was around THB 2.6 trillion (USD 74 billion). As Thailand's digital economy expands, businesses and government organizations are expected to strengthen their efforts to adopt and implement scalable IT infrastructure, cloud services, and other digital technologies. This increased digital activity further enhances the need for robust cybersecurity measures to protect valuable assets and sensitive information.

BFSI to be the Largest End User

- The BFSI industry in Thailand is witnessing a significant shift in its cybersecurity security measures, primarily driven by factors such as the digital transformation of financial services, cloud adoption, and the integration of advanced technologies like machine learning and artificial intelligence to enhance banking and finance operations. In addition, growing data breaches and cyberattacks in financial firms further necessitate adopting cybersecurity solutions in the country's BFSI sector.

- SurfShark, a secure VPN (Virtual Private Network) service provider in Thailand, published statistics in July 2023 stating that Thailand has been registering a significant number of online account breaches, showing the risk of cyber crimes, fueling the demand opportunity for cyber security solutions in Thailand.

- Furthermore, with the growing technological penetration and digital channels, such as mobile banking, Internet banking, etc., in the country's financial sector, the attack surface for cyber threats in the BFSI sector has expanded. The expansion of mobile banking, digital payment platforms, and online transactions in the country's BFSI sector has created new challenges for cybersecurity, thus driving the demand for advanced cybersecurity solutions to protect against fraud, data breaches, and other cyber risks.

- Moreover, the growth in cyberattacks in banks and financial firms has witnessed a significant rise in the past few years, necessitating the demand for robust cybersecurity measures to protect customer data. For instance, in September 2023, CardX, one of Thailand's major digital financial platforms, disclosed a data leak that exposed their customers' personal information related to personal loan and cash card applications. This information includes the customer's first and last name, address, telephone number, and email.

- Furthermore, the country's BFSI sector is undergoing a significant transformation due to technological advancements, regulatory changes, evolving customer preferences, and the rise of innovative financial models, necessitating the need to safeguard against cyberattacks and data breaches. For instance, banking institutions, including the Bank of Thai (BoT) and commercial bank members of the Thai Bankers' Association (TBA), have been upgrading their digital technology to handle cyber risks and strengthen cybersecurity. Such factors will boost investment in cybersecurity measures in the BFSI sector to guard against cyber risks.

Thailand Cybersecurity Industry Overview

The Thailand cybersecurity market is highly fragmented, with the presence of major players like IBM Corporation, Cisco Systems Inc., Fujitsu Thailand Co. Ltd (Fujitsu Group), Red Sky Digital Co.Ltd, and Check Point Software Technologies Ltd. Players in the market are adopting strategies such as partnerships and acquisitions to enhance their product offerings and gain sustainable competitive advantage.

September 2023 - Fujitsu Limited and Fujitsu Thailand Limited announced the acquisition of Thailand-based SAP consultancy

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Innovation Consulting Services to increase its managed service portfolio in the country, which may further use this expansion to offer cyber security services to the existing customers of the acquired company during the forecast period.

March 2023 - Webex by Cisco achieved Thailand's Electronic Transactions Development Agency (ETDA) certification, a public agency in the Kingdom of Thailand established to develop electronic transactions that are reliable, secure, and safe from cybersecurity threats, which shows the company's priority in offering cyber resilient solutions in the market and enhancing its cyber security solutions offering to support its market growth.

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 Industry Attractiveness - Porter's Five Forces Analysis
 - 4.3.1 Bargaining Power of Suppliers
 - 4.3.2 Bargaining Power of Buyers
 - 4.3.3 Threat of New Entrants
 - 4.3.4 Threat of Substitutes
 - 4.3.5 Intensity of Competitive Rivalry
- 4.4 Impact of Macroeconomic Trends on the Market

5 MARKET DYNAMICS

- 5.1 Market Drivers
 - 5.1.1 Increasing Demand for Digitalization and Scalable IT Infrastructure
 - 5.1.2 Need to Tackle Risks from Various Trends such as Third-party Vendor Risks, the Evolution of MSSPs, and Adoption of Cloud-first Strategy
- 5.2 Market Restraints
 - 5.2.1 Lack of Cybersecurity Professionals
 - 5.2.2 High Reliance on Traditional Authentication Methods and Low Preparedness
- 5.3 Trends Analysis
 - 5.3.1 Organizations in Thailand Increasingly Leveraging AI to Enhance their Cyber Security Strategy
 - 5.3.2 Exponential Growth to be Witnessed in Cloud Security Owing to Shift Toward Cloud-based Delivery Model

6 MARKET SEGMENTATION

- 6.1 By Offering

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

- 6.1.1 Security Type
 - 6.1.1.1 Cloud Security
 - 6.1.1.2 Data Security
 - 6.1.1.3 Identity Access Management
 - 6.1.1.4 Network Security
 - 6.1.1.5 Consumer Security
 - 6.1.1.6 Infrastructure Protection
 - 6.1.1.7 Other Security Types
- 6.1.2 Services
- 6.2 By Deployment
 - 6.2.1 Cloud
 - 6.2.2 On-premise
- 6.3 By End User
 - 6.3.1 BFSI
 - 6.3.2 Healthcare
 - 6.3.3 Manufacturing
 - 6.3.4 Government and Defense
 - 6.3.5 IT and Telecommunication
 - 6.3.6 Other End Users

7 COMPETITIVE LANDSCAPE

- 7.1 Company Profiles
 - 7.1.1 IBM Corporation
 - 7.1.2 Cisco Systems Inc
 - 7.1.3 Fujitsu Thailand Co. Ltd.
 - 7.1.4 Red Sky Digital Ventures Ltd.
 - 7.1.5 Info Security Consultant Co. Ltd.
 - 7.1.6 Dell Technologies Inc.
 - 7.1.7 Fortinet Inc.
 - 7.1.8 CGA Group Co. Ltd.
 - 7.1.9 Intel Security (Intel Corporation)

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Thailand Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

Market Report | 2024-02-17 | 115 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*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>		
Company Name*	<input type="text"/>	EU Vat / Tax ID / NIP number*	<input type="text"/>
Address*	<input type="text"/>	City*	<input type="text"/>
Zip Code*	<input type="text"/>	Country*	<input type="text"/>
		Date	2025-05-05
		Signature	

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com



Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com