

業 務

概覽

我們是中國專業智能化信息安全解決方案提供商。根據弗若斯特沙利文報告，按2025年收入計，我們在中國提供數據安全平台的專業安全提供商中排名第一(市場份額為9.7%)，在中國提供數據安全的專業安全提供商中排名第七(市場份額為3.8%)，及在中國提供信息安全的專業安全提供商中排名第十三(市場份額為1.8%)。我們亦是中國信息安全領域早期應用大數據分析和人工智能技術的參與者，我們專注於數據安全、網絡安全及其他新興領域。

我們已建立一套安全模型，旨在應對數字時代的兩項核心挑戰：即內在的數據治理及邊界層面的威脅防禦。機構需要一種「縱深防禦」架構，以保護信息技術基礎設施及其中的資產。為此，我們提供統一的框架，在該框架中，我們的網絡安全解決方案保障周邊邊界免受外部攻擊者侵害，而我們的數據安全解決方案則管控敏感信息的內部流動及完整性。通過整合這兩個關鍵維度，我們提供一個具有凝聚力的生態系統，保障靜態、傳輸中及使用中的數據安全，賦能各機構在加速其數字化轉型的同時，遵守不斷演變的法規。於往績記錄期間，我們主要為客戶提供數據安全與網絡安全解決方案，集平台、標準化軟件與專項服務三位一體。該等解決方案於其整個生命週期及運行環境中保護數據、系統及網絡。具體而言：

- **數據安全解決方案。**根據弗若斯特沙利文報告，機構可能面臨的關鍵數據安全挑戰為其敏感信息可能散落在碎片化的系統中，需要人工流程及安全控制。這可能導致機構難以維持可視化、掌握重要數據的位置、一致地執行跨多個數據資產的政策並實時響應來自多個方向的不同的風險攻擊。我們通過在數據全生命週期內提供統一控制及智能驅動的運營來應對該挑戰，涵蓋橫跨整個機構架構的收集、傳輸、存儲、使用及共享。為實現這一目標，我們並非依賴市場上可能數不勝數、相互脫節且可能互不兼容的各類軟件，而是通過涵蓋客戶所需的各項功能，量身定製適配特定客戶需求的數據安全平台，並使其作為一個具有集中管理界面的單一生態系統運行。除平台外，我們意識到機構或許需要的是能夠立即使用的專用軟件，而非高度定制化的解決方案，因此我們還提供一套全面的數據安全軟件。通過評估數據處理實踐，並制定符合業務需求的長期可行計劃，我們亦提供可支援治理框架設計的專項服務。於2023年、2024年及2025年，我們的數據安全解決方案產生的收入分別為人民幣219.5百萬元、人民幣281.8百萬元及人民幣297.2百萬元，分別佔我們總收入的42.5%、42.8%及42.0%。
- **網絡安全解決方案。**根據弗若斯特沙利文報告，隨著系統擴展至網絡、雲平台、應用程序及移動終端，組織的安全控制可能會變得碎片化且不一致。傳統工具高度依賴人工流程及靜態規則，可視化程度有限，威脅識別遲緩，並阻礙實時響應。因此，許多公司難以了解其風險敞口、評估防禦的有效性及維持持續改進的安全態勢。我們通過提供作為協調生態系統運行的網絡安全平台、標準化軟件及專項服務來應對該等挑戰。例如，我們的網絡安全平台可專門滿足客戶需求，並將文件分析、行為建模及攻擊鏈追蹤等特定功能整合到單一、全面且

業 務

具有分析能力的視圖中，減少虛假警報、發現未知威脅，並改善事件理解，這與依賴一系列不同且非集成的網絡安全軟件形成了鮮明對比。除我們的平台外，我們還提供一套全面的網絡安全軟件及服務，幫助公司設計其網絡安全架構，以符合監管期望及其業務需求。於2023年、2024年及2025年，我們從網絡安全解決方案產生的收入分別為人民幣254.1百萬元、人民幣328.4百萬元及人民幣339.7百萬元，分別佔我們總收入的49.3%、49.8%及48.0%。

- **其他解決方案。**基於特定行業需求，我們亦透過整合自有與第三方產品和服務，向客戶提供定制化的解決方案。於2023年、2024年及2025年，我們其他解決方案產生的收入分別為人民幣42.5百萬元、人民幣48.9百萬元及人民幣70.8百萬元，分別佔我們總收入的8.2%、7.4%及10.0%。

於2025年，我們為155家電信網絡運營商、41家能源及電力公司以及86家政府及公共部門實體提供服務。根據弗若斯特沙利文報告，這些機構運行著支持基本公共及商業功能的大型互聯繫統。其技術環境擴展迅速，且通常涉及許多部門、業務系統及數據流，導致難以維持一致的安全及清晰的監督。我們不同行業的客戶可能面臨類似的困難。他們存儲及使用大量數據，依賴不間斷的運營，且隨著其營運日益複雜，必須遵守日益增長的監管要求，亦因此容易受到來自多方向的攻擊。我們專注於透過定制平台、實用的軟件工具以及支持規劃、測試及日常運營的專業服務來幫助其解決這些問題。我們還認為智算中心也已成爲我們客戶群的重要組成部分。這些中心支持高性能計算及人工智能工作負載，使用的基礎設施規模宏大、具備多租戶特性且跨區域分佈。它們經常面臨資源邊界不明確、數據傳輸需求龐大以及需要同時保護硬件及雲原生環境的要求。我們的平台支持身份檢查、環境監控、資源控制、容器及虛擬化保護以及安全傳輸。

我們構建支持主動防禦、安全情報及數據驅動運營的技術架構。我們的技術架構以大數據處理、攻防創新、數據安全保障及人工智能四大核心技術為基礎，彼等透過API及共享數據系統相互連接，從而使我們的技術專長既能在我們設計的軟件之間共享，亦能在我們為客戶創建及定制的平台中應用。我們亦認為研發與創新是我們長期戰略的核心。截至2025年12月31日，我們的研發團隊由186名成員組成，分別駐於我們的上海、北京、武漢、合肥、鄭州及成都辦公室。於2023年、2024年及2025年，我們的研發開支分別佔我們總收入的23.2%、15.2%及14.4%。我們的核心技術均為內部開發。截至2025年12月31日，我們已獲得145項獲授專利(包括141項發明專利)及202項註冊軟件著作權。

業 務

我們的競爭優勢

我們是中國領先的專業數據安全平台提供商之一

根據弗若斯特沙利文報告，就收入而言，於2025年，我們在中國提供數據安全平台的專業安全提供商中排名第一(市場份額9.7%)，在中國提供數據安全的專業安全提供商中排名第七(市場份額3.8%)，在中國提供信息安全的專業安全提供商中排名第十三(市場份額1.8%)。

憑藉十多年的行業參與，我們開發了一套涵蓋數據全生命週期的集成架構，包括數據識別、分類分級、行為及訪問分析、風險監測及智能運營。我們在數據智能及人工智能方面付出的努力，亦使我們能夠在產品架構中嵌入自動化數據識別、風險分析及響應功能，跨行業支持解決方案的可擴展性以及產品的持續提升。隨著企業及公共機構持續加強其數據保護系統，此基礎架構使我們能夠很好地應對市場不斷演變的需求。

我們的技術及行業見解亦得益於我們參與國家及行業標準的制定。自2019年以來，我們參與了多項已發佈國家標準的制定，包括《數據安全法實施參考(第一版)》及《數據安全能力成熟度模型》(GB/T 37988 2019)、《電信網和互聯網數據安全風險評估實施方法》(YD/T 3801 2020)及《基礎電信企業數據分類分級方法》(YD/T 3813 2020)，以及各類行業白皮書。

我們的團隊及技術獲得行業機構多項認可。其中包括「鑄網2022」技術支持認可以及我們被評為數據要素價值創新示範基地。其他認可包括2024年「磐安」優秀案例、2023年星熠獎、2022年星河案例、2021年全國人工智能創新應用大賽一等獎、2019年吳文俊人工智能科學技術獎(二等獎)、2017年中國網絡安全技術對抗賽(第一名)及2024年「數信杯」數據安全大賽金獎。

我們的能力進一步得到專業資質的支持。例如，我們是中國少數獲得中國網絡安全審查技術與認證中心頒發的五項一級服務資質的公司之一，涵蓋軟件安全開發、應急響應、安全運營、安全集成及風險評估。我們亦持有中國信息安全測評中心在風險評估、安全工程、安全開發及大數據安全評級等領域的資質，以及中國通信企業協會與安全設計與集成、風險評估及應急響應以及培訓相關的資質。

我們的技術實力亦在國家重大活動中得到證明。我們被指定為重大活動網絡安全支撐單位，並維持著能夠進行全國範圍現場防護及應急處理的快速響應團隊。我們承擔了包括2022年北京冬季殘奧會、杭州第19屆亞運會、中國國際進口博覽會、G20

業 務

杭州峰會、「一帶一路」國際合作高峰論壇及國慶70週年慶典等活動的安全職責。聯合國訓練研究所任命我們為亞太地區唯一的大數據應用與安全培訓基地，我們亦擔任聯合國工業發展組織上海國際智能製造促進中心專家組成員。

根據弗若斯特沙利文報告，中國信息安全市場規模從2021年的人民幣732億元增長至2025年的人民幣1,057億元，複合年增長率為9.6%，預計到2030年將達到人民幣1,727億元，複合年增長率為10.6%。數據安全市場從2021年的人民幣186億元增長至2025年的人民幣290億元，複合年增長率為11.7%，預計到2030年將達到人民幣509億元，複合年增長率為12.1%。網絡安全市場從2021年的人民幣546億元增長至2025年的人民幣767億元，複合年增長率為8.9%，預計到2030年將達到人民幣1,219億元，複合年增長率為10.0%。人工智能的更廣泛採用亦帶來了新的安全缺口，促使人工智能安全、車聯網安全及物聯網安全等領域的需求上升。

鑑於這些市場動態，我們認為我們已確立的地位、技術能力、資質、在標準制定中的角色、以及在國家級部署中經驗證的表現，共同使我們處於把握行業增長機遇的有利位置。

我們的技術架構能為持續創新及質量交付提供持久基礎

我們已開發基於大數據處理、攻防創新、數據安全保障及人工智能的技術架構。

作為中國將大數據及人工智能應用於信息安全的早期企業之一，我們積累了深厚的技術專業知識，使我們能夠作為連接大規模數據治理與複雜模型訓練的閉環運行。這種整合架構若無長期積累則可能難以複製，形成了支持持續產品創新及在複雜客戶環境中可靠交付的持久技術基礎。

在數據處理方面，我們的專有架構支持對海量數據進行實時處理，同時與通用設計相比，其運行功耗顯著降低，從而提升客戶的部署效率，並為人工智能驅動的功能提供了高質量的數據輸入。在此基礎上，我們的集成算法棧及垂直領域大模型作為「安全中樞」運行，提供快速的威脅感知，維持高檢測精度並減少運營噪音。這些屬性透過提高運營效率、響應及時性及安全決策的準確性，加強了我們的競爭地位。

在攻防創新方面，我們部署了一套廣泛的攻擊檢測及降噪模型，覆蓋了攻擊鏈的多個階段。結合我們的全鏈路數據安全保障技術，該架構實現了對網絡邊界、敏感資產、外部威脅及內部風險的全方位保護。與手動方法相比，這種方法顯著提高了漏洞識別的效率及準確性，並支持對攻擊影響進行更可靠的評估。這些能力鞏固了我們在分析深度、覆蓋廣度及關鍵任務環境韌性方面的競爭優勢。

業 務

我們將內生安全嵌入人工智能全生命週期。透過對抗樣本變異引擎及紅藍對抗平台，我們在訓練期間進行大規模壓力測試及模擬攻擊，以識別與後門、投毒及基於提示詞操縱相關的風險。該開發架構使漏洞能夠被實時處理，同時模型防火牆機制保障了核心算法在對抗條件下的穩定性及可控性。隨著人工智能安全預期不斷演變，這些特性在模型魯棒性、生命週期治理及合規就緒程度方面提供了競爭優勢。

利用這一技術基礎，我們建立了一個旨在隨客戶需求演進的主動防禦產品體系。因此，我們所開發的技術知識可以在我們的平台及軟件中使用。我們的平台化架構支持收集、檢測、分析及響應的全週期，降低了運營複雜性並減少了資源需求。這種結構非常適合包括電信網絡運營商及大型企業在內的大規模且複雜的環境，該等環境需要實時性能、快速產品迭代及穩定運行。這些特點轉化為在可擴展性、交付效率、及長期服務穩定性方面的競爭優勢。

我們擁有能支持技術可擴展性與複用的研發能力

我們認為研發及創新是我們長期戰略的核心。我們的研發圍繞下列相互連接的基礎展開：大數據處理、攻防創新、數據安全保障及人工智能。這些基礎透過標準化接口及共享數據層作為一個系統運行，使我們能夠在我們的平台及軟件中共享所開發的技術知識，使其能夠感知威脅、進行分析並自動響應。我們的人工智能模型(包括為安全訓練的大模型)有助於識別異常活動、防止欺詐、追蹤網絡釣魚並從不同角度檢測惡意行為。這些基礎共同創造了一個檢測、決策及響應的循環，有助於增強系統韌性、降低成本並在多種環境中保護客戶的數據及網絡。

我們的研發團隊將內部開發與有針對性的合作相結合。截至2025年12月31日，我們的研發團隊由186名成員組成，分別駐於我們的上海、北京、武漢、合肥、鄭州及成都辦公室。於2023年、2024年及2025年，我們的研發開支分別佔總收入的23.2%、15.2%及14.4%。我們的核心技術均為內部開發。我們亦與選定的合作夥伴合作，例如國家互聯網應急中心，這有助於擴大我們獲取數據及流量資源的渠道，以進行測試及升級。我們的研發體系獲得了第三方認可。我們獲得了CMMI 3.0版本成熟度五級，並被工信部評為國家級「小巨人」企業。截至2025年12月31日，我們已獲得145項獲授權專利(包括141項發明專利)，並獲得202項軟件著作權。

我們的研發團隊包括具有中國及海外行業與學術經驗的僱員。我們研究院院長夏玉明先生曾獲2020年浦東新區科學技術進步獎。王文君先生為我們研究院副院長，並於網絡安全研究、數據安全治理及大型安全基礎設施項目方面擁有豐富經驗。彼曾參與多項省、市級工業互聯網態勢感知項目，以及大型企業級安全基礎設施部署

業 務

工作。王先生於網絡安全及數據治理界一直發揮積極作用。彼擔任OWASP上海分會主席，並獲上海市有關部門授予「網絡安全工匠」稱號。彼為中國互聯網協會數據安全與治理工作委員會專家組成員，以及中國信息通信研究院數字安全護航計劃下的高級專家。彼亦為數據安全社區倡議的專家參與者。此外，王先生亦為由聯合國訓練研究所轄下國際培訓中心認證的高級信息安全培訓講師，並於該機構為信息安全專業教育項目作出貢獻。彼亦擔任上海大數據中心的實踐導向型安全專家，為大規模數據環境中的數據保護框架及營運安全實踐提供建議。彼因對網絡安全實踐的發展及推進所作出的貢獻而獲頒CSA領導力獎。另一位副院長魏國富先生曾帶領我們的團隊贏得2017年中國網絡安全技術對抗賽一等獎（團隊）。我們的研發團隊支持我們在複雜環境下的持續技術進步及穩定交付。

我們亦建立了一個支持技術複用及可擴展性的開發基礎。透過標準化接口及模塊化組件，我們減少了集成工作並提高了可維護性。我們的組件庫包括用於流量處理、分析、圖分析及實時數據倉庫的引擎，以及用於儀表板、用戶管理、數據網關、調度及DevOps的模塊。我們亦開發了一套架構，支持具備對不同數據源實時訪問、動態上下文處理及基本智能體功能的人工智能應用開發。這種方法使我們能夠快速配置平台、響應客戶定制需求並在各個部署中維持一致的質量。

總體而言，我們的研發能力、經過驗證的流程、經驗豐富的團隊、知識產權及可複用的開發基礎形成了一個支持可擴展性及複用的穩定體系。該等能力使產品更新更迅速、集成負擔更低且在複雜環境中表現可靠，有助於我們長期維持競爭地位。

我們立足於以大型企業與公共機構為核心的高壁壘客戶生態

我們服務於對數字運營的穩定與安全有本質要求的行業中的企業、政府機構及公共機構。截至2025年12月31日，我們的客戶群包括電信網絡運營商、能源及電力公司、以及政府及公共部門實體。這些機構管理著支持日常公共及商業功能的大型互聯系統。他們依賴一致的運營、對數據活動的監督以及對行業規則的合規。許多機構運行多條業務線及技術系統，這增加了維持統一安全標準及從多個維度對其資產進行功能性保護的難度。我們專注於透過為規劃、測試及日常運營提供支持的結構化平台及實用工具來幫助其滿足這些需求。

- 電信網絡運營商管理著數據流動龐大且用戶群體廣闊的網絡。其信息通常存儲在許多系統中並由不同部門處理，這可能產生可視化缺口，使其易受到數據洩露或攻擊的影響。我們的解決方案支持結構化資產管理、協調網絡防禦、及自動化數據控制。例如，我們的態勢感知平台覆蓋了中國所有

業 務

三家國家級運營商，並觸達多個省級分公司，且我們的數據安全管控及數據資產管理平台符合國家質量要求。我們亦提供諮詢、測試、評估及事件響應服務，幫助運營商在全國及區域網絡中維持安全運營。

- 能源及電力公司在電廠、調度中心及現場站點運行混合的信息及控制系統。他們在多個系統中處理大量數據，但部分公司可能缺乏清晰的數據分類、權責歸屬或溯源。其運營必須應對數字及物理雙重風險，但鑒於能源公司的規模及複雜性，這可能具有挑戰性。例如，我們的平台能夠根據這些公司的需求進行定制，並幫助定義數據類別、支持安全共享、監控敏感傳輸，並提供整個電網狀況的統一視圖，以便更好地監控潛在攻擊。我們亦進行現場驗證，以確認防護措施按預期發揮作用。
- 政府及公共部門實體運行大型數字平台及行政網絡。其主要挑戰是在處理可能跨機構邊界流動的數據時，維持信任、穩定及協調。我們的系統結合了關鍵安全功能，包括數據監控、行為分析及政策合規，並透過持續支持幫助機構維持穩定且合規的運營以避免數據洩露或威脅。

我們亦已擴展至向智算中心提供我們的解決方案，這些中心處理高性能計算及人工智能工作負載。這些中心通常具有複雜的資源結構、龐大的數據傳輸需求以及保護物理及雲原生環境的要求。我們的平台支持身份檢查、環境監控、資源控制、容器及虛擬化保護以及安全傳輸。這為計算中心提供了符合運營及監管預期的一致且實用的安全基礎。

與這類客戶建立關係需要時間、對行業流程的熟悉以及對系統結構與約束的清晰理解。大型企業及公共機構通常傾向於與能夠維持穩定支持、確保跨系統兼容性並了解其長期需求的供應商合作。開發合適的安全解決方案通常需要跨多個業務部門進行聯合規劃、量身定製的設計及迭代測試。系統一旦部署，已安裝的平台及系統即成為客戶日常運營的一部分，這增加了更換供應商的成本及風險。因此，這些行業的客戶傾向於與已證明具備能力、可靠性及行業環境知識的供應商保持長期合作，而根據弗若斯特沙利文報告，此反映行業傾向維持業務延續性，以保障營運穩定性，並於供應商透過首次招標與客戶達成合作後，降低服務中斷風險。我們與客戶的關係為新的市場參與者創造了高准入門檻，並支持了強大的客戶留存。

我們由經驗豐富且具行業認可度的管理團隊領導

我們的管理團隊具備對行業的深刻洞察、豐富的營運經驗與紮實的技術專業能力，構成了我們持續業務表現與市場領先地位的關鍵基礎。我們的高級管理人員在信息安全領域擁有長期積累的經驗，且團隊長期保持穩定。我們的聯合創始人兼總經理

業 務

張先生是行業內廣受認可的專家，現任工業和信息化部重點實驗室數據安全與產業應用評價首屆學術委員會委員以及上海市數據合規與安全產業發展專家組專家。董事長胡先生曾參與多項國家及企業信息安全標準的起草工作，並獲得包括「吳文俊人工智能科學技術獎科技進步獎二等獎」、「全國工業和信息化系統勞動模範」及「2023年網絡安全工匠獎」。胡先生亦於2024年1月被上海市總工會評為「上海工匠」，並於2024年12月入選上海市人才工作局主辦的上海市東方英才計劃領軍項目。彼等共同領導本集團持續推動技術基礎與解決方案能力的進步。彼等之專業領導確保我們在人工智能、數據安全等關鍵領域保持標杆地位，並支持我們業務的長期可擴展性與競爭力。

我們的未來策略

我們計劃加強在數據安全領域的市場地位

我們旨在通過調整產品及服務以匹配中國數字系統的發展趨勢，從而加強我們的市場地位。隨著越來越多的機構依賴互聯系統進行日常運作，安全風險不再局限於單一設備或網絡，而是同時出現在移動終端、內部網絡及雲環境中，從而需要能夠協作、可部署於機構不同部分且能在新風險出現時進行更新的解決方案。為滿足該等需求，我們計劃擴大產品組合的覆蓋範圍，構建一套涵蓋終端、網絡及雲環境的全方位解決方案。我們亦計劃專注於基於終端的數據保護及零信任模型。藉由加強研發及交付流程的標準化、效率及質量，滿足不同行業客戶的需求並支持我們的市場地位。

此外，我們計劃提升核心技術，使我們的產品能更好地支持管理日益增長數據量的客戶。隨著眾多機構將更多工作移至線上，彼等需要能夠準確分類信息、安全傳輸信息並在其全生命週期內控制其使用的工具。為滿足此需求，我們擬投資於將人工智能與大數據分析相結合的技術，支持隱私保護方法並應用同態加密等技術。該等技術預期將協助我們提高分類、傳輸、存儲及治理等領域的安全性。

根據弗若斯特沙利文報告，中國的數字化轉型正向各行各業及城市擴展，且日益強調數字環境的安全性。這即產生了對一致標準及可信系統的需求。我們計劃通過參與國家及行業標準的制定，以及支持政府及行業領導者構建安全數字平台來參與該等發展。通過參與該等國家級倡議，我們旨在使我們的工作與長期數字發展目標保持一致，並在客戶系統擴展時為其提供支持。

業 務

我們計劃提升核心技術並通過基礎研發把握新機遇

我們擬改進技術基礎，以便在客戶面臨新型安全風險及在其業務中增加使用人工智能時為其提供支持。隨著數字系統的擴展，機構必須保護其使用的算法以及支持該等算法的數據。該等變化要求安全方法能夠處理新的攻擊模式，在信息的全生命週期內保護信息，並能在不同類型的計算環境中運行。

我們的研發戰略專注於以系統化及長期的方式構建以下能力：

- **全生命週期人工智能安全：**隨著機構日益依賴人工智能模型，圍繞模型訓練、模型使用及人工智能生成內容而產生的風險持續增長。我們計劃開發保護人工智能系統的技術，涵蓋從模型開發初期到持續運行的全過程。這包括檢測訓練期間可能出現的威脅（如數據污染或隱藏指令），以及抵禦模型使用期間的攻擊（如有害輸入或誤導性提示）。我們亦計劃加強模型訓練及運行的環境，以便監測及控制訪問、變更及內部運作。此項工作旨在提高人工智能系統的安全性、可追溯性及可靠性，而這亦是許多行業的核心要求。
- **人工智能生成內容的合規性及內容治理：**隨著人工智能工具產生更多的文本、視覺及音頻內容，機構需要切實可行的方法來識別有害或不當資料。我們正在開發能夠理解語義及上下文（而非僅依賴簡單檢查）的內容識別引擎。該等工具旨在支持對人工智能生成內容的實時審查，並協助攔截諸如受操縱媒體或誤導性信息等風險。這一方向回應了日益增長的監管預期，並可協助客戶維持對其數字系統的信任。
- **人工智能系統的評估及保護：**人工智能系統正廣泛應用於多個業務運營領域，許多機構必須證明其模型是安全、穩定且合規的。為支持這一需求，我們正在構建用於評估模型、加強模型抗攻擊能力、管理風險及支持日常安全運維的平台。該等平台將協助客戶測試其人工智能系統，了解其在不同條件下的行為，並在系統演進過程中保持受保護狀態。這種方法可為用戶提供管理相關風險的工具，進而為拓展人工智能的應用範圍提供了支持。
- **智算中心的安全運維：**隨著人工智能工作負載的增加，計算中心不斷擴大規模，並需要同時運行大量服務器、存儲海量數據及管理不同類型的應用程式。這在協調計算資源、控制訪問及保護模型免受攻擊方面帶來了新挑戰。我們計劃開發多個安全平台，幫助按照統一的方式管理該等問題。我們的工作將側重於防禦針對大模型的有害輸入、防止數據篡改並改進模型訪問控制。該等能力旨在支持複雜計算集群的穩定及安全運行。

業 務

- **數據保護及跨機構數據安全使用：**數據價值日益增加，許多機構必須在滿足監管預期的同時共享或傳輸數據。我們計劃通過開發理解數據使用方式、識別風險行為並對敏感操作應用動態控制的方法，來加強終端保護。這包括隔離高風險行為、管理數據使用方式並在需要時追蹤重要活動的工具。我們亦計劃支持數據在機構間的安全流通。隨著數據成為中國數字經濟中公認的生產要素，新的業務模式及監管要求正在湧現。我們旨在構建數據安全基礎設施，協助機構在保護隱私及符合合規規則的前提下共享數據。通過將技術保障與基於規則的審計相結合，我們計劃協助客戶以受控且可信的方式釋放其數據價值。
- **聯網設備及萬物互聯安全：**隨著智能設備在家庭、城市及行業中的普及，指令及數據往往在缺乏明確監管的情況下跨多個系統流動，因而帶來了新的風險。我們計劃基於可信硬件及我們自有的中間件平台構建設備級安全控制。該等控制將協助驗證設備身份、攔截不安全指令並隔離不同領域的操作。這為智慧城市、工業及物聯網環境提供了更強大的保護，在該等環境中，設備故障可能導致運維中斷。我們亦計劃開發將設備安全、邊緣安全及雲安全連接成一個系統的解決方案，以支持對安全人工智能oT應用日益增長的需求。
- **AI智能體安全：**我們擬加強我們AI智能體能力的安全框架。核心目標是平衡能力邊界拓展與有效風險控制。我們正在開發一套貫穿AI智能體整個生命週期的主動安全防禦系統，以全生命週期資產識別及管治為基礎，並結合由外部邊界控制及內置安全機制組成的雙重防護。此方法旨在提升我們AI智能體營運的安全性、可靠性及可控性，同時支持高效的業務執行及可擴展部署。

我們計劃擴大客戶覆蓋範圍及國際影響力

我們擬透過服務更多需要穩定且合規安全運維的行業，來擴大我們的客戶群。電信、政府及金融服務等行業由於其系統支持著基本服務並處理敏感數據而面臨著日益增長的安全壓力。隨著該等行業持續增加及升級其數字基礎設施，其需要可靠、易於維護且適用於大型複雜環境的安全解決方案。通過深耕該等行業，我們旨在滿足這一日益增長的需求並加強我們的整體市場地位。

通過與主要電信網絡運營商的長期合作，我們計劃探索面向消費者市場的機遇。隨著在線應用程式、聯網設備及雲服務更多地面向個人用戶，對實用且價格實惠的安全工具的需求正在不斷擴大。與電信網絡運營商的合作搭建了一個天然渠道，我們藉此可以大規模交付該等服務並觸達更廣泛的用戶群，開拓不斷增長的市場細分，同時利用運營已有的信任及分銷網絡。

業 務

除大型企業外，中小企業亦需要安全解決方案，但往往缺乏自行構建資源。為填補這一缺口，我們計劃提供標準化安全市場及輕量級雲端安全服務。該等產品使小型企業能以更低成本及更簡單的部署獲得關鍵安全能力。這有助於我們觸達更廣泛的客戶群，並支持不同規模企業的包容性數字發展。

在國際方面，我們計劃拓展業務範圍，將我們的產品及服務推向海外市場。我們擬在香港設立國際業務總部，包括全球安全運維中心及跨境數據安全樞紐。我們預期，我們的國際業務總部將使我們能夠依託香港作為區域金融、貿易及技術中心的地位，從而觸達香港、澳門、東南亞及其他國際市場的客戶。隨著更多機構開展跨境業務，對一致且合規的安全解決方案的需求日益增加，我們旨在為該等客戶提供端到端服務。

我們了解不同地區遵循不同的數據保護及安全規則。為滿足該等要求，我們計劃開發針對特定司法管轄區設計的安全合規產品。這使我們能夠支持必須在不同法律及監管框架下經營的客戶。我們預期採用技術輸出與本地化服務相結合的模式，通過與大型企業及國有集團的合作夥伴關係交付服務。這種方法有助於我們將技術帶入海外市場，同時確保服務能夠反映當地情況及預期。

總體而言，我們跨行業、跨客戶群及跨地區的擴張計劃旨在滿足日益增長的安全需求，支持不同規模的客戶，並參與對可信數字運維日益增長的需求。通過服務更廣泛的市場，我們旨在構建一項更平衡且更具韌性的長期業務。

我們計劃吸引、培養及留住核心人才，構建穩定且多元的人才體系

我們將人才視為長期戰略的關鍵部分。隨著安全需求增長及技術快速變化，我們需要精通人工智能安全、海量流量分析、數據管理、智能算法及大模型應用等領域的專業人士。我們計劃繼續投資於具備該等技能的人才，以便我們的團隊能夠支持新產品開發、響應市場需求並維持穩定交付。我們亦計劃通過在服務地區培養具備全球經驗及本地理解的團隊，逐步建立一支能夠支持我們國際擴張的專責員工隊伍。

為支持該等目標，我們計劃完善我們的人才管理體系。我們的方法將涵蓋員工選拔、配置、培養及留任的全週期。通過使用動態人才數據庫，我們旨在更好地了解員工隊伍的規模、結構及需求，並設計與員工發展不同階段相匹配的培訓計劃。我們亦計劃強化激勵機制，使獎勵能反映崗位職責及績效。這將有助於我們吸引及留住與我們長期戰略契合且能為組織關鍵職位做出貢獻的員工。

通過該等努力，我們旨在構建一個穩定、多元且能支持我們在不同市場及產品領域持續發展的人才體系。

業 務

我們計劃進行戰略性收購，為長期競爭優勢提供支持

我們擬探索可強化我們技術基礎並支持我們長期發展的戰略性收購及合作機遇。隨著安全風險演變及客戶需求變得更加複雜，並非所有能力都能以同樣的速度在內部構建。具體而言，我們計劃物色處於高增長細分市場且具有互補性的技術能力及擁有成熟客戶群以及地區市場佈局的公司，從而加快我們的市場滲透。預計該等交易亦將使我們能夠透過共享研發基礎設施、優化供應鏈管理及統一的市場開拓策略，實現顯著的營運及成本協同效應。通過審慎且具選擇性的方法，我們利用戰略性收購、合資企業、聯盟及合作夥伴關係來鞏固我們的技術基礎，擴展我們的能力，並在市場持續演進的過程中保持穩定的競爭力。

在考慮潛在合作夥伴或收購目標時，我們擬優先考慮其產品或技術能與我們現有產品產生協同效應的公司。此協同效應亦可支持我們研發資源的擴張，並改善我們獲取更廣泛工具、人才及市場機遇生態系統的能力。

截至最後實際可行日期，我們尚未確定具體目標，亦未就任何戰略性收購或合作訂立具約束力的協議。

我們的解決方案

於往績記錄期間，我們產生的收入主要來自數據安全解決方案及網絡安全解決方案。在這兩個主要類別，我們提供三類解決方案，即(i)平台；(ii)標準化軟件；及(iii)專項服務。我們亦提供按客戶需求定制的其他解決方案。下表載列於所示年度我們的解決方案所產生的收入明細：

	截至12月31日止年度					
	2023年		2024年		2025年	
	(人民幣千元)	(%)	(人民幣千元)	(%)	(人民幣千元)	(%)
數據安全解決方案						
—平台	84,242	16.3	127,325	19.4	148,520	21.0
—標準化軟件	62,165	12.0	46,321	7.0	31,522	4.5
—專項服務	73,129	14.2	108,170	16.4	117,172	16.5
小計	219,536	42.5	281,816	42.8	297,214	42.0
網絡安全解決方案						
—平台	45,513	8.8	88,195	13.4	90,597	12.8
—標準化軟件	25,165	4.9	44,263	6.7	36,911	5.2
—專項服務	183,441	35.6	195,933	29.7	212,175	30.0
小計	254,119	49.3	328,391	49.8	339,683	48.0
其他解決方案	42,544	8.2	48,929	7.4	70,758	10.0
總計	516,199	100.0	659,136	100.0	707,655	100.0

業 務

總體而言，我們的平台及標準化軟件主要在定制化程度、交付形式、實施複雜性以及商業化特徵方面存在差異。一般而言，各項單一軟件均具備明確界定的標準功能，可快速部署，僅需少量客製化調整。相比之下，平台整合多項功能，以滿足客戶特定的營運及行業需求。值得注意的是，我們的平台並非簡單堆疊軟件功能，而是針對客戶既有基礎設施及業務流程進行深度、專屬的整合。因此，我們的平台需要更全面的客製化工作及更長的實施週期，而標準化軟件則旨在實現更快部署與更即時的收入確認。

下表概述了這兩項業務之間的主要差異：

	平台	標準化軟件
定制化程度	高。須根據客戶的行業特點及具體營運情況進行深度定制。	低。高度標準化，僅需極少定制。
交付形式	主要以純軟件或軟硬件集成解決方案的形式提供。	主要以純軟件解決方案的形式提供。
實施週期	週期較長，一般約為一年。實施過程較為複雜，並涉及與多個內部客戶系統進行深度整合。	週期較短，一般在三個月內。部署過程靈活，通常以獨立模組的形式實現，並能快速集成。
付款里程碑	多個里程碑，通常分為三至五個階段，付款與項目進度掛鉤，例如首期款項、初步驗收、上線、試運行及最終驗收。	里程碑數量有限，通常為兩個階段，付款與初始交付及系統上線相一致。

業 務

數據安全解決方案

機構在數據安全方面面臨著同樣的核心問題並不罕見。其敏感信息散落在互不相同的不同系統中，他們可能依賴人工步驟，且其安全控制可能不匹配。這可能產生盲點，並使機構難以了解重要數據的存儲位置、數據使用者以及是否正在產生任何風險。當團隊無法清晰地看到其數據時，就難以執行規則或實時響應問題。因此，他們可能無法在整個組織架構內有效保護敏感信息，使其免受數據洩露或攻擊。我們系統的主要目標為通過打破信息孤島來消除數據碎片化。

我們透過創建一種在信息的整個全生命週期內管理數據安全的統一方法來解決這些問題。我們並非使用各自獨立運行的工具，而是將我們的平台、軟件及服務設計為一個相互連接的生態系統。我們的系統作為組織數據安全架構的核心神經系統。其為一個綜合技術層，旨在透過人工智能驅動分析攝取、處理及分析大量安全相關數據。該架構作為新一代安全營運中心的核心基礎，透過提供統一的數據基線，符合擴展檢測與回應的先進原則。通過利用人工智能將來自網絡、終端、雲環境和應用程序等不同來源的信息進行關聯分析，我們的系統能夠識別風險隱患，並自動執行複雜的安全任務。該生態系統的核心是一個管理平台，用於設定政策、協調響應並讓團隊清晰了解正在發生的情況。這種理念透過將所有安全活動納入單一架構，有助於消除混亂。

於2023年、2024年及2025年，我們數據安全解決方案所產生的收入分別為人民幣219.5百萬元、人民幣281.8百萬元及人民幣297.2百萬元，各佔我們總收入的42.5%、42.8%及42.0%。

以下案例研究說明我們為客戶提供的典型數據安全項目：

案例研究：客戶A的數據安全治理平台

項目背景

我們為中國最大電信網絡營運商之一的客戶A設計、構建並交付集團級數據安全治理平台。該項目旨在應對客戶面臨的各項挑戰，包括數據環境高度分散、監管要求日趨嚴格，以及內部與跨部門的數據使用安全需求持續攀升。該平台以集中治理為核心，透過智能分析強化風險可視性，協助客戶推動數據安全管理，轉型為更具系統性與主動性的運作模式。

項目範圍及覆蓋內容

其依四大原則建置：集中化管理、智能化分類分級、端到端監控、安全事件閉環處置。該系統已完成十個省級營運公司部署，並與現有省級平台整合，落實全集團政策統一制定及集中執行。

業 務

該數據安全治理平台針對主要業務系統、數據庫、數據欄位及外部數據介面的數據資產提供一體化管理；支持結構化數據、非結構化數據及大數據環境，涵蓋約三十種數據類型。目前全集團約十萬項數據資產均已納入平台集中治理。核心功能模組包括數據資產清單管理、敏感數據識別與分類、數據屏蔽驗證、數據流動與使用監控、風險檢測、安全營運管理。

該平台已完成大規模商業部署並持續運行。截至2024年7月31日，我們的數據安全治理平台已為客戶A旗下的31家省級附屬公司提供服務，集中管理並處理了客戶A的97,000項數據資產，以及每月識別並記錄超過47,000條敏感數據條目，並治理超過50,000起數據安全事件，於高數據量及高並發負載場景下，維持穩定系統效能。

下圖展示了該平台提供的界面：



實施

該平台透過與客戶A現有數據基礎設施及業務系統深度整合完成建置落地；同時部署人工智能模型，支持自動辨識敏感數據、識別風險及減少警報噪音。風險事件會留存記錄，並附有可追溯的操作內容，確保調查具備成效並落實責任追究。平台配置集中式儀表板，即時呈現全集團整體數據安全態勢，並配合標準化工作流程，完善問題整改與升級處理。

戰略影響

該項目協助客戶A，從過往零散、被動式的數據安全管理模式，轉型為集團統一、即時監控且主動防禦之治理架構。平台強化數據資產分類分級能力，結合數據安全流量監控，現已覆蓋九成以上受管數據資產，預警準確率超過90%。透過導入主體式降噪模型，風險處理工單的平均處理效率提升約93%。

業 務

該平台強化客戶A的監管合規能力，同時允許受控的內部及跨部門數據流通。我們認為，此部署已成為我們服務大型企業客戶時數據安全解決方案的示範案例，並透過改善數據安全營運水準，全面支持客戶A更廣泛的數字化轉型戰略。

下文載列我們向客戶提供的關鍵數據安全平台、標準化軟件及專業服務的詳情：

數據安全平台

根據弗若斯特沙利文報告，大型機構的系統往往分散在不同的網絡、雲端及設備中，這可能導致機構難以了解數據資產所在的位置、數據如何流動以及是否正在發生風險事件。許多團隊亦可能面臨日益增長的合規要求，但缺乏合適的工具來以統一、集成的方式實時監控一切，因為企業可能不得不採用大量相互脫節且互不兼容的軟件方案。我們的理念是透過構建涵蓋數據全生命週期及所有場景(從數據生成、存儲、傳輸、使用到銷毀)的全面安全體系，並提供統一的數據安全防護、治理及合規能力，以解決該等挑戰。

於2023年、2024年及2025年，我們數據安全平台所產生的收入分別為人民幣84.2百萬元、人民幣127.3百萬元及人民幣148.5百萬元，分別佔我們總收入的16.3%、19.4%及21.0%。

我們向客戶提供的關鍵定制化數據安全平台包括：

安全數據中心

機構收集海量的安全數據，但這些數據往往存放在不同的地方，使用不同的格式，且難以分析。根據弗若斯特沙利文報告，這可能導致機構難以看清其安全狀態的全貌、快速響應或確保其數據值得信賴。我們認為解決方法是將所有安全數據統一到一個具有清晰標準及一致規則的集中化的數據主幹中。我們的安全數據中心透過五個方面的統一來實現這一點：採集、存儲、授權、治理及共享。其將不一致的數據流進行標準化處理，包括日誌、事件及資產記錄，避免重複採集以節省空間。其以標準化格式翻譯及存儲所有內容，並配有清晰的保留規則，以便團隊進行更深入的分析，不會受到數據孤島的阻礙。其集中管理身份及權限，使所有連接的系統都使用相同的安全訪問方法。其治理安全數據的全生命週期，包括元數據、數據質量檢查、敏感數據分類及合規規則的執行。我們的數據安全中心可向其他平台提供高質量的數據，並為主動威脅狩獵、模式識別及自動化事件編排建立可靠的基礎。

數據資產管理平台

許多機構無法有效管理其擁有的所有系統及設備。靜態記錄與實際環境之間經常存在差異，職責不明確，團隊難以滿足報告要求。我們認為解決此問題的最佳方法是為每項資產建立單一、準確的事實來源及數碼主分類賬，並透過自動發現實現其動態更新。我們的資產管理平台透過同時整合多種發現方法來解決此問題，包括在

業 務

資產指紋支持下的探針、API連接、流量檢查、登錄數據及代理採集。其管理數據資產，並讓團隊透過視覺化編輯器創建自定義資產模型，這有助於平台適應不同行業。該平台的運行形成一個資產責任生命週期管理的閉環，確保職責始終明確。資產能夠按三層進行組織，涵蓋信息系統、硬件及組件。該平台或亦能夠支持頻繁的合規任務，如報告、等級保護檢查、關鍵信息基礎設施備案及專項檢查。其或亦能夠透過支持漏洞管理、事件響應及訪問控制來強化日常安全，實現「一次治理，多次支持」的後續安全任務模式。

數據安全態勢感知管理平台

由於信息來源廣泛且威脅不斷演變，機構可能難以實時監測數據風險。根據弗若斯特沙利文報告，用戶需要一種能夠快速檢測「危險信號」並在問題演變成災難前作出響應的方法。我們認為，正確的方法是將實時監測與人工智能驅動的行為分析相結合，以發現顯性及潛在漏洞。為此，我們的數據安全態勢感知管理平台利用內置的對抗性攻擊模型庫及用戶及實體行為分析來識別可疑行為，例如不當訪問或潛在的數據洩漏。該平台可能包含簡單的拖放式可視界面，使機構能夠設計實時顯示其風險水平的儀表板。通過結合數據建模、異常檢測及人工智能驅動的安全輔助系統，我們的數據安全態勢感知管理平台可主動協助團隊在安全事故發生前、發生期間及發生後管理整個風險週期。

數據安全管理平台

機構亦可能難以持續掌握其數據盤點、數據駐留地及數據譜系的可見性。若不清楚，保護數據或捕捉風險行為將可能變得困難。我們認為，最佳方法是將數據分類制度化，跟蹤其流動情況，並在人工智能的協助下進行持續的風險檢查。如上文案例研究所示，我們的數據安全管理平台識別數據庫、文件、系統及活動接口中的敏感數據。其利用向量化分類和自動化規則以高精確度對信息進行歸類。該平台通過分析登錄環境、時間、頻率、用戶行為及流向模式等因素，監測數據在機構內的流動情況並標記異常活動。其管理數據資源，分配生命週期標籤，並創建多維視圖以顯示數據與用戶隨時間的互動情況。其發現靜態資產及動態系統(包括API)，並能合併相似接口以保持資產記錄整潔。這些功能能夠共同協助機構了解其數據環境，識別高價值數據並採取適當的控制措施。

數據共享交換平台

根據弗若斯特沙利文報告，當敏感信息未得到妥善控制時，在機構內部或外部共享文件可能存在風險。機構可能缺乏一種安全的方式在保持加密及可追蹤性的同時交換文件。我們認為，文件共享應在不影響用戶生產力的情況下，同時保護機密性及問責制。我們的數據共享交換平台通過雲盤式的協作空間支持安全的文件協作，用於上傳、下載及組織文件。其掃描並識別共享文件中的敏感內容，然後利用人工智能驅動的分析對其進行相應分類。所有文件在存儲及傳輸過程中均需經過加密，且

業 務

每次下載均使用一次性密鑰，確保僅特定及預期用戶可以讀取。該平台還添加顯性及影性水印，若發生數據洩漏，可追蹤至確切人員、時間及通訊渠道。每項操作均需有記錄，且文件可通過完整的審計記錄進行端到端追蹤。我們的數據共享交換平台為機構提供了可靠的數據共享方式，且不會失去監管。

數據安全標準化軟件

機構可能會因缺乏對數據存儲、流動及訪問模式的可見性，而在保護其重要資料方面面臨困難。傳統工具依賴靜態、基於規則的邏輯，往往無法檢測到新威脅，並因過多的誤報而令團隊不堪重負。我們的數據安全軟件利用人工智能監控數據從收集到處置的整個生命週期。人工智能能夠有助於快速識別敏感信息、隨系統變化更新標籤、針對不同情況選擇合適的保護措施、減少冗餘的警告，並從實際使用中學習，使系統得以持續完善。我們的數據安全軟件套件夠匯集用於識別敏感信息、隱藏或標記信息、防止洩漏、審計數據庫、監測數據流動、檢查系統及保護應用程序接口安全的工具。這些工具共同為機構提供了清晰且智能的數據保護方法。

於2023年、2024年及2025年，我們數據安全標準化軟件產生的收入分別為人民幣62.2百萬元、人民幣46.3百萬元及人民幣31.5百萬元，分別佔我們總收入的12.0%、7.0%及4.5%。

我們向客戶提供的關鍵標準化數據安全軟件包括：

名稱	解決的痛點	解決該等痛點的方式
觀安觀智敏感數據發現系統	儲存在不同儲存裝置上的敏感數據可能難以識別，且會隨系統變化而過時。	快速準確地在多種類型的存儲中搜索敏感信息。利用內置預定義分類模版標記數據、檢查存儲是否符合內部及監管政策並監控合規情況、識別未被記錄的數據庫，並構建機構於安全及管治方面可信的實時數據目錄。
觀安觀智數據庫安全審計系統	在複雜的數據庫環境中難以偵測惡意或未經授權的活動，尤其是當信息跨地域存儲或通過加密鏈接發送時。	實時監測數據庫活動並透過機器學習建立行為基線。其提供對名稱、表格、用戶及操作的細緻可見性；利用輕量化工具捕獲訪問情況；顯示實時會話；指出異常工具、地址、用戶賬戶及指令；並支持快速搜索以便團隊迅速調查並應對安全事件。

業 務

名稱	解決的痛點	解決該等痛點的方式
數據監測洞察系統	信息在客戶端、應用程序、數據庫及接口之間流動造成盲點，難以識別風險或由源頭至目的地追蹤安全事件。	提供數據流的全面可視化。從流量檢查中發現資產；端到端監控敏感訪問；利用詳細指標過濾噪音。通過關聯相關風險並提供會話回放功能，該系統重構任何活動的完整路徑；並為日常安全營運及事件響應生成清晰報告。
靜態數據脫敏系統	開發人員、測試人員及合作夥伴需要真實的數據集以進行有效協作，但必須在不損害數據利用或系統功能的情況下遮蔽敏感屬性。	創建安全、高保真的數據副本，在遮蔽敏感屬性的同時，保留原有結構及業務邏輯。支持廣泛的數據來源；檢測常見敏感模式；保持表間關聯完整；在執行前進行合規性檢查；提供多樣化脫敏方法；並提供帶有告警、審批及日誌的全面跟蹤。
全智脫敏系統	單一類型的脫敏無法滿足所有需求。靜態脫敏缺乏用於互動式使用的靈活性，而實時脫敏在處理大規模批次或數據共享時往往效率低下。	結合靜態及實時脫敏，並根據不同情況自動選擇最佳方法。支持多種數據源及敏感信息類型；提供基於角色的訪問控制網關；利用可重用規則保護實時響應；允許應用程序請求精確脫敏；並確保遵守隱私法規而不影響業務連續性。
數據安全檢查工具箱	安全及合規檢查速度慢、不一致且難以比較，導致問題補救不及時。	提供從資料收集到項目規劃、執行、審查及報告的標準化工作流。包括漏洞檢測、接口檢查、日誌分析、檢測安全弱點及識別敏感數據的工具。支持自定義模板並包含知識庫，使團隊在不干擾關鍵業務運營的情況下實現「即查即走」。
數據洩漏防護系統	敏感信息可能通過各種形式洩露，包括文本、圖像及文檔，而傳統的過濾機制因無法理解語境而產生過多誤報令團隊不堪重負。	利用文本匹配、模式識別、人工智能及語言理解來識別真實風險。分析文本、圖像及文檔；自動標記數據；追蹤數據血統；理解語境以減少冗餘警報，並通過持續學習，從而持續優化檢測邏輯並逐步提高決策準確性。

業 務

名稱	解決的痛點	解決該等痛點的方式
水印溯源系統	當數據洩漏發生時，難以識別相關責任人或渠道。	對數據資產添加顯性及隱性水印。將每個唯一的水印與特定的元數據(包括用戶身份、時間戳和訪問渠道)相關聯，以確保端到端的責任追溯。對於結構化數據，其利用啟發式技術，例如添加偽造的行或列作為可溯源線索；並提供一鍵溯源以顯示數據使用人及時間。

數據安全專業服務

根據弗若斯特沙利文報告，機構面臨的行業痛點之一是其無法設計全面的數據安全框架、無法將法律及標準轉化為日常營運實務，以及無法長期維持安全項目的運作。隨著數據安全監管迅速演變且日益嚴格，機構往往感到壓力，因為其現有流程、員工能力及工作流與監管預期並不匹配。通過我們的數據安全服務，我們希望引導機構走完一個生命週期的旅程：從設計頂層規則，到評估日常營運中的風險，再到運行智能、可衡量且可持續的營運體系。我們通過提供諮詢、評估及運維服務來處理這些問題，將我們的專家經驗與人工智能及大模型技術相結合，這確保法律要求、行業標準及內部政策轉化為可操作、可衡量且自動化的營運工作流。

於2023年、2024年及2025年，我們數據安全專業服務產生的收入分別為73.1百萬元、人民幣108.2百萬元及人民幣117.2百萬元，分別佔我們總收入的14.2%、16.4%及16.5%。

我們向客戶提供的關鍵數據安全服務包括：

數據安全諮詢服務

許多機構對數據安全缺乏清晰的藍圖。各部門於收集、存儲、傳輸、使用及銷毀數據上零散的做法，往往會導致控制措施存在差距且不一致。我們認為，正確的方法是了解敏感數據的全生命週期，並設計符合機構實際業務情況的長期計劃。因此，我們提供數據安全諮詢服務，通過訪談機構內所有涉及數據處理的部門，研究敏感數據的收集、存儲、傳輸、使用及處置方式，並識別技術、流程、管理及人員方面的風險，以此解決上述挑戰。我們將對現狀進行多維度評估，涵蓋數據全生命週期各個階段的風險，並識別技術、程序、管理及人員配置方面的問題。隨後，我們設計機構整體的治理藍圖，規劃建設數據安全體系的三至五年路線圖，並為每個階段提供實用的分步指導。我們亦可根據具體業務場景定制解決方案。

業 務

數據安全評估服務

機構可能難以識別及量化由各業務領域風險引發的安全事件的潛在影響。許多機構甚至不知道如何根據《數據安全法》或《個人信息保護法》等法律來衡量合規性。我們認為，最佳方法是使用科學方法、法律標準及行業框架來評估風險，並提供清晰、可操作的補救措施。我們的數據安全評估服務通過使用基於法律、標準及行業規則構建的全面評估矩陣來識別潛在威脅。該服務關注行業特定需求，量化威脅的潛在損害並評估所有業務場景下的風險。其生成切實可行的補救方案，供機構實施，協助彼等滿足合規要求並加強整體保護。

數據安全營運

即便機構制定了規則並進行了評估，彼等往往也無法維持長期運作效能。監測流量、響應事故、管理告警及檢查合規性等日常任務分散且依賴人工。我們認為，最佳方法是構建一個跟蹤數據全生命週期的集成化、自動化、平台化且智能化的運維體系。我們的數據安全運維服務協助機構設計統一的合規運維框架，利用數據安全管理平台管理歷史數據並維持標準化營運工作流。其規劃對敏感數據流動的持續監察，為關鍵環節制定保護策略，並使風險控制與合規規則保持一致。其構建風險監測及事故響應流程，設置指標以追蹤數據流風險，繪製安全用例圖，並制定應急預案。其亦通過與策略、風險及事件掛鉤建立基於KPI的審計及優化方法。

網絡安全解決方案

現今的網絡安全團隊可能面臨著不斷擴大的攻擊面、有限的可視化、繁雜的工具碎片化以及緩慢的人工響應週期，上述問題均可能延遲機構應對日益複雜威脅的響應週期。我們的理念核心在於將安全運維從被動反應態勢轉變為情報主導策略，使機構能夠以更快的速度、更高的準確度及更強的自主性來檢測、預測及化解風險。我們認為，有效的網絡安全需要深度防禦架構，並以人工智能驅動的自動化作為補充，以加快威脅發現、加強決策並在大規模範圍內統籌響應。我們的解決方案將自研產品、全面分析及標準化服務統合成一個具凝聚力的營運框架，使機構能夠始終遠離不斷演變的威脅形勢。

我們的網絡安全能力使我們的客戶整合自動化資產繪製及外部威脅情報，以發現暴露的系統、減少盲點並預判可能的攻擊路徑。我們能通過零信任架構、網頁應用程式防火牆及終端檢測與響應解決方案加強主動防禦，提供強大的前線保護。利用全流量威脅檢測及人工智能賦能的威脅狩獵，我們精準識別安全風險，並加速發現關鍵的異常情況。為迅速遏制威脅並最大程度減少對業務運行的干擾，我們能納入誘捕技術、違反及攻擊模擬以及安全統籌、自動化及響應(「**SOAR**」)，以實現響應自動化並協調各安全工具間的操作。

業 務

於2023年、2024年及2025年，我們網絡安全解決方案產生的收益分別為254.1百萬元、328.4百萬元及339.7百萬元，分別佔我們總收益的49.3%、49.8%及48.0%。

以下案例研究說明我們向客戶提供的典型網絡安全項目：

案例研究：為客戶A提供的網絡安全平台項目

項目背景

我們為中國最大電信網絡運營商之一的客戶A開發並部署網絡安全平台，旨在建立覆蓋全網、統一化的網絡安全防禦、監控及應急響應能力。該項目針對客戶A全國範圍雲網絡、IT系統及關鍵電信基礎設施的規模與複雜性而設計，同時優化集團、省級及部門層級之間的協調機制。

該網絡安全平台定位為核心安全營運樞紐，為整個組織提供集中分析、聯動事件響應及持續安全營運支持。

項目範圍及覆蓋內容

該網絡安全平台實現中央主管部門、集團層級、省級營運公司的三級協調，支持24小時安全事件監控、設有明確上報機制的分級事件響應，並可於全網範圍內集中處理惡意IP地址、域名及網址。

網絡安全平台整合約24類業務系統的安全數據，包括互聯網存取日誌集中平台、網站監控系統、互聯網數據中心及互聯網服務提供商系統，以及惡意軟件相關系統。平台處理七大類安全數據，包括35個子類別及近200種不同數據類型，例如安全警報日誌、網絡行為數據、文件類數據、威脅情報、基礎設施元數據及指令執行記錄等，整體數據規模達到拍字節級。

在安全營運中心環境中，網絡安全平台支持主機安全監控、事件調查及自動化響應，平均每日處理數億條安全警報，透過模型驅動檢測，每日可識別數千宗安全事件。平台部署後，平均事件處理時間由約8.0小時縮短至5.9小時，緊急事件一般可透過全網閉環處置，於一小時內完成解決。

業 務

下圖展示該網絡安全平台的界面：



人工智能驅動的威脅檢測及智能營運

該網絡安全平台結合客戶A現有技術架構，整合即時分析、離線分析及基於圖形的關聯引擎。該等引擎由基於人工智能的安全模型提供支持，該模型透過歷史警報、事件及日誌數據訓練而成。系統可關聯偵察、漏洞利用、權限提升、數據外洩等不同階段的攻擊訊號，實現結構化攻擊鏈分析及可追溯的調查報告。

此外，網絡安全平台依據威脅情報及已知攻擊者行為模式開展預測分析，評估潛在後續行動並發出預警。此功能協助團隊由被動應對轉為前瞻式安全營運，同時減輕安全分析人員的人工分類篩選工作量。

戰略影響

我們的網絡安全項目協助客戶A由傳統被動防禦，轉型為情報導向、主動且更加自動化的安全防禦，強化跨機構層級的協作機制，全面提升雲端網絡、IT系統及電信基礎設施的安全治理水準。我們的網絡安全平台作為連接數據、系統、人員及流程的核心營運底座，助力客戶A實現監管合規、有效防禦及持續優化安全能力的目標。

業 務

網絡安全平台

機構可能依賴於異構網絡、雲環境及分佈式設備，於整個數字資產範圍內實現全面可視性將成為一項重大挑戰。根據弗若斯特沙利文報告，前述機構可能難以全面查看整個環境中發生的情況、識別真實威脅並在事件發生時迅速作出反應，特別是於使用大量互不連通的網絡安全工具時。安全團隊往往每天面臨大量告警，其中許多最終被證明並不重要。這減慢了其工作速度，並使其難以識別真實風險。我們認為，解決該等問題的最佳方法為採用一個綜合安全生態系統，該系統能夠統一環境監控、智能篩選告警，並自動執行常規工作流，以提升營運效能。我們的網絡安全平台旨在解決這一問題，旨在協助機構從人工、被動應對的營運模式，轉向以情報為主導的、主動的保護。我們的網絡安全平台乃針對客戶的需求而量身定製，整合了三個層面的安全分析：細查文件及代碼的微觀分析、監控用戶及潛在攻擊者行為模式的中觀分析，以及最大程度重構跨階段攻擊路徑的多源數據匯總。此外，該等平台利用警報降噪技術協助安全團隊專注於高價值威脅，突顯重大威脅，並指引團隊進行調查及修復工作。我們的網絡安全平台有助於機構提前應對新型威脅，並維持強大且靈活的防禦。

於2023年、2024年及2025年，我們網絡安全平台產生的收入分別為人民幣45.5百萬元、人民幣88.2百萬元及人民幣90.6百萬元，分別佔我們總收入的8.8%、13.4%及12.8%。

我們向客戶提供的關鍵網絡安全平台包括：

漏洞管理平台

機構缺乏對其系統性漏洞全面的可見性。根據弗若斯特沙利文報告，分散的監控往往會導致關鍵風險敞口被忽視、資源因誤報而浪費，以及難以驗證已完成修復措施的有效性。我們的方法為於統一的环境中管理整個漏洞生命週期，其特點為高精度檢測和自動化編排。我們的漏洞管理平台通過掃描系統、驗證真實問題、追蹤補救進度以確保修復措施已成功實施來實現這一點。其收集來自服務器、安全設備、數據庫等的信息，為團隊提供所有資產及潛在風險的統一視圖。該平台使用多種掃描方法來發現網頁應用程式及主機系統中的漏洞。其亦就所有安全活動維持穩健的審計追蹤記錄，使信息可追蹤並符合監管要求。我們的漏洞管理平台有助於機構減少攻擊面、履行報告義務並維持健康的安全態勢。

觀安觀鑑安全態勢與日誌分析系統

機構會在分散的系統中產生大量安全數據，這通常會導致數據孤島，從而妨礙對整體環境的全面可視性。我們認為，最有效的解決方案是將分散的安全數據整合至一個集中式情報中心，利用人工智能進行分析，並以團隊能迅速反應的方式將其可視化。我們的觀安觀鑑安全態勢與日誌分析系統通過收集日誌，對其進行標準化處理來解決該等挑戰，並應用行為分析、關聯建模及機器學習等高級檢測方法來應

業 務

對這些挑戰。該系統通過清晰且可定制的儀表板展示結果，以突出風險水平、可疑活動或重要系統事件。該系統涵蓋從檢測潛在威脅到調查並採取行動的完整工作流。通過使用SOAR，系統可攔截有害流量、隔離風險賬戶或執行預定義劇本，而無需人工干預。

網絡安全標準化軟件

在日益複雜的敵對策略及不斷增加的網絡複雜性雙重壓力的推動下，機構可能意識到要保護其數字系統安全並非易事。根據弗若斯特沙利文報告，傳統安全工具通常依賴靜態、基於規則的特徵及人工干預，可能不足以應對新型或快速變化的威脅。該等工具還會產生大量錯誤告警，使安全團隊難以專注於關鍵風險。我們的網絡安全軟件組合旨在通過能夠快速適配、分析行為及響應的智能化水平更高的工具來解決這些挑戰。我們會利用人工智能來理解系統的正常運行方式、識別異常操作、檢測新型威脅並連接不同來源的信息。我們的網絡安全軟件可能有助於機構發現漏洞、攔截攻擊、減少誤報並簡化決策。通過這種方法，我們協助客戶構建更強大、更主動的安全運維。

於2023年、2024年及2025年，我們網絡安全標準化軟件產生的收入分別為人民幣25.2百萬元、人民幣44.3百萬元及人民幣36.9百萬元，分別佔我們總收入的4.9%、6.7%及5.2%。

我們向客戶提供的關鍵數據安全軟件包括：

名稱	解決的痛點	解決該等痛點的方式
WEB應用安全防護系統	網站面臨持續的自動化攻擊，例如旨在探查潛在漏洞的殭屍網絡。基於規則的傳統工具可能無法檢測到這些由機器驅動的不斷演化的威脅。	通過對每個請求添加動態檢查來使用主動防禦，以核實真實性；通過機器學習識別可疑行為；分析請求中的語義及語境；通過對敏感輸入內容進行擾亂來防止數據洩漏；攔截自動化工具；並使用人工智能模型檢測並阻止高風險異常情況。
攻擊模擬安全驗證系統	安全產品已經安裝但未在真實條件下進行測試，導致機構僅有「虛假的安全感」及未經驗證的防禦能力。	通過在多元網絡基礎設施及系統環境中模擬真實攻擊；自動識別資產；提供多種測試場景；支持非破壞性模擬及受控的真實攻擊技術；評估安全工具對新型攻擊變體的檢測及響應能力；並提供報告，以便對已識別漏洞進行有針對性的加固。

業 務

名稱	解決的痛點	解決該等痛點的方式
威脅誘捕系統	老練的攻擊者可能部署先進的技術，以於網絡內長期保持不被發現。	創建真實的虛假系統及服務以轉移及誘捕攻擊者；檢測與這些誘餌的任何互動；捕捉及分析攻擊者於誘餌環境中的操作行為，以獲取攻擊意圖以及戰術技術、程序及模式(TTP)，為事件分析提供高置信度的預警證據；並在需要時執行安全的反制行動。
第二代防火牆系統	舊款防火牆缺乏規管現代應用程序或中和高級威脅所需的可視性。	詳細檢查流量、識別用戶及應用程序、攔截有害內容、限制不良網站、支持安全連接、平衡網絡負載並實時更新威脅情報。
入侵防禦系統	機構難以消除諸如SQL注入、偵查掃描、惡意軟件或竊取憑證等多向量攻擊。	實時檢測多種類型的攻擊；與其他安全工具集成以更快中和威脅；識別用戶及應用程序；為關鍵服務管理帶寬；並通過多個渠道發送告警。
綜合日誌分析系統	分散於不同環境中的日誌存儲使得調查工作更複雜，並妨礙滿足嚴格監管合規要求的能力。	從多個來源匯總日誌；分析其異常模式；支持監管合規審計；提供儀表板及報告；並發佈實時告警以實現快速事件響應。
安全運維管理系統	對特權賬戶及管理員活動監督不足造成意外或蓄意濫用。	管理用戶身份、權限及會話；記錄所有關鍵操作；支持多重身份驗證；並使用會話回放以進行審計及調查。
網絡流量分析系統	複雜的攻擊透過混入大規模網絡流量中規避檢測。	收集並分析網絡流量；識別可疑文件及行為；支持沙箱測試；檢測隱藏的通信渠道；重構文件及會話以便調查；並提供詳細的可搜索記錄以便快速調查。
網站雲監測平台	手動監控大型網站組合以檢查是否存在篡改、非法內容或服務中斷，既不切實際，亦容易出錯。	自動大規模監測網站；檢測異常變化；識別有害或未經授權的鏈接；發送實時告警；並生成定期風險評估報告。

業 務

名稱	解決的痛點	解決該等痛點的方式
安全垂域智能體系統	安全團隊花費大量時間分析告警及準備報告。	使用人工智能賦能的「智能體助手」，其可以通過可視化工作流編輯器調查告警、遏制惡意活動、生成報告並自動執行常規工作流。
智能代碼審計系統	軟件代碼中的安全漏洞往往發現較晚，增加了補救成本及業務風險。	使用人工智能掃描軟件源代碼、識別常見漏洞、精準提供解釋、提供建議的修復方案、支持多種編程語言並賦能團隊在軟件開發週期早期加強安全性。

網絡安全專業服務

當今機構在構建及運作完整的網絡安全體系方面面臨重大挑戰並不罕見。許多機構正面臨營運分散、流程高度依賴人工以及關鍵網絡安全技能短缺等問題，該等因素阻礙其預先化解攻擊並維持高水平防禦的能力。根據弗若斯特沙利文報告，隨著攻擊手段日益升級且監管框架日益嚴格，現有的內部能力往往難以達到所需的保護標準。我們的目的是利用我們的網絡安全服務引導機構完成完整的安全提升旅程：從規劃開始，貫穿測試及日常運作，並延伸至應急響應。我們將人才智庫與人工智能相結合，將複雜的要求轉化為切實可行、可衡量且可持續的安全行動，以確保長期營運韌性。

於往績記錄期間，我們網絡安全專業服務產生的收益分別為人民幣183.4百萬元、人民幣195.9百萬元及人民幣212.2百萬元，分別佔我們總收益的35.6%、29.7%及30.0%。

我們向客戶提供的關鍵網絡安全服務包括：

安全諮詢服務

該服務有助機構識別業務場景內的安全基線差距及規劃符合監管要求及支持業務發展的安全架構系統。各部門之間往往單獨制定安全控制措施，形成信息孤島，導致防護力度不一，並於整個環境中留下缺口。我們認為，正確的前進方向是設計一個與機構業務運營、監管責任及數字化轉型帶來的風險相匹配的協調安全架構。我們的安全諮詢服務通過對治理結構、組織角色、安全政策、技術保障及安全運維進行全面審查來解決此問題。我們會繪製責任歸屬圖，評估項目間的依賴關係，並提出分階段的實施路線圖。我們亦可能為雲環境、安全軟件開發流程及安全運維設計專題規劃，協助機構構建一個全面、協調且適配的體系。

業 務

安全運維服務

機構可能會因人手限制、不具備全天候監測能力，或無法關聯不同系統中的警報以重建完整的攻擊鏈或作出果斷回應而無法維持有效的日常安全運維。我們認為，最佳方法乃透過綜合安全營運平台，結合專家團隊的持續監控及分析，以提升安全事件偵測及響應的時效性。我們的安全運維服務通過將集中式安全運維平台與提供全天候監測、威脅分析及事件響應的遠程或現場團隊相結合來解決此問題。該平台收集告警、管理資產及漏洞，並支持工作流跟蹤。我們的專家根據機構需求設計定制的響應流程、持續性措施、報告流及服務水平目標。我們的安全運維服務形成一個協助涵蓋檢測、調查、響應及改進的閉環，幫助機構通過可預測且可衡量的結果強化其安全就緒度。

安全測試與評估服務

當資產、風險及威脅涵蓋實體基礎設施、網絡、系統、應用程序及數據存儲時，一些機構可能發現識別其多層系統中的漏洞十分困難。我們認為，有效的風險管理始於結構化且科學的評估，對物理、網絡、系統、應用程序及數據層面的風險進行評價。我們的滲透測試服務本質上是對網絡攻擊的模擬，藉此我們模擬潛在攻擊者的戰術、技術及程序，以對目標系統進行深度安全路徑檢測。測試過程嚴格遵守業務連續性原則，並在修復後提供閉環複測，以確保實質性消除安全漏洞。透過識別風險、提供針對性修復建議並執行複測驗證，該服務協助客戶建立閉環風險管理機制。這種結構化評估可以協助機構了解事故的潛在影響，並採取措施增強其系統韌性。

應急響應及重大活動保障服務

當突發網絡安全事故發生時，機構可能難以迅速作出反應、遏制損失或恢復營運。重大活動亦需要加強保護，以確保系統性能持續穩定。我們認為，最佳方法是提供由經驗豐富的專家提供支持的快速響應服務，彼等能夠遏制事故、消除威脅並協助安全恢復系統。我們的應急響應及重大活動保障服務通過為入侵事件、惡意代碼及勒索軟件提供即時支持來解決此問題。在我們網絡安全專家的支持下，該服務能夠快速遏制活躍威脅、徹底清除惡意元素、安全恢復受影響的系統，並進行詳細的取證分析以查明攻擊源頭。針對重大活動，我們可能提供現場專家、高頻率檢查及加強監測，以確保系統的安全性及穩定性。我們的應急響應及重大活動保障服務確保企業在突發事故及重大活動期間均能維持業務穩定且風險受控。

業 務

其他解決方案

除數據安全及網絡安全解決方案外，我們亦為客戶量身定製整合解決方案。我們通常透過將自有及第三方硬件、軟件及服務集成至一個統一、多層次及動態協同的安全框架中，以滿足客戶於數據安全治理、威脅防護、風險管理及監管合規等方面的全面需求。我們整合方案的核心價值主張在於打破單一安全產品的營運孤島，透過技術集成、服務融合及生態協作，實現安全能力的全局優化及智能聯動。

於2023年、2024年及2025年，我們其他解決方案產生的收入分別為人民幣42.5百萬元、人民幣48.9百萬元及人民幣70.8百萬元，分別佔我們總收入的8.2%、7.4%及10.0%。

智算項目

於2024年，我們調整戰略重心，並拓展至人工智能及算力領域。為此，我們從客戶G處獲取中國西南地區的一個國家級項目（「智算項目」），該項目佔我們2025年來自其他解決方案收入的大部分。「智算項目」建成後，將成為中國國家集成算力網絡的關鍵節點，實現計算資源的跨區域調配，推動人工智能訓練、大數據分析和雲應用的低碳、高效發展。

根據項目協議，我們主要負責(i)採購及整合軟件、硬件及服務，以建立一個涵蓋雲算力平台安全、數據安全及調度安全的綜合安全系統；(ii)提升客戶G的雲算力平台（「雲算力平台」）的安全防護能力，為其調度的跨區域及大規模算力資源提供更有效的保護；及(iii)為雲算力平台提供安全相關的技術支持服務，並執行安全系統的監控及維護服務。該項目的期限為兩年，並將分三期交付。各期項目協議(i)界定我們具體的安裝、調試及試運營任務；及(ii)訂明我們須達成的客戶開發目標。

由於智算項目是我們首次涉足人工智能及算力領域，故於2024年12月31日，尚未達成第一期客戶開發目標。儘管如此，鑒於雲平台近期上線及市場需求，我們與客戶重新磋商，將剩餘客戶開發目標的截止日期推遲至2027年12月31日。截至最後實際可行日期，我們已與一名客戶就其於雲算力平台訂閱算力簽訂意向書，該意向書的合約價值將使我們能夠於2027年年末前達成客戶第二及第三期開發目標。

研發

研發是我們策略及未來增長的重心。研發投入承諾使我們能夠滿足客戶需求，並提供差異化且前沿的解決方案。截至2025年12月31日，我們的研發團隊由186名成員組成，分別駐於我們位於上海、北京、武漢、合肥、鄭州及成都的辦事處。於2023年、2024年及2025年，我們的研發開支分別為人民幣119.9百萬元、人民幣100.1百萬元及人民幣100.1百萬元。

業 務

元及人民幣101.9百萬元，分別佔我們總收入的23.2%、15.2%及14.4%，彰顯了我們致力於持續改進及技術進步。請參閱「財務資料—經營業績—研發開支」。截至2025年12月31日，我們已獲得145項獲授權專利，包括141項發明專利，且獲得202項軟件著作權，不斷強化知識產權壁壘，為前沿技術轉化提供堅實基礎。

與依賴現成解決方案的競爭對手不同，我們對大數據及人工智能的早期投資已實現迭代創新及自適應模型，在不同場景中均衡通用性及準確度，使我們處於技術進步的前沿。

我們的研發戰略

我們的研發戰略將聚焦核心技術要求的基礎研究與強調功能性及定製化的產品線研發相結合。產品經理與我們的客戶緊密合作，收集需求並評估可行性；而我們的技術團隊則憑藉深厚的學術和行業經驗，推動大數據、人工智能及安全技術領域的創新發展。我們的核心技術均由內部自主研發，這確保了對關鍵創新的獨立性及掌控力。

於往績記錄期間，我們的研發工作專注於持續升級核心數據安全及網絡安全平台，以應對不斷變化的威脅形勢及客戶需求，尤其著重提升偵測準確性、營運效率及自動化響應能力。例如，我們以人工智能驅動的數據分類技術升級了數據安全管理平台，並以人工智能輔助的威脅分析及SOAR驅動的自動化響應技術升級了安全信息及事件管理系統。這些創新共同使我們的客戶能夠更有效地監控、調查及應對複雜的網絡威脅，同時精簡其安全營運流程。

我們的技術

我們的數據安全解決方案利用一套先進技術，旨在確保端到端可追溯性，使機構能夠在異構環境中，對信息在產生、存取、傳輸及歸檔過程中的整個數據生命週期進行管治，主要包括：

- 基於信息編碼技術的數據暗水印：以不改變數據原始內容的方式，在數據內部嵌入標識資訊，即使數據大部分內容遺失，仍可有效追溯數據洩漏源頭；
- 防隱私洩漏的可逆的數據形態保持技術：對敏感資訊實施可逆性轉換處置，既能實現敏感資訊的有效防護，亦可完整保留其可供業務流程正常使用的數據結構；
- 基於熒光標記的數據應用測繪技術：透過在敏感數據流轉的多個節點進行標記，協助我們精確重構敏感數據在各系統間的傳輸路徑；

業 務

- 全自動高性能發現訪問敏感數據的數據庫審計引擎：透過重構網絡流量中的數據庫操作行為，實現敏感資訊的精準識別，且避免對數據庫本身造成任何干擾；及
- 基於多維度評價系統的敏感數據精準發現及分類引擎：透過深度分析文件的格式、屬性及語義內涵，精準判斷文件是否包含敏感內容。

該等技術可協助機構全程掌握資訊流向，及時識別敏感數據被非預期存取的各類情形。

我們的網絡安全解決方案利用的技術旨在實現多維度威脅檢測、重建端到端攻擊路徑，並促進高速取證調查的技術，主要包括：

- 基於運維業務風險告警分析歸併引擎：分析海量告警數據，挖掘其中的統計關聯關係，精準判斷多起獨立事件是否源於同一潛在問題；
- 基於信息論的告警關聯引擎：將紛雜的告警數據梳理歸納為可識別的規律模式，協助運維人員快速洞察可能的攻擊手段；
- 用戶風險行為智能洞察引擎：對用戶操作序列進行分析，並與歷史行為模式進行對比研判，及時識別可能存在威脅的異常行為；
- 基於訪問特徵的腳本木馬檢測技術：運用機器學習，精準識別具有惡意文件特徵的異常存取模式；及
- 下一代自動化機器行為動態防禦技術：對自動化請求的行為進行驗證，判斷其是否符合合法操作規範，有效防範未經授權的自動化存取行為。

該等技術可協助機構清晰掌握網絡威脅的演變過程，當網絡行為偏離預期模式時，為機構提供更具體系化的應對處置方案。

外包研發

於往績記錄期間，我們聘用第三方開發商負責部分基本功能的編碼、系統設計及模組開發。於2023年、2024年及2025年，我們的外包研發開支分別為人民幣21.6百萬元、人民幣23.9百萬元及人民幣17.1百萬元，主要用於定製開發服務。

此戰略方針使我們能夠藉助外部專業知識及現成解決方案處理非核心或專業組件，避免重複研發，進而更高效地將內部研發資源分配至能夠提升我們競爭優勢的高價值核心技術發展項目。

業 務

知識產權

憑借我們對研發和先進技術的追求，我們不斷增強知識產權組合，我們通過結合版權、商標、專利，以及與我們的僱員及客戶訂立保密協議來保護知識產權。截至2025年12月31日，我們已獲授145項授權專利，包括141項發明專利，獲得202項軟件著作權。此外，截至最後實際可行日期，我們在中國擁有95項註冊商標及兩個域名。請參閱「附錄六—B.有關我們業務的進一步資料—2.我們的知識產權」。

我們一般要求我們的員工簽訂保密協議，確認其承認其代我們產生的發明、商業秘密、開發成果及其他工藝屬於我們的財產，並將其可能對該等作品主張的任何所有權轉讓予我們。請參閱「風險因素—與我們的業務及行業有關的風險—我們可能面臨重大的知識產權侵權指控(包括未經授權使用軟件)，這可能導致重大責任並對我們的業務及營運造成干擾。」

董事確認，於往績記錄期間及直至最後實際可行日期，我們並不知悉任何(i)我們侵犯任何第三方擁有的知識產權；或(ii)任何第三方侵犯我們擁有的任何知識產權的行為。此外，截至最後實際可行日期，我們並無捲入任何與被我們模仿或針對我們侵犯知識產權的重大索賠(無論是威脅性的還是未決的)相關的任何訴訟或法律程序，且該等訴訟或法律程序對我們的業務造成重大不利影響。

獎項、認可及認證

我們在網絡安全競賽中屢獲殊榮，且為重大國際活動提供支持，彰顯我們在提供先進安全解決方案方面的實力。我們亦持有若干中國信息安全行業的最高級別認證。例如，我們已獲得中國網絡安全審查技術與認證中心授予的信息安全服務資質，在安全軟件開發、事件響應、安全運維、系統集成、風險評估等方面達到一級標準。於全國在所有五個類別中均獲得一級資質的七家公司中，我們是其中之一。我們亦持有中國信息安全測評中心在風險評估、安全工程、安全開發、大數據安全評級等方面的認證，以及中國通信企業協會在安全設計與集成、風險評估、應急響應、安全培訓等方面的認證。此外，我們是首批獲得由中國軟件評測中心及中國計算機行業協會數據安全專業委員會聯合頒發的軟件開發頂級認證的公司之一。

我們持有ISO認證組合，包括IT服務管理ISO/IEC 20000-1:2018、信息安全管理ISO/IEC 27001:2013、質量管理ISO 9001:2015、環境管理ISO 14001:2015及職業健康與安全管理ISO 45001:2018。

業 務

我們獲得全國人工智能創新應用大賽一等獎及「網鼎杯」網絡安全大賽最高榮譽等國家級和行業獎項。我們的成就亦包括吳文俊人工智能獎、「數信杯」數據安全大賽金獎，並獲認可為數據要素價值創新示範基地。我們獲工業和信息化部評為優秀技術支持單位，並因在網絡安全信息報告方面的卓越表現而受到認可。

下表載列我們於往績記錄期間獲得的其他重要獎項及榮譽：

頒發年份	獎項或表彰名稱	簽發機構
2025年	2025 數字中國創新大賽數字安全賽道數據安全產業優秀案例評比賽優勝獎—基於自然語言處理與光學字符識別算法的數據識別創新應用	福建省通信管理局、中國軟件評測中心(工業和信息化部軟件與集成電路促進中心)、中國計算機行業協會網絡和數據安全專業委員會
2025年	2025 數字中國創新大賽數字安全賽道數據安全產業優秀案例評比賽銀獎—IPDRR驅動的數據安全體系賦能物聯網「T型」治理實踐	數字中國建設峰會組委會
2025年	中國計算機行業協會網絡和數據安全專業委員會卓越貢獻獎	中國計算機行業協會網絡和數據安全專業委員會
2024年	數據要素價值創新示範基地	中國名牌/數據要素價格形成與認定創新實驗室
2024年	磐石之星網絡與數據安全領域最具影響力企業	上海市互聯網協會
2024年	磐石之星網絡與數據安全領域本土最具實力企業	上海市互聯網協會
2024年	第二屆「數信杯」數據安全大賽金獎	數信杯數據安全大賽組委會
2024年	金靈光杯數據安全賽道二等獎—觀安觀智數據安全管控系統	中國互聯網協會
2023年	CSA2022安全創新獎	雲安全聯盟大中華區
2023年	星熠獲獎證書—基於「零信任」構建可信可控的數據安全管控體系	中國信息通信研究院

業 務

頒發年份	獎項或表彰名稱	簽發機構
2023年	星熠獲獎證書—基於流式數據處理引擎的敏感數據操作異常行為即時監測平台	中國信息通信研究院
2023年	首屆強基杯數據安全技能競賽全國一等獎	電信和互聯網行業數據安全人才強基計劃

我們的業務模式

下文載列我們業務流程的概要：

初始客戶接洽及需求識別

當客戶識別出對增強數據保護、網絡安全能力或系統升級的需求時，接洽通常隨之開始。視乎其需求、項目類別及監管要求，我們的客戶可透過以下方式向我們採購：(i)直接磋商；(ii)公開招標；或(iii)邀請報價並在多家供應商之間進行比價。我們一般會透過客戶的公開網站獲悉項目招標機會，有關網站會刊載項目相關的詳細資料。我們會根據公開資訊，評估客戶的業務目標、現有系統、營運限制及安全要求。

招標流程

對於新系統或解決方案，我們的客戶可能發佈正式招標，列出技術規格、性能要求、定價條款及交付時間表。收到招標文件後，我們將對其進行審查，並評估價格、項目範圍、技術要求、時間安排、競爭情況及資質標準等因素。我們會適時進行可行性評估，以釐定其是否符合我們的業務目標。我們會提交提案，而提案通常包含一份反映客戶需求的初步解決方案設計。截至2023年、2024年及2025年12月31日止年度，我們合共分別有983個、980個及957個項目，其中分別有300個、297個及225個項目通過招標程序獲得，中標率分別為30.5%、30.3%及23.5%。

我們觀察到，若我們成功中標，後續與同一客戶開展的相同或類似的項目，很可能會採取直接談判的方式，因為客戶可能會出於提高運營效率而選擇這種方式。因此，涉及系統升級、擴展、維護或持續運營支持的項目，通常通過直接談判方式獲得，尤其當客戶已使用我們的產品或服務時。談判可能涉及範圍、定價、監管要求、採購政策及交付時間表，並可能持續數周或數月。

框架協議的執行

於選定後，我們將訂立框架協議，其中規定主要的商業及運營條款，包括工作範圍、定價原則、責任、服務水平、保密及變更管理。當客戶通過多家附屬公司運營時，可在附屬公司層面訂立項目特定協議。

業 務

盡職調查及解決方案設計

我們嚴格按照協議中規定的交付範圍及要求，進行全面的需求發掘及研究。透過與我們客戶的管理團隊、業務部門及技術團隊進行深度訪談，並結合包括資產清單及繪製、技術評估及測試以及合規性審查的多維度方法，我們精準識別客戶的需求，並制定正式的需求規格文件，以供我們的客戶審閱並簽署確認。

一旦我們的需求規格文件定稿後，我們會進入解決方案設計及開發階段。於此階段，我們制定整體系統架構並創建詳細的設計文件。我們通常會舉行正式設計審閱會議以驗證產出成果。我們的核心技術人員隨後根據已批准的設計進行編碼，並進行單元測試及代碼審閱，以確保我們的解決方案符合質量標準。倘我們的技術人員於單元測試或代碼審閱期間發現任何問題，則將修訂和重新測試代碼，直至其符合所有要求標準。

項目執行、安裝及整合

經客戶批准後，我們即展開部署及實施階段。於部署及安裝前，我們會制定詳細的測試計劃及測試案例，以識別並解決我們軟件中存在的任何故障。所有實施工作均直接於客戶的基礎設施及現場環境內開展，包括安裝、配置、整合、測試及培訓。一般而言，我們的指定人員會親臨客戶現場，在客戶指定的電腦上進行軟件本地安裝，有關軟件絕不會安裝於我們指定人員的個人或私有設備上。我們與客戶的技術團隊協作，確保解決方案順利融入客戶現有營運流程，其後進行正式移交，以投入正式營運。該等現場安裝安排可確保解決方案在客戶環境內穩定運行，並符合其特定的技術及安全要求。

持續支持、維護及關係發展

部署完畢後，我們將持續為客戶提供軟件支持、更新及優化服務。我們亦會收集並分析客戶的反饋，並將任何新需求或優化方向納入研發流程，用於未來的產品迭代。

截至2023年12月31日、2024年12月31日及2025年12月31日，我們分別擁有892、690及612份在手合約。於往績記錄期間，我們的手頭合約數量有所減少，主要由於在行業及價格競爭加劇的背景下，我們的部分客戶傾向於將多個項目整合為單一合約，導致我們的投標數量同比減少。於2023年、2024年及2025年12月31日，我們合約的未償還結餘分別為人民幣642.2百萬元、人民幣519.7百萬元及人民幣381.9百萬元。未償還合約結餘於往績記錄期間有所減少，主要歸因於我們項目交付效率的提升，這從我們確認的收入穩步增長中得以一見。

我們的一些長期合約各自包含多個項目。於往績記錄期間，我們於若干項目錄得毛虧損，主要歸因於項目特定情況，而非我們項目管理能力存在系統性缺陷。請參閱「風險因素—與我們的業務及行業相關的風險—我們的收入模式以項目為基礎。任何重大成本超支或未能履行我們的合約義務均可能對我們的業務、財務狀況及經營業績造成重大不利影響。」

業 務

收入產生及定價

我們通過以項目為基礎的收費、解決方案授權及服務費相結合的方式產生收入。項目收入受解決方案複雜程度、定制化水平及安裝範圍的影響。經常性收入可能包括維護費、軟件更新、代管服務或長期運營支持。

我們平台及專業服務的定價機制旨在反映設計與開發階段產生的成本，並根據解決方案的類型和模式附加不同的利潤率。我們定期審查成本，以確保我們的價格與時俱進並反映當前的市場狀況。當客戶下達涉及多種解決方案和服務的綜合訂單時，我們可提供更具競爭力的價格。這與我們定制化程度較低的標準化軟件的支付和定價不同，因此價格會體現其標準化特性。我們的目標是在盈利能力與客戶滿意度之間取得平衡，確保我們的解決方案既能保證高質量，又能保持可持續性。我們通常根據多項因素向客戶授予信貸期，例如其背景、行業聲譽、付款記錄、信譽以及我們與其業務關係的持續時間。

銷售及營銷

於往績記錄期間，我們的絕大部分收入來自中國內地的銷售，其中約0.5%來自香港的銷售。通常而言，我們直接向客戶交付並部署我們的解決方案。於2023年及2024年，我們分別向三家及一家分銷商銷售若干標準化軟件，並自此獲取收入人民幣0.8百萬元及人民幣3.4百萬元，分別佔我們總收入的0.2%及0.5%。

截至2025年12月31日，我們的銷售及營銷部門由151名成員組成。我們銷售及營銷團隊的成員主要專注於維持及拓展我們與現有客戶的業務，並利用現有關係爭取引薦潛在客戶。部分成員負責對客戶的數據基礎設施及現有軟硬件系統進行售前評估，以確定我們解決方案的開發方向。此外，部分成員處理客戶的一般查詢、投訴及反饋。於2023年、2024年及2025年，我們的銷售及營銷開支分別為人民幣139.9百萬元、人民幣141.5百萬元及人民幣108.6百萬元，分別佔我們總收入的27.1%、21.5%及15.3%。我們定期舉行會議以分析及商討各個方面的問題，包括客戶的反饋及投訴。截至最後實際可行日期，我們概無接獲任何來自客戶有關向彼等提供服務的重大投訴。

市場機遇及競爭

根據弗若斯特沙利文報告，中國持續加強網絡安全、數據安全、人工智能及相關領域的能力建設。中國信息安全市場規模從2021年的人民幣732億元增長至2025年的人民幣1,057億元，複合年增長率為9.6%，預計到2030年將達到人民幣1,727億元，複合年增長率為10.6%。數據安全市場從2021年的人民幣186億元增長至2025年的人民幣290億元，複合年增長率為11.7%，預計到2030年將達到人民幣509億元，複合年增長率為12.1%。網絡安全市場從2021年的人民幣546億元增長至2025年的人民幣767億元，複合年增長率為8.9%，預計到2030年將達到人民幣1,219億元，複合年增長率為10.0%。人工智能的廣泛應用帶來了新的安全缺口，推動了對人工智能安全、車聯網安全及物聯網安全方面增強防護的需求增長。

業 務

根據弗若斯特沙利文報告，就收入而言，於2025年，我們在中國提供數據安全平台的專業安全提供商中排名第一（市場份額9.7%），在中國提供數據安全的專業安全提供商中排名第七（市場份額3.8%），及在中國提供信息安全的專業安全提供商中排名第十三（市場份額1.8%）。請參閱「行業概覽」。

季節性

我們通常在每年第四季度產生較高比例的收入，因為通常在年初獲批的大多數項目通常會在年底前交付并由客戶驗收，根據弗若斯特沙利文報告，此乃行業慣例。

我們的客戶

於2023年、2024年及2025年，我們來自五大客戶的收入分別為人民幣321.0百萬元、人民幣451.1百萬元及人民幣496.3百萬元，分別佔我們總收入的62.2%、68.4%及70.1%。於往績記錄期間，我們來自最大客戶的收入分別為人民幣182.3百萬元、人民幣297.6百萬元及人民幣259.1百萬元，分別佔我們總收入的35.3%、45.2%及36.6%。

於往績記錄期間，該等主要客戶主要為中國大型電信網絡運營商，各家均有諸多附屬公司，我們通常與其訂立基於項目的採購協議。以下載列我們與主要客戶簽訂之協議的主要條款：

服務範圍：明確我們提供的平台、軟件及專業服務。

付款條款：付款條款視乎所提供的產品及解決方案類型而定，惟通常採用里程碑式付款。

期限：各合約中我們產品與解決方案的期限取決於其具體服務範圍，且我們與客戶簽訂的合約可能因客戶與項目差異而存在顯著不同。一般直至雙方悉數履行協議項下各自義務為止。

定價：各合約中我們產品與解決方案的定價取決於其具體服務範圍，且我們與客戶簽訂的合約的價值可能因客戶與項目差異而存在顯著不同。

業 務

下表載列我們於2023年五大客戶的詳情：

客戶	收入	佔本集團 總收入的 百分比	業務關係 開始時間	本集團 提供的 主要解決 方案類型	提供的 信貸期	支付方式
	人民幣 千元	%				
客戶A ⁽¹⁾	182,302	35.3	2015年	平台、軟件及 服務	30日	電匯
客戶B ⁽²⁾	46,310	9.0	2017年	平台、軟件及 服務	30日	銀行轉賬
客戶C ⁽³⁾	44,222	8.6	2020年	服務	30日	銀行轉賬
客戶D ⁽⁴⁾	34,487	6.7	2021年	平台、軟件及 服務	30日	電匯
客戶E ⁽⁵⁾	13,645	2.6	2021年	服務	15日	銀行轉賬
總計	320,966	62.2				

附註：

- (1) 客戶A是中國三大電信網絡運營商之一，主要從事提供移動語音、數據、寬帶及其他信息和通信服務。其有一間附屬公司的股份於香港聯交所主板及上海證券交易所雙重上市。
- (2) 客戶B是中國三大電信網絡運營商之一，主要從事數字信息基礎設施及服務，涵蓋移動及有線通信、雲計算、大數據、人工智能及物聯網。其有一間附屬公司的股份於香港聯交所主板及上海證券交易所雙重上市。
- (3) 客戶C是一家於2022年註冊成立的公共事業單位，主要負責上海市公共數據的集中統一管理。
- (4) 客戶D是中國三大電信網絡運營商之一，主要從事提供移動及固網通信服務、國內及國際通信設施、數據通信及系統集成服務。其擁有兩家上市附屬公司，一家於香港聯合交易所主板上市，另一家於上海證券交易所上市。兩家附屬公司均專注於電信及信息相關服務。
- (5) 客戶E為一家於上海證券交易所上市的上市公司，主要從事基於公開金鑰基礎設施的商用密碼軟件產品的研發、製造與銷售。

業 務

下表載列我們於2024年五大客戶的詳情：

客戶	收入	佔本集團 總收入的 百分比	業務關係 開始時間	本集團 提供的 主要解決 方案類型	提供的 信貸期	支付方式
	人民幣 千元	%				
客戶A	297,649	45.2	2015年	平台、軟件及 服務	30日	電匯
客戶D	45,421	6.9	2021年	平台、軟件及 服務	30日	銀行轉賬
客戶B	41,699	6.3	2017年	平台、軟件及 服務	30日	銀行轉賬
客戶C	41,410	6.3	2020年	服務	30日	銀行轉賬
客戶F ⁽⁶⁾	24,948	3.8	2022年	服務	30日	銀行轉賬
總計	451,127	68.5				

下表載列我們於2025年五大客戶的詳情：

客戶	收入	佔本集團 總收入的 百分比	業務關係 開始時間	本集團 提供的 主要解決 方案類型	提供的 信貸期	支付方式
	人民幣 千元	%				
客戶A	259,112	36.6	2015年	平台、軟件及 服務	30日	電匯
客戶B	75,635	10.7	2017年	平台、軟件及 服務	30日	銀行轉賬
客戶G ⁽⁷⁾	64,927	9.2	2024年	平台及服務	28日	電匯
客戶D	59,893	8.5	2021年	平台及軟件	30日	銀行轉賬
客戶C	36,757	5.2	2020年	服務	30日	銀行轉賬
總計	496,324	70.2				

附註：

- (6) 客戶F是一家成立於2015年的公司，是中國能源行業信息和通信技術產品與服務的領先供應商。其有一家附屬公司的股份於上海證券交易所上市。
- (7) 客戶G是一家於2013年成立的國有公司，是推動中國西南地區工業發展及城市建設的主要參與者。其主要專注於智慧城市、大數據及信息技術、高端製造及醫療健康行業。

業 務

董事確認，截至最後實際可行日期，我們於往績記錄期間各年度的五大客戶均為獨立第三方，概無董事、彼等各自的緊密聯繫人或任何股東（就本公司董事所知，截至最後實際可行日期擁有本公司股本超過5%）直接或間接於任何該等客戶中擁有任何權益。於往績記錄期間及直至最後實際可行日期，就董事所深知，我們與客戶並無任何重大糾紛，亦無嚴重違反我們與其協議的情況。

與往績記錄期間與最大客戶的關係

於整個往績記錄期間，客戶A為我們的最大客戶，來自客戶A的收入分別為人民幣182.3百萬元、人民幣297.6百萬元及人民幣259.1百萬元，佔總收入的35.3%、45.2%及36.6%。於往績記錄期間，客戶A亦為我們的供應商之一，我們向客戶A的採購額分別為人民幣0.3百萬元、人民幣0.2百萬元及人民幣0.2百萬元。請參閱「一客戶與供應商重疊」。

客戶A為獨立第三方，且為中國三大電信網絡運營商之一。於往績記錄期間，我們與客戶A的超過40家附屬公司進行交易。我們與客戶A保持著超過十年的長期合作關係，期間我們在多項技術解決方案及平台定制方面進行了緊密合作。雖然我們並非客戶A的唯一供應商，但我們為其部署的多個平台及服務均具有高度定制化特點，並與其運維系統深度集成。該等定制增加了客戶A的更換成本，並降低了我們被另一家服供應商迅速取代的可能性。因此，我們的董事認為，雖然我們並非獨家供應商，但我們合作關係的穩定性及長期性證明了雙方存在一定程度的相互依賴關係，因此降低了客戶A終止或大幅減少與我們合作的風險。

客戶集中在中國電信技術服務行業十分普遍。電信行業受監管牌照要求、高資本投資門檻及其他結構性准入壁壘的限制，導致僅存在三大電信網絡運營商。由於客戶數量有限且合約規模巨大，在該行業經營的服務提供商通常依賴其中一家或多家運營商以獲得其大部分收益。在這一行業背景下，我們對客戶A的依賴符合現行行業慣例，並不代表存在任何異常或更高的依賴風險。

儘管如此，董事認為我們與客戶A業務關係的任何變動均不會對我們的業務產生重大不利影響，而這是因為：

- **多家附屬公司：**客戶A為一家主要的電信網絡運營商，旗下經營眾多附屬公司。各附屬公司均為獨立法律實體，且通常各自進行獨立的招標程序。

業 務

- 電信行業內客戶群的多樣化：除客戶A外，我們亦與中國其他兩大電信網絡運營商保持長期業務關係，這為我們提供了廣泛的覆蓋範圍，並減少了任何單一運營商需求波動帶來的影響。
- 向非電信領域擴張：我們已將客戶覆蓋範圍擴大至能源、電力及其他基礎設施相關行業的客戶，並持續向新興安全領域擴張。該等舉措預期將進一步使我們的收益基礎多元化，並隨時間推移減少對客戶A的依賴。
- 具備強大技術能力的持續業務模式：我們的平台融入了自研功能及特定領域的專業知識，且我們的解決方案通常需要持續的升級、維護及迭代。這創造了長期的服務連續性，使競爭對手的替代變得更加困難。
- 無重大不利發展：於整個往績記錄期間及直至最後實際可行日期，我們與客戶A的關係保持穩定且良好。

考慮到(i)我們解決方案的定制化性質，(ii)中國電信行業固有的結構性集中，及(iii)我們實現多元化並減輕依賴風險的能力，董事認為客戶A終止或大幅減少與我們業務關係的風險較低。此外，董事認為，我們對客戶A的重大依賴不會對我們的業務可持續性、營運穩定性、財務表現或[編纂]合適性產生重大不利影響。

售後服務

我們的售後服務涵蓋在規定時間內提供的軟件及服務支持，並嚴格遵守與客戶約定的條款。我們可能會制定糾正及預防管理程序，以分析和解決已發生或可能發生的任何軟件不合格項的原因。若發現某批次解決方案不符標準，我們將嚴格遵循相關程序，並及時通知相關利益相關方。

客戶滿意度是我們的首要任務之一。為此，我們通過結構化問卷定期開展客戶滿意度調查，藉此(i)記錄並追蹤客戶滿意度的變化，以及(ii)匯總並分類客戶反饋。我們依託系統性的調查結果及對客戶滿意度動態的深入分析，建立了一套快速響應機制，以便及時且高效地滿足客戶需求。與此同時，我們不斷完善售後服務系統，以切實保障客戶體驗，鞏固長期客戶關係，並穩固客戶基礎。

於往績記錄期間及直至最後實際可行日期，我們並無經歷任何重大責任索賠。此外，我們未收到任何對我們營運造成重大不利影響的客戶投訴。這一業績記錄彰顯了我們致力於提供高質量解決方案並保持穩固客戶關係的承諾。

業 務

供應商及採購

於往績記錄期間，我們的供應商主要包括外包服務提供商，以及IT設備及軟件供應商。於2023年、2024年及2025年，我們於往績記錄期間各年度向五大供應商的採購分別為人民幣46.3百萬元、人民幣85.5百萬元及人民幣88.1百萬元，分別佔我們採購總額的18.5%、30.9%及33.2%。

下表載列我們於2023年五大供應商的詳情：

供應商	採購額 (人民幣 千元)	佔採購 總額的 百分比 (%)	業務關係 開始時間	採購類型	支付方式	信貸期
供應商A ⁽¹⁾	16,952	6.8	2021年	外包安裝及 修復服務	電匯及銀行匯票	90日
供應商B ⁽²⁾	7,704	3.1	2019年	外包安裝及 修復服務	電匯及銀行匯票	45日
供應商C ⁽³⁾	7,537	3.0	2022年	外包安裝及 修復服務	電匯	5日
供應商D ⁽⁴⁾	7,272	2.9	2022年	外包安裝及 修復服務	電匯	45日
供應商E ⁽⁵⁾	6,847	2.7	2022年	IT設備	電匯	89日
總計	46,312	18.5				

附註：

- (1) 供應商A是一家成立於2001年的公司，主要從事提供一站式數智化整體解決方案，其業務聚焦於數智技術應用領域。
- (2) 供應商B是一家成立於2018年的公司，主要從事工業控制系統安全領域的技術研究與服務。
- (3) 供應商C是一家成立於2007年的公司，主要從事電腦軟硬件、通訊設備及網絡技術等領域的技術開發。
- (4) 供應商D是一家成立於2020年的主動網絡安全供應商，主要從事技術服務與技術開發。
- (5) 供應商E是一家成立於1995年及總部位於北京的網絡供應商及增值服務提供商。其母公司的股份於上海證券交易所上市。

業 務

下表載列我們於2024年五大供應商的詳情：

供應商	採購額 (人民幣千元)	佔採購總額的百分比 (%)	業務關係開始時間	採購類型	支付方式	信貸期
供應商F ⁽⁶⁾	28,373	10.3	2024年	IT設備	電匯	30日
供應商A	19,025	6.9	2021年	外包安裝及修復服務	電匯及銀行匯票	90日
供應商G ⁽⁷⁾	18,547	6.7	2022年	外包安裝及修復服務以及軟件產品	電匯	5日
供應商H ⁽⁸⁾	10,604	3.8	2023年	外包安裝及修復服務	電匯	5日
供應商D	8,956	3.2	2022年	外包安裝及修復服務	電匯	45日
總計	85,505	30.9				

附註：

- (6) 供應商F是一家成立於2020年的公司，是一家集研發、生產、銷售於一體的高科技企業。其母公司的股份於深圳證券交易所上市。
- (7) 供應商G是中國最早專業從事可靠性研究的權威機構之一。其為工信部下屬的主要技術支持單位，為電子信息產業提供認證、測試、分析及評估服務。
- (8) 供應商H是一家成立於2015年的公司，主要從事技術服務與技術開發。

下表載列我們於2025年五大供應商的詳情：

供應商	採購額 (人民幣千元)	佔採購總額的百分比 (%)	業務關係開始時間	採購類型	支付方式	信貸期
供應商A	51,326	19.3	2021年	外包安裝及修復服務	電匯及銀行匯票	90日
供應商I ⁽⁹⁾	14,972	5.6	2019年	外包安裝及修復服務	電匯及銀行匯票	45日
供應商D	10,004	3.8	2022年	外包安裝及修復服務	電匯	45日
供應商J ⁽¹⁰⁾	6,294	2.4	2022年	外包安裝及修復服務	電匯及銀行匯票	45日
供應商K ⁽¹¹⁾	5,479	2.1	2021年	外包安裝及修復服務	電匯及銀行匯票	45日
總計	88,075	33.2				

業 務

附註：

- (9) 供應商I是一家成立於2017年的公司，致力於運用基於人工智能、計算機視覺等相關技術，為客戶提供綜合性人工智能解決方案與營運服務。
- (10) 供應商J是一家成立於2020年的公司，主要從事工程與技術研究、增值電信技術服務及通訊設備銷售等領域。
- (11) 供應商K是一家成立於2010年的公司，主要從事軟件與信息技術服務行業。

董事確認，截至最後實際可行日期，我們於往績記錄期間各年度的五大供應商均為獨立第三方，而據董事所知，於往績記錄期間及直至最後實際可行日期，概無董事或彼等各自的緊密聯繫人或任何股東擁有我們已發行股份5%以上，亦無於我們五大供應商中擁有任何權益。於往績記錄期間及直至最後實際可行日期，就董事所深知，我們與供應商並無任何重大糾紛，亦無嚴重違反我們與其協議的情況。

外包服務提供商

我們通常將若干非核心服務委託予中國合資格的第三方外包服務提供商。例如，在我們的解決方案部署及獲客戶驗收後，我們通常需要派駐人員至客戶現場進行項目觀察及反饋收集。由於我們的客戶群遍及全中國，該等服務通常涵蓋上海都會區外需要現場考察及安裝的營運與任務。根據弗若斯特沙利文報告，此等做法符合業界普遍慣例。我們通過技術支持協議或項目外包服務協議來規範合作關係，其中詳細列明IT服務類型、合約價格及付款條款。我們的外包服務提供商通常為我們提供信貸期，並負責遵守我們的質量標準，同時為客戶提供維護和保修服務。

據我們的中國法律顧問告知，我們與第三方外包服務提供商的安排並不屬於勞務派遣，主要是由於根據中國法律法規（如《勞動合同法》及《勞務派遣暫行規定》），勞務派遣的特徵為按派遣人員數量結算費用、由用工單位直接管理工人，以及工作任務具有臨時性、輔助性或替代性。然而，我們與第三方外包服務提供商的安排呈現不同特徵，例如根據既定服務類別釐定固定合約總價、管理及費用結算著重於服務成果及交付項目、提供專業技術服務，以及管理界線清晰明確（即我們僅監督服務成果，而不直接管理外包人員的勞動過程），該等特徵與勞務派遣的界定特徵並不一致。請參閱「風險因素—與我們的業務及行業有關的風險—任何重大成本超支均可能對我們的業務、財務狀況及經營業績造成重大不利影響」。

業 務

下文載列我們與外包服務提供商訂立之協議中包含之主要條款：

服務範圍：服務提供商同意提供指定服務，包括硬件安裝、軟件實施、現場技術支持及相關維護任務。服務範圍通常在服務交付計劃中詳細說明，當中列明方法、時間表及交付成果。

付款條款：服務費通常按重大事件或按月支付。常見的付款安排包括：簽約後支付首期款項，根據項目進度支付中期款項，並在項目完成且交付成果通過驗收後支付尾款。

期限與續期：協議通常有固定期限（例如一年），並訂明如未發生違約情況，則可按相同條款續期。

合規義務：服務提供商必須配備持有有效資質證書、勞動合約及保險的合資格人員。該等人士必須遵守適用法律、健康與安全標準以及我們的內部質量要求。

保密性與知識產權：服務提供商有義務對所有項目相關信息保密，並確保在合作期間產生的任何工作成果或知識產權均歸我們所有。未經同意，嚴禁向第三方披露。

分包限制：未經我們事先書面同意，服務提供商不得將服務分包。若獲准分包，供應商依然須對其分包商的行為及不作為承擔全部責任。

質量標準和保修：服務提供商有責任滿足約定的質量標準，並為已安裝的硬件及已實施的軟件提供維護及保修服務。

終止及解除：如供應商造成經濟損失或未能履行合約責任，我們一般保留單方面終止或解除有關協議之權利。

法律責任及彌償保證：服務提供商通常須就違約、疏忽或未履行合約條款的行為承擔法律責任，並可能須就因其行為所引致之申索向我們作出彌償。

雖然我們聘用多家第三方服務提供商，但在某些地區，我們對有限數量提供商的依賴可能會產生集中度風險。為減輕此風險，我們定期評估各服務區域內的提供商組合，審查其財務狀況，並維持需要時可動用的備用提供商。交易對手風險通過合同保障進一步解決，包括履約保證、服務水平要求以及在不履約情況下的追索權。於2023年、2024年及2025年，我們的外包服務費用分別為人民幣184.8百萬元、人民幣257.5百萬元及人民幣239.2百萬元。

業 務

我們監測外包服務費的波動，並定期進行敏感度分析，以評估勞動力成本變動對項目盈利能力的影響。由於我們能夠將勞動力成本假設納入項目報價中，服務費的適度增加通常是可控的。對於長期或多階段項目，我們使用內部預算模型評估盈虧平衡門檻，以確保外包成本的變動不會對預期毛利產生重大影響。合格外包人員的可用性可能受季節性勞動力短缺、地區旅行限制或項目進度重疊的影響。服務團隊部署的任何延誤都可能影響項目時間表。為減輕該等風險，我們(i)維持具備重疊服務能力的多層次供應商網絡；(ii)在項目啟動前監測供應商的人員可用性；及(iii)要求供應商為大規模或時間敏感型項目分配專門或優先人員。我們亦可能在適當情況下重新分配內部人員或調整部署順序。

我們通過框架定價、競爭性重新招標及合同談判相結合的方式管理潛在的外包勞動力成本增加。在可行情況下，我們在確定期間內約定固定人工費率，以減少受短期成本波動的影響。對於無法固定價格的項目，我們評估成本增加是否可以反映在客戶報價中，特別是在勞動力需求較大或部署進度應客戶要求發生變化的情況下。

鑑於我們的經營性質，我們對外包勞動力規劃採取嚴謹的方法。向服務提供商發出的工作單通常按具體項目或具體任務發出，類似於與確認的項目需求相匹配的「背對背」安排。我們密切追蹤部署狀態、人天使用量及服務里程碑，以管理整體勞動力消耗。針對有爭議或未使用的勞務費用，我們根據未結清索賠的賬齡、服務驗收狀態及最終結算的可能性計提撥備。

我們對外包服務提供商的選擇基於嚴格的標準，包括其行業經驗、技術專長、服務質量、質量控制成效、定價、財務穩定性及滿足交付時限的能力。每位潛在提供商均需經歷嚴格的資質審核流程，包括背景調查、訪談及實地考察，通常需要一定時間方能完成。

為確保最高標準，我們密切監督和評估外包服務提供商的表現。我們每年進行檢查，重新評估其整體表現，並可能與未達到我們標準的提供商終止合作關係。評估基於多項因素進行，包括提供商的技術及行業專長、服務質量、質量保證程序及對我們政策及指引的遵守情況。這種全面的方法確保我們能夠維持高質量的服務，並有效滿足客戶的需求。

服務器及其他設備的供應鏈管理

於往績記錄期間，我們為履行合約義務而採購軟件及硬件，如服務器及及各類設備，並於我們的財務報表中將相關開支入賬為履約成本。我們強調穩健的供應鏈管理，已實施內部措施將供應商分類、開發與導入、物料選擇與認證、類別管理、稽

業 務

核管理、績效評估、供應商資格取消、資格重啟及其他流程規範化。該等措施旨在使供應商資源與我們的發展需求相協調，穩定產品及服務的供應，並確保所供應產品的品質。

於往績記錄期間及直至最後實際可行日期，我們所有供應商均位於中國，且我們並未遇到任何對我們營運造成不利影響的供應鏈問題。為應對可能出現的短缺，我們已與合資格的供應商討論，以建立長期的戰略合作夥伴關係，並已擴大我們的供應商群，從而確保關鍵組件的供應穩定。為降低供應鏈風險，我們可能會與供應商訂立一般採購協議，其主要條款載列如下：

期限：我們的採購協議通常不會訂明固定期限。供應商與我們在交付、驗收及付款後即完成履約。

產品規格：我們通常會訂明所採購產品的型號、單位、數量、單價及其他詳情。

交付：通常由供應商安排將產品交付至我們指定的地點，而我們通常會提供收貨人的姓名及電話號碼。

付款條款：我們通常在驗收產品或收到供應商開具的有效增值稅發票後以電匯或銀行匯票結算採購款項。

檢驗及驗收：我們通常負責在收貨時檢驗產品，並於特定期限內以書面形式通知任何瑕疵。若出現質量問題，供應商通常負責免費安排更換或退貨。

違約及終止：我們通常於採購協議中訂明違約金的計算方法。通常情況下，若另一方出現根本性違約，任何一方均可終止協議。

該等協議包括保密協議、質量保證協議、行為守則及供應商誠信和反腐敗協議等關鍵組成部分。

在與新供應商開展合作之前，我們會進行必要的調查和審核。現有供應商將通過一套商定的績效標準進行管理。對於未通過審核的供應商，可能會實施整改措施。倘仍未符合要求，供應商資格可能被取消。我們希望這種綜合方法能夠確保我們維持高質量的服務，並有效滿足我們的營運需求。

客戶/供應商重疊

於往績記錄期間，我們向中國三大電信網絡運營商客戶A、B及D提供數據安全及網絡安全解決方案，而我們亦為自身營運需要向該等運營商採購電信服務。此項安排主要由於中國的電信基礎設施及服務市場高度集中，在該市場中，寬頻、互聯網數據中心及全國網絡等核心服務，由少數獲國家授權的大型電信網絡運營商獨家提供。根據弗若斯特沙利文報告，此項安排符合現行行業慣例。

業 務

於往績記錄期間，客戶A一直是我們的最大客戶及其中一家供應商。於2023年、2024年及2025年，我們自客戶A產生的收入為人民幣182.3百萬元、人民幣297.6百萬元及人民幣259.1百萬元，分別佔我們總收入的35.3%、45.2%及36.6%。於2023年、2024年及2025年，我們自客戶A的採購額分別為人民幣0.3百萬元、人民幣0.2百萬元及人民幣0.2百萬元，分別佔我們採購總額的0.1%、0.05%及0.1%。

客戶B為我們於往績記錄期間各年的五大客戶之一，亦為我們於2024年及2025年的供應商。於2023年、2024年及2025年，我們自客戶B產生的收入為人民幣46.3百萬元、人民幣41.7百萬元及人民幣75.6百萬元，分別佔我們總收入的9.0%、6.3%及10.7%。於2023年、2024年及2025年，我們向客戶B的採購額為零、人民幣74,800元及人民幣0.1百萬元，分別佔我們採購總額的零、0.03%及0.04%。

客戶D為我們於往績記錄期間各年的五大客戶之一，亦為我們於2025年的供應商。於2023年、2024年及2025年，我們自客戶D產生的收入為人民幣34.5百萬元、人民幣45.4百萬元及人民幣59.9百萬元，分別佔我們總收入的6.7%、6.9%及8.5%。於2023年、2024年及2025年，我們向客戶D的採購額分別為零、零及人民幣0.1百萬元，分別佔我們採購總額的零、零及0.04%。

我們自客戶A、B及D採購及向其銷售的條款磋商乃按個別基準進行，而該等採購及銷售彼此並無關聯，亦不互為條件。因此，董事認為，我們與客戶A、B及D進行的所有採購及銷售均按正常商業條款基於我們的真實業務需求及公平磋商，於日常業務過程中進行。

我們的僱員

我們視僱員為寶貴資產，彼等為我們的成功作出重大貢獻。我們強調公平、透明和多元化，歡迎來自不同背景的人才加入，以營造多元化的工作環境。我們遵守公開、公平、公正及擇優的用人原則，確保工作崗位基於實際需要，並在聘用期間確保人才與崗位的適當配對。下表載列我們截至2025年12月31日按職能劃分的全職僱員人數及百分比：

職能／部門	僱員人數	估僱員 總數百分比
部署	376	45.6
研發	186	22.6
銷售及營銷	151	18.3
董事會和高級管理層	6	0.7
行政及其他	106	12.9
總計	825	100.0

業 務

我們的招聘流程由多個因素決定，包括行業經驗、教育背景以及當前的職位空缺。我們一般會根據僱員各自的職位及職責，向其支付固定薪資及其他津貼。我們與僱員訂立個人勞動合同，涵蓋薪金、福利、受僱範圍及終止僱傭理由等方面。截至最後實際可行日期，我們的僱員概無通過任何工會或集體談判協議磋商其僱傭條款。我們的董事確認，於往績記錄期間及直至最後實際可行日期，我們概無收到任何地方當局針對我們的僱員或相關勞動法律及法規的任何罰款、處罰、警告或行政行動，從而對我們的經營業績造成重大不利影響。

我們認為，我們已與僱員維持良好的工作關係。於往績記錄期間及直至最後實際可行日期，我們並無發生任何導致我們營運中斷的重大勞資糾紛、停工、罷工或工作安全事故。

保險

於往績記錄期間及直至最後實際可行日期，我們未曾投保任何業務中斷保險，亦未投保任何涵蓋對手方責任的保單，根據弗若斯特沙利文報告，這符合行業慣例。董事亦確認，於往績記錄期間，我們並無經歷任何對我們的業務、財務狀況或經營業績造成重大不利影響的業務中斷或損失或設施損害。

物業

截至最後實際可行日期，我們並無擁有任何物業，並於中國租賃15項獨立第三方的物業，總建築面積約為8,056平方米，主要用作辦公樓。於往績記錄期間及直至最後實際可行日期，我們於與業主磋商續租事宜時並無遇到任何重大困難。

截至最後實際可行日期，我們尚未將我們租賃物業的租賃協議向中國相關政府部門登記或備案。據我們的中國法律顧問告知，儘管未進行登記不會影響租賃協議的有效性，但相關政府部門可能責令我們限期登記相關租賃，否則我們可能會就每項未登記租賃處以人民幣1,000元至人民幣10,000元的罰款。請參見「風險因素－與我們的業務及行業有關的風險－我們尚未完成租賃物業所必要的備案及登記。」

為防止上述與未登記租賃物業相關的不合規事件再次發生，我們已加強租賃管理及監管備案的內部控制措施，包括(i)建立租賃備案登記冊，記錄關鍵資料及證明文件；(ii)指定行政管理部門監督租賃執行、備案及與相關方的協調；及(iii)定期進行內部檢查，以確保按照適用中國法規及時辦理租賃協議的登記與更新。因此，董事認為，上述不合規情況將在通過強化內部控制得到適當處理，並在主管部門要求時進行整改的前提下，不會對我們的[編纂]合適性產生重大不利影響。

業 務

就整改而言，若相關政府主管部門發出任何指令或命令，我們隨時準備進行任何所需的備案、提交或支付罰款或滯納金。由於整改的時間及具體步驟取決於主管部門的評估（現階段無法確定），我們目前無法確定所需的具體整改行動。我們的中國法律顧問確認，若主管部門強制要求採取該等行動，則在[編纂]後完成必要的登記或備案不存在法律障礙。我們將在中期報告及年度報告中披露任何所需整改的進展以及任何延誤的說明。截至最後實際可行日期，由於中國主管部門未發出任何命令或通知，故未採取任何整改行動。

牌照及許可證

下表載列我們截至最後實際可行日期所持且對我們的營運屬重要的主要許可證詳情：

證書名稱	證書編號	發證機關	發證日期	有效期至
網絡安全專用產品安全檢測證書	25SW01635-A	信息產業信息安全測評中心	2025年12月5日	2027年12月5日
網絡安全專用產品安全檢測證書	26SS00S30-A	信息產業信息安全測評中心	2026年4月3日	2028年4月3日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2021-CS007-147	中國網絡安全審查技術與認證中心	2023年7月13日	2028年7月12日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2024-CS006-875	中國網絡安全審查認證和市場監管大數據中心	2024年8月9日	2029年8月8日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2024-CS013-948	中國網絡安全審查認證和市場監管大數據中心	2024年10月14日	2029年10月13日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2024-CS023-1023	中國網絡安全審查認證和市場監管大數據中心	2024年12月16日	2029年12月15日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2024-CS013-1029	中國網絡安全審查認證和市場監管大數據中心	2024年12月19日	2029年12月18日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2024-CS012-1037	中國網絡安全審查認證和市場監管大數據中心	2024年12月23日	2029年12月22日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2024-CS015-1040	中國網絡安全審查認證和市場監管大數據中心	2024年12月25日	2029年12月24日

業 務

證書名稱	證書編號	發證機關	發證日期	有效期至
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2024-CS032-1052	中國網絡安全審查認證和市場監管大數據中心	2025年1月14日	2030年1月13日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2025-CS024-1063	中國網絡安全審查認證和市場監管大數據中心	2025年1月23日	2030年1月22日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2025-CS012-1074	中國網絡安全審查認證和市場監管大數據中心	2025年2月11日	2030年2月10日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2025-CS023-1146	中國網絡安全審查認證和市場監管大數據中心	2025年4月22日	2030年4月21日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2025-CS012-1183	中國網絡安全審查認證和市場監管大數據中心	2025年5月16日	2030年5月15日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2025-CS034-1281	中國網絡安全審查認證和市場監管大數據中心	2025年8月20日	2030年8月19日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2025-CS035-1338	中國網絡安全審查認證和市場監管大數據中心	2025年11月10日	2030年11月9日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2025-CS024-1340	中國網絡安全審查認證和市場監管大數據中心	2025年11月11日	2030年11月10日
網絡關鍵設備和網絡安全專用產品安全認證證書	CCRC-2026-CS012-1407	中國網絡安全審查認證和市場監管大數據中心	2026年2月9日	2031年2月8日
信息安全服務資質證書(安全工程類二級)	CNITSEC2024SRV-11-207	中國信息安全測評中心	2024年1月16日	2027年1月15日
信息安全服務資質證書(風險評估二級)	CNITSEC2024SRV-RA-11-119	中國信息安全測評中心	2024年1月16日	2027年1月15日
信息安全服務資質證書(安全開發類一級)	CNITSEC2025SRV-SD-1-158	中國信息安全測評中心	2025年12月26日	2028年12月25日
信息安全服務資質證書(數據安全類一級)	CNITSEC2023SRV-DS-1-2	中國信息安全測評中心	2023年12月8日	2026年12月7日

業 務

證書名稱	證書編號	發證機關	發證日期	有效期至
信息安全服務資質證書(信息系統審計一級)	CNITSEC2025SRV-SA-I-43	中國信息安全測評中心	2025年12月5日	2028年12月4日
信息安全服務資質認證證書	CCRC-2018-ISV-ER-243	中國網絡安全審查認證和市場監管大數據中心	2025年5月27日	2028年5月26日
信息安全服務資質認證證書	CCRC-2018-ISV-RA-555	中國網絡安全審查認證和市場監管大數據中心	2025年5月27日	2028年5月26日
信息安全服務資質認證證書	CCRC-2018-ISV-SM-452	中國網絡安全審查認證和市場監管大數據中心	2025年5月27日	2028年5月26日
信息安全服務資質認證證書	CCRC-2020-ISV-SI-1793	中國網絡安全審查認證和市場監管大數據中心	2025年5月27日	2028年5月26日
信息安全服務資質認證證書	CCRC-2020-ISV-SD-254	中國網絡安全審查認證和市場監管大數據中心	2025年5月27日	2028年5月26日
通信網絡安全服務能力評定證書(風險評估二級)	CESSCN-2023-RA-B-012	中國通信企業協會	2023年12月24日	2026年12月23日
通信網絡安全服務能力評定證書(安全設計與集成二級)	CESSCN-2025-SDI-B-023	中國通信企業協會	2025年8月29日	2028年8月28日
通信網絡安全服務能力評定證書(應急響應二級)	CESSCN-2025-ERS-B-012	中國通信企業協會	2025年8月29日	2028年8月28日
通信網絡安全服務能力評定證書(安全培訓一級)	CESSCN-2023-ST-C-008	中國通信企業協會	2023年12月24日	2026年12月23日
信息安全等級保護安全建設服務機構能力評估合格證書	DJJS2018001001	公安部第一研究所	2018年3月16日	2024年3月15日 ⁽¹⁾

業 務

證書名稱	證書編號	發證機關	發證日期	有效期至
數據安全服務能力評定 資格證書	CHINADS-08-20230301	中國計算機行業協會數據安全專業 委員會、中國軟件評測中心(工業 和信息化部軟件與集成電路促進 中心)	2023年3月8日	2029年2月27日
數據安全服務能力評定 資格證書	CHINADS-09-20230301	中國計算機行業協會數據安全專業 委員會、中國軟件評測中心(工業 和信息化部軟件與集成電路促進 中心)	2023年3月8日	2026年3月7日 ⁽¹⁾

附註：

- (1) 根據公安部第一研究所於2024年6月17日出具的《證書辦理說明》，因該單位對信息安全等級保護安全建設服務機構能力評估業務進行調整，對已下發的《信息安全等級保護安全建設服務機構能力評估合格證書》續證工作暫停受理，原證書有效。
- (2) 中國計算機行業協會網絡和數據安全專業委員會已批准本公司啟動證書的展期及續證程序，並就我們證書的續證授予展期，該展期於2026年7月7日屆滿。於此展期內，我們的原證書狀態為「續證有效」，不影響我們合法開展數據安全建設及其他相關業務活動。

董事確認，截至最後實際可行日期，我們已獲得在中國開展業務營運所需的所有必要牌照及許可證，從而在所有重大方面均符合相關法律法規。董事亦確認，於往績記錄期間及直至最後實際可行日期，我們在獲取及/或續期該等牌照及許可證方面並無遇到任何重大困難。此外，我們的董事並不知悉任何會於該等牌照及許可證到期時嚴重阻礙或延誤重續的情況。因此，董事預期在遵守有關領取牌照規定方面不會遭遇任何重大困難以致對我們的營運及業務造成重大不利影響。

法律程序與合規事宜

於日常業務過程中，我們可能會捲入法律、仲裁或行政程序。請參閱「風險因素－與我們的業務及行業有關的風險－抗辯或解決針對我們提起的任何訴訟、法律及合同糾紛、索償或行政訴訟可能成本高昂且耗費時間，並可能導致負面報導」。截至最後實際可行日期，據我們的董事所深知，概無任何針對我們或任何董事會成員且會對我們業務、財務狀況或經營業績造成不利影響的正在進行或即將發生的重大訴訟、索賠或仲裁程序。

據中國法律顧問告知，我們的董事確認，於往績記錄期間及直至最後實際可行日期，我們已在所有重大方面遵守中國所有適用法律法規，且並無發生對我們的業務、財務狀況或經營業績造成重大不利影響的任何不合規事件。

業 務

數據安全與隱私

作為我們業務模式的一部分，我們於客戶場地部署技術人員並交付我們的解決方案。我們不會訪問或控制儲存於該等部署中的客戶數據。在日常業務過程中，我們主要收集我們客戶的聯絡信息、交付地址及採購記錄，僅用於促進我們解決方案的提供與支持。

我們已建立並持續維護一套全面的信息安全與數據管理計劃，旨在保障我們系統的完整性與可用性以及我們所控制數據的隱私與安全。我們的保障措施包括(其中包括)防火牆、入侵防禦系統、定期滲透測試、定期漏洞掃描及書面災難恢復計劃。我們擬持續強化該框架，著重創新與適應性，以滿足數據保護方面不斷演變的標準與期望。

我們的中國法律顧問認為，於往績記錄期間及直至最後實際可行日期，我們在所有重大方面均遵守中國有關個人數據及隱私保護的相關法律法規。請參閱「監管概覽」。

此外，根據我們中國法律顧問，截至最後實際可行日期，我們無須根據《網絡安全審查辦法》接受網絡安全審查，原因如下：

- (i) 根據《關鍵信息基礎設施安全保護條例》，我們並無接獲負責該等基礎設施安全的有關部門的通知，將我們指定為關鍵信息基礎設施運營者；
- (ii) 我們並不持有超過一百萬名用戶的個人信息；
- (iii) [編纂]並不構成海外上市；及
- (iv) 本公司未曾接獲網絡安全審查部門發出的任何正式通知，要求我們根據《網絡安全審查辦法》接受網絡安全審查。

第三方付款安排

第三方付款安排的背景及原因

於2025年，我們的一名客戶（「**相關客戶**」）透過不屬於相應買賣協議項下訂約方的賬戶與我們結算款項（「**第三方付款安排**」）。相關客戶為一家政府平台公司，且其第三方付款人為相關客戶的主管政府部門。第三方付款安排的付款總額為人民幣10.7百萬元，佔我們總收入的1.5%。

業 務

據董事所深知，相關客戶主要由於其內部資金安排及政策而作出第三方付款安排。為保障我們的利益並確保及時收回貿易應收款項，我們認定有關安排對相關客戶履行其付款義務而言屬商業上的必要之舉。我們與相關客戶直接核對交易金額，以確保準確性，從而降低與接收第三方付款相關的風險。因此，我們並不反對由相關客戶發起的第三方付款安排。

於往績記錄期間及直至最後實際可行日期，(i)我們並無向相關客戶或指定第三方付款人提供任何折讓、佣金、回扣或其他利益以促使或激勵第三方付款安排；及(ii)我們並無發起任何第三方付款安排，且第三方付款安排乃根據相關客戶的要求安排。據我們所深知，於往績記錄期間，相關付款乃基於真實的相關交易及有效合約關係而作出。我們提供給相關客戶的定價及付款條款與未參與第三方付款安排的客戶一致。經我們的中國法律顧問告知，我們透過第三方付款安排接受付款並無違反中國法律及法規項下的任何禁止性規定。據我們所深知，於往績記錄期間及直至最後實際可行日期，我們未因參與第三方付款安排而受到任何調查、詢問、被處罰或被徵收附加費。此外，於往績記錄期間及直至最後實際可行日期，我們並未因第三方付款安排而遇到任何退款請求、實際或待決的爭議或分歧，亦無收到與第三方付款安排有關的任何重大申索。

有關第三方付款安排的強化內部控制措施

於往績記錄期間，我們(i)對第三方付款人進行KYC盡職調查，並評估其財務狀況及合規情況；及(ii)對我們的僱員進行反洗錢培訓，以監控及管理與第三方付款安排有關的風險。

我們亦已強化下列內部控制措施，監察存入我們銀行賬戶的款項：

- (i) 我們已向全體員工發出內部通告，禁止彼等接受任何第三方付款安排下的付款；
- (ii) 我們的財務部門已制定管理應收賬款結算的範本，其中須載有交易說明、客戶名稱、付款日期、客戶賬戶名稱、涉及的任何第三方付款安排以及任何發現的異常情況；及
- (iii) 我們的財務部門已指定人員負責監察匯入的付款。倘再次出現第三方付款安排，指定人員應向部門經理報告，以便採取進一步行動。

業 務

於往績記錄期間，鑒於相關客戶透過第三方付款安排貢獻的收入不大，董事認為終止第三方付款安排不會對我們的業務、經營業績及財務表現造成任何重大影響。

第三方付款安排的法律影響

據我們的中國法律顧問告知，鑒於(i)於往績記錄期間及截至最後實際可行日期，我們的第三方付款安排並無違反中國適用法律法規的強制性規定；(ii)於往績記錄期間及直至最後實際可行日期，我們並未因第三方付款安排就任何洗錢活動、可能與洗錢有關的活動或任何相關調查遭受相關主管部門的任何調查、詢問或行政處罰；(iii)於往績記錄期間及直至最後實際可行日期，我們的第三方付款安排並未涉及與相關方之間的任何爭議或糾紛，包括但不限於追索權主張或退款要求；(iv)第三方付款安排的相關方已確認該等付款安排，第三方付款安排被視為構成《中華人民共和國刑法》所規定的洗錢罪的風險極低，第三方付款安排被相關方追索的風險較低。

基於上文所述，董事確認，據其所深知且基於已實施的「了解客戶」程序及內部控制措施，於往績記錄期間，(i)相關付款乃基於真實的相關交易及有效合約關係而作出；以及(ii)並無涉及與第三方付款安排有關的商業賄賂、洗錢、逃稅，或與本集團的現存或潛在爭議之情況。

於往績記錄期間及直至最後實際可行日期，據董事所深知及基於公開可得資料，所有相關客戶及根據第三方付款安排結算付款的指定第三方付款人，均為獨立第三方。

環境、社會及管治事宜

我們致力於可持續增長，將社會價值觀無縫融入我們的業務營運。我們致力於在我們的客戶群、合作夥伴以及參與供應鏈金融生態系統的更廣泛社區中，促進對環境、社會及管治（「ESG」）產生持久的積極影響。我們深知自身在環境保護和社會責任方面的義務，並知悉可能影響我們業務的潛在氣候相關挑戰。

業 務

ESG 管治

我們將ESG考量融入我們的日常業務營運及決策過程。董事會作為ESG事宜的最高管治機構，承擔監督和評估ESG相關風險與機遇的責任。透過董事會討論，董事會制定及採納ESG政策、策略及目標，以有效管理重大ESG風險。其亦對照該等目標監控我們的表現，並在出現重大偏差時根據需要調整ESG策略。此外，本公司ESG工作小組負責評估並就我們的環境、社會及管治政策及實踐提出建議。ESG工作小組支持董事會監督ESG舉措的制定與實施，以確保符合法律及監管要求，並在推進我們的ESG議程方面發揮著關鍵作用。此外，我們鼓勵各職能部門的僱員通力合作，共同推進ESG政策與目標的實施，同時持續追求卓越營運，以提升我們的ESG表現。

我們正在建立一套全面的內部政策，以指導我們的管理層處理ESG相關事宜。重點關注領域如下：

- **環境事宜：**我們的政策將涵蓋節能、碳減排以及處理廢氣、廢水及固體廢物。
- **社會事宜：**我們的政策涵蓋僱員健康及職場安全、產品質量及維護、僱員晉升、薪酬、福利及培訓。
- **管治事宜：**我們已為僱員制定商業道德準則，其中包括利益衝突、保密及反貪腐政策。僱員接受定期合規培訓，以加強內部監管合規及道德商業實踐。

[編纂]後，董事會確認，我們將持續關注並嚴格遵守上市規則附錄C1及附錄C2，同時全面遵守所有與ESG相關的規則與規例。此外，我們將每年刊發ESG報告，披露我們的重大ESG議題、風險管理實踐、目標的完成情況及整體表現。同時我們通過多種溝通渠道，確保與主要利益相關方之間的有效溝通。

ESG 風險管理

基於風險規避、風險降低、風險轉移及風險承擔的理念，我們積極緩解ESG風險的方針可處理潛在風險，亦把握提升ESG表現的機會，從而推動價值創造並為本公司及利益相關方締造可持續的未來。

我們已建立強大的內部ESG管理系統以提升我們的監察及預警能力、進行定期風險評估以確保及時識別潛在問題並制定具針對性的對策，旨在優化生產流程以最大程度減少環境污染、提升員工福利以強化社會責任，以及完善公司治理結構以提高透明度與問責性。透過系統性地整合這些措施，我們致力於降低ESG風險、促進可持續發展、增強投資者信心並鞏固企業社會責任，從而為業務的長期增長奠定堅實基礎。

業 務

ESG 機遇

我們亦認為，通過提升我們價值鏈內的ESG管理，我們能夠加強其抗ESG風險的能力，並通過可持續採購實踐符合國際客戶標準，藉此鞏固我們的品牌信譽。通過採用前瞻性技術策略及升級的管治模式，我們希望將自身的ESG能力轉化為對抗現有及潛在競爭者的差異化市場壁壘，推動長期增長。

環境事宜

我們致力於可持續發展戰略，旨在通過合理利用能源和資源，同時最大限度地減少消耗，實現環境、自然與社會的和諧統一。我們將嚴格遵守經營所在地區的環境保護法律法規。

我們將通過全面環境影響評估有系統性地識別潛在環境風險。該等計劃將概述應急程序、資源分配及角色和責任。我們亦將進行定期緊急演習，以提高僱員的準備意識，確保我們的風險預防能力與我們的業務擴充工作一致。

我們將積極培養綠色職場文化，鼓勵所有僱員採取低碳習慣。我們的措施或會包括實施精細的節水節電管理、推進廢物分類及推廣無紙辦公環境。此外，我們將為所有僱員提供環保意識培訓，在日常運營中推廣可持續的習慣，以減少我們的碳足跡，同時提升環境效益及組織效率。

指標及目標

本公司的業務主要以辦公室為主，根據現行中國法規，無需進行環境影響評估。我們所採用的方法無需大量文書工作和手工操作。這種轉變不僅減少我們的生態足跡，亦提升營運效率、透明度和生產力。我們的線上服務套件可減少實地出行需求及其相關的碳排放。

我們密切監控資源利用情況，並採取提高能源效率的措施。截至2023年、2024年及2025年12月31日止年度，我們的用電水平分別為1.02百萬千瓦時、2.31百萬千瓦時及1.25百萬千瓦時。

業 務

就溫室氣體排放而言，我們每年監控溫室氣體排放水平。我們採用溫室氣體議定書企業準則並根據聯交所環境關鍵績效指標匯報指引的參數計算的溫室氣體排放量及密度詳述如下：

範圍	釋義	示例	截至12月31日止年度		
			2023年	2024年	2025年
			(噸二氧化碳當量)	(噸二氧化碳當量)	(噸二氧化碳當量)
1	由我們直接擁有或控制的來源產生的所有直接排放 ⁽¹⁾	用於運營自有車隊的燃料	7.4	6.4	4.4
2	我們購買及使用的電力產生的所有間接排放 ⁽²⁾	我們辦公室所用的電力	536.0	1,212.2	658.5

附註：

- (1) 透過將年度柴油消耗量乘以柴油排放系數（約為每升 2.68 kg CO₂e），再除以 1,000，將千克換算為公噸計算得出。該排放系數乃根據中國生態環境部發佈之《企業溫室氣體排放核算方法與報告指南》釐定。
- (2) 透過將年度用電量（單位：千瓦時）乘以區域電網排放系數，並除以 1,000，將千克換算為公噸計算得出。就上海而言，採用華東電網平均排放系數（每千瓦時 0.524 kg CO₂e），該排放系數乃根據中國生態環境部發佈之《企業溫室氣體排放核算方法與報告指南》釐定。

[編纂]後，董事會將於各財政年度開始時根據上市規則的披露規定及其他相關規則及法規設定目標。相關目標將接受年度審查，以確保其持續符合本集團的需求。在設定 ESG 相關目標時，我們將不僅考慮過去的消耗和排放水平，還將綜合考量未來業務擴張、集團整體目標以及業內同行的信息。我們將採取全面而審慎的做法，力求在業務增長與環境保護之間取得平衡，以實現可持續發展。

我們致力於控制資源消耗和廢棄物產生的增幅。我們將根據我們的實際業務營運調整目標及指標，並密切監控我們的行動對實現該等目標的財務和非財務影響。我們深明準確測量範圍3排放量對於尋找解決方案應對排放而言至關重要。我們將建立測量與核算機制，以精確測算在我們眾多利益相關方之間，由我們服務所產生收益對應的溫室氣體排放當量。我們的目標是[編纂]後遵守上市規則下的披露要求。

業 務

氣候相關風險的潛在影響及緩解方案

我們須遵守中國多項氣候相關法律及法規。於整個往績記錄期間及直至最後實際可行日期，我們概無因違反環境法律或法規而面臨任何罰款或處罰。基於董事的所知及所信，我們預計未來不會面臨重大環境負債風險或產生顯著合規成本。鑒於我們的業務性質，我們的董事相信氣候變化不會對我們的業務營運造成重大影響。然而，近年來由氣候變化引發的極端天氣事件可能對我們的辦公室造成重大損害，導致臨時或長期關閉，並產生高昂的維修或更換費用。全球變暖若得不到遏制，可能導致氣溫升高，從而需要增加電力消耗並推高營運成本。從中長期來看，為應對氣候變化的潛在影響，可能會有立法和法規的增加。監管環境的這種轉變可能因業務合作夥伴的合規要求而直接或間接影響我們的營運，可能導致額外成本和限制，例如能源費用增加，以及處理污染物或危險廢物的成本增加。

我們將繼續識別、評估、管理及降低ESG相關風險。我們的方法包括但不限於：

- 監察相關法律、法規及行業標準，以定期評估我們對適用監管規則的遵守情況；
- 查閱和評估業內類似公司的ESG報告，確保及時識別所有相關的氣候相關風險；
- 管理層不時進行討論，以確保已識別及報告所有重大ESG議題；
- 與主要利益相關方討論重要ESG原則及慣例，以確保涵蓋重要方面；
- 組織ESG風險管理專項程序，以識別及管理ESG相關風險及機遇，並將其作為整體業務風險及機遇的一部分；
- 設定適當的目標，包括有關排放、污染及其他環境影響的目標，以減少排放及自然資源消耗；及
- 建立完善的業務持續性管理體系，以應對各類氣候相關風險，最大程度保證業務持續性。

我們將定期評估本集團面臨的風險，同時考慮當前和潛在風險，包括與ESG方面及氣候變化等顛覆性力量相關的風險。我們的董事會將評估該等風險，並在必要時尋求外部專家的意見，以檢討本集團的戰略、目標、內部控制，並作出任何必要的改進以減少風險。

董事會將監督我們的風險管理方法，包括氣候相關風險以及通過標準操作流程監控的風險，以確保採取適當措施。我們亦將致力於將ESG考量納入風險管理機制，以加強監控及緩解本集團範圍內的ESG相關風險。

業 務

減輕、轉移、接受或控制風險的決定受多種因素影響，如政府監管及公眾輿論。我們將把氣候相關議題，包括物理風險及轉型風險的分析，納入風險評估流程及風險偏好設定。倘該等風險和機會被視為重大，我們將在策略和財務規劃過程中解決有關風險。對ESG相關風險及本集團應對風險的表現進行年度審查後，我們可能會在必要時修訂及調整ESG策略。

於工作場所中應對氣候相關風險的措施

在我們致力於擁抱低碳世界的過程中，我們已實施若干內部環保政策以盡量減少碳排放。該等政策包括：

- 在我們的辦公室實施節能型照明；
- 通過在顯著區域展示節水和節能標識，提高員工對環境保護的意識，從而促進減少紙張浪費、節約用水和節能的行為；
- 強制執行在不使用時及離開場所前關閉燈光、設備及電子設備的做法；
- 利用節能照明解決方案，例如LED照明；
- 確保空調的使用得當且處於最佳溫度；及
- 持續激勵我們的僱員盡量減少列印硬拷貝，並在可行時推廣雙面列印。

社會事宜

我們優先促進多元化，並確保在本公司內的招聘、培訓、健康以及職業和個人發展中給予所有僱員平等和尊重的待遇。我們致力於保持工作與生活的平衡，營造積極的工作環境，為每個員工提供平等的工作機會。為確保遵守有關社會事務的適用法律法規，我們的人力資源部門定期審查及調整我們的政策。該等調整於與我們的法律顧問協商後方會進行，以適應勞動與安全法律法規的任何重大變更。

僱傭

我們遵守我們經營所在地區的勞動管理法律法規。我們已制定僱員招聘管理的政策及僱員手冊，以確保遵循合法的僱傭實踐。根據中國相關法律法規，我們需要為僱員就各種社會福利計劃作出供款，包括社會保險和住房公積金。

業 務

發展及培訓

我們秉持以人才為核心的理念，注重以人為本的實踐、團隊協作以及持續的專業發展。我們提供清晰明確的職業晉升機會，以及一系列旨在提升僱員技能和能力的培訓計劃。請參閱本節「我們的僱員」。

職業健康與安全

我們堅持為僱員提供健康和安全的工作環境。於整個往績記錄期間及直至最後實際可行日期，我們於所有重要方面均遵守職業健康與安全法律法規。雖然我們預計與遵守當前及未來健康及安全法律相關的成本不會大幅增加，但要求的變化可能會影響我們準確預測該等成本的能力。

反貪腐

我們遵守經營所在司法管轄區的反貪腐法律法規，並已制定制度及守則，如僱員商業道德規範以及僱員申訴投訴制度。該等制度明確界定商業道德的各個方面。此外，我們每年組織自檢匯總及管理改善，持續監測控制貪腐及商業道德風險，保障本公司健康運行。

風險管理及內部控制

我們的董事會及高級管理層肩負設計及監察內部控制架構的執行及有效性的責任。該架構結構嚴謹，可確保我們持續遵守規管業務活動及企業管治的相關法律法規要求，從而避免不合規情況的再次發生。我們堅信，現有的內部控制機制及程序在覆蓋範圍、可行性及運作效能方面均充足。

為證實此信念，我們已聘請一位內部控制專家（「**內部控制顧問**」），對我們集團的內部控制流程、系統及協議的充分性與效率進行全面評估。該等評估涵蓋我們營運的各個方面，包括管理監督、財務報告、信息披露、信息技術治理、企業營運、企業管治架構、監管合規以及風險管理策略。內部控制顧問所進行評估的初步結果已得到細緻檢討。經此檢討，我們的董事會確認已認真考慮內部控制顧問提交的所有重要建議。針對該等推薦意見，我們承諾在[編纂]前採取一切必要整改措施，以糾正組織架構中已發現的任何不足。

於我們的日常業務活動中，我們固有地承受一系列風險，包括營運風險、市場風險及財務風險。認識到該等風險後，我們堅信，實施健全且適應性強的風險管理策略對我們的持久成功至關重要。我們正是透過採取措施降低風險，確保我們的營運免受潛在不利因素的影響，從而保障我們的競爭優勢及財務穩定性。

業 務

為有效管理風險，我們將採取或已實施以下措施：

- 我們的董事會負責全面評估我們營運的固有風險，確保所有具重大風險影響的重大決策均經董事會審查及同意；
- 我們的管理團隊致力於密切關注市場趨勢；
- 我們執行嚴格的IT控制，大幅降低IT系統發生故障的可能性，保障我們營運的完整性；
- 為吸引及挽留專業技術人才，我們定期對管理層及僱員的薪酬架構進行評估及調整，確保其保持競爭力，並與我們的戰略發展相一致；
- 我們的董事對我們的流動資金及財務健康狀況進行嚴格監督，於認為必要及有利的情況下，隨時準備獲取融資，支持我們的業務活動及擴張計劃；及
- 我們已成立由全體獨立非執行董事組成的審核委員會，以審閱及監督我們的財務申報程序及內部控制系統。

我們的內部網絡安全措施

我們優先保障自身網絡安全以保護公司資產。我們實施多層次的策略以保護我們的系統及數據。截至最後實際可行日期，我們已獲得ISO:27001信息安全管理體系認證，彰顯我們系統的實力。透過將以下技術措施與安全意識文化相結合，我們相信我們可維持穩健且韌力十足的信息技術基礎設施，以保障我們的業務營運：

- **嚴格的訪問控制及認證：**我們將實施訪問控制及認證機制，確保僅有獲授權人員可以訪問敏感系統及數據。基於角色而定的訪問控制將根據用戶在機構內擔任的角色限制訪問，從而減少未經授權訪問的風險。定期審核及審查訪問權限能夠有助維持訪問控制政策的完整性。
- **定期更新及補丁：**保持我們的軟件和硬件實時更新十分重要。我們將透過更新及應用補丁防範已知漏洞，降低因過時軟件而遭受網絡攻擊的風險。我們的專責團隊將監察有否來自供應商的近期更新及補丁，並確保及時應用有關更新及補丁。此外，我們將於部署前在受控環境下測試更新，以確保更新不會中斷我們的運營。

業 務

- **網絡監控及審核：**持續監控及審核網絡活動可幫助我們發現可疑活動並迅速作出反應。我們將使用監控工具追蹤網絡流量並識別可能表示存在安全威脅的異常情況。實時告警可讓我們的安全團隊在檢測發現潛在問題時及時採取行動。定期審核網絡日誌可讓我們深入了解過去的活動，並有助識別可能預示數據洩露的模式。
- **數據加密：**我們將對傳輸中及靜態的敏感數據均進行加密，以防止未經授權訪問。加密將數據轉換為編碼格式，只能使用正確的解密密鑰進行破譯，確保即使數據被攔截，仍然不可讀。我們將使用行業標準協議來保護我們的數據，並對所有通訊渠道，包括電子郵件及文件傳輸，進行加密。我們將定期審查我們的加密實踐以管理不斷變化的威脅。
- **防火牆及入侵檢測系統：**實施防火牆及入侵檢測系統將幫助我們防止及檢測未經授權的訪問企圖。防火牆將充當我們內部網絡與外部威脅之間的屏障，根據預定義的安全規則過濾輸入及輸出流量。該等系統將監控網絡流量是否存在可疑活動，並在檢測發現潛在威脅時發出告警。我們定期更新防火牆規則及入侵檢測系統特徵庫，可確保其能夠有效抵禦新興威脅。
- **僱員培訓：**我們將定期為僱員舉辦安全意識培訓，以確保彼等了解最新的安全威脅及最佳實踐。培訓計劃涵蓋網絡釣魚、密碼管理及安全使用互聯網等主題。我們旨在通過教育僱員如何識別及應對安全威脅，降低人為錯誤的風險，而人為錯誤通常是安全漏洞的重要因素。我們亦將進行模擬網絡釣魚練習，以測試僱員的警覺意識，並加強培訓，促進組織內部建立安全意識文化。
- **備份及災難恢復：**我們將定期進行數據備份，並測試我們的災難恢復計劃，以確保在發生安全事件時的業務連續性。備份可存儲在安全的異地場所，以防因硬件故障、網絡攻擊或自然災害導致數據丟失。我們的災難恢復計劃將概述在事故發生後快速有效恢復運營的步驟。我們將定期測試該等計劃的成效及讓團隊作好應對任何事故的準備，將宕機和數據丟失的情況降至最低。