China Cybersecurity - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 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 18.90 billion in 2024, and is expected to reach USD 49.66 billion by 2029, growing at a CAGR of 21.31% during the forecast period (2024-2029).

Organizations must take proactive measures to address cyber threats that have increased as a result of the recent COVID-19 epidemic. Because of this, cyber resilience, the capacity of a sector or organization to respond to, plan for, and recover from cyberattacks, has in the present situation turned into a requirement rather than a choice.

Key Highlights
-The Chinese government is developing a plan to maximize its cybersecurity sector as it becomes increasingly worried about the security of its data in response to increased international conflict and requests for more personal safeguards.
-The Ministry of Industry and Information Technology (MIIT) of China mandated that significant industries like telecoms allocate 10% of their IT upgrade budget to cybersecurity by 2023 in the draught of its most comprehensive policy yet for the growth of China's cybersecurity industry.
-The government anticipates the industry to be valued at more than CNY 250 billion (USD 38.6 billion/HKD 299.73 billion) by 2023 by encouraging the development of an increasing demand for goods and technologies, including data security monitoring and AI threat detection.
-The quantity of personal information and transaction data that all Chinese firms have on hand is growing. Sensitive data is frequently exposed due to organizational system weaknesses, making these firms the prime targets of cyberattacks.
-The usage of cybersecurity solutions is anticipated to increase as the Internet becomes more widely used in China. Additionally, due to increasing data susceptibility brought on by the expansion of wireless networks for mobile devices, cybersecurity is now a crucial component of any enterprise in China. The Chinese cybersecurity business is expanding due to growing cybercrime events

and laws demanding reports. However, the lack of cybersecurity professionals has been a concerning factor, limiting the growth of the cybersecurity market in China.
-Due to rising trend of cyber-attacks involving malware and ransomware in the context of COVID-19, which is forcing organizations to adopt cybersecurity solutions as many of them have switched to remote work environments amid lockdown in various countries, the China cybersecurity market is anticipated to experience significant growth as a result of the COVID-19 outbreak.

China Cybersecurity Market Trends

Cloud Deployment to Hold a 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 embrace cloud-based solutions more frequently. Cloud platforms and ecosystems are anticipated to be the starting point for an explosion in the speed and scope of digital innovation during the coming few years.
- The Ministry of Industry and Information Technology's information-sharing platform for cybersecurity threats and vulnerabilities compiled 143,319 information system vulnerabilities in 2021. There were 40,498 vulnerabilities with high risk and 86,217 vulnerabilities with medium risk.
- China Telecom, China Mobile, and China Unicom recorded 753,018 distributed denial-of-service (DDoS) attacks in 2021, which is a 43.9% decrease from 2020. As of 2021, the Ministry of Industry and Information Technology's information-sharing portal for cybersecurity threats and vulnerabilities has received 88,799 occurrences, a reduction of 60.9 percent over the same period in 2020.
- According to the notice released on December 2021, MIIT has suspended a collaboration with the cloud unit about cyber-security risks and information-sharing platforms to be reevaluated in six months and perhaps resumed. This most recent action demonstrates Beijing's determination to increase control over crucial cyberinfrastructure and data for national security. By the end of the year, state-owned businesses in China are required to transfer their data from private operators like Alibaba and Tencent to a state-backed cloud infrastructure.

Rapidly Increasing Cybersecurity Incidents and Regulations Requiring Reporting

- The rising organizational tendency toward digitization and the use of linked technologies as part of their operations has led to a sharp spike in cybersecurity incidents in China. The number of connected devices has increased in China due to technical improvements. The interconnectivity of the devices will also rise dramatically with 5G and 5G equipped devices. As a result, there are more linked devices, which immediately raises the market's requirement for security goods.
- Data on an estimated 1 billion Chinese residents taken from the Shanghai police were listed for sale in July 2022 by an anonymous user on a well-known internet cybercrime site. One of the biggest heists in history, it involved highly sensitive information such as government ID numbers, criminal records, and in-depth case summaries with charges of rape and domestic violence.
- According to China's internet regulator, the ride-hailing company has unlawfully acquired customers' personal data, which is why it ordered smartphone app retailers to cease selling Didi Global Inc.'s app in July 2022. Four days after Didi started trading on the New York Stock Exchange after raising USD 4.4 billion in an initial public offering, the Cyberspace Administration of China (CAC) said that it had instructed Didi to make improvements to comply with Chinese data protection laws.

- As per China Internet Network Information Center (CNNIC), internet users reported not having encountered cybersecurity concerns in the previous six months in 62.0% of cases as of December 2021, a figure that was relatively consistent with December 2020.
- In addition, the percentage of Internet users who experienced personal information leakage was the highest at 22.1%; internet fraud was experienced by 16.6% of users; viruses or Trojan horses infected their devices at a 9.1% rate, and accounts or passwords were stolen by 6.6% of users.

China Cybersecurity Industry Overview

The China cybersecurity market is moderately fragmented. Players in the market adopt strategic initiatives such as partnerships, investments, and new product offerings due to increasing awareness regarding mobility security among enterprises.

- November 2021 - The next-generation Cloud Access Security Broker (CASB) from Palo Alto Networks uses machine learning to improve the security of collaboration and software-as-a-service (SaaS) programs. According to the business, its next-generation CASB platform will leverage ML and AI to offer features like automated application discovery and enhanced data loss protection for sensitive data.
- July 2021 - Chaitin Future Technology Co Ltd, a network security solution provider under Aliyun, released a new generation network security analysis and management platform to battle network threats in the modern era. The venue, Cosmos, fully considers the actual business circumstances of the organizations and assists the realization of unified data analysis, key data processing, and secure operation standardization and automation by the enterprises. Additionally, the platform creatively integrates platform and users to process risks from a more macro viewpoint, assess risks, deal with threats, and accomplish closed-loop disposal of risks, which is more logical, secure, and practical.

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 2019 - 2029

Market Report | 2024-02-17 | 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