

INDUSTRY OVERVIEW

The information presented in this section, unless otherwise indicated, is derived from various official government publications and other publications and from the market research report prepared by Frost & Sullivan, which was commissioned by our Company. Our Company believes that the information has been derived from appropriate sources and has taken reasonable care in extracting and reproducing the information. Our Company has no reason to believe that the information is false or misleading in any material respect or that any fact has been omitted that would render the information false or misleading in any material respect. The information has not been independently verified by our Company or any of its respective directors, officers or representatives or any other party involved in this document nor is any representation given as to its accuracy or completeness.

OVERVIEW OF CHINA’S INFORMATION SECURITY MARKET

Definition and classification

Information security is an umbrella term that covers all the work done to protect information. It refers to the protection of information from unauthorized access, damage, alteration and leakage during production, transmission, processing and storage, to ensure the availability, confidentiality, integrity and non-repudiation of information and to ensure the reliability and controllability of information systems. Specifically, information security includes several major segments: cybersecurity, data security and others. Cybersecurity focuses more on the security protection of computing resources and network environment, while data security focuses on the protection of the entire lifecycle from data generation to destruction, both of which belong to the category of information security.

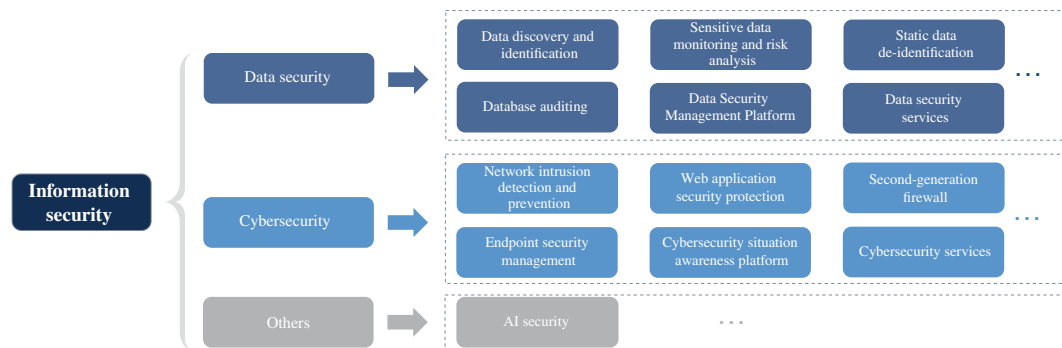


Fig 1. Classification of information security

Source: Frost & Sullivan; Official website of Market Players; Interviews with Industry Experts

Market drivers of China’s information security

Technology: With the continuous progress of technology, especially the development of emerging technologies such as cloud computing, big data, artificial intelligence and the internet-of-things, higher requirements are put forward for information security. The application of these technologies has brought new security challenges, such as data breaches and cyberattacks and also spawned new security technologies and solutions. For example, AI technology is increasingly being used in the field of cybersecurity, where it can help predict and identify potential security threats and improve response speed and accuracy.

Policy: The government attaches increasing importance to information security and has issued a series of policies and regulations to strengthen information security management and protection. For example, China’s Cybersecurity Law, Data Security Law and Personal Information Protection Law provide legal support for the security of cyberspace. The implementation of these policies has promoted the growth of demand for information security products and services and promoted the standardization and marketization of the industry.

Events: In recent years, frequent security incidents such as web phishing, security vulnerabilities, malicious programs, web tampering, network backdoors, DDoS attacks, etc., have not only brought direct losses to affected organizations, but also increased the awareness and demand of the entire society for information security. For example, the “network protection action” is one of the important layout of the national response to network security issues.

INDUSTRY OVERVIEW

Industry chain of China’s information security market

With the development of China’s information security industry, the industrial chain has gradually become more sophisticated. At the upstream end of the chain are primarily providers of basic hardware and software, such as hardware suppliers of chips, memory, storage devices, servers, and industrial computers, which provide the physical infrastructure required for information security; and software suppliers of operating systems, databases, and middleware, which provide the foundational technologies and underlying operating environments for information security systems.

The midstream of the industry chain consists of information security product and service providers, which can be categorized by product type into providers of standard information security products, information security platform and information security services. Specifically, each product category can be further divided into two major categories: cybersecurity and data security. For example, standard information security products can be subdivided into standard cybersecurity products and standard data security products.

The downstream of the industry chain consists of application sectors and end-users, including telecommunications, government, energy and power, finance, industrial manufacturing, and healthcare, which are the sources of demand for information security.

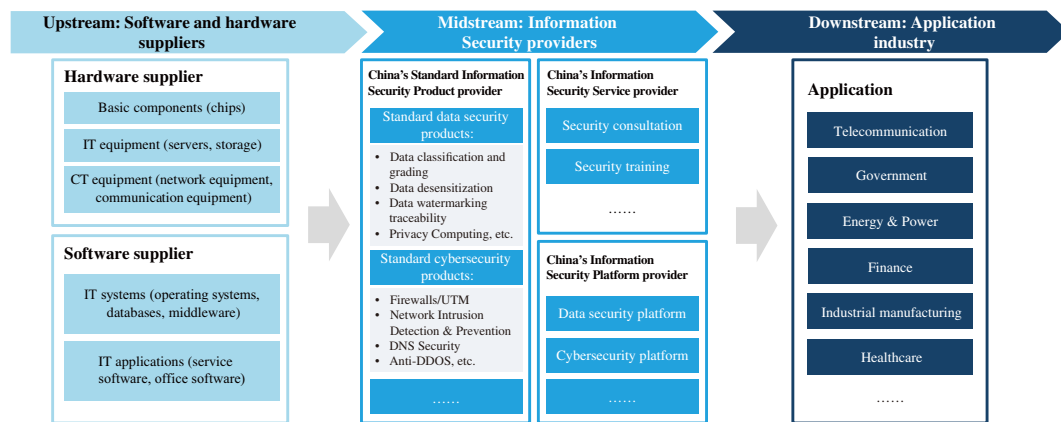


Fig 2. Industry chain of information security market

Source: Frost & Sullivan; Interviews with Industry Experts

Market Size of China’s information security market

The size of China information security market has grown from RMB73.2 billion in 2021 to RMB105.7 billion in 2025, with a CAGR of 9.6%. The growth is mainly driven by policy compliance and frequent security incidents, which compelled enterprises to accelerate their investment in information security.

From 2026 to 2030, the market size is expected to grow from RMB115.4 billion to RMB172.7 billion, with a CAGR of 10.6%. The convergence of AI technology has given rise to a surge in demand for “AI + Security” solutions, while the accelerated release of demand for AI security, the Internet of Vehicles (IoV), the Internet of Things (IoT) and cloud security and other emerging fields have collectively constructed the core driving force for the market’s continued expansion.

From the perspective of the specific roles of midstream participants in information security market, they can be broadly classified into two categories: (i) traditional Internet/ICT vendors such as Huawei, Alibaba, Tencent, and China Telecom, etc.; (ii) specialized security vendors such as QAX, Guan An Info., DBAPP Security, Venustech, etc.

This classification of participants in the information security market stems primarily from the distinct differences in their business positioning and growth strategies: the former typically treats security as a complementary capability to cloud, networking, or digital solutions, with security revenue dispersed across their overall ICT business; the latter, however, focuses on cybersecurity and data security as their core business, concentrating on in-depth scenarios such as offensive operations, data governance, and compliance operations. Consequently, their business performance provides a more direct reflection of the industry’s actual needs and technological advancements. Therefore, when conducting market analysis, it is necessary to analyze specialized security vendor groups separately.

INDUSTRY OVERVIEW

The size of China’s specialized security vendors sub-market of information security has grown from RMB28.3 billion in 2021 to RMB39.0 billion in 2025, with a CAGR of 8.4%. This growth is primarily driven by specialized security vendors deepening their technological expertise and accelerating scenario penetration, as well as policy compliance requirements and security incidents.

From 2026 to 2030, the market size is expected to grow from RMB42.1 billion to RMB65.0 billion, with a CAGR of 11.5%. As specialized security vendors focus on cutting-edge domains to rapidly respond to emerging threats, their deep expertise in vertical industries enables them to precisely address sector-specific pain points, paving the way for further market expansion.

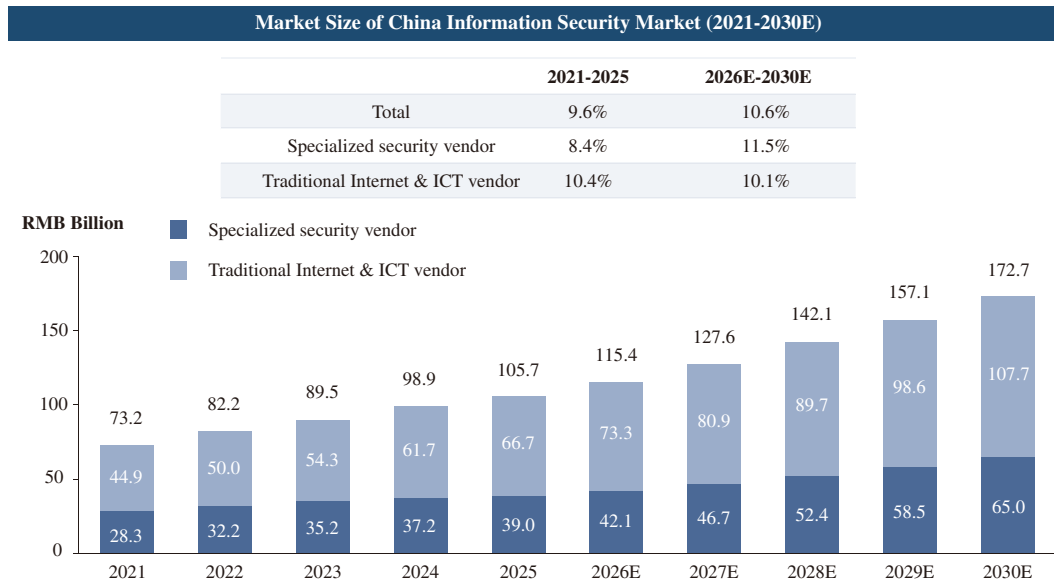


Fig 3. Size of China’s information security market

Source: Frost & Sullivan; Interviews with Industry Experts

Future trends of China’s information security market

The large-scale application of digital technology creates new security gaps. With the widespread commercial adoption of digital technologies such as AI, cloud computing and big data, traditional security boundaries are being disrupted. AI systems may have endogenous security issues such as vulnerabilities in large models and algorithmic biases. The cross-domain scheduling and sharing of computing power resources may also bring risks of data leakage and computing power abuse. These new scenarios present security demands that traditional network/data security measures cannot address, which will drive the development of emerging security domains.

AI security will become a critical trend in the digital age. AI security requires a balance between AI innovation and risk management: Technically, AI not only empowers threat detection but also faces risks such as data poisoning. Protective technologies like adversarial training are accelerating their implementation. In terms of governance, many countries have introduced regulations and standards, clearly stipulating the requirements for high-risk AI assessment. On the product front, emerging and evolving solutions like security agents – operating on the principles of “proactive autonomous defense, full lifecycle protection and countering models with models” – hold promise for addressing AI security pain points. In terms of application, it penetrates into fields such as finance and industry and integrates with network security and data security to form an integrated protection solution.

The deep binding of the IoT with security requirements. The popularization of the IoT has broken the traditional security boundaries. The extensive penetration of IoT devices has significantly expanded the attack surface. Previously isolated device risks have become systemic security risks through network connections, linking public safety and economic stability and promoting IoT security to upgrade from a marginal demand

INDUSTRY OVERVIEW

to a core essential need. Policy compliance constraints and exclusive technological innovations (such as lightweight encryption and trusted authentication) further enhance its track independence, while the integration with emerging technologies has built a full-chain protection ecosystem, making it a key direction for ensuring digital transformation and leading the development of the information security market.

Enhanced regulatory constraints on emerging security scenarios. Regulations such as the Data Security Law and Personal Information Protection Law impose explicit requirements on privacy protection for AI training data and compliance in data flow during computing power sharing. Documents such as the Three-Year Action Plan for Building New Infrastructure for the Internet of Things have further clarified mandatory requirements including device identity verification, encrypted communication and secure firmware updates. Enterprises seeking to deploy AI applications or engage in cross-domain computing power collaboration must meet these compliance standards. This rigid constraint will directly promote investment in the emerging security market.

Platform-driven integration of products, operations and services has become a pivotal development path for the security industry. Digital transformation has driven security threats toward greater complexity and diversity, rendering single-product protection inadequate for addressing holistic risks. Platform-based development has thus become an industry imperative. The integrated model of products, platforms and services consolidates comprehensive security capabilities around a platform core. Professional security services serve as the link, encompassing end-to-end offerings such as security consulting and emergency response. These services address gaps in enterprise security teams and resolve the pain point of “overemphasizing deployment while neglecting operations.” Specialized products lay the foundation, while customized services ensure effectiveness and dynamic adaptation. This approach not only meets compliance requirements but also drives the shift from reactive defense to proactive operations, helping build an efficient security ecosystem. It has become a key driver for high-quality development in the industry.

OVERVIEW OF CHINA’S DATA SECURITY MARKET

Definition and classification

Data security refers to taking the necessary measures to ensure that data is in a state of effective protection and lawful use, as well as the ability to ensure a state of continuous security. Specifically, it refers to a data-centric security system that covers the entire lifecycle of data, including data collection, transmission, storage, processing (usage), exchange (sharing) and destruction. It focuses on protection throughout the entire lifecycle from data generation to destruction, emphasizing data ownership, jurisdiction, privacy rights, etc. With the continuous improvement of informatization and the arrival of the data age, the storage nodes and regions of data have become complex, the flow of data has shown exponential growth, and the usage methods have become increasingly diversified. The original protection methods no longer meet the current security needs, and data security has become an independent security system.

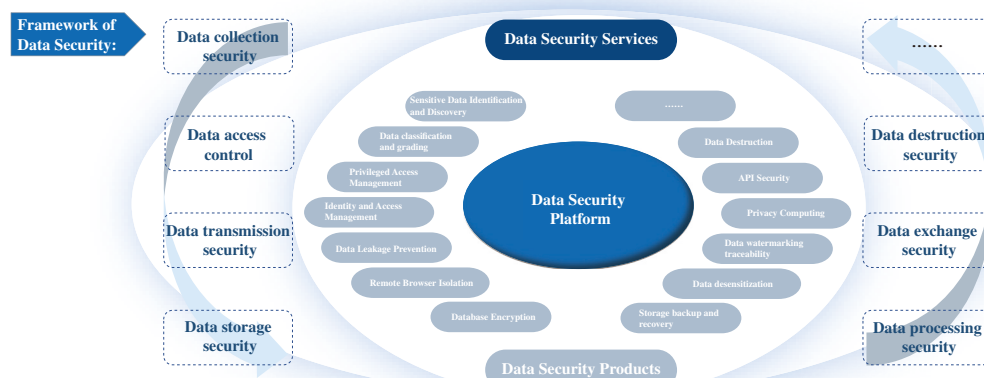


Fig 4. Framework of the data security market

Source: Frost & Sullivan; Official website of Market Players; Interviews with Industry Experts

INDUSTRY OVERVIEW

Definition of data security platform

Data security platform is a comprehensive security system covering the entire life cycle and all scenarios, encompassing the entire process of data from generation, storage, transmission, use to destruction and providing unified data security protection, governance and compliance capabilities. Its core objective is to achieve data being “knowable, controllable, preventable and traceable” and to integrate multiple subsystems including data leakage prevention, data encryption, access control, risk monitoring and compliance auditing through a unified architecture. Its characteristics are:

- (i) It is the top-level platform for enterprise-level data security governance.
- (ii) It includes data security management platform, security data center, data asset and risk assessment platform, etc.
- (iii) Provide a unified security view and policy linkage across departments and systems.

Market drivers of China’s data security

External factors: compliance requirements, stable growth

Trends in data security supervision: The supervision and attention of the regulatory authorities to Data Security increased year by year and is mainly led by the central government and the Ministry of Industry and Information Technology. The telecommunications, government, energy and power, finance and manufacturing industries are the industries with stricter data security supervision.

Internal factors: endogenous value, demand activation

Rapid increase in data volume stimulates awareness of data security: According to Frost & Sullivan’s statistics, the total amount of data in China has surged from 9.8ZB in 2019 to 52.3ZB in 2025. With the increase of data volume, the information hidden behind the data that can be mined is gradually becoming richer. Data has evolved from a merely auxiliary resource to a core strategic asset for the development of governments and enterprises. Its value in decision support, efficiency improvement and business innovation has become increasingly prominent. Against this backdrop, governments and enterprises have been placing greater emphasis on the value of data and are actively exploring how to fully tap into the potential of data and maximize its value in a controllable and secure environment.

The Rising Cost of data leakage drives up the demand for enterprise Data Security. The average cost of global data breaches in 2025 is millions of dollars, growing rapidly. Due to their data sensitivity, industries such as healthcare, financial services and new energy vehicles have seen the cost of data breaches increase year by year. The high cost of data breaches has made enterprises deeply aware of the importance of data security, prompting management to pay more attention to data security protection work, incorporate data security into the core strategy of enterprises, increase investment in data security and actively take various measures to protect the data assets of enterprises. At the same time, in order to reduce the risk of data breaches and potential losses, enterprises have significantly increased their procurement demand for data security products and services. In addition, facing the constantly rising cost of data breaches, enterprises have stronger motivation to explore and apply new security technologies and innovative solutions, such as the application of artificial intelligence, machine learning, blockchain and other technologies in the field of data security.

The development of big data and AI models bring opportunities and demands. The development of big data and AI models brings many opportunities for data security, such as improving monitoring and protection capabilities, optimizing data management, providing governance decision support, promoting technological innovation and enhancing user security awareness. At the same time, this development has

INDUSTRY OVERVIEW

also given rise to new demands for data security, covering aspects such as data lifecycle protection, model reliability assurance, privacy enhancement, improved collaborative sharing mechanisms and professional talent and technical support.

Industry pain points of China’s data security market

Accounts, permissions and APIs become vulnerable links in data protection: Among them, privileged accounts have become one of the most serious “security vulnerabilities” and permission issues have become a serious security challenge in the new IT environment. API protection has been neglected and has become the biggest risk exposure for data security.

The difficulty in implementing continuous protection of data security status: Data is now characterized by its extensive distribution, massive scale, scattered assets, and rapid circulation across complex scenarios, which presents unprecedented difficulties in security protection. Meanwhile, diverse data access sources complicate the establishment of unified joint prevention and control mechanisms. The traditional approach of deploying discrete data security tools in a superposed manner only addresses risks in a fragmented manner, making it impossible to realize holistic and systematic joint prevention and control.

Failure of traditional protection system and upgrading of attack methods: Most enterprises still rely on traditional firewalls and intrusion detection systems, which make it difficult to identify malicious code implanted through the supply chain and can easily lead to customer transaction data leakage. Generative AI is used to create highly realistic phishing emails, increasing the success rate of attacks and only a few generative AI projects take sufficient security measures.

Structural defects in the data governance system: There exists a misalignment between compliance requirements, technical frameworks and actual business needs. Specifically, the compliance costs associated with cross-border data flow remain high, and internal governance mechanisms fail to effectively mitigate supply chain risks and internal threats. Meanwhile, the performance and effectiveness of technologies such as privacy computing and data anonymization are still insufficient to meet practical business demands.

Breakdown of China’s data security market

Size of China’s data security market

From 2021 to 2025, the size of China’s data security market has jumped from RMB18.6 billion to RMB29.0 billion, with a CAGR of 11.7%.

From 2026 to 2030, the market size is expected to grow from RMB32.3 billion to RMB50.9 billion, with a CAGR of 12.1%. The drivers of market growth will become increasingly diverse, primarily driven by the convergence of technologies such as artificial intelligence, privacy-preserving computing, and quantum cryptography, as well as the rapidly growing demand for data security in industry sectors such as finance, the Internet of Vehicles (IoV), and the Internet of Things (IoT).

And in China’s specialized security vendors sub-market of data security, it has jumped from RMB5.3 billion in 2021 to RMB7.8 billion in 2025, with a CAGR of 10.1%. The main driving force behind this change is the simultaneous explosion of scenario-based demands brought about by the digital transformation of the industry and the technological innovation of various vendors driving the leap in product capabilities. From 2026 to 2030, it is expected to grow from RMB8.5 billion to RMB13.7 billion, with a CAGR of 12.6%. Looking ahead, the convergence of “AI and data security” will drive accurate and efficient protection throughout the entire data lifecycle. At the same time, as data security requirements continue to evolve in vertical industries such as telecommunications, government, and finance, this will fuel growing demand for scenario-specific and customized products and services.

INDUSTRY OVERVIEW

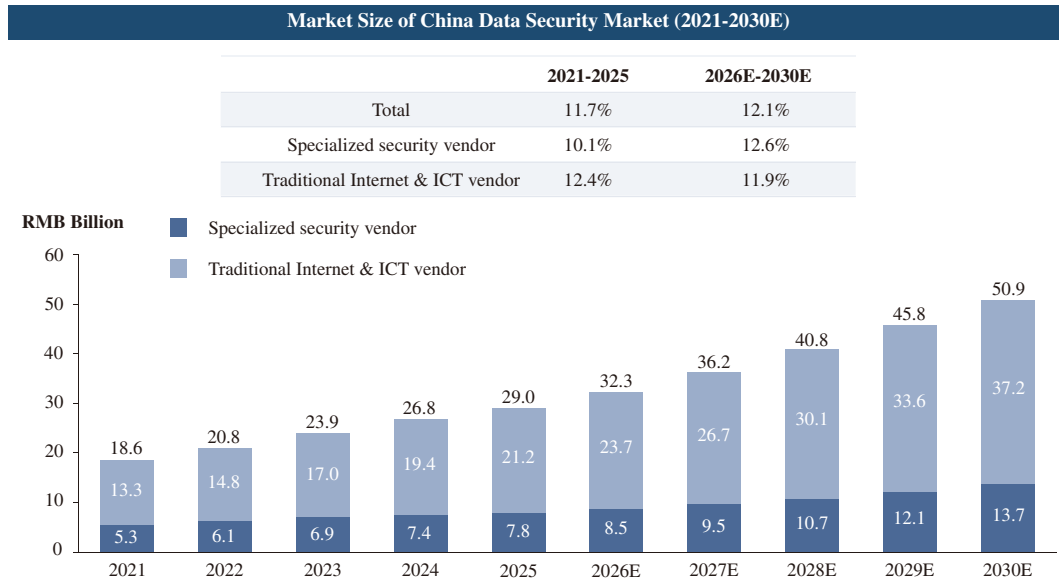


Fig 5. Size of China's data security market

Source: Frost & Sullivan; Interviews with Industry Experts

Size of China's data security platform market

Under the obvious trend of market platformization, intelligence and scenario-based applications, the data security product urgently needs to upgrade from “single-module” solutions to integrated platforms that encompass data “discovery, governance, protection, and operations”, which has promoted the development of data security platform market.

From 2021 to 2025, the size of China's data security platform market has grown from RMB4.5 billion to RMB7.6 billion, with a CAGR of 13.9%. And it is expected to grow to RMB15.4 billion by 2030, with a CAGR of 15.3% from 2026 to 2030.

From the perspective of the specialized security vendor sub-market of data security, the market size has grown from RMB0.9 billion to RMB1.5 billion, with a CAGR of 13.9% from 2021 to 2025. And it is expected to grow to RMB3.1 billion by 2030, with a CAGR of 15.5% from 2026 to 2030, demonstrating strong growth potential.

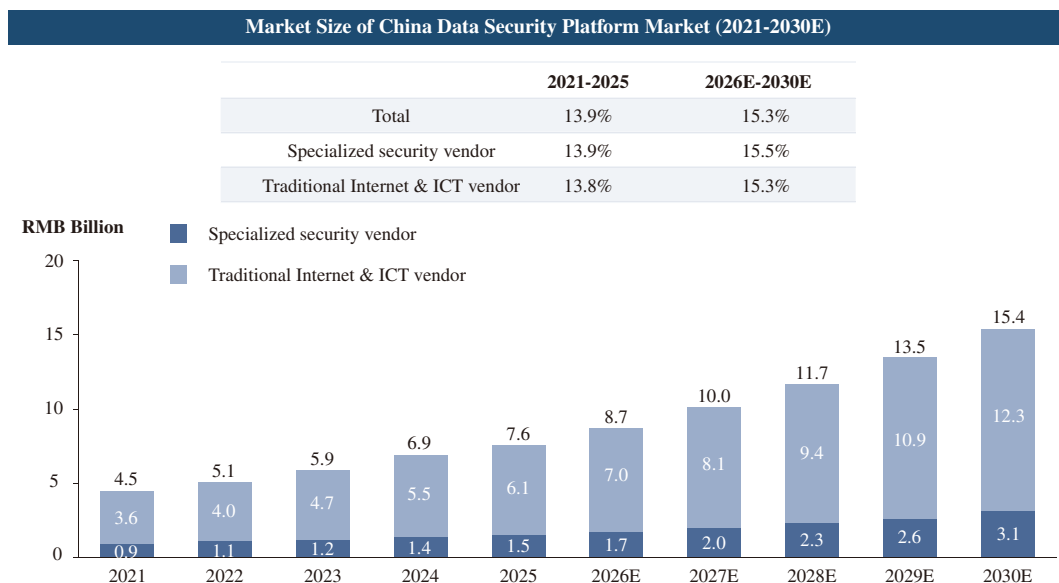


Fig 6. Size of China's data security platform market

Source: Frost & Sullivan; Interviews with Industry Experts

INDUSTRY OVERVIEW

Future trends of China’s data security market

Integration and platformization of data security

The increasing complexity of data security has led to the gradual integration of different data security functions. The current situation of data security construction is not only due to the lack of attention or investment in data security, but more often than not, even if some enterprises have invested sufficient budget in data security, due to the complexity of data security technology and the procurement of different security products from different security vendors and managed by different teams, the security budget invested in the early stage has not received good results. The current growth rate of complexity in data security technology far exceeds the speed at which security vendors integrate and consolidate various emerging technologies, resulting in a continuous increase in the difficulty of applying data security technology on the user side. The data security platform integrates existing independent data security technologies and functions into a unified platform, providing users with data security services across data types, storage islands and ecosystems, thereby achieving simpler and more consistent end-to-end data security.

“Data security + artificial intelligence” has become major trends

By utilizing artificial intelligence technology, it is possible to quickly identify and learn patterns from massive compliance policies, threat intelligence, industry dynamics and best practices, mine and analyze valuable information and conduct intelligent decision analysis to provide targeted policies and strategies for data security. By using automated tools and methods, the efficiency and accuracy of multiple steps in data security assessment, such as questionnaire surveys, personnel interviews, document review, configuration verification, on-site verification, technical testing, expert analysis and report preparation, can be improved to help enterprises better identify and respond to data security risks. In terms of data security strategy, artificial intelligence can automatically adjust data access control and encryption policies based on the sensitivity and usage scenarios of data to ensure data security.

Privacy computing has become the current hottest topic

The most promising technology for industrial application in the field of data security in recent years is privacy computing. Privacy computing can achieve privacy protection for the data computing process and results on the basis of completing computing tasks, while participants cannot obtain additional information other than the computing results throughout the entire computing process. Privacy computing is not a single technology, but a set of technology systems composed of multiple technologies. Key technologies include multi-party computing, federated learning, verifiable de identification, confidential computing, homomorphic encryption, etc. Different technology routes can greatly affect the usage scenarios, functions and performance of products.

OVERVIEW OF CHINA’S CYBERSECURITY MARKET

Definition and classification

Cybersecurity is the protection of network systems (including hardware, software, services, etc.) from attacks, intrusions, destruction and illegal use through technical, managerial and legal means, ensuring the availability, integrity and confidentiality of the network. Cybersecurity specifically encompasses the security of both cyberspace and physical space, covering the operational security of network systems, the content security of network information, the security of network transmission and the security of physical assets of network entities:

- (i) From an industry perspective, the downstream market of cybersecurity can be divided into operators, finance, government, industrial manufacturing, medical, education, etc.
- (ii) From the perspective of product forms, the cybersecurity market can be divided into the standard cybersecurity product market, the cybersecurity platform market and the cybersecurity service market.

INDUSTRY OVERVIEW

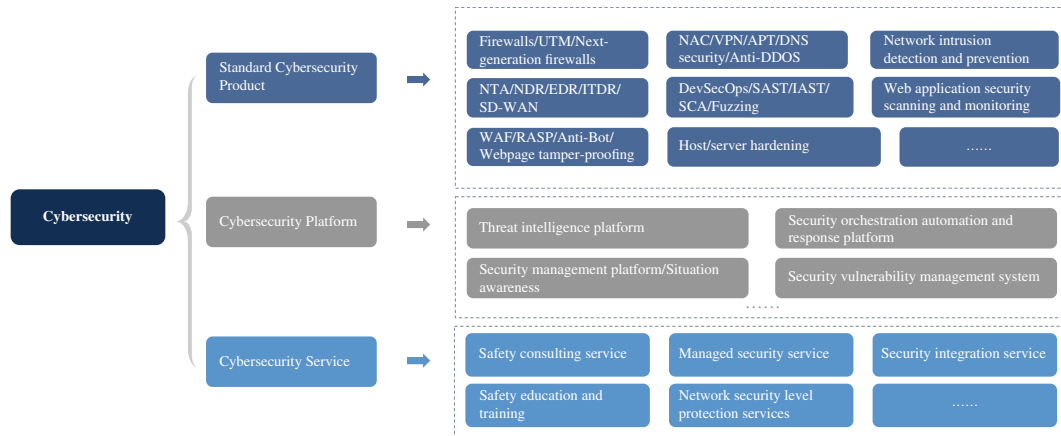


Fig 7. Classification of cybersecurity

Source: Frost & Sullivan; Official website of Market Players; Interviews with Industry Experts

Breakdown of China’s cybersecurity market

Size of China’s cybersecurity market

Since 2021, the China’s cybersecurity market has shown a significant growth trend driven by policies, technological upgrades and industry demand. The market size has increased from RMB54.6 billion to RMB76.7 billion from 2021 to 2025, with a CAGR of 8.9%. It is expected to grow to RMB121.9 billion by 2030, with a CAGR of 10.0% from 2026 to 2030.

And China’s cybersecurity market – specifically the sub-market for specialized security vendors – grew from RMB23.0 billion in 2021 to RMB31.2 billion in 2025, achieving a CAGR of 8.0%. This growth is primarily driven by the strong demand for compliance in key information infrastructure sectors – including government, enterprise, finance, and energy – combined with a comprehensive increase in corporate security awareness amid digital transformation, which has fueled continued expansion in the procurement of specialized cybersecurity products and services. It is projected to reach RMB51.4 billion by 2030, with a CAGR of 11.2% from 2026 to 2030. Leveraging the technological barriers established by specialized security vendors in areas such as advanced attack and defense, security governance, and operations, these vendors will hold a core competitive advantage in scenarios requiring high compliance and stringent security standards, thereby supporting steady market growth.



Fig 8. Size of China’s cybersecurity market

Source: Frost & Sullivan; Interviews with Industry Experts

INDUSTRY OVERVIEW

Size of China’s cybersecurity platform market

The cybersecurity platform is an integrated security solution that integrates multiple security technologies, products, and services, including threat intelligence platform, security orchestration automation and response platform, situation awareness platform, and others. By establishing a closed-loop system of “monitoring, analysis, response and improvement”, it assists enterprises in developing normalized and systematic security operation capabilities.

China’s cybersecurity platform market has grown from RMB12.3 billion in 2021 to RMB19.8 billion in 2025, achieving a CAGR of 12.6%. It is expected to grow to RMB35.1 billion by 2030, with a CAGR of 12.4% from 2026 to 2030.

As an important segment of the cybersecurity market, specialized security vendors focus more on in-depth scenarios such as cybersecurity offensive and defensive technologies, security operations, and governance. They can better reflect the real security needs and technological development directions of the industry. China’s specialized security vendors sub-market of cybersecurity platform market has grown from RMB3.9 billion in 2021 to RMB5.9 billion in 2025, achieving a CAGR of 10.7%. It is expected to grow to RMB10.3 billion by 2030, with a CAGR of 12.5% from 2026 to 2030.

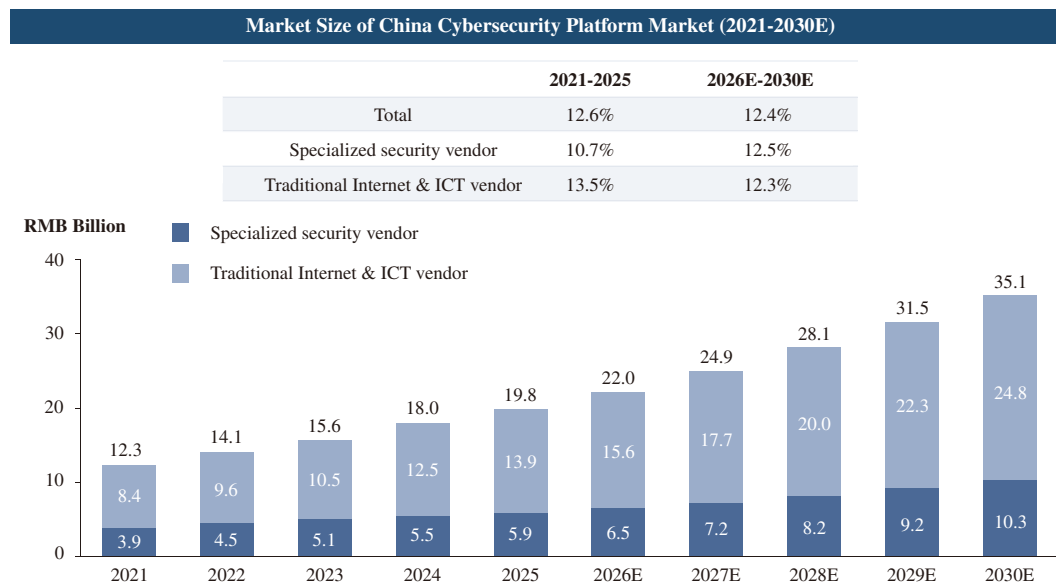


Fig 9. Size of China’s cybersecurity platform market

Source: Frost & Sullivan; Interviews with Industry Experts

Future trends of the cybersecurity market

AI deeply empowers the cybersecurity defense system: The application of AI in the field of cybersecurity will become more extensive and in-depth. AI technology has been upgraded from an auxiliary tool to a defense core. Through machine learning, behavioral baselines are constructed to identify threats such as abnormal traffic and phishing emails in real time. In the future, AI will dominate the attack and defense of cybersecurity, promote the intelligent development of security products and achieve automatic monitoring, analysis and response to cyber threats.

Zero-trust architecture and identity first: With the failure of border defense, zero trust has become the mainstream security strategy. Organizations tend to adhere to the principle of “never trust, always verify”, strictly control access to resources and continuously monitor behavioral patterns. In the future, building integrated identity tools and services compatible with multiple products will be crucial. Continuous multi-factor authentication (MFA), behavioral analysis and the principle of least privilege will be closely integrated with AI threat detection to achieve more dynamic access control.

Evolving Toward Platformization and Service Orientation. Digital transformation has spawned large-scale, cross-domain complex cyber threats. Traditional single-point defenses struggle to adapt to dynamic risks across the entire domain. Platformization has emerged as a critical pathway for building a layered defense system – leveraging security operations and situational awareness platforms to integrate

INDUSTRY OVERVIEW

diverse security capabilities, break down product silos and achieve comprehensive risk visibility and control. Simultaneously, security services are evolving from reactive incident response to proactive, routine operations. Comprehensive services – including consulting, managed services and compliance assessments – address enterprise capability gaps and adapt to dynamic risks, serving as the critical enabler for realizing platform effectiveness.

COMPETITIVE LANDSCAPE

Analysis of information security vendors in China

The information security market is highly competitive with a large number of participants. They can mainly be divided into two categories. One category consists of traditional Internet & ICT vendors such as Huawei, Alibaba and Tencent. These traditional vendors, relying on infrastructure layouts such as cloud, network and terminal, have formed unique competitiveness in the fields of network security and data security.

Another category consists of specialized security vendors, including specialized cybersecurity vendors, as well as specialized data security vendors, such as QAX, Guan An Info., DBAPP Security, Venustech, etc. These specialized security vendors focus on technological depth, vertical scenarios and rapid response, establishing defensive barriers and rapidly expanding market share.

Specialized security vendors serve as the core pillar of expertise in the information security market. Dedicated to advancing security capabilities, they have cultivated deep expertise in offensive and defensive technologies alongside sustained innovation. Focusing on cutting-edge domains, they rapidly respond to emerging threats and build highly effective protection systems, making them critical participants in the security ecosystem.

Ranking of information security vendors in China (by specialized security vendors)

The size of the information security market in China by revenue of competitors reaches RMB105.7 billion in 2025. Among them, specialized security vendors accounts for 36.9%, with a market size of RMB39.0 billion. In 2025, according to revenue statistics, the top five leading companies in this sub-market are Company A, Company B, Company C, Company D and Company E, with a total market share of 39.3%. Among the specialized security vendors, our Company ranks the 13th among the competitors, holding a market share of 1.8%.

The China information security market is booming amid digital transformation and rising cyber threats. Fueled by regulatory mandates (e.g., Cybersecurity Law) and surging demands for data, AI and IoT security, the market expands steadily. Enterprises compete to innovate, shaping a dynamic landscape that underpins industries’ secure digital evolution, signaling exceptional growth potential in China’s information security arena. As a specialized security vendor, our Company ranks 13th among them, underscoring its robust tech prowess and market adaptability.

Ranking	Company	Market share (by Revenue)
1	Company A	11.2%
2	Company B	9.1%
3	Company C	6.5%
4	Company D	6.5%
5	Company E	5.9%
6	Company F	5.8%
7	Company G	5.5%
8	Company H	3.6%
9	Company I	3.1%
10	Company J	2.3%
11	Company K	2.1%
12	Company L	1.8%
13	Our Company	1.8%
14	Company M	1.4%
15	Company N	1.4%
Others		31.7%
Total		100%

Fig 10. Top 15 information security vendors by revenue in 2025 (China, by specialized security vendors)

Source: Frost & Sullivan; Annual Reports of Each Market Player; Interviews with Industry Experts

INDUSTRY OVERVIEW

Notes: Company A was founded in 2014 and is headquartered in Beijing. It listed on the Shanghai Stock Exchange. The company specializes in providing next-generation cybersecurity products and services to government and enterprise users.

Company B was founded in 2000 and is headquartered in Shenzhen. It listed on the Shenzhen Stock Exchange. The company specializes in providing innovative products and services for enterprise-level cybersecurity, cloud computing and the IoT.

Company C was founded in 1985 and is headquartered in Shantou. It listed on the Shenzhen Stock Exchange. The company provides a full suite of cybersecurity and intelligent computing cloud products, services, and integrated solutions.

Company D was founded in 2000 and headquartered in Beijing, listed on the Shenzhen Stock Exchange. The company is an innovative enterprise focused on the security sector, providing comprehensive security products and services covering infrastructure security, data security, cloud security, and more.

Company E was founded in 1996 and is headquartered in Beijing. It listed on the Shenzhen Stock Exchange. The company specializes in cybersecurity products, services, and solutions, serving clients across government, telecom, finance, and other sectors.

Company F was founded in 1998 and headquartered in Sichuan, listed on the Shenzhen Stock Exchange. The company specializes in the field of information security, with operations spanning cybersecurity, data security, and other scenarios.

Company G was founded in 2007 with headquarters in Hangzhou and listed on the Shanghai Stock Exchange. The company primarily engages in network and information security software development, security consulting services and the manufacturing and sales of information security equipment.

Company H was founded in 2014 with headquarters in Nanjing and listed on the Shanghai Stock Exchange. As a specialized enterprise in security and digital intelligence, it focuses on cloud security and endpoint security domains.

Company I was founded in 2008 and headquartered in Hangzhou, listed on the Shenzhen Stock Exchange in 2019. It is one of the important information security manufacturers, specializing in network security and application delivery.

Company J was founded in 2011 with headquarters in Suzhou and listed on the Shanghai Stock Exchange. The company specializes in cybersecurity, providing products and services including perimeter security, cloud security, and data security.

Company K was established in 2001 and headquartered in Beijing, listed on the Shenzhen Stock Exchange in 2016. It is an enterprise specializing in cybersecurity and electronic certification services.

Company L was established in 2002 and headquartered in Jinan, listed on the Shenzhen Stock Exchange in 2017. It is a leading provider of cybersecurity and confidentiality security product R&D as well as overall solution providers.

Company M was founded in 2011 and headquartered in Beijing, listed on the Shanghai Stock Exchange in 2019. It focuses on the R&D, sales, and services of core technologies and underlying platforms in the field of cybersecurity.

Company N was founded in 2009 and headquartered in Beijing. It is a privately-owned, specialized provider of data security products and services.

Ranking of data security vendors in China (by specialized security vendors)

In 2025, the competitive landscape of China’s specialized security vendors sub-market of data security is fiercely competitive, with the top 10 vendors occupying a total market share of 60.9%, led by companies such as Company A, Company D, Company E and our Company.

Our Company, as a specialized security vendor, ranks 7th in the China’s specialized security vendors sub-market of data security, with a 3.8% share. This shows its technological strength and market insight, indicating that it has enormous growth potential in the constantly evolving field of data security.

China’s data security market is booming, driven by stringent regulations (e.g., Data Security Law), the digital economy’s expansion and growing needs for data governance, compliance and privacy protection.

Ranking	Company	Market share (by Revenue)
1	Company A	13.4%
2	Company D	8.3%
3	Company E	7.7%
4	Company C	6.5%
5	Company G	6.2%
6	Company K	5.0%
7	Our Company	3.8%
8	Company B	3.6%
9	Company I	3.2%
10	Company N	3.2%
Others		39.1%
Total		100%

Fig 11. Top 10 data security vendors by revenue in 2025 (China, by specialized security vendors)

Source: Frost & Sullivan; Annual Reports of Each Market Player; Interviews with Industry Experts

INDUSTRY OVERVIEW

Ranking of data security platform vendors in China (by specialized security vendors)

The data security platform market represents a critical growth segment within China’s data security industry, with a market size of RMB1.5 billion (2025). Characterized by accelerating demand for centralized governance solutions, this sub-sector addresses evolving regulatory compliance (e.g., DSL, PIPL) and hybrid-cloud data protection needs. Key drivers include increased adoption in telecommunications, government, energy and power, finance, and manufacturing industries. The platform capabilities – particularly in big data throughput, AI-powered early warning, dynamic monitoring, automated policy enforcement and API-based integration – are becoming decisive competitive differentiators. Enterprise investment priorities now emphasize unified control planes that significantly reduce operational cost compared to point solutions.

In 2025, the data security platform market shows a certain degree of concentration, with the top 10 vendors having a market share of 56.9%, indicating a significant remaining market space.

Our Company ranks first among named vendors with a market share of 9.7%, outperforming key competitors such as Company G (8.3%) and Company A (7.2%), Company O (5.6%), etc. Its leadership reflects strong positioning in secure platform architecture and industry customization.

Ranking	Company	Market share (by Revenue)
1	Our Company	9.7%
2	Company G	8.3%
3	Company A	7.2%
4	Company O	5.6%
5	Company E	5.5%
6	Company N	5.2%
7	Company D	4.3%
8	Company B	4.1%
9	Company M	3.8%
10	Company C	3.3%
Others		43.1%
Total		100%

Fig 12. Top 10 data security platform vendors by revenue in 2025 (China, by specialized security vendors)

Source: Frost & Sullivan; Annual Reports of Each Market Player; Interviews with Industry Experts

Notes: Company O was founded in 2005 and headquartered in Hangzhou, is a privately held provider of data security and digital transformation products and services.

Ranking of cybersecurity vendors in China (by specialized security vendors)

In 2025, the market size of China’s specialized security vendors sub-market of cybersecurity by revenue reaches RMB31.2 billion. Companies such as Company B, Company A, and Company F hold important positions in the market, with the top 15 cybersecurity vendors collectively accounting for 65.1% of the total market.

Our Company, ranking 14th with a market share of 1.1%, stands out as a rising competitor. The China’s cybersecurity market is highly competitive and rapidly evolving, driven by technological advancements and rising demands for digital protection. Key competitive factors include solution comprehensiveness, scalability, security robustness, and brand reputation. Our Company has demonstrated significant growth with its professional cybersecurity products and customer networks, demonstrating strong market competitiveness.

INDUSTRY OVERVIEW

Ranking	Company	Market share (by Revenue)
1	Company B	10.4%
2	Company A	8.0%
3	Company F	6.9%
4	Company C	6.6%
5	Company D	6.0%
6	Company E	5.5%
7	Company G	5.3%
8	Company H	3.8%
9	Company I	3.1%
10	Company J	2.6%
11	Company L	2.0%
12	Company K	1.4%
13	Company M	1.2%
14	Our Company	1.1%
15	Company P	1.1%
Others		34.9%
Total		100%

Fig 13. Top 15 cybersecurity vendors by revenue in 2025 (China, by specialized security vendors)

Source: Frost & Sullivan; Annual Reports of Each Market Player; Interviews with Industry Experts

Notes: Company P was founded in 2005 and headquartered in Beijing. It is a private information security technology enterprise specializing in data security, public security and cloud security.

Ranking of cybersecurity platform vendors in China (by specialized security vendors)

The Top 15 leading vendors, including Company A, Company F, Company B, Company G, and Company E hold over 64.4% of the market share. Among them, Company A ranks first with a share of 9.4%, followed closely by Company F, Company B and Company G.

Our Company holds a 1.5% market share alongside Company H. It applies AI and big data modeling algorithms to cybersecurity, making it highly competitive in the cybersecurity platform market.

Ranking	Company	Market share (by Revenue)
1	Company A	9.4%
2	Company F	9.2%
3	Company B	8.9%
4	Company G	6.2%
5	Company E	6.1%
6	Company D	6.1%
7	Company C	4.2%
8	Company I	3.6%
9	Company M	2.2%
10	Company H	2.0%
11	Our Company	1.5%
12	Company P	1.4%
13	Company N	1.3%
14	Company Q	1.2%
15	Company K	1.1%
Others		35.6%
Total		100%

Fig 14. Top 15 cybersecurity platform vendors by revenue in 2025 (China, by specialized security vendors)

Source: Frost & Sullivan; Annual Reports of Each Market Player; Interviews with Industry Experts

Notes: Company Q was founded in 1999 and headquartered in Xiamen, listed on the Shenzhen Stock Exchange in 2011. It focuses on electronic data forensics, public safety big data, new cyberspace security, and digital government services.

INDUSTRY OVERVIEW

SOURCE OF INFORMATION

Our Company has commissioned Frost & Sullivan, an independent market research and consulting company, to conduct an analysis to prepare a report on the China’s information security market, China’s data security market, China’s cybersecurity market. The report prepared by Frost & Sullivan for our Company is referred to in this document as the Frost & Sullivan Report. Our Company paid Frost & Sullivan a fee of RMB568,000 which our Company believes reflects market rates for reports of this type.

Founded in 1961, Frost & Sullivan has 40 offices with more than 2,000 industry consultants, market research analysts, technology analysts and economists globally. Frost & Sullivan’s services include technology research, independent market research, economic research, corporate best practices advising, training, client research, competitive intelligence and corporate strategy.

The Frost & Sullivan Report includes information on China’s information security market, China’s data security market, China’s cybersecurity market as well as other economic data, which have been quoted in the Document. Frost & Sullivan’s independent research consists of both primary and secondary research obtained from various sources in respect of the target market. Primary research involved in-depth interviews with leading industry participants and industry experts. Secondary research involved reviewing company reports, independent research reports and data based on Frost & Sullivan’s own research database. Projected data were obtained from historical data analysis plotted against macroeconomic data with reference to specific industry-related factors. Except as otherwise noted, all of the data and forecasts contained in this section are derived from the Frost & Sullivan Report, various official government publications and other publications.

In compiling and preparing the Frost & Sullivan Report, Frost & Sullivan has adopted the following assumptions: (i) China’s economy is likely to maintain a steady growth in the next decade; and (ii) China’s social, economic and political environment is likely to remain stable in the forecast period, which ensures the stable and healthy development of China’s information security market, China’s data security market, China’s cybersecurity market.