India 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:

India's cybersecurity market is expected to register a CAGR of 15.1% over the forecast period. The increasing demand for digitalization and scalable IT infrastructure and the ongoing need to tackle risks from various trends, such as third-party vendor risks, the evolution of MSSPs, and the adoption of a cloud-first strategy, lead to the rising demand for the market.

Key Highlights
The rise in malware and phishing threats among enterprises, the increased adoption of IoT, and the BYOD trend propel the cyber security market forward. Also, the increased demand for cloud-based cybersecurity solutions positively impacts market growth. Increased adoption of mobile device applications and platforms, the need for strong authentication methods, and transformation in the traditional antivirus software industry are expected to provide lucrative opportunities for market expansion during the forecast period.
The Indian government has made cyber security a top priority for national policy, establishing task teams and communicating with the USG to discuss collaboration, information sharing, and enhancing their cyber defense capacity. In the area of cyber security, a bilateral collaboration between India and the United States is progressing favorably. Notably, the government and businesses in India are anticipated to place even greater emphasis on digitalization and IT across all sectors as the country recovers from and acclimates to a post-COVID future.
The demand for Security Information and Event Management (SIEM) technology and services has increased due to the rise in cyberattacks and data breaches across the country. SIEM technology and services gather real-time security events from various data sources and events to identify threats and produce responses to security incidents. Large corporations used to focus their efforts on risk avoidance.
A consequence of the nationwide lockdown in India is a boom in remote working, which has been predominantly supported by cloud computing technologies that enable people to operate effectively anywhere. With the help of cloud services, businesses and

governments can easily handle huge amounts of data.

Cybersecurity requirements are growing faster than the budgets allocated to meet them. Most small businesses need more money and IT security expertise to implement enhanced cybersecurity solutions to protect their networks and IT infrastructures from various cyber-attacks. Limited capital funding can impede some small and medium-sized businesses from embracing the cybersecurity model.

Lastly, to combat the spread of COVID-19, many organizations were forced to implement work-from-home policies. Remote working, on the other hand, increases the risk of various cyber-attacks, such as intrusions, man-in-the-middle (MITM) attacks, and spear phishing, hence leading to a rising demand for cyber hygiene practices to ensure robust security policies and practices amid the COVID-19 pandemic. Also, due to the pandemic crisis, the demand for cybersecurity solutions skyrocketed in healthcare, manufacturing, and government.

India Cybersecurity Market Trends

Rising frequency of target-based cyber attacks

The increasing sophistication of cyber attacks can be attributed to the market's growth. The frequency and severity of cyber scams and crimes have increased over the last decade, resulting in massive losses for businesses across the country. According to cyber security intelligence firm CloudSEK, India witnessed 7.7% of the world's total incidence of cyberattacks on the healthcare sector last year, making it the second-most attacked nation overall.

The primary goal of targeted attacks is to infiltrate the networks of targeted companies or organizations and steal critical information. As a result of these targeted attacks, organizations' business-critical operations suffer in terms of business disruptions, intellectual property loss, financial loss, and the loss of critical and sensitive customer information.

Targeted attacks have grown in popularity in recent years, infiltrating targets' network infrastructure while remaining anonymous. Attackers with a specific goal usually go after endpoints, networks, on-premises devices, cloud-based applications, data, and other IT infrastructures.

Attackers steal personally identifiable information (PII) like names, phone numbers, addresses, driver's license numbers, and social security numbers. This can lead to more security breaches and identity thefts.

Technologies that use AI or ML for threat detection were ranked as the top priority for cybersecurity investment by 32% of poll respondents last year. Due to the coronavirus pandemic, a large number of workers began working from home, which increased the number of endpoint devices and the risk of cybersecurity breaches.

Robust growth to be Witnessed in Cloud Security

The exponential rise of IoT solutions is witnessing increasing popularity in the information security sector. Meanwhile, the rapid adoption of emerging technologies like big data and cloud computing in cyber security is currently one of the key market trends. Due to its powerful and flexible infrastructure, the cloud computing model is widely used. Many organizations are shifting their preference toward cloud solutions to simplify data storage and provide remote server access via the internet, allowing access to unlimited computing power.

Cloud implementation can enable organizations to combine supplementary infrastructure technologies, such as software-defined perimeters, to create robust and highly secure platforms. Many governments issue special guidelines and regulations for cloud platform security, which drives the cyber security market's growth.

Speed, scalability, interoperability, automation, and cooperation are all features of cloud security operations. Automated solutions are used six times more frequently by key enterprises across the country that are further along their cloud security journeys than

those that are just starting. The performance of these similar businesses is twice as good across the threat remediation lifecycle.
Due to its powerful and flexible infrastructure, the cloud computing model is widely used. Many organizations are shifting their preference toward cloud solutions to simplify data storage and provide remote server access via the internet, allowing access to unlimited computing power.

Cloud implementation can enable organizations to combine supplementary infrastructure technologies, such as software-defined perimeters, to create robust and highly secure platforms. Many governments issue special guidelines and regulations for cloud platform security, which drives the cyber security market's growth.

The cloud-based cybersecurity architecture approach enables cloud applications to use single sign-on (SSO) and multi-factor authentication (MFA), giving each user access to a specific set of applications and data. As SMEs plan to address data and information security concerns via the cloud, demand for cloud-based cybersecurity solutions is expected to rise, presenting market growth opportunities.

According to a survey done in 2020, over 37% of Indian businesses have their digital infrastructure hosted on the cloud. More than 60% of infrastructure was expected to be in the cloud this year, replacing third-party co-location and on-site or captive availability.

India Cybersecurity Market Competitor Analysis

The India cybersecurity market is moderately concentrated and dominated by a few major players, like Palo Alto Networks (India) Private Limited, Juniper Networks India Private Limited, IBM India Private Limited, Norton LifeLock India Private Limited, and Quick Heal Technologies Limited. With a prominent market share, these major players focus on expanding their customer base across foreign countries.

In November 2022, Quick Heal released the 23rd version of its flagship product on the back of GoDeep. AI is a tool for finding malware. A mix of deep learning, behavioral analysis, and predictive analytics is used by the solution to stop such threats, in addition to monitoring the systems to detect cyberattacks and assessing the threat's seriousness.

In October 2022, Norton released the Norton AntiTrack app in India to avoid internet monitoring. Further, with cutting-edge anti-fingerprinting technology, the software quickly recognizes and disables trackers. Windows and Mac computers can use the AntiTrack browser extension and software. The app's anti-fingerprinting technology aids in protecting the user's digital identity from tracking and fingerprinting efforts.

Additional Benefits:

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

Table of Contents:

India 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	2026-02-27
		Signature	