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

Market Report | 2025-04-28 | 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 China Cybersecurity Market size is estimated at USD 27.60 billion in 2025, and is expected to reach USD 71.84 billion by 2030, at a CAGR of 21.09% during the forecast period (2025-2030).

China's cybersecurity market has been rapidly growing with the country's increasing digitization and the corresponding rise in cyber threats. The Chinese government has been actively enhancing its cybersecurity measures to protect critical infrastructure, sensitive data, and businesses against cyber attacks.

Key Highlights
- The number of connected devices has increased in China due to technological advancements. The interconnectivity of the devices also grows exponentially with 5G-enabled devices. As a result, there are more connected devices, which immediately increases the market's need for security products.
- Industrial Revolution 4.0 aids cellular connectivity throughout the industry with the rise of IoT. Machine-to-machine connections have also been instrumental in driving the market. According to CNNIC, in December 2023, approximately 2.33 billion internet users in China had access to cellular Internet of Things (IoT) services. Smart public utility, manufacturing, and transportation accounted for over half of the IoT end users.
- One of the major causes of growing cyberattacks is the lack of skilled cybersecurity personnel in each industry. In China, experienced cybersecurity professionals are less than security professionals, who are required to handle cyber threats for financial institutes, government organizations, and private sector/industrial businesses.
- Large businesses are implementing more data-based AI solutions for security and sales. Cybersecurity experts have turned to geospatial data to shore up the lines of defense. Companies can strengthen emergency management, national intelligence, infrastructure protection, and national defense platforms by implementing geospatial data into pre-existing security systems.

China Cyber Security Market Trends

Cloud Deployment Mode Segment is Expected to Hold Significant Market Share

- The need for cloud-based solutions and subsequent growth in the use of on-demand security services is driven by businesses' growing awareness of the value of saving money and resources by transferring their data to the cloud rather than creating and maintaining new data storage. Due to these advantages, major businesses and SMEs in China adopt cloud-based solutions more frequently.
- The increasing realization among enterprises about the importance of saving money and resources by moving their data to the cloud instead of building and maintaining new data storage drives the demand for cloud-based solutions. Owing to multiple benefits, cloud platforms and ecosystems are anticipated to serve as a launchpad for an explosion in the pace and scale of digital innovation over the next few years.
- As IT provision has shifted from on-premise to outside the boundaries of the business, security has been crucial at every stage of the cloud adoption cycle. SMEs prefer cloud deployment because it frees them up to concentrate on their core skills rather than investing their limited cybersecurity funds in security infrastructure. Furthermore, using public cloud services expands the organization's confidence boundary, making security an essential component of the cloud infrastructure. However, the increasing usage of cloud-based solutions has significantly simplified enterprises' adoption of cybersecurity practices.
- With the increased adoption of cloud services, such as Google Drive, Dropbox, and Microsoft Azure, and with these tools emerging as an integral part of business processes, enterprises must deal with security issues, such as losing control over sensitive data. This gives rise to the increased incorporation of on-demand cybersecurity solutions.
- Cloud-based solutions also benefit from lower capital expenditure requirements, thus making the business much more compelling. Deploying cloud-based services can significantly reduce the Capex requirement as the companies need not invest in hardware components. Cloud solutions also enable better prediction of the cost of an application, and companies do not need to incur as much upfront cost to incorporate the technology. The hardware and IT support savings make cloud-based solutions much more affordable.
- Companies considering moving from on-premise software to a cloud-based solution are primarily checking the potential solutions for their capabilities concerning key security features, including standards compliance, intrusion prevention, and detection.
- A CNNIC survey conducted in June 2023 found that a troubling 20% of internet users in China have been victims of online fraud.

Data Security Offering Segment is Expected to Hold Significant Market Share

- The financial sector has been recognized as a prime adopter of regulatory frameworks to implement adequate information and data security standards. These ensure a reliable provision of products and services, safe data processing by its systems, and responsible use of personal data.
- Data security helps reduce risks associated with protecting sensitive data from threats and helps organizations maintain compliance. The data security platforms provide data risk analytics, data monitoring, protection solutions, and protection of the organization's data from database vulnerability. Governments are tightening the mandates on data security, requiring companies to use cybersecurity solutions.
- This trend, including the use of antivirus and antispyware software, is expected to create a booming market for cyber solutions in the coming years. Compliance is expected to be the key driver of data loss prevention solutions. However, an enterprise's digital transformation strategies, most notably cloud adoption, Big Data analytics, and IoT enablement are also driving enterprise

security teams in the region to adopt these products to identify and classify crucial data throughout the organization and reallocate data security controls primarily based on the criticality of the information.
- As organizations continue to digitize their operations and deal with increasingly complex data protection challenges, investment in effective data security measures will be essential to safeguard sensitive information, maintain regulatory compliance, and protect their reputation.
- As digital transformation accelerates and data protection issues become more complex, organizations must invest in adequate security measures to protect sensitive data, meet regulatory requirements, and save their brand image. Increasing data volumes, changing data protection regulations, and the necessity of customers' related concerns are expected to create robust demand for data security solutions.
- A CNNIC survey conducted in June 2023 found that online fraud is the most common internet security issue faced by internet users in China. Around 38% of respondents encountered prize or lottery-winning scams online.

China Cyber Security Industry Overview

The Chinese cybersecurity market is fragmented, with the presence of major players like Palo Alto Networks, ThreatBook, IBM Corporation, QI-ANXIN Technology Group Inc., and Beijing Chaitin Future Technology Co. Ltd. Players in the market are adopting strategies such as partnerships and acquisitions to enhance their product offerings and gain sustainable competitive advantage. For instance,

- In April 2024, Palo Alto Networks, one of the global cybersecurity leaders, and Google Cloud announced the expansion of their partnership with a ten-figure, multi-year commitment. Palo Alto Networks named Google Cloud its AI and infrastructure provider of choice. Google Cloud has long considered Palo Alto Networks its preferred next-generation firewall (NGFW) provider and the expanded agreement solidified that relationship. The collaboration also underscores the critical importance of platformization fueled by AI to automate and consolidate multiple solutions and deliver near-real-time security resolutions.
- In October 2023, IBM unveiled the evolution of its managed detection and response service offerings with AI technologies, including automatically escalating or closing up to 85% of alerts and accelerating security response timelines for clients.

Additional Benefits:

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

Table of Contents:

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

Market Report | 2025-04-28 | 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	2026-02-07
		Signature