OVERVIEW

We are a specialized provider of intelligent information security solutions in China. According to Frost & Sullivan, in terms of revenue in 2025, we ranked first among China's specialized security vendors in providing data security platforms with a market share of 9.7%, seventh among China's specialized security vendors in providing data security with a market share of 3.8% and thirteenth among China's specialized security vendors in providing information security with a market share of 1.8% share. We are also an early participant in applying big data analytics and AI technologies across the information security domain in China, with a focus on data security, cybersecurity and other emerging fields.

We have established a security model designed to address the two core challenges of the digital era, namely inherent data governance and boundary-level threat defense. Organizations require a "defense-in-depth" architecture that protects both the infrastructure and the assets residing within it. To this end, we deliver a unified framework where our cybersecurity solutions secure the perimeter against external attackers, while our data security solutions govern the internal flow and integrity of sensitive information. By integrating these two critical dimensions, we provide a cohesive ecosystem that secures data at rest, in motion and in use, empowering organizations to comply with evolving regulations while accelerating their digital transformation. During the Track Record Period, we primarily offered our customers data security and cybersecurity solutions, supported by platforms, standardized software and specialized services. These solutions protect data, systems and networks across their lifecycle and operating environments. In particular:

- **Data security solutions.** According to Frost & Sullivan, a key data security challenge that organizations may face is that their sensitive information may be scattered across fragmented systems, requiring manual processes and security controls. This may lead to difficulties for organizations to maintain visibility, understand where important data resides, enforce policies consistently across multiple data assets and respond to different risks attacks from multiple directions in real time. We address this challenge by delivering unified control and intelligence driven operations across the full data lifecycle, covering collection, transmission, storage, use and sharing across an organization's architecture. In order to do so, rather than relying on a potentially endless list of disconnected and possibly incompatible software that are readily available in the market, we tailor our data security platforms to suit the needs of specific customer by encapsulating the various functionalities desired and operate as a single ecosystem with a centralized management interface. In addition to our platforms, we offer a comprehensive suite of data security software, recognizing that organizations may need single-purpose software that is promptly accessible, instead of requiring highly-customized solutions. We also provide specialized services that can support the design of governance frameworks by assessing data handling practices and developing long term, actionable plans aligned with business needs. In 2023, 2024 and 2025, our data security solutions had generated a revenue of RMB219.5 million, RMB281.8 million and RMB297.2 million, representing 42.5%, 42.8% and 42.0% of our total revenue, respectively.

- **Cybersecurity solutions.** According to Frost & Sullivan, as systems expand across networks, cloud platforms, applications and mobile terminals, security controls of an organization may become fragmented and inconsistent. Traditional tools depend heavily on manual processes and static rules, limiting visibility, delaying threat identification and hindering real time response. As a result, many companies struggle to understand their risk exposure, assess the effectiveness of defenses and maintain a continuously improving

security posture. We address these challenges by providing cybersecurity platforms, standardized software and specialized services that operate as a coordinated ecosystem. For example, our cybersecurity platforms can be tailored to customers' needs and integrate specific functions such as file analysis, behavior modeling and attack chain tracking into a single, wholistic and analytical view to reduce false alerts, uncover unknown threats and improve incident understanding, in contrast to relying on an array of different cybersecurity software that are not integrated. In addition to our platforms, we offer a comprehensive suite of cybersecurity software and services that can help companies design their cybersecurity architectures to align with regulatory expectations and their business needs. In 2023, 2024 and 2025, our revenue generated from cybersecurity solutions amounted to RMB254.1 million, RMB328.4 million and RMB339.7 million, representing 49.3%, 49.8%, and 48.0%, of our total revenue, respectively.

- **Other solutions.** Based on specific industry needs, we also provide customized solutions to customers by integrating of proprietary and third-party products and services. In 2023, 2024 and 2025, our revenue generated from other solutions amounted to RMB42.5 million, RMB48.9 million and RMB70.8 million, representing 8.2%, 7.4% and 10.0%, of our total revenue, respectively.

In 2025, we served 155 telecommunications network operators, 41 energy and power companies and 86 government and public sector entities. According to Frost & Sullivan, these organizations run large, interconnected systems that support essential public and commercial functions. Their technology environments expand quickly and often involve many departments, business systems and data flows, which makes it difficult to maintain consistent security and clear oversight. Our customers in different sectors may face similar difficulties. They store and use large amounts of data, rely on uninterrupted operations and must comply with growing regulatory requirements as their operations become more complex and thus prone to multi-directional attacks. We focus on helping them address these issues through customized platforms, practical software tools and specialized services that support planning, testing and daily operation. We also believe that intelligent computing centers have also become an important part of our customer base. These centers support high performance computing and AI workloads, using infrastructure that is large, multi-tenant and spread across regions. They often face unclear resource boundaries, heavy data transfer needs and the requirement to protect both hardware and cloud-native environments. Our platforms support identity checks, environmental monitoring, resource control, container and virtualization protection and secure transmission.

We have built a technology framework that supports proactive defense, security intelligence and data-driven operations. Our technology framework is based on four main foundations: big data processing, offense and defense innovation, data security assurance and AI. These foundations connect through APIs and a shared data system so that our technological know-how can be shared among the software we design and also the platforms that we create and customize for our customers. We also believe that R&D and innovation are central to our long-term strategy. As of December 31, 2025, our R&D team consisted of 186 members who were based in our Shanghai, Beijing, Wuhan, Hefei, Zhengzhou and Chengdu offices. In 2023, 2024 and 2025, our R&D expenses represented 23.2%, 15.2% and 14.4% of our total revenue, respectively. Our core technologies are developed in-house. As of December 31, 2025, our efforts had resulted in 145 granted patents, including 141 invention patents, and 202 registered software copyrights.

OUR COMPETITIVE STRENGTHS

We are one of China's leading specialized vendors of data security platforms

According to Frost & Sullivan, in terms of revenue in 2025, we ranked first among China's specialized security vendors in providing data security platforms with a market share of 9.7%, seventh among China's specialized security vendors in providing data security with a market share of 3.8% and thirteenth among China's specialized security vendors in providing information security with a market share of 1.8%.

Drawing on more than a decade of industry participation, we have developed an integrated architecture that addresses the full life cycle of data, including data identification, classification and grading, behavior and access analysis, risk monitoring and intelligent operations. Our work in data intelligence and AI can also allow us to embed automated data recognition, risk analysis and response capabilities within our product architecture, thus supporting both solution scalability and ongoing product enhancement across sectors. As enterprises and public institutions continue to strengthen their data protection systems, this foundation positions us well to respond to the markets' evolving requirements.

Our technical and industry insights have also been shaped by our participation in national and industry standard-setting. Since 2019, we have contributed to multiple issued national standards, including the Data Security Law Implementation Reference (First Edition) and the Data Security Capability Maturity Model (GB/T 37988-2019), the Telecommunication and Internet Data Security Risk Assessment Method (YD/T 3801-2020) and the Basic Telecom Enterprise Data Classification and Grading Method (YD/T 3813-2020), as well as various industry white papers.

Our teams and technologies have received various recognition from industry institutions. These include the "Zhu Wang 2022" technical support recognition and our designation as a Data Element Value Innovation Demonstration Base. Additional recognitions include the 2024 "Pan'an" Outstanding Case, the 2023 Xingyi Award, the 2022 Xinghe Case, the 2021 National Artificial Intelligence Innovation Application Competition first prize, the 2019 Wu Wenjun Artificial Intelligence Science and Technology Award (second prize), the 2017 China Cybersecurity Technology Contest (first place) and the 2024 "Shuxin Cup" Data Security Competition gold award.

Our capabilities are further supported by professional qualifications. For instance, we are among the few companies in China to have obtained five Grade One service qualifications issued by the China Cybersecurity Review Technology and Certification Center, covering software security development, emergency response, security operations, security integration and risk assessment. We also hold qualifications from the China Information Security Evaluation Center in areas such as risk assessment, security engineering, security development and big data security rating, as well as qualifications from the China Communications Enterprise Association relating to security design and integration, risk assessment and emergency response and training.

Our technical strength has also been demonstrated in major national events. We are designated as a major-event network security support unit and maintain rapid-response teams capable of nationwide on-site protection and emergency handling. We have undertaken security responsibilities for events including the Beijing 2022 Winter Paralympics, the 19th Asian Games Hangzhou, the China International Import Expo, the G20 Hangzhou Summit, the Belt and Road Forum for International Cooperation and the 70th National Day celebrations. The United

Nations Institute for Training and Research appointed us as the only big data application and security training base in the Asia-Pacific region and we serve as a member of the expert group of the United Nations Industrial Development Organization's Shanghai International Smart Manufacturing Promotion Center.

According to Frost & Sullivan, China's information security market increased from RMB73.2 billion in 2021 to RMB105.7 billion in 2025 with a CAGR of 9.6%, and is expected to grow to RMB172.7 billion by 2030 with a CAGR of 10.6%. The data security market grew from RMB18.6 billion in 2021 to RMB29.0 billion in 2025 with a CAGR of 11.7%, and is forecast to reach RMB50.9 billion in 2030 with a CAGR of 12.1%. The cybersecurity market increased from RMB54.6 billion in 2021 to RMB76.7 billion in 2025 with a CAGR of 8.9%, and is projected to grow to RMB121.9 billion by 2030 with a CAGR of 10.0%. The broader adoption of AI is also introducing new security gaps, contributing to rising demand for protection in areas such as AI security, vehicle network security and IoT security.

Given these market dynamics, we believe that our established position, technical capabilities, qualifications, role in standard-setting and proven performance in national-level deployments collectively place us in a strong position to capture the industry's growth opportunities.

Our technology framework can provide a durable foundation for continuous innovation and quality delivery

We have developed a technology framework that is based on the foundations of big data processing, offense and defense innovation, data security assurance and AI.

As one of the early companies in China to apply big data and AI to information security, we have accumulated a depth of technical expertise that enables us to operate as a closed loop linking large-scale data governance with complex model training. This integrated framework, which may be difficult to replicate without long-term accumulation, forms a durable technical foundation that supports sustained product innovation and reliable delivery across complex customer environments.

On the data-processing front, our proprietary architecture supports real-time processing of substantial data volumes while operating at significantly reduced power requirements compared with general-purpose designs, which enhances deployment efficiency for customers and provides high-quality data inputs for AI-driven functions. Building on this foundation, our integrated algorithm stack and vertical domain large models operate as a "security central hub," delivering rapid threat awareness, maintaining high detection precision and reducing operational noise. These attributes strengthen our competitive position by improving operational efficiency, response timeliness and the accuracy of security decision-making.

With respect to offense and defense innovation, we deploy a broad set of attack-detection and noise-reduction models that provide coverage across numerous stages of the attack chain. Combined with our full link-data-security assurance technologies, this framework enables comprehensive protection across network boundaries, sensitive assets, external threats and internal risks. Compared with manual methods, this approach significantly improves the efficiency and accuracy of vulnerability identification and supports more reliable assessments of attack impact. These capabilities reinforce our competitive strengths in analytical depth, breadth of coverage and resilience in mission-critical environments.

We embed intrinsic security throughout the AI lifecycle. Through adversarial sample-mutation engines and red-blue confrontation platforms, we conduct large-scale stress testing and simulated attacks during training to identify risks related to backdoors, poisoning and promp-based manipulation. This development framework enables vulnerabilities to be addressed in real time, while a model-firewall mechanism safeguards the stability and controllability of core algorithms under adversarial conditions. These features provide competitive advantages in model robustness, lifecycle governance and compliance readiness as AI-safety expectations continue to evolve.

Leveraging such technical foundation, we have established a proactive-defense product system designed to evolve with customer requirements. Hence, the technological know-how developed can be utilized in our platforms and software. Our platform-based architecture supports the complete cycle of collection, detection, analysis and response, reducing operational complexity and lowering resource demands. This structure is well suited to large-scale and complex environments, including telecommunications network operators and major enterprises, which require real-time performance, rapid product iteration and stable operation. These characteristics translate into competitive strengths in scalability, delivery efficiency and long-term service stability.

We possess R&D capabilities that can support scalability and reuse of technologies

We consider R&D and innovation central to our long term strategy. Our R&D is organized around the connected foundations of big data processing, offense and defense innovation, data security assurance and AI. These foundations operate as one system through standardized interfaces and a shared data layer, which allows us to share the technological know-how developed among our software and platforms, allowing them to sense threats, analyze them and respond automatically. Our AI models, including large models trained for security, help identify unusual activity, prevent fraud, trace phishing and detect malicious behavior from different angles. Together, these foundations create a cycle of detection, decision and response that supports system resilience, lowers cost and protects customers data and network across many environments.

Our R&D team combines internal development with targeted collaboration. As of December 31, 2025, our R&D team consisted of 186 members who were based in our Shanghai, Beijing, Wuhan, Hefei, Zhengzhou and Chengdu offices. In 2023, 2024 and 2025, our R&D expenses were 23.2%, 15.2% and 14.4% of total revenue, respectively. Our core technologies are developed in-house. We also work with selected partners, such as the China Internet First Response Center, which helps broaden our access to data and traffic resources for testing and improvement. Our R&D system has received third party recognition. We obtained CMMI Version 3.0 Maturity Level 5 and we have been recognized as a National-level Specialized, Sophisticated, Distinctive and Innovative "Little Giant" Enterprise by the MIIT. As of December 31, 2025, we had secured 145 granted patents, including 141 invention patents, and obtained 202 software copyrights.

Our R&D team includes employees with industry and academic experience both in China and overseas. The head of our research institute, Mr. Xia Yuming, received the 2020 Pudong New Area Science and Technology Progress Award. Mr. Wang Wenjun is the Deputy Head of our Research Institute and has extensive experience in cybersecurity research, data security governance and large-scale security infrastructure projects. He has participated in multiple provincial and municipal industrial internet situational awareness initiatives as well as major enterprise-level security infrastructure deployments. Mr. Wang has played an active role in the

cybersecurity and data governance community. He serves as the Chair of the OWASP Shanghai Chapter and has been recognized as a "Cybersecurity Craftsman" by the Shanghai municipal authorities. He is a member on the Expert Panel of the Data Security and Governance Working Committee of the Internet Society of China and a senior expert under the Digital Security Escort Program of the China Academy of Information and Communications Technology. He is also an expert participant in the Data Security Community Initiative. In addition, Mr. Wang is a senior information security training instructor certified by the International Training Centre for Authorities and Leaders under the United Nations Institute for Training and Research, where he has contributed to professional education programs in information security. He also serves as a practice-oriented security expert for the Shanghai Big Data Center, advising on data protection frameworks and operational security practices in large-scale data environments. He has received the CSA Leadership Award in recognition of his contributions to the development and advancement of cybersecurity practices. Another deputy head, Mr. Wei Guofu, led our team to win the First Prize (Team) in the 2017 China Cybersecurity Technology Defense Competition. Our R&D team supports our ongoing technical progress and stable delivery in complex environments.

We have also built a development foundation that supports technology reuse and scalability. Through standardized interfaces and modular components, we reduce integration effort and improve maintainability. Our component library includes engines for traffic processing, analytics, graph analysis and real time data warehousing, as well as modules for dashboards, user management, data gateways, scheduling and DevOps. We have also developed an architecture that supports AI application development with real time access to different data sources, dynamic context handling and basic agent functions. This approach allows us to configure platforms quickly, respond to customers' customization needs and maintain consistent quality across deployments.

Overall, our R&D capabilities, validated processes, experienced team, intellectual property and reusable development foundation form a stable system that supports scalability and reuse. These capabilities enable faster product updates, lower integration burden and dependable performance in complex environments, helping us maintain a competitive position over time.

We operate within a high-barrier customer ecosystem anchored by major enterprises and public institutions

We serve enterprises, government agencies and public institutions in sectors where stable and secure digital operations are essential. As of December 31, 2025, our customer base included telecommunications network operators, energy and power companies and government and public sector entities. These organizations manage large and interconnected systems that support daily public and commercial functions. They rely on consistent operations, clear oversight of data activity and compliance with sector rules. Many operate multiple business lines and technology systems, which increases the difficulty of maintaining a unified security standard and to functionally defend their assets from multiple directions. We focus on helping them address these needs through structured platforms and practical tools that support planning, testing and daily operation.

- Telecommunications network operators manage wide networks with heavy data movement and large user populations. Their information is often stored across many systems and handled by different departments, which can create gaps in visibility making them vulnerable to data leakage or attacks. Our solutions support structured asset management, coordinated network defense and automated data control. For example, our situational awareness platforms cover all three national operators in

China and reach many provincial branches and our data security control and data asset management platforms align with national quality requirements. We also provide consulting, testing, assessment and incident response services that help operators maintain safe operations across national and regional networks.

- Energy and power companies operate mixed information and control systems across plants, dispatch centers and field locations. They handle significant data volumes across many systems, yet some may lack clear data classification, ownership or traceability. Their operations must address both digital and physical risks which can be challenging considering the size and complexity of energy companies. For example, our platforms can be tailored to these companies' needs and help define data categories, support safe sharing, monitor sensitive transmissions and provide a unified view of conditions across the grid in order to allow better monitoring of potential attacks. We also conduct on site validation to confirm that protective measures perform as intended.

- Government and public sector entities operate large digital platforms and administrative networks. Their main challenge is maintaining trust, stability and coordination while handling data that may move across institutional boundaries. Our systems combine key security functions, including data monitoring, behavior analysis and policy compliance and help agencies maintain stable and compliant operations with continuous support, to avoid data leakage or threats.

We have also expanded into offering our solutions to intelligent computing centers, which handle high performance computing and AI workloads. These centers often have complex resource structures, heavy data transfer needs and requirements to secure both physical and cloud native environments. Our platforms support identity checks, environmental monitoring, resource control, container and virtualization protection and secure transmission. This gives computing centers a consistent and practical security foundation that meets operational and regulatory expectations.

Building relationships with these types of customers requires time, familiarity with industry processes and a clear understanding of system structure and constraints. Large enterprises and public institutions generally prefer to work with providers that can maintain stable support, ensure compatibility across systems and understand their long term needs. Developing a suitable security solution often requires joint planning, tailored design and iterative testing across multiple business units. Once deployed, the platforms and software installed become part of the customers' daily operations, which increases the cost and risk of switching providers. As a result, customers in these sectors tend to maintain long term cooperation with vendors that have demonstrated capability, reliability and knowledge of their industry environment, which, according to Frost & Sullivan, reflects the industry preference for continuity to preserve operational stability and reduce the risk of interruptions once a vendor has succeeded in its initial tender with the customer. Our relationships with our customers create high entry barriers for new market participants and support strong customer retention.

We are led by an experienced and industry recognized management team

Our management team brings deep insight into our industry, extensive operating experience and strong technical expertise, forming a critical foundation for our sustained business performance and market leadership. Our senior executives collectively possess long-standing experience in the information security sector and the team has remained stable over

time. Our co-founder and general manager, Mr. Zhang, is a widely recognized expert in the industry. He currently serves as a Member of the Inaugural Academic Committee, MIIT Key Laboratory of Data Security and Industrial Application Evaluation and an expert of the Shanghai Data Compliance and Security Industry Development Expert Group. Our Chairman, Mr. Hu, has participated in drafting multiple national and corporate information security standards and has received a number of prestigious industry awards, including the Wu Wenjun Artificial Intelligence Science and Technology Award for Scientific and Technological Progress, Second Class, the "National Model Worker of the Industrial and Information Technology System" and the "Cybersecurity Craftsmanship Award 2023." Mr. Hu was also recognized as the "Shanghai Craftsman" by the Shanghai Federation of Trade Unions in January 2024 and selected for the Shanghai Oriental Talents Program – Top Project by the Shanghai Talent Work Bureau in December 2024. Together, they lead our Group in driving continuous advancement of our technology infrastructure and solution capabilities. Their leadership ensures that we maintain a benchmark position in key domains such as artificial intelligence and data security, supporting the long term scalability and competitiveness of our business.

OUR FUTURE STRATEGIES

We plan to strengthen our market position in the data security sector

We aim to strengthen our market position by adjusting our products and services to match how digital systems in China are developing. As more organizations rely on connected systems for daily operations, security risks are no longer limited to a single device or network. Instead, they appear across mobile terminals, internal networks and cloud environments at the same time, requiring solutions that work together, can be deployed across different parts of an organization and can be updated when new risks appear. To meet these needs, we plan to expand the reach of our product portfolio and build a full set of solutions that cover endpoint, network and cloud environments. We also plan to focus on endpoint based data protection and zero trust models. Strengthening the standardization, efficiency and quality of our development and delivery processes will help us meet the needs of customers in different sectors and support our market position.

In addition, we plan to advance our core technologies so that our products can better support customers who manage growing amounts of data. As organizations move more of their work online, they need tools that can classify information accurately, transfer it safely and control its use throughout its lifecycle. To address this need, we intend to invest in technologies that combine AI with big data analytics, support privacy preserving methods and use techniques such as homomorphic encryption. These technologies are expected to help us improve security in areas such as classification, transmission, storage and governance.

According to Frost & Sullivan, China's digital transformation is expanding across industries and cities, with increasing emphasis on secure digital environments. This creates a need for consistent standards and trusted systems. We plan to take part in these developments by contributing to national and industry standards and by supporting governments and industry leaders in building secure digital platforms. By participating in these national initiatives, we aim to align our work with long term digital development goals and support customers as their systems grow.

We plan to advance core technologies and capture new opportunities through foundational R&D

We intend to improve our technology base so that we can support customers as they face new types of security risks and increased use of AI across their operations. As digital systems expand, organizations must protect both the algorithms they use and the data that supports them. These changes require security methods that can handle new attack patterns, protect information throughout its lifecycle and operate across different types of computing environments.

Our R&D strategy focuses on building the following: capabilities in a systematic and long term manner:

- ***AI security across the full lifecycle:*** As organizations rely more on AI models, the risks surrounding model training, model use and AI generated content continue to grow. We plan to develop technologies that protect AI systems from the beginning of model development through ongoing operation. This includes detecting threats that may appear during training, such as data corruption or hidden instructions and resisting attacks during model use, such as harmful inputs or misleading prompts. We also plan to strengthen the environments in which models are trained and run so that access, changes and internal operations can be monitored and controlled. These efforts aim to improve the safety, traceability and reliability of AI systems, which is becoming a core requirement for many industries.

- ***Compliance and content governance for AI generated material:*** As AI tools produce more written, visual and audio content, organizations need practical ways to identify harmful or inappropriate material. We are developing content recognition engines that understand meaning and context rather than relying only on simple checks. These tools are intended to support real time review of AI generated content and help block risks such as manipulated media or misleading information. This direction responds to growing regulatory expectations and helps customers maintain trust in their digital systems.

- ***Evaluation and protection of AI systems:*** AI systems are becoming widely used in business operations and many organizations must prove that their models are safe, stable and compliant. To support this need, we are building platforms that evaluate models, strengthen them against attacks, manage risks and support daily security operations. These platforms will help customers test their AI systems, understand how they behave under different conditions and keep them protected as they evolve. This approach supports the broader adoption of AI by giving users tools to manage related risks.

- ***Security operations for intelligent computing centers:*** As computing centers grow to support AI workloads, they operate large numbers of servers, store significant amounts of data and manage different types of applications at the same time. This creates new challenges in coordinating computing resources, controlling access and protecting models from attacks. We plan to develop security platforms that help manage these issues in a unified way. Our work will focus on defending against harmful inputs aimed at large models, preventing data tampering and improving model access control. These capabilities are intended to support stable and secure operation of complex computing clusters.

- ***Data protection and the safe use of data across organizations:*** The value of data is increasing and many organizations must share or transfer data while still meeting regulatory expectations. We plan to strengthen endpoint protection by developing methods that understand how data is used, identify risky behavior and apply dynamic controls to sensitive operations. This includes tools that isolate high risk actions, manage how data can be used and trace important activities when needed. We also plan to support the safe circulation of data between organizations. As data becomes a recognized production factor in China's digital economy, new business models and regulatory requirements are emerging. We aim to build data security infrastructure that helps organizations share data while protecting privacy and meeting compliance rules. By combining technology safeguards with rule based auditing, we plan to help customers unlock the value of their data in a controlled and trusted way.

- ***Security for connected devices and the Internet of Everything:*** The spread of intelligent devices in homes, cities and industries creates new risks because commands and data often flow across many systems without clear oversight. We plan to build device level security controls based on trusted hardware and our own middleware platform. These controls will help authenticate devices, block unsafe instructions and separate actions across different domains. This supports stronger protection for smart city, industrial and IoT environments, where device failures may lead to operational disruption. We also plan to develop solutions that connect device security, edge security and cloud security into one system, supporting the growing demand for secure AIoT applications.

- ***AI agent security:*** We intend to strengthen the safety framework of our AI Agent capabilities. The core objective is to balance capability boundary expansion with effective risk control. We are developing an active security defense system across the full AI Agent lifecycle, anchored on full lifecycle asset identification and governance, together with dual protection comprising external boundary controls and built-in security mechanisms. This approach is designed to enhance the security, reliability and controllability of our AI Agent operations while supporting efficient business execution and scalable deployment.

We plan to expand our customer coverage and international presence

We intend to broaden our customer base by serving more industries that require steady and compliant security operations. Sectors such as telecommunications, government and financial services face rising security pressures because their systems support essential services and handle sensitive data. As these sectors continue to grow and upgrade their digital infrastructure, they require security solutions that are reliable, easy to maintain and suitable for large and complex environments. By deepening our presence in these sectors, we aim to meet this increasing demand and strengthen our overall market position.

Through our long term cooperation with major telecommunications network operators, we plan to explore opportunities in consumer facing markets. As individuals use more online applications, connected devices and cloud services, the need for practical and affordable security tools is expanding. Working with telecommunications network operators provides a natural channel to deliver these services at scale and reach a broader user base. This helps us tap into a growing segment of the market while using the trust and distribution networks that operators already have.

In addition to large enterprises, small and medium sized businesses also need security solutions but often lack the resources to build them on their own. To address this gap, we plan to offer standardized security marketplaces and lightweight cloud based security services. These offerings allow smaller businesses to access key security capabilities at lower cost and with simpler deployment. This helps us reach a wider customer base and supports inclusive digital development across different business sizes.

Internationally, we plan to expand our footprint and make our products and services available to overseas markets. We intend to establish an international business headquarters in Hong Kong, including a global security operations center and a cross-border data security hub. We expect that our international business headquarters will allow us to leverage Hong Kong's role as a regional center for finance, trade and technology, thereby accessing customers across Hong Kong, Macau, Southeast Asia and other international markets. As more organizations operate across borders, the need for consistent and compliant security solutions increases and we aim to support these customers with end to end services.

We understand that different regions follow different rules for data protection and security. To meet these requirements, we plan to develop security compliance products designed for specific jurisdictions. This allows us to support customers who must operate under varying legal and regulatory frameworks. We expect to use a model that combines technology export with localized services delivered through partnerships with large enterprises and state owned groups. This approach helps us bring our technology to overseas markets while ensuring that services reflect local conditions and expectations.

Overall, our planned expansion across industries, customer groups and regions aims to meet rising security needs, support customers of different sizes and participate in the growing demand for trusted digital operations. By serving a broader range of markets, we aim to build a more balanced and resilient business over the long term.

We plan to attract, develop and retain core talent to build a stable and diverse talent system

We view talent as a key part of our long term strategy. As security needs grow and technologies change quickly, we need professionals who understand areas such as AI security, high volume traffic analysis, data management, intelligent algorithms and large model applications. We plan to continue investing in talent with these skills so that our teams can support new product development, respond to market needs and maintain steady delivery. We also plan to gradually build a designated group of employees who can support our international expansion by developing teams with global experience and local understanding in the regions we serve.

To support these goals, we plan to improve our talent management system. Our approach will cover the full cycle of selecting, placing, developing and retaining employees. Using a dynamic talent database, we aim to better understand the size, structure and needs of our workforce and design training programs that match different stages of employee development. We also plan to strengthen our incentive system so that rewards reflect job responsibilities and performance. This will help us attract and retain employees who fit well with our long term strategy and who can contribute to key roles within the organization.

Through these efforts, we target to build a talent system that is stable, diverse and able to support our continued development across different markets and product areas.

We plan to pursue strategic acquisitions that support long term competitiveness

We intend to explore strategic acquisition and partnership opportunities that can strengthen our technology base and support our long term development. As security risks evolve and customer needs become more complex, not all capabilities can be built internally at the same pace. Specifically, we plan to target companies with complementary technological capabilities in high-growth segments and established customer bases as well as regional market footprints to accelerate our market penetration. These transactions are expected to also enable us to achieve meaningful operational and cost synergies through shared R&D infrastructure, optimized supply chain management and unified go-to-market strategies. Through a careful and selective approach, we use strategic acquisitions, joint ventures, alliances and partnerships to reinforce our technology foundation, expand our capabilities and maintain steady competitiveness as the market continues to evolve.

When considering potential partners or acquisition targets, we plan to prioritize companies whose products or technologies can create synergies with our existing offerings. Such synergies will also support the expansion of our R&D resources and improve our access to a wider ecosystem of tools, talent and market opportunities.

As of the Latest Practicable Date, we had not identified specific targets or entered into binding agreements for any strategic acquisitions or partnership.

OUR SOLUTIONS

During the Track Record Period, we generated our revenue primarily from data security solutions and cybersecurity solutions. Within these two key categories, we provided three types of solutions, namely (i) platforms; (ii) standardized software; and (iii) specialized services. We also provided other solutions that are tailored to our customers' needs. The following table sets forth a breakdown of revenue generated by our solutions for the years indicated:

	Year ended December 31,					
	2023		2024		2025	
	(RMB'000)	*(%)*	*(RMB'000)*	*(%)*	*(RMB'000)*	*(%)*
Data security solutions						
– Platforms	84,242	16.3	127,325	19.4	148,520	21.0
– Standardized software	62,165	12.0	46,321	7.0	31,522	4.5
– Specialized services	73,129	14.2	108,170	16.4	117,172	16.5
Subtotal	**219,536**	**42.5**	**281,816**	**42.8**	**297,214**	**42.0**
Cybersecurity solutions						
– Platforms	45,513	8.8	88,195	13.4	90,597	12.8
– Standardized software	25,165	4.9	44,263	6.7	36,911	5.2
– Specialized services	183,441	35.6	195,933	29.7	212,175	30.0
Subtotal	**254,119**	**49.3**	**328,391**	**49.8**	**339,683**	**48.0**
Other solutions	42,544	8.2	48,929	7.4	70,758	10.0
Total	**516,199**	**100.0**	**659,136**	**100.0**	**707,655**	**100.0**

In general, our platforms and standardized software differ primarily in the level of customization, delivery format, implementation complexity and commercialization characteristics. Typically, each individual software provides a well-defined standard function that can be deployed quickly with minimal adaptation. By contrast, a platform bundles multiple functions to address a customer's specific operational and industry requirements. Notably, our platforms are not a mere stacking of software; rather, they involve deep, purpose-built integration that aligns with our customers' existing infrastructure and business processes. Consequently, our platforms require more extensive customization and longer implementation timelines, whereas our standardized software is designed for faster deployment and more immediate revenue realization.

The table below summarizes the key differences between these two businesses:

	Platforms	**Standardized software**
Degree of customization	High. Requires deep customization based on the customer's industry characteristics and specific operational conditions.	Low. Highly standardized, with minimal customization required.
Delivery format	Primarily delivered as pure software or integrated software-hardware solutions.	Primarily delivered as pure software solutions.
Implementation cycle	Long cycle, typically around one year. Implementation is complex and involves deep integration with multiple internal client systems.	Short cycle, generally within three months. Deployment is agile and typically implemented as a standalone module with rapid integration.
Payment milestones	Multiple milestones, usually three to five stages, with payments linked to project progress such as initial payment, preliminary acceptance, go-live, trial operation and final acceptance.	Limited milestones, typically two stages, with payments aligned with initial delivery and system go-live.

Data security solutions

It is not uncommon that organizations struggle with the same core problem in relation to data security. Their sensitive information is spread across different systems that do not communicate with each other, they may rely on manual steps and their security controls may not match. This may create blind spots and difficulties for organizations to understand where important data is stored, who is using it and whether any risks are developing. When teams cannot see their data clearly, it becomes difficult to enforce rules or respond to issues in real time. Consequently, they may fail to protect sensitive information effectively against data leakage or attacks across their organizational structure. The primary objective of our system is to eliminate data fragmentation by dismantling information silos.

We address these problems by creating a unified way to manage data security throughout the entire lifecycle of information. Instead of using separate tools that work on their own, we design our platforms, software and services to function as one connected ecosystem. Our system serves as the central nervous system of an organization's data security architecture. It is an integrated technology layer designed to ingest, process and analyze massive volumes of security-related data through AI-driven analytics. This architecture functions as the core foundation for a next-generation security operations center and aligns with the advanced principles of extended detection and response by providing a unified data baseline. By utilizing AI to correlate information from disparate sources, including networks, endpoints, cloud environments and applications, our system identifies hidden risks and automates complex security tasks. At the center of this ecosystem is a management platform that sets policies, coordinates responses and gives teams a clear view of what is happening. This philosophy helps remove disorder by bringing all security activities under a single framework.

In 2023, 2024 and 2025, the revenue that we generated from our data security solutions amounted to RMB219.5 million, RMB281.8 million and RMB297.2 million, representing 42.5%, 42.8% and 42.0% of our total revenue, respectively.

The following case study illustrates a typical data security project that we provide to our customers:

Case Study: A data security governance platform for Customer A

Project background

We designed, built and delivered a group-level data security governance platform for Customer A, one of the largest telecommunications network operators in China. The project was initiated to address challenges arising from the customer's highly distributed data environment, growing regulatory requirements and increasing need for secure internal and crossdepartmental data use. The platform is intended to enable centralized governance, improve risk visibility through intelligent analytics and support the customer's transition towards more systematic and proactive data security management.

Project scope and coverage

It was developed around four key principles: centralized management, intelligent classification and grading, end-to-end monitoring and closed-loop handling of security events. The system has been deployed across ten provincial operating companies and integrated with existing provincial platforms, allowing group-wide policy formulation and centralized enforcement.

The data security governance platform provides unified management of data assets across major business systems, databases, data fields and external data interfaces. It supports structured data, unstructured data and big data environments, covering approximately 30 different data types. To date, the platform has brought under centralized governance nearly one hundred thousand data assets across the group. Core functional modules include data asset inventory management, identification and classification of sensitive data, data masking validation, data flow and usage monitoring, risk detection and security operations management.

The platform has undergone large-scale commercial deployment and continuous operation. As of July 31, 2024, our data security governance platform had provided services to 31 provincial subsidiaries of Customer A, centrally managed and processed 97,000 data assets of Customer A as well as identified and recorded over 47,000 sensitive data entries and governed over 50,000 data security incidents monthly, demonstrating stable system performance under high data volumes and concurrent workloads.

The following diagram illustrates the interface the platform provided:

Implementation

The platform was implemented through deep integration with Customer A's existing data infrastructure and business systems. AI-based models were deployed to support automated sensitive data discovery, risk identification and noise reduction in alerts. Risk events are recorded with traceable operational context, enabling effective investigation and accountability. Centralized dashboards provide realtime visibility into data security posture across the group, while standardized workflows support issue remediation and escalation.

Strategic impact

This project enabled Customer A to move from fragmented and reactive data security practices toward a unified, realtime and proactive governance model at the group level. By strengthening data asset classification and grading capabilities and combining them with data security traffic monitoring, the platform achieved coverage for over 90% of governed data assets, with alert accuracy exceeding 90%. Through the application of subject-based noise reduction models, the average processing efficiency of risk handling tickets improved by approximately 93%.

The platform enhances Customer A's preparedness for regulatory compliance while allowing controlled internal and crossdepartmental data circulation. We believe that it has become a reference deployment for our data security solutions when serving large enterprise customers and supports Customer A's broader digital transformation strategy through improved data security operationalization.

The following sets forth the details of our key data security platforms, standardized software and specialized services that we offer to our customers:

Data security platforms

According to Frost & Sullivan, the systems of large organizations are often scattered across different networks, clouds and devices, which may lead to difficulties for organizations to see where data assets are, how data moves and whether something risky is happening. Many teams may also face growing compliance requirements but lack the suitable tools to monitor everything in real time in a consolidated and integrated manner, as organizations might have to adopt endless software options that may be disconnected and incompatible. Our philosophy is to solve these challenges by building a comprehensive security system covering the entire lifecycle of data and all scenarios, from data generation, storage, transmission, use to destruction and providing unified data security protection, governance and compliance capabilities.

In 2023, 2024 and 2025, the revenue that we generated from data security platforms amounted to RMB84.2 million, RMB127.3 million and RMB148.5 million, representing 16.3%, 19.4% and 21.0% of our total revenue, respectively.

Key customized data security platforms that we offer to customers include:

Security Data Center

Organizations collect huge amounts of security data, but it often sits in separate places, uses different formats and is hard to analyze. According to Frost & Sullivan, this may lead to difficulties for organizations to see the full picture of their security status, respond quickly, or ensure their data is trustworthy. We believe the solution is to unify all security data into a centralized data backbone with clear standards and consistent rules. Our Security Data Center does so through five forms of unification: collection, storage, authorization, governance and sharing. It normalizes disparate data streams, including logs, events and asset records and avoids duplicate collection to save space. It translates and stores everything in a standardized format with clear retention rules so teams can run deeper analysis without being blocked by data silos. It centralizes identity and permission management, so all connected systems work with the same secure access method. It governs the full lifecycle of security data, including metadata, data quality checks, sensitive data classification and enforcement of compliance rules. Our security data center makes high-quality data available to other platforms and create a reliable base for proactive threat hunting, patterns recognition and automated incident orchestration.

Data Asset Management Platform

Many organizations cannot effectively manage all the systems and devices they own. There are often discrepancies frequently exist between static records and the actual environment, responsibilities are unclear and teams struggle to meet reporting requirements. We believe the best way to fix this is to build a single, accurate source of truth for every asset, a digital master ledger and keep it updated through automatic discovery. Our Asset Management

Platform solves this by incorporating multiple functions simultaneously, including probes, API connections, traffic checks, login data and agent collection, supported by asset fingerprints. It manages data assets and lets teams create custom asset models through a visual editor, which helps the platform fit different industries. It runs a closed loop of asset accountability lifecycle management so responsibility is always clear. Assets can be organized across three layers, covering information systems, hardware and components. This platform may also be able to support frequent compliance tasks such as reporting, graded protection checks, critical infrastructure filings and special inspections. It may also be able to strengthen daily security by supporting vulnerability management, incident response and access control, allowing one round of governance to support many later security tasks.

Data Security Posture Management Platform

Organizations may fail to monitor data risks in real time because information comes from many sources and threats are constantly changing. According to Frost & Sullivan, users would need a way to detect "red flags" quickly and respond before problems grow into disasters. We believe the right approach combines real time monitoring with AI driven behavioral analytics to uncover both manifest and latent vulnerabilities. To this end, our Data Security Posture Management Platform uses built-in libraries of adversarial attack models and User and Entity Behavior Analytics to identify suspicious actions, such as improper access or possible data leaks. The platform may include simple drag-and-drop visible screens so organizations can design dashboards that show their risk level in real time. By combining data modeling, anomaly detection and AI-powered security copilot, our Data Security Posture Management Platform helps teams proactively manage the entire risks lifecycle – before, during and after security incidents.

Data Security Management Platform

Organizations may also struggle to maintain visibility into their data inventory, data residency and data lineage. Without this clarity, it may become difficult to protect data or catch risky behavior. We believe the best approach is to institutionalize data classification, track its movement and apply ongoing risk checks with help from AI. Our Data Security Management Platform, as illustrated in the case study above, identifies sensitive data across databases, files, systems and active interfaces. It uses vectorized classification and automated rules to categorize information with high precision. It monitors how data flows across the organization and flags strange activity by analyzing factors such as login environment, time, frequency, user behavior and flow patterns. It manages data resources, assigns lifecycle labels and creates multi-dimensional views showing how data and users interact over time. It discovers both static assets and dynamic systems, including APIs and can merge similar interfaces so the asset record stays clean. Together, these features can be able to help organizations understand their data environment, spot high value data and apply the right level of control.

Data Sharing and Exchange Platform

According to Frost & Sullivan, sharing files inside or outside the organization can be risky when sensitive information is not properly controlled. Organizations may lack a secure way to exchange files while keeping them encrypted and traceable. We believe file sharing should protect both confidentiality and accountability without compromising user productivity. Our Data Sharing and Exchange Platform supports safe file collaboration through a cloud drive style workspace for uploading, downloading and organizing files. It scans and identifies sensitive content in shared files and then classifies it accordingly using AI-powered analysis. All files will

need to be encrypted during both storage and transfer and each download uses a one-time key so only the specific and intended user can read it. The platform also includes visible and invisible watermarks that can be traced back to the exact person, time and communication channel involved if a data leak occurs. Every action will need to be logged and files can be traced end to end through full audit records. Our Data Sharing and Exchange Platform gives organizations a reliable way to share data without losing oversight.

Data security standardized software

Organizations may face difficulties in protecting their important information due to a lack of visibility into data storage, movement and access patterns. Traditional tools rely on static, rule-based logic, which often fail to detect emerging threats and overwhelm teams with excessive false positives. Our data security software use AI to monitor the entire life of the data, from collection to disposal. AI can help identify sensitive information quickly, update labels as systems change, choose the right protection for each situation, reduce redundant alerts and learn from real use so the system can continuously improve. Our suite of data security software, which can be used on a standalone basis, can bring together tools for identifying sensitive information, hiding or marking it, preventing leaks, checking databases, monitoring data movement, inspecting systems and keeping application interfaces safe. Together, they can give organizations a clear and intelligent way to protect their data.

In 2023, 2024 and 2025, the revenue that we generated from our data security standardized software amounted to RMB62.2 million, RMB46.3 million and RMB31.5 million, accounting for 12.0%, 7.0%, and 4.5%, of our total revenue, respectively.

Key standardized data security software that we offer to customers include:

Name	Pain points addressed	Means to address such pain points
Sensitive Data Discovery System	Sensitive data stored on different storages may be difficult to identify and become obsolete as systems change.	Searches quickly and accurately for sensitive information across many types of storage. Uses built in pre-defined classification templates to label data, checks whether storage and monitor compliance with internal and regulatory policies, identifies databases that were never recorded and builds a real-time catalog of data the organization can trust for security and governance.
Database Security Audit System	It is hard to detect malicious or unauthorized activities within complex database environments, especially when information is stored across different locations or sent through encrypted connections.	Monitors database activity in real time and establishes behavioral baselines through machine learning. It provides granular visibility into names, tables, users and actions, captures access with light tools, shows live sessions, points out unusual tools, addresses, user accounts and commands and allows fast searching so teams can investigate and respond to security incidents quickly.

Name	Pain points addressed	Means to address such pain points
Insight for Data Monitoring System	Information flows between clients, applications, databases and interfaces, creating blind spots that make it hard to identify risks or trace security incidents from origin to destination.	Provides full visibility into data flow. Discovers assets from traffic inspection, monitors sensitive access from end to end, uses detailed indicators to filter noise. By correlating related risks and offering session replay capabilities, the system reconstructs the full path of any activity and generates clear reports for daily security operations and incident response.
Static Data Masking System	Developers, testers and partners need realistic datasets for effective collaboration, but sensitive attributes must be obscured without compromising data utility or system functionality.	Creates secure, high-fidelity clones of data that preserve original structures and business logic while masking sensitive attributes. Supports a wide range of data sources, detects common sensitive pattern, keeps table relationships intact, perform pre-execution compliance checks, offers a diverse masking methods and provides full tracking with alerts, approvals and logs.
OmniMask Data De Identification System	One type of masking cannot support all needs. Static masking lacks flexibility for interactive use and real time masking is often inefficient for large-scale batches or data sharing.	Combines both static and real time masking and automatically select the optimal method for each situation. Supports a wide array of data sources and sensitive information types, offers a control gateway with role based access control, protects real time responses with reusable rules, lets apps request precise masking and ensures compliance with privacy regulations without disrupting business continuity.
Data Security Inspection Toolkit	Checks for safety and compliance are slow, inconsistent and difficult to compare, so problems are delayed remediation.	Provides a standardized workflow from information collection to project planning, execution, review and reporting. Includes tools for vulnerability detection, checking interfaces, analyzing logs, detecting security weaknesses and identifying sensitive data. Supports custom templates and includes knowledge libraries so teams can "check and go" without disrupting critical business operations.
Data Leakage Prevention System	Sensitive information can leak through various formats, including text, images and documents, while conventional filters miss context and overwhelm teams with excessive false positives.	Uses text matching, pattern recognition, artificial intelligence and language understanding to identify real risks. Analyses text, images and documents, labels data automatically, traces lineage, understands context to reduce redundant alerts and learns over time to refine its detection logic and enhance decision-making accuracy over time.

Name	Pain points addressed	Means to address such pain points
Watermark Traceability System	When data leaks occur, it is hard to identify the person or channel responsible.	Marks visible and invisible watermarks into the data assets. Linking each unique watermark to specific metadata, including user identity, timestamps and access channels in order to ensure end-to-end accountability. For structured data, it utilizes heuristic techniques such as adding fake rows or columns as traceable clues and provides one click tracing to show who used the data and when.

Data security specialized services

According to Frost & Sullivan, an industry pain point faced by organizations is their inability to design a comprehensive data security framework, translate laws and standards into daily operational practice and operate security programs over time. As regulations in data security are evolving rapidly and becoming increasingly stringent, organizations often feel the pressure because their current processes, staff capabilities and workflows do not match regulatory expectations. With our data security services, we hope to guide organizations through a lifecycle journey: from designing top-level rules, to evaluating risks in daily operation, to running an intelligent, measurable and sustainable operating system. We handle this by offering consulting, assessment and operations services that combine our expert experience with AI and large-model technology, this ensures that legal requirements, industry standards and internal policies can become actionable, measurable and automated operational workflows.

In 2023, 2024 and 2025, the revenue that we generated from data security specialized services amounted to RMB73.1 million, RMB108.2 million and RMB117.2 million, representing 14.2%, 16.4% and 16.5% of our total revenue, respectively.

Key data security services that we offer to customers include:

Data Security Consulting Service

A number of organizations lack of a clear blueprint for data security. Fragmented practices across departments in data collection, storage, transmission, usage and destruction often create gaps and inconsistent controls. We believe the right way is to understand the full lifecycle of sensitive data and design a long-term plan that fits the organization's real business situations. For such reasons, we provide our Data Security Consulting Service and handles such challenges by interviewing all departments of an organization involved in data processing, studying how sensitive data is collected, stored, transmitted, used and disposed and identifying risks across technology, processes, management and personnel. We will create a multi-dimensional assessment of the current state, covers risks across every stage of the data lifecycle and identifies technical, procedural, managerial and staffing problems. We then design a organization-wide governance blueprint, plans a three-to-five-year roadmap for building the data security system and provides practical, step-by-step guidance for each phase. We can also customize solutions based on specific business scenarios.

Data Security Assessment Service

Organizations may struggle to identify and quantify the potential impact of security incidents arising from risks across all business areas. Many organizations may not even know how to measure compliance with laws such as the Data Security Law or the Personal Information Protection Law. We believe the optimal approach is to use scientific methodologies, legal standards and industry frameworks to evaluate risks and provide clear, actionable remediation. Our Data Security Assessment Service handles it by using a comprehensive assessment matrix built from laws, standards and industry rules to identify potential threats. It focuses on industry-specific needs, quantifies the potential harm of threats and evaluates risks across all business scenarios. It produces practical remediation solutions that organizations can implement, helping them meet compliance requirements and strengthen their overall protection.

Data Security Operations

Even when organizations establish rules and perform assessments, they often cannot maintain long-term operational efficacy. Daily tasks such as monitoring flows, responding to incidents, managing alerts and checking compliance are scattered and manual. We believe the optimal approach is to build an integrated, automated, platform-based and intelligent operating system that tracks the full data lifecycle. Our Data Security Operations Service handles it by helping organizations design a unified compliance operation framework, using the data security management platform to manage historical data and maintain standardized operational workflows. It plans continuous monitoring of sensitive data flows, creates protection strategies for key points and aligns risk controls with compliance rules. It builds risk monitoring and incident response processes, sets indicators to track data flow risks, maps security use cases and formulate emergency plans. It also creates KPI driven auditing and optimization methods tied to strategies, risks and events.

Cybersecurity solutions

Modern cybersecurity teams may face expanding attack surfaces, limited visibility, cumbersome tool fragmentation and slow manual response cycles, all of which may delay response cycles against increasingly sophisticated threats to organizations. Our philosophy centers on transforming security operations from reactive postures to intelligence led strategies, enabling organizations to detect, predict and neutralize risks with greater speed, accuracy and autonomy. We believe that effective cybersecurity requires a defense in depth architecture augmented by AI-driven automation that accelerate threat discovery, enhance decision making and orchestrate response at scale. Our solutions are designed to unify proprietary products, comprehensive analytics and standardized services into a cohesive operating framework that empowers organizations remain ahead of the evolving threat landscape.

Our cybersecurity capabilities allow our customers to integrate automated asset mapping and external threat intelligence to uncover exposed systems, reduce blind spots and anticipate likely attack paths. We can reinforce proactive defense through zero trust architectures, web application firewall and endpoint detection and response solutions, providing strong front line protection. Using full traffic threat detection and AI-enabled threat hunting, we identify security risks with precision and accelerate the discovery of critical anomalies. To contain threats rapidly and minimize operational disruption, we can incorporate deception technologies, breach and attack simulation and security orchestration, automation and response ("**SOAR**") to automate response and coordinate actions across security tools.

In 2023, 2024 and 2025, the revenue that we generated from cybersecurity solutions amounted to RMB254.1 million, RMB328.4 million and RMB339.7 million, representing 49.3%, 49.8% and 48.0% of our total revenue, respectively.

The following is a case study illustrating a typical cybersecurity project we provide to our customers:

Case Study: Cybersecurity platform Project for Customer A

Project background

We developed and deployed a cybersecurity platform for Customer A, one of the largest telecommunications network operators in China, with the objective of establishing a unified, network-wide capability for security defense, monitoring and emergency response. The project was designed to address the scale and complexity of Customer A's nationwide cloud networks, IT systems and mission-critical telecommunications infrastructure and to improve coordination across group, provincial and departmental levels.

The cybersecurity platform was positioned as a core security operations hub, supporting centralized analysis, coordinated incident response and continuous security operations across the organization.

Project scope and coverage

The cybersecurity platform enables three-tier coordination across the central authority, group level and provincial operating companies. It supports 24-hour security event monitoring, graded incident response with defined escalation mechanisms and centralized handling of malicious IP addresses, domain names and URLs across the entire network.

The cybersecurity platform integrates security data from approximately 24 categories of business systems, including centralized internet access log platforms, website monitoring systems, internet data center and internet service provider systems and malware related systems. It processes seven major classes of security data, comprising 35 sub-categories and close to 200 distinct data types, such as security alert logs, network behavior data, file based data, threat intelligence, infrastructure metadata and command execution records. The overall data scale is at the petabyte level.

Within the security operations center environment, the cybersecurity platform supports host security monitoring, incident investigation and automated response. On average, it processes hundreds of millions of security alerts per day. Model-driven detection identifies several thousand security events daily. Following deployment, the average incident handling time was reduced from approximately 8.0 to 5.9 hours, while urgent incidents are typically resolved through closed-loop, networkwide handling within one hour.

The following diagram illustrates the interface of the cybersecurity platform:

AI-driven threat detection and intelligent operations

The cybersecurity platform integrates realtime analysis, offline analytics and graph-based correlation engines aligned with Customer A's existing technical architecture. These engines are supported by an AI-based security model trained on historical alerts, incidents and log data. The system correlates related attack signals across different stages, such as reconnaissance, exploitation, privilege escalation and data exfiltration, enabling structured attack chain analysis and traceable investigation reports.

In addition, the cybersecurity platform applies predictive analysis based on threat intelligence and observed attacker behavior patterns to assess potential next-step actions and issue advance warnings. This capability supports a transition from reactive response to anticipatory security operations, while reducing manual triage workloads for security analysts.

Strategic impact

Our cybersecurity project supported Customer A's transition from primarily passive defense to an intelligence-driven, proactive and increasingly automated cybersecurity operations model. It strengthened collaboration mechanisms across organizational levels and improved overall security governance for cloud networks, IT systems and telecommunications infrastructure. Our cybersecurity platform serves as a central operational foundation linking data, systems, personnel and processes and supports Customer A's objectives of regulatory compliance, effective operational defense and continuous security improvement.

Cybersecurity platforms

Organizations may rely on heterogeneous networks, cloud environments and distributed devices, achieving holistic visibility across the entire digital estate becomes a significant challenge. According to Frost & Sullivan, it may become difficult for the aforementioned organizations to see what is happening across the whole environment, spot real threats and react quickly when incidents occur, especially when using a high number of cybersecurity software that may be disjointed. Security teams often face a significant amount of alerts every day, many of which turn out to be unimportant. This slows them down and creates difficulties to identify real risks. We believe an optimal approach to solve these issues is to use one integrated security ecosystem capable of unifying environmental monitoring, intelligently triaging alerts and automating routine workflows to enhance operational efficacy. Our cybersecurity platforms are built to address this issue, with the aims of helping organizations transit from manual, reactive operations to intelligence-led, proactive protection. Our cybersecurity platforms are tailored to a customer's needs, then bring together three levels of security analysis: micro level analysis that examines files and code closely, meso-level analysis that monitor behavioral patterns of users and potential attackers and multi-source data aggregation that maximizes the reconstruction of cross-stage attack paths. In addition, these platforms leverage alert noise reduction technology to help security teams focus on high-value threats, highlight the threats that matter and guide teams through investigation and remediation. Our cybersecurity platforms help organizations stay ahead of new threats and maintain a strong, flexible defense.

In 2023, 2024 and 2025, the revenue that we generated from cybersecurity platforms amounted to RMB45.5 million, RMB88.2 million and RMB90.6 million, representing 8.8%, 13.4% and 12.8% of our total revenue, respectively.

Key cybersecurity platforms that we offer to customers include:

Vulnerability Management Platform

Organizations lack a comprehensive visibility into their systemic vulnerabilities. According to Frost & Sullivan, fragmented monitoring often leads to overlooked critical exposures, resources wasted on false positives and difficulties in validating the effectiveness of completed fixes. Our approach is to manage the entire vulnerability lifecycle within a unified environment, characterized by high-precision detection and automated orchestration. Our Vulnerability Management Platform delivers this by scanning systems, verifying real problems, tracking the remediation progress in order to ensure that fixes are successfully implemented. It collects information from servers, security devices, databases and more, giving teams a single view of all assets and potential risks. The platform uses multiple scanning methods to uncover vulnerabilities in both web applications and host systems. It also maintains a robust audit trail of all security activities, so information can be traceable and compliant with regulatory requirements. Our vulnerability management platform helps organizations reduce their attack surface, fulfill reporting obligations and maintain a healthy security posture.

Security Information and Event Management System

Organizations generate huge amounts of security data across fragmented systems, often resulting in data silos that impede holistic environmental visibility. We believe the most effective solution is to consolidate disparate security data into a centralized intelligence hub, analyze it with AI and visualize it in a way on which teams can react rapidly. Our Security Information and Event Management System addresses these challenges by collecting logs, normalizing them and applying advanced detection methodologies such as behavior analysis, correlation modeling and machine learning. It delivers the results through clear dashboards that can be customized

to highlight risk levels, suspicious activity, or important system events. The system covers the full workflow from detecting a possible threat to investigating it and taking action. By using SOAR, it is able to block harmful traffic, isolate risky accounts, or execute predefined playbooks without requiring manual intervention.

Cybersecurity standardized software

Organizations may find it difficult to keep their digital systems safe, driven by the dual pressures of increasingly sophisticated adversarial tactics and growing network complexity. According to Frost & Sullivan, traditional security tools often depend on static, rule-based signatures and manual intervention, which may be insufficient to address new or fast-changing threats. They also create vast volume of false alerts, making it hard for security teams to focus on the critical risks. Our cybersecurity software portfolio is designed to address these challenges with tools that can adapt quickly, analyze behavior and respond more intelligently. We would use AI to understand how systems normally operate, identify unusual actions, detect new types of threats and connect information from different sources. Our cybersecurity software may help organizations discover weaknesses, block attacks, reduce false alarms and streamline decision-making. With this approach, we help our customers build stronger, more proactive security operations.

In 2023, 2024 and 2025, the revenue that we generated from cybersecurity standardized software amounted to RMB25.2 million, RMB44.3 million and RMB36.9 million, representing 4.9%, 6.7% and 5.2% of our total revenue, respectively.

Key data security software that we offer to customers include:

Name	Pain points addressed	Means to address such pain points
Web Application Security System	Websites face constant automated attacks, such as botnets designed to probe for latent vulnerabilities. Traditional rule-based tools may not detect these evolving, machine-driven threats.	Uses active defense by adding dynamic checks to each request in order to verify authenticity; identifies suspicious behavior through machine learning; analyzes meaning and context in requests; safeguard against data exfiltration by scrambling sensitive inputs; blocks automated tools; and uses AI models to detect and block high-risk anomalies.
Breach and Attack Simulation Platform	Security products have been installed but not tested in real conditions, leaving organizations with a "false sense of security" and unverified defensive capabilities.	Simulates realistic attacks across diverse network infrastructures and system environments; identifies assets automatically; offers a vast array of testing scenarios; supports both non-disruptive simulations and controlled real-attack techniques; evaluates the detection and response capabilities of security products and protect against new attack variations; and delivers reports that facilitate the targeted fortification of identified vulnerabilities.

Name	Pain points addressed	Means to address such pain points
Distributed Deception System	Sophisticated attackers may employ advanced techniques to remain undetected within a network for long periods.	Creates realistic fake systems and services to divert and entrap attackers; detects any interaction with these decoys; captures and analyzes the attacker's operational behavior in the decoy environment to obtain attack intent and tactical techniques, procedures and patterns (TTPs), providing high-confidence warning evidence for incident analysis; and can execute safe counter-actions when needed.
Next-Generation Firewall System	Older firewalls lack the visibility required to govern modern applications or neutralize advanced threats.	Conducts traffic analysis in detail, identifies users and applications, blocks harmful content, restricts inappropriate websites, supports secure connections, balances network load and updates threat intelligence in real time.
Intrusion Prevention System	Organizations struggle to mitigate multi-vector attacks such as SQL injection, reconnaissance scanning, malware or credential harvesting.	Detects many types of attacks in real-time; integrates with other security tools to neutralize threats faster; identifies users and applications; manages bandwidth for critical services; and sends alerts through multiple channels.
Comprehensive Log Analysis System	Fragmented log storage across disparate environments complicates investigations and hinders the ability to satisfy stringent regulatory meet compliance requirements.	Aggregates logs from diverse sources; analyzes them for anomalous patterns; supports regulatory compliance audits; provides dashboards and reports; and issues real-time alerts to enable rapid incident response.
Security Operation and Maintenance Management System	Inadequate oversight of privileged accounts and administrator activities creates accidental or intentional misuse.	Manages user identities, permissions and sessions; logs all critical actions; supports multi-factor authentication; and enables session replay of for auditing and investigation.
Network Traffic Analysis System	Sophisticated attacks evade detection by blending into massive volumes of network traffic.	Collects and analyzes network traffic; identifies suspicious files and behavior; supports sandbox testing; detects hidden communication channels; reconstructs files and sessions for investigation; and provides detailed searchable records for rapid investigation.
Website Cloud Monitoring Platform	Manually monitoring large website portfolios for defacement, illegal content, or outages is impractical and error-prone.	Monitors websites automatically at scale; detects abnormal changes; identifies harmful or unauthorized links; sends real-time alerts; and generates periodic risk assessment reports.

Name	Pain points addressed	Means to address such pain points
Security AI Agent Platform	Security teams spend significant time analyzing alerts and preparing reports.	Uses AI-powered "Security AI Agent Platform" that can investigate alerts, contain malicious activity, generate reports and automate routine workflow through a visual workflow editor.
Intelligent Code Audit System	Security flaws in software code are often discovered late, increasing remediation cost and business risk.	Uses AI to scan source code of software, identify common vulnerabilities, provide explanation precisely, provide recommended fixes, support multiple programming languages and empower teams to enhance security early in the software development cycle.

Cybersecurity specialized services

It is not uncommon that organizations today face significant challenges in building and operating a complete cybersecurity system. Many organizations contend with operational fragmentation, manual-heavy processes and critical cybersecurity skill gaps, which impede their ability to preemptively neutralize attacks and sustain high-level defenses. According to Frost & Sullivan, as adversarial tactics escalate and regulatory frameworks become more stringent, existing internal capabilities often fall short of required protection standards. We target to guide organizations with our cybersecurity services, through a full security improvement journey that begins with planning, continues through testing and daily operations and extends into emergency response. We combine expert knowledge with AI, to turn complex requirements into practical, measurable and sustainable security actions that ensure long-term operational resilience.

During the Track Record Period, the revenue that we generated from cybersecurity specialized services amounted to RMB183.4 million, RMB195.9 million and RMB212.2 million, representing 35.6%, 29.7% and 30.0% of our total revenue, respectively.

Key cybersecurity services that we offer to customers include:

Security Consulting Service

Our security consulting service assists organizations in identifying security baseline gaps within business scenarios and planning a security architecture system that complies with regulatory requirements and supports business development. Security controls are often developed in information silos across departments, resulting in inconsistent protection and gaps across the environment. We believe the right way forward is to design a coordinated security architecture that matches the organization's business operations, regulatory obligations and risks brought by digital transformation. Our Security Consulting Service addresses this through conducting a comprehensive review of governance structures, organizational roles, security policies, technical safeguards and security operations. We would map accountability, assess dependencies among projects and deliver a phased implementation roadmap. We may also design thematic plans for cloud environments, secure software development processes and security operations, enabling organizations to build a system that is comprehensive, coordinated and adaptable over time.

Security Operations Service

Organizations may be unable to maintain effective daily security operations because of limitation of manpower, lack of around-the-clock monitoring capability, or inability to correlate alerts across disparate systems to reconstruct full attack chains or respond decisively. We believe the optimal approach is to enhance the timeliness of security incident detection and response through an integrated security operations platform combined with continuous monitoring and analysis by a team of experts. Our Security Operations Service addresses this by combining a centralized security operations platform with a remote or onsite team that provides around-the-clock monitoring, threat analysis and incident response. The platform collects alerts, manages assets and vulnerabilities and supports workflow tracking. Our experts design customized response processes, continuity measures, reporting flows and service level targets based on the organization's needs. Our security operations service creates a closed loop that helps cover detection, investigation, response and improvement, helping organizations strengthen their security readiness with predictable and measurable results.

Security Testing and Assessment Service

Some organizations may find it difficult to identify vulnerabilities across their multiple layers of systems when the assets, risks and threats span physical infrastructure, networks, systems, applications and data stores. We believe that effective risk management begins with a structured and scientific assessment that evaluates physical, network, system, application and data level risks. Our penetration testing service is essentially a simulation of cyber-attack whereby we mimic potential attackers' tactics, techniques and procedures to perform in-depth security path detection on target systems. The testing process strictly adheres to the principle of business continuity and after remediation, a closed-loop retest is provided to ensure that security vulnerabilities are substantially eliminated. By identifying risks, providing targeted remediation recommendations and performing retest verification, the service helps clients establish a closed-loop risk management mechanism. Such structured evaluation can help organizations understand the potential impact of incidents and take steps to make their systems more resilient.

Emergency Response and Critical Protection Service

When a sudden cybersecurity incident occurs, organizations may struggle to react quickly, contain damage, or restore operations. Major events also require enhanced protection to ensure continuous and stable system performance. We believe the optimal approach is to provide rapid response services supported by experienced specialists who can contain the incident, eliminate the threat and help restore systems safely. Our Emergency Response and Critical Protection Service addresses this by providing immediate support for intrusion events, malicious code and ransomware. Backed by our cybersecurity specialists, the service enables rapid containment of active threats, thorough eradication of malicious elements, secure restoration of affected systems and detailed forensic analysis to identify the origin of the attack. For major activities, we may provide on-site experts, high frequency inspections and strengthened monitoring to ensure system security and stability. Our emergency response and critical protection service ensures that businesses remain stable and that risks remain under control during both unexpected incidents and high profile events.

Other solutions

In addition to our data security and cybersecurity solutions, we also tailor for our customers integrated solutions. We typically develop our integrated solutions by integrating proprietary and third-party hardware, software and services into a unified, multi-layered and dynamically coordinated security framework that meets customers' comprehensive requirements in data security governance, threat protection, risk management and regulatory compliance. The core value proposition of our integrated solutions lies in breaking down the operational silos of standalone security products and achieving global optimization and intelligent linkage of security capabilities through technology integration, service convergence and ecosystem collaboration.

In 2023, 2024 and 2025, the revenue that we generated from other solutions amounted to RMB42.5 million, RMB48.9 million and RMB70.8 million, representing 8.2%, 7.4% and 10.0% of our total revenue, respectively.

The Intelligent Computing Project

In 2024, we adjusted our strategic focus and expanded into the AI and computing power sectors. To this end, we secured a national-level project in Southwestern China from Customer G (the "**Intelligent Computing Project**"), which accounted for the majority of our revenue from other solutions in 2025. Upon its completion, the Intelligent Computing Project will serve as a key node of China's national integrated computing power network, enabling cross-regional allocation of computing resources and driving low-carbon, high-efficiency development of AI training, big data analytics and cloud applications.

Pursuant to the project agreements, we are primarily responsible for (i) procuring and integrating software, hardware and services to build a comprehensive security system covering cloud computing power platform security, data security and scheduling security; (ii) upgrading the security protection capabilities of Customer G cloud computing power platform (the "**Cloud Computing Power Platform**") to provide more effective protection for the cross-regional and large-scale computing power resources it dispatches; and (iii) providing security-related technical support services and performing security system monitoring and maintenance services for the Cloud Computing Power Platform. The project has a term of two years and will be delivered in three phases. For each phase, the project agreements (i) define our specific installation, commissioning and trial operation tasks; and (ii) stipulate the customer sourcing targets that we are required to achieve.

As the Intelligent Computing Project represented our first foray into the AI and computing power sectors, the customer sourcing target of the first phase was not met on December 31, 2024. Nonetheless, in consideration of the recent launch of the cloud platform and market demands, we renegotiated with the customer to postpone the deadline for meeting our remaining customer sourcing targets to December 31, 2027. As of the Latest Practicable Date, we had entered into a letter of intent with a customer for its subscription of computing power from the Cloud Computing Power Platform, the contract value of which would enable us to meet our customer sourcing targets in the second and third phases by the end of 2027.

R&D

R&D is central to our strategy and future growth. Our commitment to R&D allows us to meet customer needs and deliver differentiated, cutting-edge solutions. As of December 31, 2025, our R&D team consisted of 186 members who were based in our Shanghai, Beijing,

Wuhan, Hefei, Zhengzhou and Chengdu offices. In 2023, 2024 and 2025, we incurred RMB119.9 million, RMB100.1 million and RMB101.9 million in R&D expenses, representing 23.2%, 15.2% and 14.4% of our total revenue, respectively, underscoring our dedication to continuous improvement and technological advancement. See "Financial Information—Results of Operations—R&D Expenses." As of December 31, 2025, we had secured 145 granted patents, including 141 invention patents, and obtained 202 software copyrights, continuously strengthening our intellectual property barriers and providing a solid foundation for the transformation of cutting-edge technologies.

Unlike some of our competitors who rely on off-the-shelf solutions, our early investment in big data and AI has enabled iterative innovation and adaptive models that balance generality and accuracy across diverse scenarios, positioning us at the forefront of technological advancement.

Our R&D Strategy

Our R&D strategy combines foundational research focused on core technical requirements with product line R&D that emphasizes functionality and customization. Our product managers work closely with our customers to gather requirements and assess feasibility, while our technical teams leverage deep academic and industry experience to drive innovation in big data, AI and security technologies. Our core technologies are developed in-house, which ensures independence and control over critical innovations.

During the Track Record Period, our R&D efforts focused on continuously upgrading our core data security and cybersecurity platforms to address evolving threat landscapes and customer needs, with particular emphasis on enhancing detection accuracy, operational efficiency and automated response capabilities. For instance, we advanced our Data Security Management Platform with AI-driven data classification and our Security Information and Event Management System with AI-assisted threat analysis and SOAR-powered automated response. These innovations collectively enable our customers to more effectively monitor, investigate and respond to sophisticated cyber threats while streamlining their security operations.

Our technologies

Our data security solutions utilize a suite of sophisticated technologies designed to ensure end-to-end traceability, enabling organizations to govern the entire data lifecycle as information is originated, accessed, transmitted and archived across heterogeneous environments, which primarily include:

- Data dark watermarking based on information encoding technology (基於信息編碼技術的數據暗水印), which embeds identifiers inside data in a way that leaves the original content unchanged, allowing the source of a leak to be traced even when most of the content is missing;

- Reversible data morphology preservation technology for privacy protection (防隱私洩露的可逆的數據形態保持技術), which applies a reversible transformation to sensitive information so that it can be protected while still retaining a usable structure for business processes;

- Fluorescent marking for data application mapping (基於熒光標記的數據應用測繪技術), which helps us reconstruct the path that sensitive data takes across systems by marking its movement at various points;

- High-performance database audit engine for sensitive data discovery (全自動高性能發現訪問敏感數據的數據庫審計引擎), which identifies sensitive information by rebuilding database activity from network traffic to avoid interfering with the database itself; and

- Precision sensitive data discovery and classification engine based on multidimensional evaluation system (基於多維度評價系統的敏感數據精準發現及分類引擎), which studies the format, attributes and meaning of files to determine whether they contain sensitive material.

These technologies help organizations maintain visibility over their information and identify instances where sensitive data may be accessed in unexpected ways.

Our cybersecurity solutions utilize technologies designed to achieve multi-dimensional threat detection, reconstruct the end-to-end attack lineage and facilitate high-velocity forensic investigations, which primarily include:

- Operational risk alert analysis and correlation engine (基於運維業務風險告警分析歸並引擎), which examines large volumes of alerts and identifies statistical relationships that show when separate events may be part of the same underlying issue;

- Alarm correlation engine based on information theory (基於信息論的告警關聯引擎), which organizes complex alarm data into patterns that help operators identify possible attack methods;

- User risk behavior intelligent insight engine (用戶風險行為智能洞察引擎), which studies sequences of user actions and compares them to historical patterns to determine when behavior may indicate a threat;

- Webshell detection technology based on access features (基於訪問特徵的腳本木馬檢測技術), which uses machine learning to identify unusual access patterns that may indicate the presence of malicious files; and

- Next-generation automated machine behavior dynamic defense technology (下一代自動化機器行為動態防禦技術), which verifies whether automated requests behave in a manner consistent with legitimate activity, which helps prevent unauthorized automated access.

These technologies give organizations a clearer picture of how threats develop and support a more structured response when network behavior deviates from expected patterns.

Outsourced R&D

During the Track Record Period, we engaged third-party developers to undertake the coding, system design and module development for certain basic functionality. In 2023, 2024 and 2025, our outsourced R&D expenses was RMB21.6 million, RMB23.9 million and RMB17.1 million, respectively, primarily for customized development services.

Such strategic approach allows us to avoid reinventing the wheel by leveraging external expertise and pre-existing solutions for non-core or specialized components, enabling us to allocate our internal R&D resources more efficiently to high-value, core technology development initiatives that drive our competitive advantage.

INTELLECTUAL PROPERTY

As a result of our strive for R&D and advanced technologies, we have continued to enhance our intellectual property portfolio. We protect our intellectual property rights through a combination of copyrights, trademarks, patents as well as confidentiality agreements with our employees and customers. By December 31, 2025, we had been granted 145 granted patents, including 141 invention patents, and obtained 202 software copyrights. Moreover, as of the Latest Practicable Date, we had registered 95 trademarks and two domain names in the PRC. See "Appendix VI—B. Further information about our business—2. Our Intellectual Property Rights."

We generally require our employees to enter into confidentiality agreements to acknowledge that inventions, trade secrets, developments and other processes generated by them on our behalf are our property and assigning to us any ownership rights that they may claim in those works. See "Risk Factors—Risks Relating to Our Business And Industry—We may be subject to significant intellectual property infringement claims, including for the unauthorized use of software, which may result in substantial liabilities and disruption to our business and operations."

Our Directors confirm that, during the Track Record Period and up to the Latest Practicable Date, we were not aware of any infringement (i) by us of any intellectual property rights owned by third parties; or (ii) by any third parties of any intellectual property rights owned by us. Further, as at the Latest Practicable Date, we were not involved in any litigation or legal proceedings in relation to any material claims of infringement, either threatened or pending, of any intellectual property rights imitated by or against us that had a material and adverse effect on our business.

AWARDS, RECOGNITIONS, AND CERTIFICATIONS

We have earned awards in cybersecurity competitions and supported major international events, demonstrating our strength in delivering advanced security solutions. We also hold some of the highest-level of certifications in China's information security industry. For instance, we have been granted the Information Security Service Qualification by the China Cybersecurity Review Technology and Certification Center, meeting Level 1 standards in secure software development, incident response, security operations and maintenance, system integration and risk assessment. We are one of seven companies nationwide to achieve Level 1 qualifications in all five categories. We also hold certifications from the China Information Security Evaluation Center for risk assessment, security engineering, secure development and big data security ratings, as well as certifications from the China Communications Enterprise Association for security design and integration, risk assessment, emergency response and security training. In addition, we were among the first companies to receive top-tier certification for software development, jointly issued by the China Software Evaluation Center and the Data Security Professional Committee of the China Computer Industry Association.

We maintain a portfolio of ISO certifications, including ISO/IEC 20000-1:2018 for IT service management, ISO/IEC 27001:2013 for information security management, ISO 9001:2015 for quality management, ISO 14001:2015 for environmental management and ISO 45001:2018 for occupational health and safety management.

We have earned national and industry awards, including the first prize in the National Artificial Intelligence Innovation Application Competition and top honors in the "Wangding Cup" Cybersecurity Competition. Our achievements also include the Wu Wenjun Artificial Intelligence Award, gold medals in the "Shuxin Cup" Data Security Competition and recognition as a Data Element Value Innovation Demonstration Base. We have been named an Outstanding Technical Support Unit by the Ministry of Industry and Information Technology and recognized for excellence in cybersecurity information reporting.

The following table sets forth the other notable awards and recognitions that we have been accredited with during the Track Record Period:

Year of issue	Name of award or recognition	Issuing authority
2025	2025 Digital China Innovation Competition – Digital Security Track Outstanding Case Award (Winner) – Data Identification Innovation Application Based on Natural Language Processing and Optical Character Recognition Algorithms	Fujian Communications Administration, China Software Testing Center (Software and Integrated Circuit Promotion Center of MIIT), China Computer Industry Association Network and Data Security Professional Committee
2025	2025 Digital China Innovation Competition – Digital Security Track Outstanding Case Award (Silver) – IPDRR-driven Data Security System Empowering IoT "T-type" Governance Practice	Organising Committee of Digital China Construction Summit
2025	Outstanding Contribution Award – China Computer Industry Association Network and Data Security Professional Committee	China Computer Industry Association Network and Data Security Professional Committee
2024	Data Element Value Innovation Demonstration Base	China Famous Brand/Data Element Price Formation and Recognition Innovation Laboratory
2024	Panshizhixing – Most Influential Enterprise in Network and Data Security	Shanghai Internet Association
2024	Panshizhixing – Most Competitive Local Enterprise in Network and Data Security	Shanghai Internet Association
2024	Second "ShuXin Cup" Data Security Competition – Gold Award	ShuXin Cup Data Security Competition Organising Committee
2024	Second Prize of Jin Lingguang Cup Data Security Track – Data Security Management System	China Internet Association
2023	CSA 2022 Security Innovation Award	CSA Greater China
2023	Xingyi Award Certificate – Building a Trusted and Controllable Data Security Control System Based on "Zero Trust"	China Academy of Information and Communications Technology

Year of issue	Name of award or recognition	Issuing authority
2023	Xingyi Award Certificate – Real-time Monitoring Platform for Abnormal Behaviour in Sensitive Data Operations Based on Streaming Data Processing Engine	China Academy of Information and Communications Technology
2023	First QiangJi Cup Data Security Skills Competition – National First Prize	Telecom and Internet Industry Data Security Talent QiangJi Programme

OUR BUSINESS MODEL

The following sets forth a summary of our business flow:

Initial customer engagement and needs identification

Engagements typically begin when a customer identifies a need for enhanced data protection, cybersecurity capabilities, or system upgrades. Depending on their requirements, the types of projects and regulatory requirements, our customers may procure from us through (i) direct negotiation; (ii) public tendering; or (iii) invited quotation with comparative bidding among multiple vendors. We would normally become aware of the opportunities to tender for projects through publicly accessible websites of our customers which would make available the relevant details pertaining to the projects. Based on publicly available information, we assess our customers' objectives, existing systems, operational constraints and security requirements.

Tender process

For new systems or solutions, our customers may issue formal tenders setting out technical specifications, performance requirements, pricing terms and delivery schedules. Upon receipt, we review the tender documents and assess factors such as pricing, project scope, technical requirements, timelines, competition and qualification criteria. Where appropriate, we conduct a feasibility assessment to determine alignment with our business objectives. We would submit a proposal that typically includes a preliminary solution design reflecting the customer's requirements. During the years ended December 31, 2023, 2024 and 2025, we had 300, 297, 225 of our projects out of a total of 983, 980 and 957 gone through a bidding process, representing a success rate of 30.5%, 30.3% and 23.5%, respectively.

We have observed that should we succeed in a tender, the subsequent engagement of the same or similar nature with the same customer would likely be a direct negotiation, as our customers may opt to do so for more efficient operations. Thus, projects involving system upgrades, expansions, maintenance, or ongoing operational support are more commonly awarded through direct negotiation, particularly where the customer already uses our products or services. Negotiations may cover scope, pricing, regulatory requirements, procurement policies and delivery timelines and may extend over several weeks or months.

Execution of framework agreements

Following selection, we enter into a framework agreement that sets out key commercial and operational terms, including scope of work, pricing principles, responsibilities, service levels, confidentiality and change management. Where customers operate through multiple subsidiaries, project-specific agreements may be entered into at the subsidiary level.

Due diligence and solution design

We conduct comprehensive requirements discovery and research in strict accordance with the delivery scope and requirements stipulated in the agreement. Through in-depth interviews with our customer's management team, business departments and technical teams, coupled with multi-dimensional approaches, including asset inventory and mapping, technical assessment and testing as well as compliance review, we accurately identify our customer's requirements and develop a formal requirement specification document subject to our customer's review and sign-off.

Once we have a finalized requirement specification document, we move on to the design and development of solutions. During this stage, we formulate an overall system architecture and create detailed design documents. We typically hold formal design review meetings to validate the outputs. Our core technicians then code according to the approved design and conduct unit testing as well as code reviews to ensure that our solutions meet our quality standards. If our technicians identify any issue during unit testing or code reviews, the code will be revised and retested until it meets all required standards.

Project execution, installation and integration

Upon customer approval, we commence deployment and implementation phase. Before deployment and installation, we prepare detailed test plans and test cases to identify and resolve any malfunctions in our software. All implementation activities are performed directly within the customer's infrastructure and on-premises, encompassing installation, configuration, integration, testing and training. Typically, our designated personnel conducts an on-site visit to the customer's premises to perform local installation of our software on the customer's designated computers and under no circumstances are the software installed on our designated personnel's personal or privately owned devices. We work with the customer's technical teams to ensure the solution is integrated into their existing operational workflows, followed by a formal handover for production-ready operations. This on site installation ensures that the solution operates within the customer's environment and accommodates their specific technical and security requirements.

Ongoing support, maintenance and relationship development

After deployment, we continuously provide the customer with software support, update and optimization services. We also collect and analyze feedback from the customer and channel any new requirements or improvement opportunities into our R&D process for future iterations.

As of December 31, 2023, 2024 and 2025, we had 892, 690 and 612 contracts on hand, respectively. The number of our contracts on hand decreased over the Track Record Period, primarily because against the backdrop of intensifying industry and price competitions, some of our customers tended to consolidate multiple projects into a single contract, resulting in a year-on-year contraction in our tender volume. As of December 31, 2023, 2024 and 2025, the outstanding balance of our contracts amounted to RMB642.2 million, RMB519.7 million and RMB381.9 million, respectively. The outstanding balance of our contracts decreased over the Track Record Period, primarily attributable to our improved project delivery efficiency, as evidenced by the steadily increasing revenue that we recognized.

Some of our long-term contracts each comprises multiple projects. During the Track Record Period, we incurred gross losses on certain projects, which was primarily attributable to project-specific circumstances rather than systemic deficiencies in our project management capabilities. See "Risk Factors—Risks Relating to Our Business and Industry—Our revenue model is project-based. Any significant cost overruns or failure to fulfill our contractual obligations may materially and adversely affect our business, financial condition and results of operations."

Revenue generation and pricing

We generate revenue through a combination of project based fees, solution licensing and service charges. Project revenue is influenced by solution complexity, customization level and installation scope. Recurring revenue may include maintenance fees, software updates, managed services, or long term operational support.

The pricing mechanism for our platforms and specialized services is designed to reflect the costs incurred during the design and development phases, plus a profit margin that varies depending on the type and model of the solution. We periodically review our costs to ensure our prices are up-to-date and reflective of current market conditions. In cases where customers place comprehensive orders involving multiple solutions and services, we may offer more competitive pricing. This is contrasted with payments and pricing for our standardized software, which customizations are minimum, so the price would reflect their standardized nature. Our goal is to balance profitability with customer satisfaction, ensuring that our solutions are both high-quality and sustainable. We typically provide our customers with a credit period based on various factors, such as their background, reputation within the industry, payment history, creditworthiness and the duration of our business relationship with them.

SALES AND MARKETING

During the Track Record Period, we derived substantially all of our revenue from sales in the Chinese Mainland, with approximately 0.5% from sales in Hong Kong. Generally, we directly deliver to and deploy our solutions for our customers. In 2023 and 2024, we sold certain standardized software to three and one distributors, respectively, and derived RMB0.8 million and RMB3.4 million of revenue from them, which accounted for 0.2% and 0.5% of our total revenue, respectively.

As of December 31, 2025, our sales and marketing department consisted of 151 members. Members on our sales and marketing team primarily focus on retaining and expanding our business with existing customers and leveraging the current relationships to gain introductions to potential customers. Some of the members are responsible for conducting pre-sales assessments of our customers' data infrastructure and existing software and hardware systems to determine the development direction of our solutions. In addition, some of the members handle general inquiries, complaints and feedback from our customers. In 2023, 2024 and 2025, our sales and marketing expenses amounted to RMB139.9 million, RMB141.5 million and RMB108.6 million, which represented 27.1%, 21.5% and 15.3% of our total revenue, respectively. We hold regular meetings to analyze and deliberate on various aspects, including customer feedback and complaints. As of the Latest Practicable Date, we had not received any material complaints from our customers in relation to the services provided to them.

Market opportunities and competition

According to Frost & Sullivan, China continues to strengthen capabilities in cybersecurity, data security, AI and related fields. China's information security market increased from RMB73.2 billion in 2021 to RMB105.7 billion in 2025 with a CAGR of 9.6%, and is expected to grow to RMB172.7 billion by 2030 with a CAGR of 10.6%. The data security market grew from RMB18.6 billion in 2021 to RMB29.0 billion in 2025 with a CAGR of 11.7%, and is forecast to reach RMB50.9 billion in 2030 with a CAGR of 12.1%. The cybersecurity market increased from RMB54.6 billion in 2021 to RMB76.7 billion in 2025 with a CAGR of 8.9%, and is projected to grow to RMB121.9 billion by 2030 with a CAGR of 10.0%. Broader adoption of AI introduces new security gaps, creating additional demand for enhanced protection in AI security, vehicle network security and IoT security.

According to Frost & Sullivan, in terms of revenue, in 2025, we ranked the first among China's specialized security vendors in providing data security platform with a market share of 9.7%, we also ranked seventh among China's specialized security vendors in providing data security with a market share of 3.8% and thirteenth among China's specialized security vendors in providing information security with a market share of 1.8%. See "Industry Overview."

Seasonality

We typically generate a relatively higher proportion of our revenue during the fourth quarter of each year, as most projects that are typically approved in the beginning of the year are typically delivered to and accepted by our customers by the end of the year, which, according to Frost & Sullivan, is an industry norm.

OUR CUSTOMERS

In 2023, 2024 and 2025, the revenue that we generated from our five largest customers amounted to RMB321.0 million, RMB451.1 million and RMB496.3 million, representing 62.2%, 68.4% and 70.1% of our total revenue, respectively. The revenue that we generated from our largest customer during the Track Record Period amounted to RMB182.3 million, RMB297.6 million and RMB259.1 million, representing 35.3%, 45.2% and 36.6% of our total revenue, respectively.

During the Track Record Period, these major customers were primarily large telecommunications network operators in China, each comprising a large number of subsidiaries, with whom we typically entered into project-based purchase agreements. The following sets forth the salient terms of the agreements with our major customers:

Scope of services: Defines the platform, software and specialized services we provide.

Payment terms: Payment terms depend on the types of products and solutions offered but are typically structured as milestone-based payments.

Duration: The duration of our products and solutions in each contract is determined by its specific service scope of our contracts with customers can vary substantially from customer to customer and from project to project. Generally until both parties fulfill their respective obligations under the agreement.

Pricing: The pricing of our products and solutions in each contract is determined by its specific service scope and the value of our contracts with customers can vary substantially from customer to customer and from project to project.

The following table sets forth details of our five largest customers in 2023:

Customer	Revenue	Percentage of total revenue of our Group	Business relationship since	Major type of solutions provided by our Group	Credit period granted	Payment method
	RMB'000	*%*				
Customer A[(1)]	182,302	35.3	2015	Platform, software and services	30 days	Telegraphic transfer
Customer B[(2)]	46,310	9.0	2017	Platform, software and services	30 days	Bank transfer
Customer C[(3)]	44,222	8.6	2020	Services	30 days	Bank transfer
Customer D[(4)]	34,487	6.7	2021	Platform, software and services	30 days	Telegraphic transfer
Customer E[(5)]	13,645	2.6	2021	Services	15 days	Bank transfer
Total	**320,966**	**62.2**				

Notes:

(1) Customer A is one of the three major telecommunications network operators in China, primarily engaged in the provision of mobile voice, data, broadband and other information and communications services. It has a subsidiary whose shares are dually listed on the Main Board of the Stock Exchange of Hong Kong and Shanghai Stock Exchange.

(2) Customer B is one of the three major telecommunications network operators in China, primarily engaged in the digital information infrastructure and services, covering mobile and wireline communications, cloud computing, big data, AI and IoT. It has a subsidiary whose shares are dually listed on the Main Board of the Stock Exchange of Hong Kong and the Shanghai Stock Exchange.

(3) Customer C is a public institution incorporated in 2022, primarily responsible for the centralized and unified management of public data in Shanghai.

(4) Customer D is one of the three major telecommunications network operators in China, primarily engaged in the provision of mobile and fixed-line communications services, domestic and international communications facilities, data communications and systematic integration services. It has two listed subsidiaries, one on the Main Board of the Stock Exchange of Hong Kong and the other on the Shanghai Stock Exchange. Both subsidiaries focus on telecommunications and information-related services.

(5) Customer E is a public company listed on the Shanghai Stock Exchange, primarily engaged in the R&D, manufacturing and sale of commercial passwords software products based on public key infrastructure.

The following table sets forth details of our five largest customers in 2024:

Customer	Revenue	Percentage of total revenue of our Group	Business relationship since	Major type of solutions provided by our Group	Credit period granted	Payment method
	RMB'000	*%*				
Customer A	297,649	45.2	2015	Platform, software and services	30 days	Telegraphic transfer
Customer D	45,421	6.9	2021	Platform, software and services	30 days	Bank transfer
Customer B	41,699	6.3	2017	Platform, software and services	30 days	Bank transfer
Customer C	41,410	6.3	2020	Services	30 days	Bank transfer
Customer F[6]	24,948	3.8	2022	Services	30 days	Bank transfer
Total	**451,127**	**68.5**				

The following table sets forth details of our five largest customers in 2025:

Customer	Revenue	Percentage of total revenue of our Group	Business relationship since	Major type of solutions provided by our Group	Credit period granted	Payment method
	RMB'000	*%*				
Customer A	259,112	36.6	2015	Platform, software and services	30 days	Telegraphic transfer
Customer B	75,635	10.7	2017	Platform, software and services	30 days	Bank transfer
Customer G[7]	64,927	9.2	2024	Platform and services	28 days	Telegraphic transfer
Customer D	59,893	8.5	2021	Platform and software	30 days	Bank transfer
Customer C	36,757	5.2	2020	Services	30 days	Bank transfer
Total	**496,324**	**70.2**				

Notes:

(6) Customer F is a company established in 2015 and a leading provider of information and communication technology products and services for China's energy industry. It has a subsidiary whose shares are listed on the Shanghai Stock Exchange.

(7) Customer G is a state-owned company established in 2013 and a key player in driving industrial development and urban construction in Southwestern China. It primarily focuses on smart city, big data and information technology, high-end manufacturing and healthcare industries.

Our Directors confirm that, as of the Latest Practicable Date, our five largest customers in each year during the Track Record Period were all Independent Third Parties and none of our Directors, their respective close associates or any Shareholder (which to the knowledge of our Directors owning more than 5% of our share capital as of the Latest Practicable Date) had any interest, directly or indirectly, in any of such customers. During the Track Record Period and up to the Latest Practicable Date, to the best knowledge of our Directors, we did not have any material disputes with our customers, nor were there any material breaches of our agreements with them.

Relationship with our largest customer during the Track Record Period

Throughout the Track Record Period, Customer A was our largest customer and our revenue derived from Customer A amounted to RMB182.3 million, RMB297.6 million and RMB259.1 million, representing 35.3%, 45.2% and 36.6% of our total revenue, respectively. During the Track Record Period, Customer A was also one of our suppliers and our purchases from Customer A amounted to RMB0.3 million, RMB0.2 million and RMB0.2 million, respectively. See "—Overlapping Customers/Suppliers."

Customer A is an Independent Third Party and one of the three major telecommunications network operators in China. During the Track Record Period, we conducted transactions with over 40 subsidiaries of Customer A. We have maintained an established relationship with Customer A for over ten years, during which we have collaborated closely on multiple technology solutions and platform customizations. While we are not the sole supplier of Customer A, a number of our platforms and services deployed by Customer A are highly customized and integrated with its operational systems. Such customization increases the switching costs for Customer A and reduces the likelihood of rapid replacement by another service provider. Our Directors therefore consider that although we are not the exclusive supplier, the stable and long standing nature of our collaborations evidences a degree of mutual reliance and reduces the risk of Customer A terminating or materially reducing its engagement with us.

Customer concentration is common in the telecommunications technology service industry in China. The telecommunications sector is subject to regulatory licensing requirements, high capital investment thresholds and other structural entry barriers, resulting in only three major telecommunications network operators. Service providers operating in this sector typically rely on one or more of these operators for a significant portion of their revenue due to the limited number of customers and large contract scale. Against this industry backdrop, our reliance on Customer A is consistent with prevailing industry norms and not indicative of an atypical or heightened reliance risk.

Notwithstanding the above, our Directors are of the view that any change in our business relationship with Customer A will not have a material adverse impact on our business for the following reasons:

- *Multiple subsidiaries*: Customer A is a major telecommunications network operator that operates numerous subsidiaries under its corporate umbrella. Each subsidiary is an independent legal entity and generally conducts its own independent tendering processes.

- *Diversified customer base within the telecommunications sector*: In addition to Customer A, we also maintain long term business relationships with the other two major telecommunications network operators in China, providing us with broad coverage and reducing the impact of fluctuations in demand from any single operator.

- *Expansion into non telecommunications segments*: We have extended our client coverage to customers in the energy, power and other infrastructure related sectors and we continue to expand into emerging security fields. These initiatives are expected to further diversify our revenue base and reduce reliance on Customer A over time.

- *Sustainable business model with strong technical capability*: Our platforms incorporate proprietary functionalities and domain specific expertise and our solutions typically require continuous upgrades, maintenance and iteration. This creates long term service continuity and makes substitution by competitors more difficult.

- *No material adverse developments*: Throughout the Track Record Period and up to the Latest Practicable Date, our relationship with Customer A remained stable and positive.

Having considered (i) the customized nature of our solutions, (ii) the structural concentration inherent in the PRC telecommunications industry and (iii) our ability to diversify and mitigate reliance risk, our Directors believe that the risk of Customer A terminating or materially reducing its business relationship with us is low. Further, our material reliance on Customer A does not, in the Directors' view, materially and adversely affect our business sustainability, operational stability, financial performance or our suitability for **[REDACTED]**.

After-sales services

Our post-sales services encompass software and services support within specified time periods, adhering to the terms agreed upon with our customers. We may put in place corrective and preventive management procedures to analyze and address the causes of any software non-conformities that have occurred or may potentially occur. Should a batch of solutions be found unsuitable, we strictly follow these procedures and promptly inform the relevant stakeholders.

Customer satisfaction is one of our highest priorities. To that end, we conduct regular customer satisfaction surveys via structured questionnaires, through which we (i) document and track shifts in customer satisfaction and (ii) compile and categorize customer feedback. Leveraging systematic survey results and in-depth analysis of customer satisfaction dynamics, we have established a rapid response mechanism to address customer needs in a timely and efficient manner. In parallel, we continuously refine our after-sales service system to reliably safeguard customer experience, cement long-term customer relationships and consolidate our customer base.

During the Track Record Period and up to the Latest Practicable Date, we did not experience any material liability claims. Additionally, we did not receive any customer complaints that materially and adversely affected our operations. This track record underscores our commitment to delivering high-quality solutions and maintaining strong customer relationships.

SUPPLIERS AND PROCUREMENT

During the Track Record Period, our suppliers mainly comprised outsourced service providers as well as IT equipment and software suppliers. In 2023, 2024 and 2025, purchases from our five largest suppliers in each year during the Track Record Period amounted to RMB46.3 million, RMB85.5 million and RMB88.1 million, representing 18.5%, 30.9% and 33.2% of our total purchases, respectively.

The following table sets forth details of our five largest suppliers in 2023:

Supplier	Purchase amount	Percentage of total purchase	Business relationship since	Types of procurement	Payment method	Credit term
	(RMB'000)	*(%)*				
Supplier A[(1)]	16,952	6.8	2021	Outsourced installation and repair services	Telegraphic transfer and bank draft	90 days
Supplier B[(2)]	7,704	3.1	2019	Outsourced installation and repair services	Telegraphic transfer and bank draft	45 days
Supplier C[(3)]	7,537	3.0	2022	Outsourced installation and repair services	Telegraphic transfer	5 days
Supplier D[(4)]	7,272	2.9	2022	Outsourced installation and repair services	Telegraphic transfer	45 days
Supplier E[(5)]	6,847	2.7	2022	IT equipment	Telegraphic transfer	89 days
Total	**46,312**	**18.5**				

Notes:

(1) Supplier A is a company established in 2001 and primarily engaged in providing one-stop digital-intelligent integrated solutions, with its business focus on the field of digital-intelligent technology applications.

(2) Supplier B is a company established in 2018 and primarily engaged in technology research and services in the field of industrial control system security.

(3) Supplier C is a company established in 2007 and primarily engaged in technology development in the fields of computer software and hardware, communication equipment and network technology.

(4) Supplier D is a proactive cybersecurity vendor established in 2020 and primarily engaged in technical services and technology development.

(5) Supplier E is a network provider and value-added service provider established in 1995 and based in Beijing. The shares of its parent company are listed on Shanghai Stock Exchange.

The following table sets forth details of our five largest suppliers in 2024:

Supplier	Purchase amount	Percentage of total purchase	Business relationship since	Types of procurement	Payment method	Credit term
	(RMB'000)	*(%)*				
Supplier F[6]	28,373	10.3	2024	IT equipment	Telegraphic transfer	30 days
Supplier A	19,025	6.9	2021	Outsourced installation and repair services	Telegraphic transfer and bank draft	90 days
Supplier G[7]	18,547	6.7	2022	Outsourced installation and repair services and software products	Telegraphic transfer	5 days
Supplier H[8]	10,604	3.8	2023	Outsourced installation and repair services	Telegraphic transfer	5 days
Supplier D	8,956	3.2	2022	Outsourced installation and repair services	Telegraphic transfer	45 days
Total	**85,505**	**30.9**				

Notes:

(6) Supplier F is a company established in 2020 and operating as a high-technology enterprise integrated with R&D, production and marketing. The shares of its parent company are listed on the Shenzhen Stock Exchange.

(7) Supplier G is one of China's earliest authoritative institutions specializing in reliability research. It serves as a key technical support unit under the MIIT, providing certification, testing, analysis and evaluation services for the electronics and information industry.

(8) Supplier H is a company established in 2015 and primarily engaged in technical services and technology development.

The following table sets forth details of our five largest suppliers in 2025:

Supplier	Purchase amount	Percentage of total purchase	Business relationship since	Types of procurement	Payment method	Credit term
	(RMB'000)	*(%)*				
Supplier A	51,326	19.3	2021	Outsourced installation and repair services	Telegraphic transfer and bank draft	90 days
Supplier I[9]	14,972	5.6	2019	Outsourced installation and repair services	Telegraphic transfer and bank draft	45 days
Supplier D	10,004	3.8	2022	Outsourced installation and repair services	Telegraphic transfer	45 days
Supplier J[10]	6,294	2.4	2022	Outsourced installation and repair services	Telegraphic transfer and bank draft	45 days
Supplier K[11]	5,479	2.1	2021	Outsourced installation and repair services	Telegraphic transfer and bank draft	45 days
Total	**88,075**	**33.2**				

Notes:

(9) Supplier I is a company established in 2017 dedicated to utilizing technologies based on artificial intelligence, computer vision and related fields to provide customers with integrated artificial intelligence solutions and operational services.

(10) Supplier J is a company established in 2020 and primarily engaged in the fields of engineering and technology research, value-added telecommunications technology services and communication equipment sales.

(11) Supplier K is a company established in 2010 and primarily engaged in software and information technology services industry.

Our Directors confirm that, as of the Latest Practicable Date, our five largest suppliers in each year during the Track Record Period were all Independent Third Parties and, during the Track Record Period and up to the Latest Practicable Date, none of our Directors or their respective close associates or any of our Shareholders, to the knowledge of our Directors, owned more than 5% of our issued Shares, had any interest in any of our five largest suppliers. During the Track Record Period and up to the Latest Practicable Date, to the best knowledge of our Directors, we did not have any material disputes with our suppliers, nor were there any material breaches of our agreements with them.

Outsourced service providers

We typically engage qualified third-party outsourced service providers in China to perform certain non-core services. For instance, following the deployment and customer acceptance of our solutions, we typically need to place personnel on-site at customer premises to conduct project observation and feedback collection. These services typically encompass operations and tasks require on-site visit and installation external of the Shanghai metropolitan area, as our customer base spans across the entire China. According to Frost & Sullivan, such practice is consistent with common industry practice. We formalize our engagements through technical support agreements or project outsourcing service agreements, detailing the types of IT services, contract prices and payment terms. Our outsourced service providers generally offer us a credit term and are responsible for adhering to our quality standards and providing maintenance and warranty to our customers.

As advised by our PRC Legal Advisors, our arrangements with the third-party outsourced service providers are not labor dispatching, primarily because according to PRC laws and regulations, such as the Labor Contract Law and the Interim Provisions on Labor Dispatch, labor dispatching is characterized by features such as fee settlement based on the number of dispatched personnel, the direct management of workers by the user entity and the temporary, auxiliary or substitutable nature of the work assignments. However, our arrangements with the third-party outsourced service providers exhibit distinct characteristics, such as a fixed total contract price based on defined service categories, management and fee settlement focused on service outcomes and deliverables, the provision of specialized technical services, and clearly defined management boundaries where we only supervise service outcomes without directly managing the labor process of the outsourcing personnel, which are inconsistent with the defining characteristics of labor dispatching. See "Risk Factors—Risks Relating to Our Business and Industry—Any significant cost overruns may materially and adversely affect our business, financial condition and results of operations."

The following sets forth the salient terms of the agreements with our outsourced service providers:

Scope of services: The service provider agrees to deliver specified services, which may include hardware installation, software implementation, on-site technical support and related maintenance tasks. The scope is usually detailed in a service delivery plan outlining methodologies, timelines and deliverables.

Payment terms: Service fees are typically structured around milestones or monthly payments. Common arrangements include an initial payment upon contract signing, interim payments tied to project progress and a final payment upon completion and acceptance of deliverables.

Term and renewal: Agreements often run for a fixed term, such as one year, with provisions for renewal under equal conditions if no breaches occur.

Compliance obligations: Service providers must maintain qualified personnel with valid certifications, labor contracts and insurance. They are also required to comply with applicable laws, health and safety standards and our internal quality requirements.

Confidentiality and IP: The service providers are obligated to keep all project-related information confidential and ensure that any work products or intellectual property developed during the engagement belong to us. Disclosure to third parties without consent is prohibited.

Subcontracting restrictions: Service providers may not subcontract services without our prior written consent. If subcontracting is permitted, the supplier remains fully responsible for the acts and omissions of its subcontractors.

Quality standards and warranties: Service providers are responsible for meeting agreed quality standards and providing maintenance and warranty services for installed hardware and implemented software.

Termination and rescission: We typically reserve the right to terminate or rescind the agreement unilaterally if the supplier causes economic loss, or fails to meet contractual obligations.

Liability and indemnity: Service providers are generally liable for breaches, negligence, or failure to comply with contractual terms and may be required to indemnify us against claims arising from their actions.

Although we engage multiple third party service providers, in certain regions our reliance on a limited number of providers may give rise to concentration risk. To mitigate such risk, we regularly assess the provider mix within each service region, review their financial standing and maintain standby providers that can be mobilized when needed. Counterparty risk is further addressed through contractual protections, including performance guarantees, service level requirements and rights of recourse in the event of non-performance. In 2023, 2024 and 2025, our outsourced service expenses amounted to RMB184.8 million, RMB257.5 million and RMB239.2 million, respectively.

We monitor fluctuations in outsourced service fees and conduct periodic sensitivity analyses to evaluate the impact of labor cost changes on project profitability. A moderate increase in service fees is generally manageable due to our ability to incorporate labor cost assumptions into project quotations. For longer term or multi-phase projects, we assess breakeven thresholds using internal budgeting models to ensure that variations in outsourcing costs do not materially affect expected margins. The availability of qualified outsourced personnel may be affected by seasonal labor shortages, regional travel restrictions, or overlapping project schedules. Any delays in deploying service teams could affect project timelines. To mitigate such risks, we (i) maintain a multi tiered supplier network with overlapping service capabilities, (ii) monitor supplier staffing availability in advance of project commencement and (iii) require suppliers to allocate dedicated or priority personnel for large scale or time sensitive projects. We may also reassign internal personnel or adjust deployment sequencing where appropriate.

We manage potential increases in outsourced labor costs through a combination of framework pricing, competitive re-tendering and contract negotiations. Where feasible, we agree fixed labor rates for defined periods to reduce exposure to short term cost volatility. For projects where pricing cannot be fixed, we evaluate whether any cost increases can be reflected in customer quotations, particularly where labor requirements are substantial or where deployment schedules change at the customer's request.

Given the nature of our operations, we adopt a disciplined approach to outsourced workforce planning. Work orders to service providers are typically issued on a project specific or task specific basis, similar to a back to back arrangement aligned with confirmed project requirements. We closely track the deployment status, man day usage and service milestones to manage overall labor consumption. Provisions for disputed or unutilized labor charges are made based on the age of outstanding claims, service acceptance status and the likelihood of final settlement.

The selection of our outsourced service providers is based on stringent criteria, including their industry experience, technical expertise, service quality, quality control effectiveness, pricing, financial stability and the ability to meet delivery timelines. Each potential provider undergoes a rigorous qualification process, which includes background checks, interviews and site visits, typically taking a specified period to complete.

To ensure the highest standards, we closely monitor and evaluate the performance of our outsourced service providers. We conduct annual inspections to reassess their overall performance and may terminate relationships with those who fail to meet our standards. Evaluations are based on several factors, including the providers' technology and industry expertise, service quality, quality assurance procedures and compliance with our policies and guidelines. This comprehensive approach ensures that we maintain high-quality services and effectively meet our customers' needs.

Supply chain management regarding servers and other equipment

During the Track Record Period, we purchased software and hardware, such as servers and various equipment, in order to fulfil our contractual obligations, and recorded the relevant expenses as contract performance cost in our financial statements. Emphasizing robust supply chain management, we have implemented internal measures to standardize processes for supplier classification, development and onboarding, material selection and certification, category management, audit management, performance evaluation, supplier qualification cancellation,

reinstatement and other procedures. These measures are designed to align supplier resources with our development needs, stabilize the supply of products and services and ensure the quality of the products supplied.

During the Track Record Period and up to the Latest Practicable Date, all of our suppliers were located in China and we did not experience any supply chain issues that adversely impacted our operations. To prepare for potential shortages, we have engaged in discussions with qualified suppliers to establish long-term strategic partnerships and broadened our supplier base, thus securing a stable supply of critical components. To mitigate supply chain risks, we may enter into general procurement agreements with our suppliers, the salient terms of which are set forth below:

Duration: Our procurement agreements typically do not specify a fixed term. The performance of our supplier and us is completed upon delivery, acceptance and payment.

Product specification: We typically specify the model, unit, quantity, unit price and other details of the products that we procure.

Delivery: Delivery is typically arranged by our suppliers to our designated location, and we typically provide the names and phone numbers of the consignee.

Payment terms: We typically settle the procurement price via telegraphic transfer or bank draft upon our acceptance of the products or receipt of a valid VAT invoice from the supplier.

Inspection and Acceptance: We are typically responsible for inspecting the products upon receipt and notify any defects in writing within a certain period of time. If there is a quality issue, the suppliers are typically responsible for facilitating product replacement or return at no cost.

Default and Termination: We typically specify the calculation of liquidated damage in our procurement agreement. Typically, either party may terminate the agreement in case of the other party's fundamental breach.

These agreements include key components such as confidentiality agreements, quality assurance agreements, codes of conduct and supplier integrity and anti-corruption agreements.

Before engaging new suppliers, we would conduct necessary investigations and audits. Our existing suppliers would be managed through an agreed set of performance standards. For suppliers that fail such audits, corrective measures may be implemented. If requirements are still not met, the supplier's qualification may be canceled. We hope that this comprehensive approach can ensure that we maintain high-quality services and effectively meet our operational needs.

OVERLAPPING CUSTOMERS/SUPPLIERS

During the Track Record Period, we provided data security and cybersecurity solutions to Customers A, B and D, the three largest telecommunications network operators in China, from whom we also procured telecommunications services for our own operational needs. Such arrangement arose primarily from the highly concentrated nature of China's telecommunications infrastructure and service market, where essential services, such as broadband, internet data center and nationwide network, are exclusively provided by a small number of state-authorized, major telecommunications network operators. According to Frost & Sullivan, such arrangement is consistent with the prevailing industry practice.

Customer A was our largest customer and one of our suppliers throughout the Track Record Period. In 2023, 2024 and 2025, the revenue that we derived from Customer A was RMB182.3 million, RMB297.6 million and RMB259.1 million, representing 35.3%, 45.2% and 36.6% of our total revenue, respectively. In 2023, 2024 and 2025, our purchases from Customer A was RMB0.3 million, RMB0.2 million and RMB0.2 million, representing 0.1%, 0.05% and 0.1% of our total purchases, respectively.

Customer B, one of our five largest customers in each year during the Track Record Period, was also one of our suppliers in 2024 and 2025. In 2023, 2024 and 2025, the revenue that we derived from Customer B was RMB46.3 million, RMB41.7 million and RMB75.6 million, representing 9.0%, 6.3% and 10.7% of our total revenue, respectively. In 2023, 2024 and 2025, our purchases from Customer B was nil, RMB74,800 and RMB0.1 million, representing nil, 0.03% and 0.04% of our total purchases, respectively.

Customer D, one of our five largest customers each year during the Track Record Period, was also one of our suppliers in 2025. In 2023, 2024 and 2025, the revenue that we derived from Customer D was RMB34.5 million, RMB45.4 million and RMB59.9 million, representing 6.7%, 6.9% and 8.5% of our total revenue, respectively. In 2023, 2024 and 2025, our purchases from Customer D was nil, nil and RMB0.1 million, representing nil, nil and 0.04% of our total purchases, respectively.

Negotiations of the terms of our purchases from and sales to Customers A, B and D were conducted on an individual basis and such purchases and sales were neither inter-connected nor inter-conditional with each other. As such, our Directors are of the view that all of our purchases from and sales to Customers A, B and D were conducted in our ordinary course of business under normal commercial terms, based on our genuine business needs and in arm's length.

OUR EMPLOYEES

We consider our employees to be invaluable assets that significantly contribute to our success. We emphasize on fairness, transparency and diversity, welcoming talents from various backgrounds to foster a diverse workplace. We adhere to principles of openness, fairness, impartiality and merit-based selection, ensuring that job positions are based on actual needs and that there is a proper match between talent and post during employment. The following table sets forth the numbers and percentages of our full-time employees by function as of December 31, 2025:

Function/department	Number of employees	% of total employees
Deployment	376	45.6
R&D	186	22.6
Sales and marketing	151	18.3
Board and senior management	6	0.7
Administrative and others	106	12.9
Total	**825**	**100.0**

Our recruitment process is guided by several factors, including industry experience, educational background and current vacancies. Employees are generally compensated with a fixed salary and other allowances based on their respective positions and responsibilities. We enter into individual employment contracts with our employees, covering aspects such as wages, benefits, employment scope and grounds for termination. As of the Latest Practicable Date, our employees had not negotiated their terms of employment through any labor union or collective bargaining agreements. Our Directors confirm that during the Track Record Period and up to the Latest Practicable Date, we had not received any fines, penalties, warnings, or administrative actions from local authorities concerning our employees or relevant labor laws and regulations that had resulted in material adverse impact on our result of operations.

We believe that we have maintained good working relationships with our employees. During the Track Record Period and up to the Latest Practicable Date, we did not experience any major labor disputes, work stoppages, labor strikes, or work safety incidents that disrupted our operations.

INSURANCE

During the Track Record Period and up to the Latest Practicable Date, we did not maintained any business interruption insurance or any insurance policies that cover counterparty liabilities, which, according to Frost & Sullivan, was consistent with the industry norm. Our Directors also confirm that, during the Track Record Period, we did not experience any business interruptions or losses or damage to our facilities that had a material adverse effect on our business, financial conditions, or results of operation.

PROPERTY

As of the Latest Practicable Date, we did not own any property and we leased 15 properties in China from Independent Third Parties with an aggregated GFA of approximately 8,056 sq.m., which are primarily used as office buildings. We did not experience any material difficulties in negotiating a renewal of our leases with our landlords during the Track Record Period and up to the Latest Practicable Date.

As of the Latest Practicable Date, we had not registered or filed the lease agreements of our leased properties with the relevant government authorities in the PRC. As advised by our PRC Legal Advisors, while the lack of registration will not affect the validity of the lease agreements, we may be ordered by the relevant government authorities to register the relevant leases within a prescribed period, failing which we may be subject to a fine ranging from RMB1,000 to RMB10,000 for each unregistered lease. See "Risk Factors—Risks Relating to Our Business and Industry—We have not completed the necessary filing and registration for our leased properties."

To prevent recurrence of the above non-compliances relating to unregistered leased properties, we have enhanced our internal control measures for lease management and regulatory filings, including (i) maintaining a lease filing register recording key information and supporting documentation; (ii) designating the administrative department to oversee lease execution, filing and coordination with relevant parties; and (iii) conducting periodic internal checks to ensure timely registration and updates of lease agreements in accordance with applicable PRC regulations. Accordingly, our Directors are of the view that the above non-compliances, which will be properly addressed through enhanced internal controls and subject to rectification as and when required by the authorities, do not materially and adversely affect our suitability for **[REDACTED]**.

With regard to rectification, we remain prepared to make any required filings, submissions or payments of penalties or surcharges should the relevant government authorities issue any directives or orders. As the timing and specific rectification steps depend on the authorities' assessment, which cannot be determined at this stage, we are presently unable to ascertain the precise rectification actions required. Our PRC Legal Advisors confirmed that there is no legal impediment to completing the necessary registrations or filings after **[REDACTED]**, should such actions be mandated by the authorities. We will disclose the progress of any required rectification, as well as explanations for any delays, in our interim and annual reports. As of the Latest Practicable Date, no rectification actions have been taken because no orders or notifications have been issued by the competent PRC authorities.

LICENSES AND PERMITS

The following table sets forth details of the key permits we held that are material to our operations as of the Latest Practicable Date:

Name of certificate	Certificate no.	Issuing authority	Issue date	Valid until
Security Inspection Certificate for Specialized Cybersecurity Products	25SW01635-A	China Information Technology Security Evaluation Center	December 5, 2025	December 5, 2027
Security Inspection Certificate for Specialized Cybersecurity Products	26SS0OS30-A	China Information Technology Security Evaluation Center	April 3, 2026	April 3, 2028
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2021-CS007–147	China Cybersecurity Review Technology and Certification Center	July 13, 2023	July 12, 2028
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2024-CS006–875	China Cybersecurity Review, Certification And Market Regulation Big Data Center	August 9, 2024	August 8, 2029
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2024-CS013–948	China Cybersecurity Review, Certification And Market Regulation Big Data Center	October 14, 2024	October 13, 2029
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2024-CS023–1023	China Cybersecurity Review, Certification And Market Regulation Big Data Center	December 16, 2024	December 15, 2029
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2024-CS013–1029	China Cybersecurity Review, Certification And Market Regulation Big Data Center	December 19, 2024	December 18, 2029
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2024-CS012–1037	China Cybersecurity Review, Certification And Market Regulation Big Data Center	December 23, 2024	December 22, 2029
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2024-CS015–1040	China Cybersecurity Review, Certification And Market Regulation Big Data Center	December 25, 2024	December 24, 2029

Name of certificate	Certificate no.	Issuing authority	Issue date	Valid until
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2024-CS032–1052	China Cybersecurity Review, Certification And Market Regulation Big Data Center	January 14, 2025	January 13, 2030
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2025-CS024–1063	China Cybersecurity Review, Certification And Market Regulation Big Data Center	January 23, 2025	January 22, 2030
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2025-CS012–1074	China Cybersecurity Review, Certification And Market Regulation Big Data Center	February 11, 2025	February 10, 2030
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2025-CS023–1146	China Cybersecurity Review, Certification And Market Regulation Big Data Center	April 22, 2025	April 21, 2030
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2025-CS012–1183	China Cybersecurity Review, Certification And Market Regulation Big Data Center	May 16, 2025	May 15, 2030
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2025-CS034–1281	China Cybersecurity Review, Certification And Market Regulation Big Data Center	August 20, 2025	August 19, 2030
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2025-CS035–1338	China Cybersecurity Review, Certification And Market Regulation Big Data Center	November 10, 2025	November 9, 2030
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2025-CS024–1340	China Cybersecurity Review, Certification And Market Regulation Big Data Center	November 11, 2025	November 10, 2030
Safety Certificate for the Key Network Equipment and Specialized Cybersecurity Products	CCRC-2026-CS012–1407	China Cybersecurity Review, Certification And Market Regulation Big Data Center	February 9, 2026	February 8, 2031
Information Security Service Qualification Certificate (Security Engineering, Level II)	CNITSEC2024SRV-11–207	China Information Technology Security Evaluation Center	January 16, 2024	January 15, 2027
Information Security Service Qualification Certificate (Risk Assessment, Level II)	CNITSEC2024SRV-RA-11–119	China Information Technology Security Evaluation Center	January 16, 2024	January 15, 2027
Information Security Service Qualification Certificate (Security Development, Level I)	CNITSEC2025SRV-SD-1–158	China Information Technology Security Evaluation Center	December 26, 2025	December 25, 2028
Information Security Service Qualification Certificate (Data Security, Level I)	CNITSEC2023SRV-DS-1–2	China Information Technology Security Evaluation Center	December 8, 2023	December 7, 2026

Name of certificate	Certificate no.	Issuing authority	Issue date	Valid until
Information Security Service Qualification Certificate(Information System Audit, Level I)	CNITSEC2025SRV-SA-I-43	China Information Technology Security Evaluation Center	December 5, 2025	December 4, 2028
Information Security Service Qualification Certification	CCRC-2018-ISV-ER-243	China Cybersecurity Review, Certification And Market Regulation Big Data Center	May 27, 2025	May 26, 2028
Information Security Service Qualification Certification	CCRC-2018-ISV-RA-555	China Cybersecurity Review, Certification And Market Regulation Big Data Center	May 27, 2025	May 26, 2028
Information Security Service Qualification Certification	CCRC-2018-ISV-SM-452	China Cybersecurity Review, Certification And Market Regulation Big Data Center	May 27, 2025	May 26, 2028
Information Security Service Qualification Certification	CCRC-2020-ISV-SI-1793	China Cybersecurity Review, Certification And Market Regulation Big Data Center	May 27, 2025	May 26, 2028
Information Security Service Qualification Certification	CCRC-2020-ISV-SD-254	China Cybersecurity Review, Certification And Market Regulation Big Data Center	May 27, 2025	May 26, 2028
Capability Assessment Certificate for Communications Network Security Services (Risk Assessment, Level II)	CESSCN-2023-RA-B-012	China Communications Enterprise Association	December 24, 2023	December 23, 2026
Capability Assessment Certificate for Communications Network Security Services (Security Design & Integration, Level II)	CESSCN-2025-SDI-B-023	China Communications Enterprise Association	August 29, 2025	August 28, 2028
Capability Assessment Certificate for Communications Network Security Services (Emergency Response, Level II)	CESSCN-2025-ERS-B-012	China Communications Enterprise Association	August 29, 2025	August 28, 2028
Capability Assessment Certificate for Communications Network Security Services (Security Training, Level I)	CESSCN-2023-ST-C-008	China Communications Enterprise Association	December 24, 2023	December 23, 2026
Certificate of Qualification for MLPS Security Construction Service Organizations	DJJS2018001001	First Research Institute of the Ministry of Public Security	March 16, 2018	March 15, 2024[(1)]

Name of certificate	Certificate no.	Issuing authority	Issue date	Valid until
Qualification Certificate for Data Security Service Capability Assessment	CHINADS-08–20230301	Data Security Professional Committee of China Computer Industry Association, China Software Evaluation Center (Software and Integrated Circuit Promotion Center of the Ministry of Industry and Information Technology)	March 8, 2023	February 27, 2029
Qualification Certificate for Data Security Service Capability Assessment	CHINADS-09–20230301	Data Security Professional Committee of China Computer Industry Association, China Software Evaluation Center (Software and Integrated Circuit Promotion Center of the Ministry of Industry and Information Technology)	March 8, 2023	March 7, 2026[2]

Notes:

(1) According to the Certificate Handling Notice issued on June 17, 2024 by the First Research Institute of the Ministry of Public Security, as the institute adjusted its capability assessment business for information security level protection construction service institutions, applications for the renewal of the issued "Competency Evaluation Certificate for the Information Security Grade Protection and Security Construction Service Institution" are temporarily suspended, and the original certificate remains valid.

(2) The Network and Data Security Professional Committee of China Computer Industry Association has approved the initiation of the certificate extension and renewal process by the Company and granted an extension period to the renewal of our certificate, expiring on July 7, 2026. During such extension period, our original certificate has a status of "valid pending renewal" and shall not affect our lawful conduct of data security construction and other related business activities.

Our Directors confirm that, as of the Latest Practicable Date, we had obtained all necessary licenses and permits for our business operations in the PRC, thus being in compliance with relevant laws and regulations in all material respects. Our Directors also confirm that, during the Track Record Period and up to the Latest Practicable Date, we did not experience any material difficulties in obtaining and/or renewing such licenses and permits. Further, our Directors are not aware of any circumstances that would significantly hinder or delay the renewal of such licenses and permits upon their expiration. Therefore, our Directors do not foresee any major difficulties in compliance with such licensing requirements that would cause material or adverse impacts on our operations and business.

LEGAL PROCEEDINGS AND COMPLIANCE

In our ordinary course of business, we may be involved in legal, arbitral or administrative proceedings. See "Risk Factors—Risks Relating to Our Business and Industry—Any litigation, legal and contractual disputes, claims or administrative proceedings against us could be costly and time-consuming to defend or settle and could result in negative publicity." To the best knowledge of our Directors, as of the Latest Practicable Date, there were no material ongoing or imminent litigations, claims or arbitration proceedings against us or any member of our Board that would adversely impact our business, financial position or results of operation.

As advised by our PRC Legal Advisors, our Directors confirm that we had complied with all applicable laws and regulations in the PRC in all material aspects and there had not been any non-compliance incidents the nature of which had materially and adversely affected our business, financial position, or results of operation during the Track Record Period and up to the Latest Practicable Date.

DATA SECURITY AND PRIVACY

As part of our business model, we deploy technical personnel and deliver our solutions at our customers' premises. We do not access or exercise control over customer data stored within such deployments. In the ordinary course of business, we primarily collect our customers' contact information, delivery addresses and purchase records solely to facilitate the provision and support of our solutions.

We have established and maintain a comprehensive information security and data management program designed to safeguard the integrity and availability of our systems and the privacy and security of data within our control. Our safeguards include, among other measures, firewalls, intrusion prevention systems, regular penetration testing, periodic vulnerability scanning and documented disaster recovery planning. We intend to continue strengthening this framework, emphasizing innovation and adaptability to meet evolving standards and expectations for data protection.

Our PRC Legal Advisors are of the view that we have been in compliance with the relevant PRC laws and regulations relating to personal data and privacy protection in all material aspects during the Track Record Period and up to the Latest Practicable Date. See "Regulatory Overview."

Furthermore, according to our PRC Legal Advisors, we are not required to undergo a cybersecurity review under the Measures for Cybersecurity Review as of the Latest Practicable Date, for the following reasons:

(i) we did not receive any notification designating us as a critical information infrastructure operator by the relevant authority responsible for the security of such infrastructure, in accordance with the Regulations on the Security Protection of Critical Information Infrastructure (《關鍵信息基礎設施安全保護條例》);

(ii) we do not possess the personal information of more than one million users;

(iii) the **[REDACTED]** does not constitute an overseas listing; and

(iv) our Company has not received any official notice from the cybersecurity review authorities requiring us to undergo a cybersecurity review under the Measures for Cybersecurity Review.

THIRD-PARTY PAYMENT ARRANGEMENT

Background and reasons relating to the Third-party Payment Arrangement

In 2025, one of our customers (the "**Relevant Customer**") settled payments with us through accounts that do not belong to the contractual parties under the corresponding sales and purchase agreements (the "**Third-Party Payment Arrangement**"). The Relevant Customer was a government platform company and its third-party payor is a sponsoring government department of the Relevant Customer. The aggregate amounts of payments for the Third-Party Payment Arrangement were RMB10.7 million, accounting for 1.5% of our total revenue.

To the best knowledge of our Directors, the Relevant Customer made the Third-Party Payment Arrangement primarily due to its internal funding arrangements and policies. To safeguard our interests and ensure the timely recovery of trade receivables, we determined that such arrangement was a commercial necessity for the Relevant Customer to fulfill its payment obligations. We performed direct reconciliations of the transaction amounts with the Relevant Customer to ensure accuracy and thereby mitigating the risks associated with receiving third-party payments. Therefore, we did not object to Third-party Payment Arrangement initiated by the Relevant Customer.

During the Track Record Period and up to the Latest Practicable Date, (i) we did not provide any discount, commission, rebate or other benefits to the Relevant Customer or the designated third-party payor to facilitate or incentivize the Third-Party Payment Arrangement; and (ii) we did not initiate any Third-Party Payment Arrangement and the Third-Party Payment Arrangement was arranged based on the Relevant Customer's requests. To the best of our knowledge, during the Track Record Period, the relevant payments were based on bona fide underlying transactions and valid contractual relationships. The pricing and payment terms we provided to the Relevant Customer were in line with those customers not involved in the Third-Party Payment Arrangement. As advised by our PRC Legal Advisor, our acceptance of payments through the Third Party Payment Arrangement does not contravene any prohibitive provisions under PRC laws and regulations. To the best of our knowledge, we were not the subject of any investigations, enquiries, penalties or surcharges as a result of our involvement in the Third-Party Payment Arrangement during the Track Record Period and up to the Latest Practicable Date. In addition, we had not encountered any refund requests, actual or pending dispute or disagreement due to Third-Party Payment Arrangement or any material claims against us in relation to the Third-Party Payment Arrangement during the Track Record Period and up to the Latest Practicable Date.

Enhanced internal control measures relating to the Third-party Payment Arrangement

During the Track Record Period, we conducted (i) KYC due diligence on the third-party payor and assessed its financial standing and compliance posture; and (ii) anti-money laundering training among our employees to monitor and manage the risks relating to third-party payment arrangements.

We have also enhanced the following internal control measures for monitoring deposits to our bank accounts:

(i) we have issued an internal notice to all our employees to prohibit them from accepting payment under any third-party payment arrangements;

(ii) our finance department has developed templates for managing the settlement of accounts receivables which shall include transaction description, customer name, payment date, account name of the customers, any third-party payment arrangement involved and any irregularities noted; and

(iii) we have assigned personnel in our finance department for monitoring incoming payment. In the event of re-occurrence of third-party payment arrangements, the assigned personnel shall report to the department manager for further action.

Given the immaterial revenue contribution from the Relevant Customer through Third-party Payment Arrangement during the Track Record Period, our Directors are of the view that the cessation of Third-party Payment Arrangement will not have any material impact on our business, results of operations and financial performance.

Legal implications of the Third-party Payment Arrangement

As advised by our PRC Legal Advisors, considering that (i) our Third-Party Payment Arrangement was not in breach or contravention of mandatory requirements of applicable laws or regulations in China during the Track Record Period and as of the Latest Practicable Date; (ii) we were not subject to any investigation, inquiry or administrative penalty by the relevant competent authorities for any money laundering activities, activities that could be related to money laundering or any relevant investigations during the Track Record Period and up to the Latest Practicable Date as a result of the Third-Party Payment Arrangement; (iii) our Third-Party Payment Arrangement did not involve any disputes or controversies with relevant parties, including but not limited to claims for recourse or refund requests during the Track Record Period and up to the Latest Practicable Date; (iv) the relevant parties to the Third-Party Payment Arrangement have acknowledged such payment arrangement, the risk of the Third-Party Payment Arrangement being deemed to constitute a crime of money laundering under the Criminal Law of the PRC is remote, and the risk of the Third-Party Payment Arrangement being subject to recourse by relevant parties is low.

Based on the foregoing, our Directors confirm that, to the best of their knowledge and based on the know-your-customer procedures and internal control measures implemented, during the Track Record Period, (i) the relevant payments were based on bona fide underlying transactions and valid contractual relationships; and (ii) there were no instances of commercial bribery, money laundering, tax evasion, or existing or potential disputes with our Group related to the Third-Party Payment Arrangement.

During the Track Record Period and up to the Latest Practicable Date, to the best knowledge of our Directors and based on publicly available information, all Relevant Customer and the designated third-party payor who settled payments under the Third-Party Payment Arrangement were independent third parties.

ENVIRONMENT, SOCIAL, AND GOVERNANCE MATTERS

Our commitment to sustainable growth lies in the seamless integration of social values into our business operations. We are fully devoted to fostering a long-lasting positive impact on the environment, society and governance ("**ESG**") within our customer base, partners and the wider community involved in the supply chain finance ecosystem. Recognizing our duty towards environmental protection and social responsibilities, we are conscious of the potential climate-related challenges that may affect our business.

ESG governance

We incorporate ESG considerations into our daily business operations and decision-making processes. Our Board serves as the highest governing body for ESG matters, taking on the responsibility of overseeing and assessing ESG-related risks and opportunities. Through boardroom discussions, the Board establishes and adopts ESG policies, strategies and targets to effectively manage material ESG risks. It also monitors our performance against these targets and adjusts ESG strategies as needed in case of significant deviations. Additionally, ESG Working Group of our Company is tasked with evaluating and providing recommendations on our environmental, social and governance policies and practices. ESG Working Group supports the Board in supervising the development and implementation of ESG initiatives to ensure compliance with legal and regulatory requirements and plays a crucial role in advancing our ESG agenda. Furthermore, we encourage employees across our functional departments to collaborate in promoting our ESG policies and objectives, while continuously striving for operational excellence to enhance our ESG performance.

We are in the process of establishing a comprehensive set of internal policies to guide our management on ESG-related issues. Here are the key areas of focus:

- ***Environmental Matters:*** Our policies will cover energy conservation, carbon emission reduction and the treatment of exhaust gas, wastewater and solid waste.

- ***Social Matters:*** Our policies address employee health and workplace safety, product quality and maintenance, employee promotion, compensation, benefits and training.

- ***Governance Matters:*** We have formulated a code of business ethics for employees that includes policies on conflict of interest, confidentiality and anti-corruption. Employees receive regular compliance training to reinforce internal regulatory compliance and ethical business practices.

Following our **[REDACTED]**, the Board of Directors confirms that we will stay focused on and strictly adhere to Appendix C1 and Appendix C2 to the Listing Rules, while ensuring full compliance with all ESG-related rules and regulations. Additionally, we will publish an ESG report annually to disclose our significant ESG issues, risk management practices, fulfillment of objectives and overall performance. We also maintain effective communication with key stakeholders through various communication channels.

ESG risks management

Our proactive approach to ESG risk mitigation based on the concepts of risk avoidance, risk reduction, risk transfer and risk acceptance can address potential risks but also seize opportunities to enhance our ESG performance, thereby driving value creation and fostering a sustainable future for our Company and stakeholders.

We have a robust internal ESG management system to enhance our monitoring and early warning capabilities, conducting regular risk assessments to ensure timely identification of potential issues and formulating targeted countermeasures with the aim of optimizing production processes to minimize environmental pollution, improving employee benefits to strengthen our social responsibility and refining corporate governance structures to increase transparency and accountability. By systematically integrating these measures, we aim to reduce ESG risks, promote sustainable development, bolster investor confidence and reinforce corporate social responsibility, thereby laying a solid foundation for long-term business growth.

ESG opportunities

We also believe that, by enhancing ESG management within our value chain, we can strengthen its resilience against ESG risks and comply with international customer standards through sustainable procurement practices, thereby reinforcing our brand credibility. By adopting forward-thinking technological strategies and upgraded governance models, we hope to position ourselves to transform ESG capabilities into a differentiated market barrier against existing and potential competitors, driving long-term growth.

Environmental Matters

We are committed to a sustainable development strategy, aiming to harmonize the environment, nature and society by rationally using energy and resources while minimizing consumption. We will rigorously comply with environmental protection laws and regulations in the areas where we operate.

We will systematically identify potential environmental risks through comprehensive environmental impact assessments. These plans will outline emergency procedures, resource allocation and roles and responsibilities. We will also conduct regular emergency drills to enhance employee preparedness, ensuring that our risk prevention capabilities align with our business expansion efforts.

We will actively foster a green workplace culture, encouraging all employees to adopt low-carbon practices. Our initiatives may include implementing refined water and electricity conservation management, advancing waste sorting and promoting a paperless office environment. Additionally, we will provide environmental awareness training for all employees, promoting sustainable habits in daily operations to reduce our carbon footprint while enhancing environmental benefits and organizational efficiency.

Metrics and targets

Our Company's operations are primarily office-based, negating the necessity for an environmental impact assessment as per current PRC regulations. We have embraced an approach that does need extensive paperwork and manual tasks. This shift not only reduces our ecological footprint but also enhances the efficiency, transparency and productivity of our operations. Our suite of online services can cut down on the need for physical travel and its associated carbon emissions.

We have closely monitored our utilization of resources and taken steps to enhance energy efficiency. During the years ended December 31, 2023, 2024 and 2025, our recorded electricity consumption levels were 1.02 million kWh, 2.31 million kWh and 1.25 million kWh, respectively.

In terms of greenhouse gas emissions, we have monitored our greenhouse gas discharge levels on an annual basis. Our greenhouse gas emissions and intensity are detailed below by adopting the GHG Protocol corporate standards and calculations based on parameters from the Reporting Guidance on Environmental KPIs from the Stock Exchange:

Scope	Definition	Example	Year ended December 31, 2023	2024	2025
			(tCO_2e)	*(tCO_2e)*	*(tCO_2e)*
1	All direct emissions that are generated from sources that are directly owned or controlled by us[(1)]	Fuels used to run a fleet of owned vehicles	7.4	6.4	4.4
2	All indirect emissions from the generation of the electricity purchased and used by us[(2)]	The electricity that we use for our offices	536.0	1,212.2	658.5

Notes:

(1) Calculated by multiplying the annual diesel consumption by the diesel emission factor (approximately 2.68 kg CO_2 e per litre) and dividing by 1,000 to convert kilograms to metric tons. This emission factor is based on the China National Guidelines for Accounting and Reporting of Greenhouse Gas Emissions issued by the Ministry of Ecology and Environment.

(2) Calculated by multiplying the annual electricity consumption (in kWh) by the regional grid emission factor and dividing by 1,000 to convert kilograms to metric tons. For Shanghai, the East China Grid average emission factor of 0.524 kg CO_2 e per kWh is applied, based on the China National Guidelines for Accounting and Reporting of Greenhouse Gas Emissions issued by the Ministry of Ecology and Environment.

Our Board will set targets at the beginning of each financial year in accordance with the disclosure requirements of the Listing Rules and other relevant rules and regulations upon **[REDACTED]**. The relevant targets will undergo an annual review to ensure their continued suitability for our Group's needs. When setting ESG-related targets, we will consider not only our past consumption and discharge levels, but also our future business expansion, overall Group goals and information from industry peers. Our approach will be thorough and cautious, aiming to strike a balance between business growth and environmental protection for sustainable development.

We strive to limit the increase in resource consumption and waste generation. We will adjust our targets and goals based on our actual business operations and closely monitor the financial and non-financial impact of our actions to achieve these objectives. We recognize that accurately measuring our scope 3 emissions is crucial for finding solutions to address them. We will establish surveying and measurement mechanisms to accurately determine the greenhouse gas emissions equivalent of the revenue generated from our services among our numerous stakeholders. Our aim is to comply with the disclosure requirements under the Listing Rules upon **[REDACTED]**.

Potential impacts and mitigation of climate-related risks

We are bound by various climate-related laws and regulations in China. Throughout the Track Record Period and up to the Latest Practicable Date, we have not faced any fines or penalties for violating environmental laws or regulations. Based on the knowledge and belief of our Directors, we do not anticipate significant environmental liability risks or substantial compliance costs in the future. Considering the nature of our business, our Directors believe that climate change will not have a major impact on our business operations. However, extreme weather events caused by climate change in recent years could potentially lead to significant damage to our offices, resulting in temporary or long-term closures and substantial expenses for repairs or replacements. Unchecked global warming may lead to higher temperatures, necessitating increased electricity consumption and higher operating costs. Over the medium to long term, there may be a rise in legislation and regulations in response to the potential effects of climate change. This shift in the regulatory landscape could directly or indirectly impact on our operations due to compliance requirements from our business partners, potentially resulting in additional costs and restrictions such as increased energy expenses, as well as costs for treating pollutants or hazardous waste.

We will continue to identify, assess, manage and mitigate the ESG-related risks. Our approach includes but is not limited to:

- monitoring relevant laws, regulations and industry standards to regularly assess our compliance with applicable regulatory rules;
- reviewing and assessing the ESG reports of similar companies in the industry to ensure that all relevant climate-related risks are identified on a timely basis;
- discussing among management from time to time to ensure all the material ESG issues are recognized and reported;
- discussing with key stakeholders on key ESG principles and practices to ensure that the significant aspects are covered;
- organizing a specific ESG risk management process to identify and manage ESG-related risks and opportunities as an integrated part of overall business risks and opportunities;
- setting appropriate targets, including with regard to emission, pollution and other impact on the environment aimed at reducing emissions and natural resource consumption; and
- building up sophisticated business continuity management system to handle various kinds of climate-related risks and assure our business continuity to the most extent.

We will regularly assess the risks faced by our Group, taking into account current and potential risks, including those related to ESG aspects and disruptive forces like climate change. Our Board will evaluate these risks and, if necessary, seek external expertise to review our Group's strategy, targets, internal controls and make any necessary improvements to mitigate the risks.

Our Board will oversee our risk management approach, including climate-related risks and risks monitored through standard operating processes, to ensure that appropriate measures are in place. We will also work towards integrating ESG considerations into our risk management mechanism to enhance monitoring and mitigation of ESG-related risks across our Group.

The decision to mitigate, transfer, accept, or control risks is influenced by various factors, such as government regulations and public perception. We will incorporate climate-related issues, including analysis of physical and transition risks, into our risk assessment processes and risk appetite setting. If these risks and opportunities are deemed significant, we will address them in our strategy and financial planning process. After conducting an annual review of ESG-related risks and our Group's performance in addressing them, we may make revisions and adjustments to our ESG strategies as necessary.

Measures to combat climate-related risks in the workplace

In our commitment to embracing a low-carbon world, we have implemented several environmentally friendly internal policies to minimize carbon emissions. These include:

- Implementation of energy-efficient lighting in our offices;
- Promoting paper waste reduction, water conservation and energy-saving practices among our staff by displaying water-saving and power-saving signs in prominent areas to raise awareness about environmental protection;
- Enforcing the practice of turning off lights, equipment and electronic devices when not in use and before leaving the premises;
- Utilizing energy-efficient lighting solutions, such as LED lighting;
- Ensuring air-conditioning is used judiciously and at optimal temperatures; and
- Continuously motivating our employees to minimize printing hard copies and promoting double-sided printing whenever feasible.

Social matters

We prioritize promoting diversity and ensuring equal and respectful treatment for all employees in recruitment, training, health and professional and personal development within our Company. We are committed to maintaining work-life balance, fostering a positive working environment and providing equal job opportunities for everyone. In order to ensure compliance with applicable laws and regulations regarding social matters, our human resources department periodically reviews and adjusts our policies. These adjustments are made in consultation with our legal advisers to accommodate any significant changes in labor and safety laws and regulations.

Employment

We adhere to labor management laws and regulations in the regions where we operate. We have established policies for employee recruitment management and an employee handbook to ensure compliance with legal employment practices. In accordance with relevant laws and regulations in the PRC, we are required to contribute to various social welfare schemes for our employees, including social insurance and housing provident funds.

Development and training

We prioritize a talent-centric approach, emphasizing people-oriented practices, collaboration and ongoing professional development. We offer clearly defined career advancement opportunities and a range of training programs designed to enhance employees' skills and competencies. See "—Our Employees."

Occupational health and safety

We are committed to providing a healthy and safe working environment for our employees. Throughout the Track Record Period and up to the Latest Practicable Date, we have adhered to occupational health and safety laws and regulations in all material aspects. While we do not anticipate a significant increase in costs related to compliance with current and future health and safety laws, changes in requirements may impact our ability to accurately forecast these costs.

Anti-corruption

In compliance with anti-corruption laws and regulations in the jurisdictions where we operate, we have established systems and codes such as a code of business ethics for employees and an employee grievance, complaint. These systems clearly define various aspects of business ethics. Additionally, we organize annual self-inspections, summarizations and management improvements to ensure ongoing monitoring and control of corruption and business ethics risks, supporting our Company's sound operations.

RISK MANAGEMENT AND INTERNAL CONTROL

Our Board and senior management shoulder the responsibility for devising and supervising the execution and efficacy of our internal control framework. This framework is meticulously structured to guarantee continuous adherence to pertinent legal and regulatory mandates that govern our business activities and corporate governance, thereby averting any reoccurrence of compliance failures. Our conviction stands firm that the existing internal control mechanisms and procedures epitomize adequacy in scope, feasibility and operational effectiveness.

To substantiate this belief, we have procured the services of an internal control specialist (the "**Internal Control Consultant**") to conduct a thorough evaluation of the sufficiency and efficiency of our conglomerate's internal control processes, systems and protocols. Such evaluation encompasses various facets of our operations, including management oversight, financial reporting, information disclosure, information technology governance, enterprise operations, corporate governance structures, regulatory compliance and risk management strategies. The preliminary findings from the assessment undertaken by the Internal Control Consultant have been meticulously reviewed. Following this review, our Board affirms that all significant proposals tendered by the Internal Control Consultant have been earnestly contemplated. In response to these recommendations, we are committed to implementing all necessary corrective measures to rectify any identified shortcomings within our organizational structure prior to the **[REDACTED]**.

In the regular progression of our business activities, we are inherently subject to a spectrum of risks, encompassing operational, market and financial risks. Recognizing these exposures, we hold the conviction that the implementation of robust and adaptable risk management strategies is essential to our enduring success. It is through this lens that we approach risk mitigation, ensuring that our operations are safeguarded against potential adversities, thereby securing our competitive edge and financial stability.

For the purpose of effective risk management, we will adopt or have put in place the following measures:

- Our Board is tasked with the comprehensive assessment of risks inherent to our operations, ensuring that all major decisions with significant risk implications are subjected to their scrutiny and consent;

- Our management team is committed to vigilantly observing market trends;

- We uphold stringent IT controls to significantly reduce the likelihood of IT system failures, safeguarding our operational integrity;

- To attract and retain skilled professionals, we regularly evaluate and adjust our compensation structures for management and staff, ensuring they remain competitive and congruent with our strategic growth;

- Our Directors maintain diligent oversight of our liquidity and financial health, prepared to secure financing to support our business activities and expansion initiatives when deemed necessary and advantageous; and

- we have established an audit committee which is comprised of all our independent non-executive Directors to review and supervise our financial reporting process and internal control system.

Our in-house cybersecurity measures

We prioritize our own cybersecurity to protect our assets. We have implemented a multi-layered strategy to safeguard our systems and data. As of the Latest Practicable Date, we have received the ISO: 27001 Information Security Management System certification, underscoring the strength of our systems. By combining the following technical measures with a culture of security awareness, we believe that we can maintain a robust and resilient IT infrastructure that safeguards our business operations:

- ***Strong access controls and authentication:*** We will implement access controls and authentication mechanisms to ensure that only authorized personnel can access sensitive systems and data. Role-based access control will limit access based on the user's role within the organization, minimizing the risk of unauthorized access. Regular audits and reviews of access permissions can help maintain the integrity of our access control policies.

- ***Regular updates and patches:*** Keeping our software and hardware up to date is crucial. We will apply updates and patches to protect against known vulnerabilities, mitigating the risk of cyberattacks that exploit outdated software. Our dedicated team will monitor for recent updates and patches from vendors and ensures they are applied promptly. Additionally, we will test updates in a controlled environment before deployment to ensure they do not disrupt our operations.

- ***Network monitoring and auditing:*** Continuous monitoring and auditing of network activities can help us detect and respond to suspicious activities promptly. We will use monitoring tools to track network traffic and identify anomalies that may indicate a security threat. Real-time alerts can enable our security team to take timely action when potential issues are detected. Regular audits of network logs will provide insights into past activities and help us identify patterns that could signify a breach.

- ***Data encryption:*** We will encrypt sensitive data both in transit and at rest to prevent unauthorized access. Encryption converts data into a coded format that can only be deciphered with the correct decryption key, ensuring that even if the data is intercepted, it remains unreadable. We will use industry-standard protocols to secure our data and implement encryption for all communication channels, including emails and file transfers. We will regularly review our encryption practices to manage evolving threats.

- ***Firewalls and intrusion detection systems:*** Implementing firewalls and intrusion detection systems will help us prevent and detect unauthorized access attempts. Firewalls will act as a barrier between our internal network and external threats, filtering incoming and outgoing traffic based on predefined security rules. These systems will monitor network traffic for suspicious activities and generate alerts when potential threats are detected. Regular updates to our firewall rules and intrusion detection system signatures can ensure they remain effective against new and emerging threats.

- ***Employee training:*** We will hold regular security awareness training for our employees to ensure they are knowledgeable about the latest security threats and best practices. Training programs cover topics such as phishing, password management and safe internet usage. By educating employees on how to recognize and respond to security threats, we aim to reduce the risk of human error, which is often a significant factor in security breaches. We will also conduct simulated phishing exercises to test employees' awareness and reinforce training, fostering a security-conscious culture within our organization.

- ***Backup and disaster recovery:*** We will perform regular data backups and test our disaster recovery plans to ensure business continuity in case of a security incident. Backups can be stored in secure, offsite locations to protect against data loss due to hardware failure, cyberattacks, or natural disasters. Our disaster recovery plans will outline the steps to restore operations quickly and efficiently following an incident. We will regularly test the effectiveness of these plans and prepare our team for any incident, minimizing downtime and data loss in the event of a security breach.