Report on Cybersecurity Competitiveness of China (Hong Kong) (Phase I)

（2026 年 3 月）

Report on Cybersecurity Competitiveness of China (Hong Kong) (Phase I)

（2026 年 3 月）

数字安全是指，在全球数字化背景下，合理控制个人、组织、国家在各种活动中面临的数字风险，保障数字社会可持续发展*的政策法规、管理措施、技术方法等安全手段的总和。

这里的风险，不再局限于围绕数字化资产的攻防对抗，还包括了数字资产所承载业务的稳定性、连续性和健康性。这里的安全不再特指有意还是无意，天灾还是人祸，保安还是保险，而是更为广义的安全状态（SecSafe）。

*“世界环境与发展委员会出版的《我们共同的未来》报告中，将可持续发展定义为：“既能满足当代人的需要，又不对后代人满足其需要的能力构成危害的发展。”

——数世咨询，2023 年 11 月

以安全能力、数字资产和数字活动为三元素，以数据安全为核心目标，即三元一核的“数字安全三元论”。

“数字安全三元论”由“网络安全三元论”（数世咨询于 2020 年提出）更新迭代而来，旨在匹配数字中国建设的进程，保障数字基础设施稳定、可持续运行，保障数据有效流动、激发数据要素价值。

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构 . 网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

数世咨询

数世智库 数字安全能力研究院

Report Information

Report Direction: Industry Research

Report Name: China (Hong Kong) Cybersecurity Competitiveness Report

Report ID: DWC_20260301

Lead Analyst: Jin Huichao, Strategic Analyst, Digital World Consulting (DWC)

Analysis Team: Digital Security Research Institute, DWC

Report Reviewer: Li Shaopeng, Chief Analyst, DWC

Executive Summary

The core content of this report is a summary and analysis of information obtained by Digital World Consulting through industry research and professional interviews, focusing on the current state and development of Hong Kong's cybersecurity industry. It is part of the China Cybersecurity Industry Going Global Research series.

Since 2022, Digital World Consulting has initiated research and investigation into the globalization of China's cybersecurity industry and has compiled a series of reports for relevant government departments. This report is the first publicly released research report and serves as the inaugural edition of the China (Hong Kong) Cybersecurity Competitiveness series.

Research Methodology

Selection Criteria for Survey Subjects:

Survey participants and recommended companies met the following criteria.

- **Legal operation:** possess valid business licenses and are in normal operation in Hong Kong

- **Core business presence**: have established core business operations in Hong Kong with verified success cases

- **Intellectual property:** core products carry independent intellectual property rights with demonstrated technical leadership in at least one specialized domain

Selection Criteria for Recommended Products:

- Core products have completed localization adaptation for the Hong Kong market

- Products possess functional and performance capabilities sufficient to replace comparable international offerings

- Companies maintain a broad user base and strong reputation in Hong Kong

- Companies possess established track records with leading clients in China

Background

Hong Kong, as an important window for China's opening up to the outside world and as an international center for finance, trade, and shipping, has cybersecurity that is not only crucial to local social stability and economic prosperity, but also directly related to the country's overall security and development. Moreover, given its unique role in connecting the domestic and international spheres and its international advantages, it can actively participate in global cyberspace governance, serving as an ideal platform for China to demonstrate its responsibility as a major power and showcase its strength in security technologies.

To enhance Hong Kong's cybersecurity capabilities, the key lies in strengthening cyber governance and promoting the application of secure, autonomous, and controllable technologies. Expanding the influence of China's security technologies hinges on gaining a stronger voice in global cyberspace governance and advancing the international expansion of domestic cybersecurity enterprises.

The core objective of this report is to act as an independent third-party research body

to build a bridge for communication between Hong Kong and mainland enterprises, facilitate the overseas expansion of cybersecurity companies, and promote Chinese cybersecurity solutions. In addition, through in-depth insights into the cybersecurity industry, the report aims to support government agencies and Chinese-funded enterprises in accelerating the localization (domestic substitution) process, while also providing a third-party reference for foreign enterprises in their security and compliance efforts.

Overview of Chinese-funded Cybersecurity Industry

Localization Replacement

Based on the institutional advantages of "One Country, Two Systems," as well as a highly free and open economic system and globally leading financial and professional service capabilities, Hong Kong has become the most internationally oriented region in China and a strategic pivot for the country to connect with the world and promote high-level opening-up. Therefore, the business systems of Hong Kong government departments, public utilities, and local enterprises predominantly operate on IT equipment and information systems from foreign brands.

With the continuous rise of China comprehensive strength, especially through the advancement of Chinese-style modernization, information systems from Chinese brands have gradually reached functional and performance metrics comparable to international brands, and even demonstrate innovation and leadership in many aspects. Through comprehensive considerations of economy, technology, and politics, government departments, public utilities, and local enterprises in Hong Kong have officially initiated the localization replacement process. In recent years, the rapid changes in global geopolitical and economic situations have accelerated the localization replacement process for cybersecurity products and services.

The first batch of Chinese-funded cybersecurity enterprises to commence core business in Hong Kong, represented by Huawei, Sangfor, and Hillstone Networks, are the trailblazers of the Chinese-funded cybersecurity industry, with operating histories exceeding 10 years. Around 2019, another batch of Chinese-funded cybersecurity enterprises arrived in Hong Kong, embarking on the path of international development. Starting from 2023, more Chinese-funded cybersecurity enterprises have entered the Hong Kong market, registering local companies, recruiting employees, and formally accepting the stringent selection by Hong Kong clients, facilitating the smooth advancement of the localization replacement process.

With the formal implementation of the "Protection of Critical Infrastructure (Computer Systems) Ordinance" on January 1, 2026, this presents a historic opportunity for Chinese-funded cybersecurity enterprises intending to conduct global business. It is believed that as more Chinese-funded cybersecurity enterprises conduct business in Hong Kong, the localization replacement process will be significantly accelerated, the global influence of Chinese-funded cybersecurity enterprises will be enhanced, China cybersecurity strength will be fully demonstrated, and Hong Kong will become a bridgehead for the global development of Chinese-funded cybersecurity enterprises.

Market Overview

According to incomplete statistics, the Hong Kong cybersecurity market is estimated to reach approximately USD 343 million in 2025. However, Chinese-funded cybersecurity enterprises account for less than 10% of this market, with revenues below USD 30 million. This indicates a massive potential for growth in the Hong Kong market, making it highly attractive to these enterprises. Furthermore, based on this survey and an analysis of market performance and operational status, achieving a total revenue of USD 1.5 million has emerged as a key metric for evaluating the initial operational success of Chinese-funded cybersecurity firms.

At the current stage, the customer base of Chinese-funded cybersecurity enterprises is primarily concentrated in sectors such as government, public utilities, finance, telecommunications operators, and the internet industry. The main drivers for localization (domestic substitution) are largely derived from regulations, policies, and group-level institutional requirements, often combined with economic considerations such as cost-effectiveness. In addition, a smaller portion of demand arises from customized requirements driven by specialized innovation projects.

At the overall demand level, the Hong Kong cybersecurity market is primarily focused on products such as perimeter protection, threat detection, endpoint management and control, and data loss prevention, as well as services including security planning and attack-defense exercises. Most enterprises have a strong awareness of the importance of cybersecurity, and during procurement, their final evaluation is typically based on the actual performance of products in comprehensive testing—covering performance, functionality, and alignment with business requirements.

Starting from 2026, based on the above products, Chinese-funded cybersecurity enterprises will also accelerate the promotion of security data analysis, situational awareness, and SaaS-based security capabilities, further strengthening the comprehensive competitiveness of Chinese-funded cybersecurity enterprises in Hong Kong.

Localization Adaptation

Given Hong Kong's fully internationalized environment, Chinese cybersecurity enterprises undertaking core business operations in the region have implemented comprehensive localization across products, services, and operational models. This extends far beyond simple linguistic translation to encompass deep adaptation of IT culture, industry scenarios, and commercial practices.

IT Culture Adaptation

- **Empowering self-service troubleshooting:** Technical documentation is upgraded to include detailed functional descriptions, step-by-step operating procedures, and troubleshooting guides, enabling users to resolve issues independently.
- **Maintaining product reliability:** Ensuring product stability and functional effectiveness to avoid increasing users' security liability exposure due to product failures.
- **Third-party evaluations:** Engaging independent third-party institutions for testing and assessment, helping users objectively understand products' genuine technical capabilities and effectively enhancing brand recognition.

Industry Scenario Adaptation

- **Dedicated R&D headquarters support:** Matching IT infrastructure environments and actual business processes through specialized technical professional support.
- **Full on-site POC support:** Technical professionals fully cooperate with customers' complete proof-of-concept testing, with issues promptly fed back.
- **Global IT environment compliance:** Upgrading product compatibility with mainstream international information systems based on customers' actual IT environments.
- **Business process-aligned security modifications:** Adapting security architecture and data processing functionalities to align with actual customer business workflows.
- **Expanded local technical support personnel:** Responding to users' immediate needs with locally deployed support teams.

Commercial Cooperation Adaptation

Unlike the mainland model of **"relationships → price → effectiveness,"** Hong Kong follows a **"effectiveness → price → relationships"** paradigm:

- **Accurate self-representation:** Marketing materials are consistent with actual product and service capabilities — no overstatement.
- **Privacy and compliance:** Strict adherence to relevant regulations, institutional constraints, and commercial rules, including channel and integrator considerations.

- **Mutual Growth:** Prioritizing the success and profitability of channel partners and integrators.
- **Frontline user experience:** Prioritizing the experience and feedback of frontline personnel.
- **Contractual integrity:** Strictly delivering services in accordance with contractual terms.

Domestic Substitution Recommendations

Strategic Significance

Domestic substitution in cybersecurity holds strategic importance in coordinating domestic and international considerations, fully leveraging regional security synergies, accelerating the construction of a new development pattern, and steadily enhancing the influence of independently developed security technologies. Such substitution is not an overnight process — guided by the core principle of coordinating development with security, it progresses through key node replacement, parallel operation validation, scenario-based substitution, and large-scale substitution across distinct phases.

The current stage of Hong Kong's cybersecurity environment, marked by the implementation of the Protection of Critical Infrastructure (Computer Systems) Ordinance, is at the critical node substitution stage. Cybersecurity scenarios suitable for prioritized localization substitution exhibit the following characteristics:

High standardization and Usage Familiarity

Many Chinese cybersecurity enterprises have operated internationally for years, possessing globally competitive technical capabilities. Their core products adapt to international standards and align with local Hong Kong user workflows. Adopting these products for localization substitution incurs no extra communication or learning costs, allowing local users to transition seamlessly in their daily work.

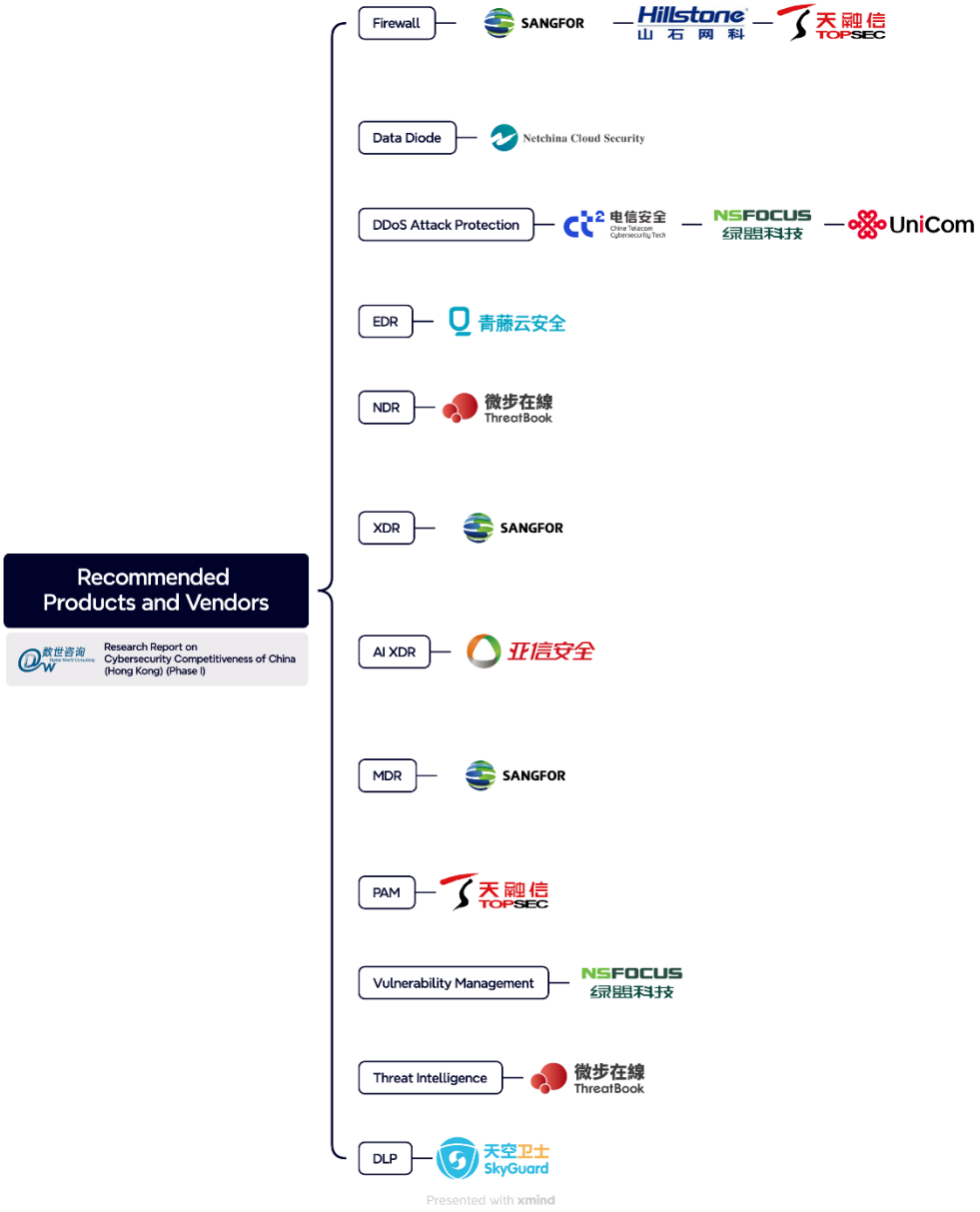
Mature Mainland technology with Proven Value

Based on China's massive digital market, Chinese cybersecurity enterprises' technical capabilities cover the vast majority of global security scenarios — and have produced several uniquely Chinese security use cases. Security products already proven in large enterprise (group/headquarters) deployments on the mainland, validated by practical value and reinforced by organizational mandates, represent optimal candidates for substitution

Recommended Products and Companies

Drawing on an analysis of the current landscape and future trends within Hong Kong's local cybersecurity market, this report identifies key sectors ripe for prioritized domestic substitution. Based on comprehensive research and a rigorous selection process, we hereby recommend the following products and enterprises.

(Market segment — Target international benchmark products — Key differentiators)



Next-Generation Firewall (NGFW)

SANGFOR

Sangfor Technologies (Hong Kong) Limited

Primary competitive target: Fortinet FortiGate

Key differentiators:

Capability	Detail
Built-in Full-Feature Integration	Native WAF and IPS integrated directly within the firewall, including passive vulnerability scanning.
AI-Powered Threat Detection (Engine Zero)	Proprietary Engine Zero AI engine leveraging deep learning for static and dynamic analysis. Ransomware variant and unknown malware interception rates demonstrated exceptional results in live testing — rated **CyberRatings AAA certified**.
SOC Lite Visualization Center	Downstream deployment of SOC concepts within the firewall console. Displays traffic reports and auto-generates asset-based risk assessments and remediation recommendations.
Regulatory Compliance & Forensics	Enhanced local storage and log search capabilities tailored to Hong Kong's common log retention and compliance audit requirements. Supports detailed application behavior auditing (social media, cloud drive upload details). One-click generation of compliance-ready security summary reports.
Local Expert Technical Support	Exceptionally strong in-house technical team in Hong Kong. During complex policy migration, red/blue team exercises, or incident response, response speed and communication effectiveness are substantially superior.

Hillstone 山石网科

Hillstone Networks Co., Ltd.

Primary competitive target: Fortinet FortiGate

Key differentiators:

Capability	Detail
A-Series Firewall (1U Design)	Compact form factor, low power consumption, high-density ports — up to 20× 10GE and 4× 100GE optical ports with multiple expansion interfaces. SSL hardware decryption engine onboard.
High-End Series Performance	Hardware acceleration engine dedicated to offloading CPU pressure under high traffic loads. Maximum throughput: **320 Gbps**; small packet performance: **140 Gbps**; latency as low as a few microseconds.
X-Series Data Center Firewall	Innovative fully distributed architecture with proprietary intelligent traffic distribution and resource management algorithms. Linearly scalable concurrent and new connection performance across multiple modules.
Comprehensive Threat Detection	Built-in advanced threat detection engine with intrusion prevention based on deep application analysis, protocol inspection, and attack mechanism analysis. Cloud sandbox integration for detecting malicious intrusion attempts via web and email.
NAT Port Multiplexing	Single IP address NAT concurrent session capacity increased by up to **16**×, effectively resolving access bottlenecks caused by limited address resources.
Threat Intelligence Integration	Hillstone Cloud Intelligence Center integrated with third-party intelligence feeds, providing full-lifecycle protection ("pre-attack / during-attack / post-attack").
Intelligent Policy Operations	Full lifecycle management covering policy deployment, management, optimization, and operations.
Network Adaptability	Supports RIP, OSPF, IS-IS, and BGP dynamic routing protocols with automatic dynamic routing table adjustment. Outbound traffic dynamic probing, inbound SmartDNS, and intelligent link load balancing across multiple links.

天融信 TOPSEC

Topsec Technologies Group Inc.

Primary competitive targets: Palo Alto Networks, Check Point

Key differentiators:

Capability	Detail
Pan-Domain Security	Platform-based convergence of network security, application security, web security, and data security functions. Provides network detection and response, converged security protection, advanced threat detection, asset security analysis and remediation, and attack chain visualization.
AI Detection and Protection	Real-time detection and protection against advanced threats including DGA (Domain Generation Algorithm), covert channels, and malicious encrypted traffic.
Cloud-Network-Endpoint Coordination	Cloud-network-endpoint multi-dimensional synergy enhances perception and analysis of network assets and security events, improving overall network protection levels.
Virtualization and Cloud-Native Architecture	Virtualization and cloud-readiness capabilities enabling rapid deployment for new business scenarios and extended border protection coverage.
Deep Asset Security	Asset-centric approach deeply enhancing network asset risk and anomalous behavior analysis capabilities.
LLM Security Protection	Built-in pre-trained security detection models providing AI recognition, LLM session parsing, application and API protection, prompt injection prevention, and value-based content filtering — safeguarding LLM application security and controllability.
Intelligent Security Operations	Suite of intelligent operations management tools including security monitoring, data center management, security center, security policy management, centralized management, and third-party management interfaces for comprehensive network situational awareness and automated, visualized security operations.

Data Diode (Unidirectional Security Gateway)

Netchina Cloud Security

NetChina Cloud Security Group Co. Ltd.

Primary competitive target: Waterfall Security Solutions (Unidirectional Security Gateway); ST Engineering CyberTransporter

Key differentiators:

Capability	Detail
Physical Unidirectional Transmission	Dual-host architecture combined with optical unidirectional transmission characteristics ensures physical unidirectionality of data flow.
Comprehensive Business Support	Port data import, POST push, KAFKA proxy, and other application data import methods. Supports FTP/SAMBA and other protocol-based services and file synchronization.
File Synchronization	Supports both local server and external import file transfer modes, enabling unidirectional file synchronization.
Database Synchronization	Supports unidirectional data synchronization for Oracle, SQL Server, MySQL, and other mainstream databases.
Management and Monitoring	Optional independent/in-band management; customizable interfaces with icon-based and function-based display; SNMP monitoring; NTP time synchronization; traffic visualization; and multi-level log forwarding.
Enhanced Security	Integrated antivirus, anti-scanning, anti-attack, and ARP binding security components, enhancing both device security and business data security.
Scalability	Supports series deployment at network boundaries, combinable with secure exchange platforms to build unidirectional or dual-unidirectional security boundaries.
Operational Ease	Configuration wizard, backup/restore, email alerts, online packet capture, multi-dimensional network diagnostics — simplifying operations and management.

DDoS Attack Protection

China Telecom Cybersecurity Technology Co., Ltd

Primary competitive target: Radware DDoS Protection; AWS Shield (Standard/Advanced)

Key differentiators:

Capability	Detail
Global Traffic Monitoring	Full-network monitoring integrating threat intelligence across the entire network. Precise traffic monitoring with rapid alert triggering for timely response to network anomalies.
Global Attack Protection	Proprietary globally distributed **130+** near-source scrubbing nodes; **22 Tbps+** protection capacity; distributed architecture for handling large-scale volumetric attacks.
Full-Scope Analysis and Attribution	Based on authoritative China Telecom operator traffic data. Attribution precision to local IDC. Immune to false source IP addresses. Supports law enforcement with credible attribution evidence, strengthening clients' network security posture.
Multi-Tier Coordination	Multi-tier architecture integrating backbone near-source, IDC near-destination, international gateway, and metropolitan network near-site coordination. Effectively defends against domestic and international scan sweeps, pulse, and hybrid attacks.
AI Profiling	Based on the Jianwei large language model. Deep mapping of botnets — extracting botnet controller, compromised host, and access behavior information. LLM-generated learning model library from botnet sample capture, analysis, and reverse engineering. Generates behavioral profile data for malicious attack originators.
Cloud-Network-Edge-Endpoint Unified Management	Integrates with endpoint SASE (Yunmai), edge security gateways, and network security resource pools via the MSSP situational awareness platform for modular unified management.

UniCom

China Unicom Global Limited (UniCom)

Key differentiators:

Function	Detail
Attack Monitoring	Real-time monitoring of traffic anomalies across Unicom's network based on multi-dimensional traffic analysis models. Provides DDoS attack notifications, traffic trends, anomaly analysis, and attack attribution.

Function	Detail
Traffic Scrubbing	Near-source traffic diversion and same-path reinjection through Unicom's full-network scrubbing node deployment. Leading-edge volumetric DDoS mitigation at the Unicom backbone level.
Traffic Blocking	Full-network or regional traffic blocking toward target IPs via Unicom's routing capabilities. Prevents internet export bandwidth congestion from impacting unaffected services, preserving overall bandwidth resources.
Self-Service Platform	Customers independently submit scrubbing or blocking protection tasks, configure task parameters, and review attack reports via the DDoS self-service portal.
Security Operations Center (SOC)	24/7 real-time monitoring and continuous support in Mandarin, Cantonese, and English. Highly elastic, flexibly providing customized security operations services tailored to specific customer requirements.

NSFOCUS 绿盟科技

NSFOCUS Technologies Hong Kong Ltd.

Primary competitive targets: NetScout Arbor Sightline / Arbor Cloud; Radware Defense Pro / Cloud DDoS Protection Service

Key differentiators:

Capability	Detail
Specially Designed Intelligent Defense Algorithms	Multi-layered intelligent defense algorithm design combining static filtering rules and dynamic defense algorithms. Ensures accurate DDoS attack filtering, minimizing false positives and negatives, effectively countering complex attack campaigns.
Full-Network, High-Volume Attack Detection	DFI/DPI dual-stack detection technology — satisfies 100 Gbps-level traffic detection requirements for carriers and IDCs, as well as high-precision, high-timeliness monitoring for finance and government enterprises.
Cloud Reputation Database	Integration with NSFOCUS professional cloud-based NTI (NSFOCUS Threat Intelligence) data. Enables detailed attack source IP inquiry and one-click bot filtering. NTI platform integrates bot attack source data from all NSFOCUS products and data mining teams — achieving efficient combination of intelligent scrubbing and simplified operations.

Capability	Detail
Cloud-Local Integrated Protection	Self-built Cloud DPS international cloud scrubbing service with TB-level protection capacity. Provides large-volume scrubbing backup for local scrubbing solutions, helping customers form a cost-optimal three-dimensional hybrid scrubbing architecture ensuring business security under large-scale attacks.
Value-Added Service Ready	Integrated value-added operations platform for carriers, IDCs, and public cloud providers — enabling customers to expand new business models by offering DDoS attack protection value-added services to end users.

Endpoint Detection and Response (EDR)

青藤云安全

Beijing Shengxin Network Technology (Hong Kong) Limited

Primary competitive targets: CrowdStrike EDR; Palo Alto Networks EDR

Key differentiators:

Capability	Detail
Highly Integrated Intrusion Detection, Risk Discovery, and Response	Unifies intrusion detection, vulnerability scanning, patch and weak password checks, compliance baseline, and automated response within a single platform. Eliminates multi-tool complexity — security operations efficiency exceeds comparable products.
Industry-Leading Asset Identification and Risk Visualization	Auto-identifies **180+** asset types and **2,000+** behavioral and application classifications. Constructs asset-risk correlation graphs supporting risk tracing and attack chain analysis.
Lightweight Agent Design	Minimal agent resource footprint. Suitable for long-term deployment on databases, transaction systems, and high-concurrency servers without impacting business performance.
Verified at Hyper-Scale Production Environments	Unified management and real-time protection of **300,000+** hosts in a single customer environment — demonstrating mature large-scale deployment, centralized management, and performance scheduling capabilities.

Capability	Detail
Mature Automated Response and Policy Orchestration	Supports automated remediation including process termination, network isolation, host isolation, and policy linkage — reducing manual intervention in large-scale environments.

Network Detection and Response (NDR)

ThreatBook Co., Limited

Primary competitive targets: Darktrace Network; Trellix NDR

Key differentiators:

Capability	Detail
Throughput and Encryption Analysis	Supports **20 Gbps** traffic mirroring. Encrypted traffic analysis with **>99%** encrypted communication identification rate.
Precision Detection	Bidirectional full-flow traffic detection combined with ThreatBook's industry-leading threat intelligence, multi-dimensional traffic feature analysis, and scenario-specific machine learning models for in-depth attack behavior analysis. Automated determination of attack success/failure, minimizing alert fatigue. Long-term tracking data on hundreds of APT groups enables timely and accurate detection of targeted attacks.
Combat-Oriented Approach	Comprehensive attack surface mapping via traffic analysis from the attacker's perspective — identifying all possible attack entry points. Intelligent identification of web and non-web login portals; login behavior auditing; weak password and brute-force detection; business API and upload interface risk identification. Non-intrusive passive listening imposes no pressure on servers or network bandwidth, helping security teams establish comprehensive asset baselines.

Capability	Detail
Closed-Loop Response	**99% effective** passive blocking and automated integration with third-party devices. Significantly shortens threat response times. Automated forensic processes enhance organizational attribution capabilities and enable better remediation of security weaknesses exposed during attack paths. East-west traffic and internal asset risk visualization. Full-spectrum threat event analysis from defensive, external attack, internal tracing, and alert perspectives.

Extended Detection and Response (XDR)

Sangfor Technologies (Hong Kong) Limited

Primary competitive target: Palo Alto Networks Cortex XSIAM

Key differentiators:

Capability	Detail
Local Presence and Response	Exceptionally deep local service team in Hong Kong. Compared with Cortex XSIAM's reliance on global support systems, Sangfor scores higher in Gartner Hong Kong evaluations for "Service and Support" and "Delivery Effectiveness."
Security GPT Native LLM Capability	Deeply integrated Security GPT demonstrates superior understanding of Chinese and Asian enterprise office language environments. Generates analytical conclusions through conversational interfaces — not merely displaying complex raw logs.
Native Endpoint-Network Deep Integration	Many Hong Kong enterprises already deploy Sangfor firewalls or endpoint products. XDR achieves zero-latency, second-level integration with these native components.
Intuitive Business-Context Visualization (Attack Storyline)	Prioritizes attack storyline visualization — automatically stitching fragmented alerts into logically coherent full attack sequences directly correlated with specific business assets.

Capability	Detail
Lower TCO and Investment Protection	XSIAM's bundled architecture incurs extremely high storage costs and subscription fees. Sangfor XDR provides more flexible deployment models (SaaS or on-premises) with exceptionally strong compatibility with existing Sangfor devices.

AI XDR

Asiainfo Security Technologies Co., Ltd.

Primary competitive target: CrowdStrike Falcon Insight XDR

Key differentiators:

Capability	Detail
One-Point Detection, Network-Wide Remediation	AI-native data-driven detection framework deeply integrating cloud, network, edge, and endpoint data collection and remediation capabilities. A single micro-anomaly auto-correlates and extends across all customer network assets, forming a "global threat perspective" — ensuring threats are completely intercepted before proliferation. With customer consent, threats auto-upload to cloud threat intelligence, achieving true "single-point detection triggers network-wide remediation."
Extended Detection, Comprehensive Empowerment	Asset management enabling complete lifecycle asset inventory — making the enterprise security asset baseline transparent. Vulnerability identification as a security "health check" — precisely discovering vulnerabilities, weak passwords, high-risk ports, and other defensive gaps. Local cloud-based massive malware file library for rapid file threat comparison. Local TI (Threat Intelligence) accumulating proprietary threat intelligence, strengthening atomic-level detection and analysis.
Multi-Dimensional Orchestration, Precise Closed-Loop	Comprehensive coverage of terminals, IPs, domains, files, processes, startup items, services, and scheduled tasks. Constructs a three-dimensional defense network of "precise terminal clearance + comprehensive network blocking. Truly complete security closed loop — ensuring threats are completely eradicated.

Capability	Detail
AI-Augmented, Intelligent Evolution	AI-powered security operations intelligence upgrade. Provides data query statistics, security Q&A, alert/event interpretation, asset interpretation, AI noise reduction, and assisted remediation — reducing professional skill requirements and substantially saving analysis time. Advanced AI techniques including semantic noise reduction, asset-contextual noise reduction, and endpoint-network fusion analysis — precisely reducing noise. Liberates security teams from massive invalid alerts, focusing on critical attack events, significantly reducing operations costs.

Managed Detection and Response (MDR)

Sangfor Technologies (Hong Kong) Limited

Primary competitive target: Sophos MDR

Key differentiators:

Capability	Detail
Security GPT-Powered Interactive Expert Services	Deeply integrated Security GPT. Cloud experts not only provide analytical conclusions but also answer user questions immediately in natural language through AI assistants.
Localized Expert Monitoring Adapted to Hong Kong Customers	Dedicated technical support and security services teams stationed in Hong Kong. Sophos's service centers are primarily distributed in Europe and the Americas, introducing cultural and timezone limitations.
Endpoint-Network-Cloud Deep Orchestrated Closed-Loop Response	Strength derived from control over Sangfor's own integrated product suite (firewalls, EDR, etc.). Upon threat discovery by experts in the cloud, cross-device precision coordinated blocking can be executed.

Capability	Detail
Asia-Threat-Environment Proactive Threat Hunting	Threat intelligence database holds deeper accumulated knowledge of Asian, particularly Greater China, hacker organizations, exploit utilization, and targeted attack scripts.
Intuitive Service Results Visualization Dashboard	Operations visualization center aligned with management-level aesthetics. Not only displays virus interception counts but also quantifies response time (MTTR) and business risk trends.

Privileged Access Management (PAM) / Jump Server

Topsec Technologies Group Inc.

Primary competitive target: CyberArk PAM

Key differentiators:

Capability	Detail
Account Management	Master and subordinate account management. Master accounts are user accounts; subordinate accounts are original IT system accounts. The master/subordinate account approach separates identity and authorization, enhancing identity authentication and system authorization reliability — fundamentally resolving account management 混乱. Provides guarantee for authentication, authorization, and auditing.
Identity Authentication	High-strength authentication to enhance access security. Supports local authentication and integration with third-party authentication servers (AD domain, LDAP, RADIUS). Supports OTP dynamic tokens, SMS, USB Key, digital certificates, and facial recognition for dual-factor strong authentication — ensuring identity reliability.
Centralized Authorization	"Centralized" refers to logical centralization, not physical centralization. Unified authorization interface provides both coarse-grained authorization (e.g., which assets a user can access) and fine-grained authorization (e.g., restricting specific user operational behaviors).

Capability	Detail
Operational Auditing	Personnel operational records maintained as logs viewable by administrators. Audits account management, authentication, account assignment, permission assignment, and account usage (login, resource access, operational behaviors) — all operations traceable.
Automatic Password Rotation	Supports automatic password changes for Windows, Linux/Unix, databases, and network devices. Manual or periodic auto-execution with customizable password complexity. Solves time-consuming and error-prone multi-asset, multi-account password management challenges. Enables intervention-free periodic batch password changes during asset operation — effectively implementing organizational strong password policies, enforcing security management systems, reducing administrator workload, and enhancing asset security.

Vulnerability Management

NSFOCUS 绿盟科技

NSFOCUS Technologies Hong Kong Ltd.

Primary competitive targets: Tenable Nessus Pro / Web App Scanning / Security Center / Nessus Vulnerability Management; Qualys Vulnerability Management (VMDR) / Web Application Scanning (WAS) / Compliance Solutions

Key differentiators:

Capability	Detail
Extensive Vulnerability and Configuration Knowledge Base	Supports scanning of **300,000+** vulnerabilities covering mainstream systems, databases, and applications. Supports CVE, CNVD, CNNVD, and other international and Chinese professional vulnerability databases. Configuration audit knowledge base covers **7 major categories, 60+ products, and 150+ system versions** with professional hardening recommendations and multiple industry security configuration audit standards.
Full Coverage of New IT Assets, Comprehensive Vulnerability Discovery	Discovers vulnerabilities in cloud computing, big data, IoT, container images, AI, and LLM new IT assets, as well as traditional system vulnerabilities — generating comprehensive security risk reports.

Capability	Detail
Professional Cloud Intelligence Support	Based on years of NSFOCUS Threat Intelligence Center (NTI) operations. First-time tracking of emergency vulnerability outbreaks for rapid early warning and remediation.
Innovative Vulnerability Remediation Priority Algorithm	Multi-dimensional threat-based prioritization (popularity, POCs, malware presence) combined with business multi-dimensional factors (importance, tier, protective status) and proprietary algorithms to redefine vulnerability remediation priorities.
Multi-Source Vulnerability Fusion	Supports unified integration, fusion analysis, and centralized remediation of vulnerability data from heterogeneous vendor scanners, penetration test findings, external notifications, and vulnerability intelligence.

Threat Intelligence

微步在線 ThreatBook

THREATBOOK CO., LIMITED

Primary competitive targets: Mandiant Threat Intelligence; RSA FraudAction

Key differentiators:

Capability	Detail
Massive Data Scale and High Precision	ATI (Advanced Threat Intelligence) relies on a **10 billion-level** threat sample database and **100 billion-level** infrastructure data. Both NGTIP and ATI achieve **99.9%** precision — ensuring intelligence confidence.
Professional APT and Advanced Threat Tracking	Core capability derived from ThreatBook Intelligence Bureau's research output. ATI and NGTIP expose exclusive APT organizations, incidents, and zero-day vulnerabilities.
Flexible Delivery: Local Deployment and Cloud Services	NGTIP provides local deployment solutions meeting high-compliance and data isolation requirements. ATI (SaaS and cloud API) provides agile, scalable cloud subscription and service-oriented integration.
Systematic Vulnerability	NGTIP provides systematic vulnerability detection, remediation, and early

Capability	Detail
Management and Early Warning	warning. Platform enables real-time monitoring of hundreds of intelligence sources and intelligence research.
Real-Time, Multi-Source Intelligence Production and Update System	ATI and NGTIP share **3,000+** intelligence sources and ThreatBook Intelligence Bureau exclusive research findings — a dynamic intelligence network of multi-language reports supporting report-level and hourly-level updates.
Significant Security Operations Efficiency Improvement	NGTIP's high-precision compromised host intelligence directly achieves **≥85%** alert noise reduction for SOC/SIEM platforms, improving response efficiency.
Automated Digital Risk Exposure Monitoring and Remediation	DRPS (Digital Risk Protection Service) provides 24/7 automated monitoring and professional remediation of digital risks — including counterfeit apps, phishing websites, and asset leaks — for enterprises in and outside China.

Data Loss Prevention (DLP)

Beijing Skyguard Network Security Technology Co., Ltd.

Primary competitive targets: Forcepoint DLP; Symantec DLP

Key differentiators:

Capability	Detail
Full-Dimension Overseas Ecosystem Compatibility	Exceptional cross-ecosystem compatibility. Seamlessly integrates with mainstream overseas office and system ecosystems. Fully compatible with Windows AD domain management, proxy services, and stable compatibility across the entire Microsoft 365 suite — ensuring smooth operation of core office scenarios including email, document collaboration, and cloud storage. Full support for MIP (Microsoft Information Protection) — data encryption, permission control, and other security operations without additional compatibility plugins or system modifications. Direct integration into existing overseas IT ecosystems — ensuring unimpeded cross-ecosystem business collaboration and adapting to overseas office and business deployment requirements.

Capability	Detail
High-Standard Full-Scenario Stable Operation	Focused on end-to-end stability, with particular emphasis on endpoint device stability optimization. Dramatically reduces business interruptions caused by device failures or functional anomalies. Core functions precisely effective; edge functions without stuttering or crashes; stable operation under high-load and multi-task concurrent complex scenarios — reducing maintenance troubleshooting and operational costs.
Highly Consistent Cross-Platform Functionality and Experience	Full support for Windows, macOS, and Linux. Multi-platform 1:1 feature parity without platform-differentiated feature deletion or degradation — ensuring consistent user experience across different systems. Unified standardized configuration interface with consistent layout, operational logic, and configuration paths across platforms.
Professional High-Efficiency Technical Support Services	Comprehensive full-process technical support system. Professional English-language services adapting to overseas users and international business communication needs. Complete knowledge base (KB) covering FAQs, operation guides, and troubleshooting. Efficient ticket system supporting rapid submission, real-time progress tracking, and guaranteed issue closed-loop resolution.

Best Practices

Construction Concept

Data-Driven Security Implementation
Platform Fills Capability Gaps

Core Concept

Quality, Complete First-Hand Telemetry Data
+
Rich Detection and Analysis Frameworks
= Good Results

Centralized aggregation of assets, vulnerabilities, and threats with mutual correlation for unified operations

Closed-Loop Operations

- Security operations closed-loop, connecting multi-person collaborative response and handling processes
- Vulnerability closed-loop management process
- Security incident analysis, containment, and handling closed-loop process
- Comprehensive asset management with basic inbound/outbound processes

System Openness for Continuous Expansion

Standard Data Sets & Detection Frameworks
Multi-source security component effectiveness improvement

Open APIs
Flexible data access, correlation modeling, SOAR playbook orchestration, component integration, visualization expansion

Requirements Analysis

1 Ministry Network (Level 1 Network) → 2 Provincial Network (Level 2 Network) → 3 Regional Network (Level 3 Network) → 4 Local Network (Level 4 Network)

⚠ Complex Network Environment with Multi-level Security Issues

1 Incomplete Organizational Mechanisms
Lack of effective collaborative operation mechanisms

2 Unclear Information Assets
Cannot accurately grasp dynamic asset information in real-time

3 Basic Security Issues Remain Major Risks
Lack of threat discovery and analysis capabilities for business scenarios. Heterogeneous security components fail to achieve 1+1>2 effect.

4 Industry Shortcomings Are Prominent
Lack of industry-wide joint defense and control

Ultimately manifested as: Heavy operational workload before construction, but unsatisfactory results in HW attack-defense exercises

Project Initiation Drivers – Technical Level

1 Lack of Systematic Security Construction

Lack of systematic security construction causes frequent security issues. Existing technical tools cannot assist operators but instead divert their energy.

- Fragmented security devices cannot see the overall situation
- Rapid changes in internal/external environment create frequent security gaps
- Massive security logs make it difficult to locate real attacks

2 Reactive Security Operations

Reactive "closing the stable door after the horse has bolted" security operations are not the original intention of security work. Meanwhile, heavy operational workload and insufficient personnel capabilities severely constrain operational effectiveness.

- Passive response does not reduce problem occurrence
- Daily massive alerts delay response timeliness
- Personnel capability gaps prevent effective protection

3 Workflow Mechanisms Only on Paper

Work mechanisms that only remain on paper are unclear and not implemented. Operational work execution is not standardized enough to achieve expected results.

- Unclear responsibilities and authority among departments
- Incident scenarios not classified, no basis for handling
- Mechanisms and processes remain on paper with poor

Project Initiation Drivers – Management Level

Establish "Security and Practicality" as the Fundamental Principle

Strengthen the cybersecurity baseline and advance smart water conservancy construction

Legal Compliance

Article 31 of the Cybersecurity Law of the People's Republic of China explicitly requires that critical information infrastructure, including water conservancy, be subject to key protection based on the cybersecurity classification protection system. Article 32 requires that security technical measures be planned, constructed, and used simultaneously .

Leadership Attention

Ministry leadership attaches great importance to cybersecurity. At the cyber information work conference, the leadership clearly stated: "Cybersecurity is the baseline, a non-negotiable matter. No matter how difficult, we must do everything possible to eliminate risks, and we must act quickly."

External Perspective

The organization has the characteristic of "one point breached, entire line compromised." With its massive scale, cybersecurity construction levels vary among subordinate river basin agencies and institutions. IT information assets have not yet formed a unified and effective inventory and monitoring system.

Internal Perspective

With the development and application of new attack and defense technologies, unknown threats are becoming more prevalent, and 0-day vulnerabilities are frequently emerging . The impact and destructive power of cybersecurity incidents continue to increase, placing higher demands on organizational security construction.

Customer Background

As a constituent department of the State Council, the Ministry comprises 22 internal divisions and 30 directly-affiliated units nationwide, operating at a massive scale. The Information Center bears significant responsibility and pressure for cybersecurity management and supervision.

With the formal implementation of the Cybersecurity Law and the gradual expansion of national-level cyber attack and defense exercises, cybersecurity construction has entered deep waters. Practical defense effectiveness and operational response efficiency have become the primary construction objectives.

Six Key Construction Areas

1. Supplement and improve cybersecurity defense facilities
2. Build cybersecurity threat information collection system
3. Build cybersecurity big data platform
4. Build cybersecurity threat perception and early warning system
5. Build cybersecurity decision command system
6. System integration

Characteristics: Multiple branches, large business scale, relatively complete basic security construction, but previous security results were unsatisfactory

XDR BENCHMARK CASE

Ministry of Water Resources

DIRECTORY

Project Achievements and Industry Recognition

Cybersecurity Technology Application Pilot
Ministry of Water Resources Information Center Joint Project

CSO Top 20 Outstanding Security Projects
Ministry of Water Resources Cybersecurity Threat and Decision Command System

Key Promotion Directory of Advanced Water Conservancy Technologies
2023 Edition

Digital Transformation Pioneer
From Water Management to "Smart" Water - Ministry of Water Resources Situation Awareness Dashboard Display (Xinhua News Agency)

Dayu Water Conservancy Science and Technology Award
"Key Information Infrastructure (Water Conservancy) Cybersecurity Key Technologies and Application" - First Prize (2022)
Jointly completed by Ministry of Water Resources Information Center, Hohai University, Sangfor Technology Co., Ltd.

Digital Twin Water Conservancy Construction
Selected for Typical Directory

Industry-Wide Recognition and Promotion
Demonstrating the value and effectiveness of XDR+GPT solutions in the water conservancy industry

Outstanding Performance in National Cyber Attack and Defense Exercises

6
Consecutive Years
Excellent Performance in National-Level Cyber Attack and Defense Exercises

2019	2020	2021	2022
Excellent	Excellent	Excellent	Excellent

Information Source: http://www.mwr.gov.cn/ztpd/2024ztbd/slwxszlsslsjdspx23/jggs/

Overall Security Effectiveness and Efficiency Improvement

Focusing on cybersecurity threats and vulnerabilities, relying on Sangfor XDR+GPT solution, establishing a cybersecurity joint defense and control mechanism

Gradually achieving the goal of "one place warned, all places defended; one place threatened, all places handled"

In 2022 alone: Industry shared threat warnings 5,000+ times, jointly handled 70+ high-risk cybersecurity attacks

Protecting 300+ important information systems, using 30+ security devices	Only log in to 1 platform daily to complete security monitoring and analysis
Daily security alert volume at tens of millions level	Automatic analysis and accurate classification, daily <100 precise security incidents
Average alert handling closure time 5+ hours	Average handling closure time ~30 minutes
Lack of multi-source heterogeneous data analysis capability and APT attack discovery capability	XDR+GPT dual engine, enhanced threat discovery and analysis capabilities
Low security operations efficiency, large on-site requirements, difficult to guarantee 7×24	Security GPT加持, 1 person on-site + remote support sufficient for daily threat operations

Effect Summary: Detection Effect Improvement

Building a unified operations interface for security work based on security data governance capabilities

Response Efficiency Improvement

Through clear personnel role settings and operational process mechanisms, combined with automated playbook construction

Hours → <1 Hour

Disposal work time reduced

Threat Discovery Capability

Operations team threat mining helps the ministry discover multiple hidden attacks

Attack path analysis repairs security gaps

Advanced Threat Detection

100+

Threat Models

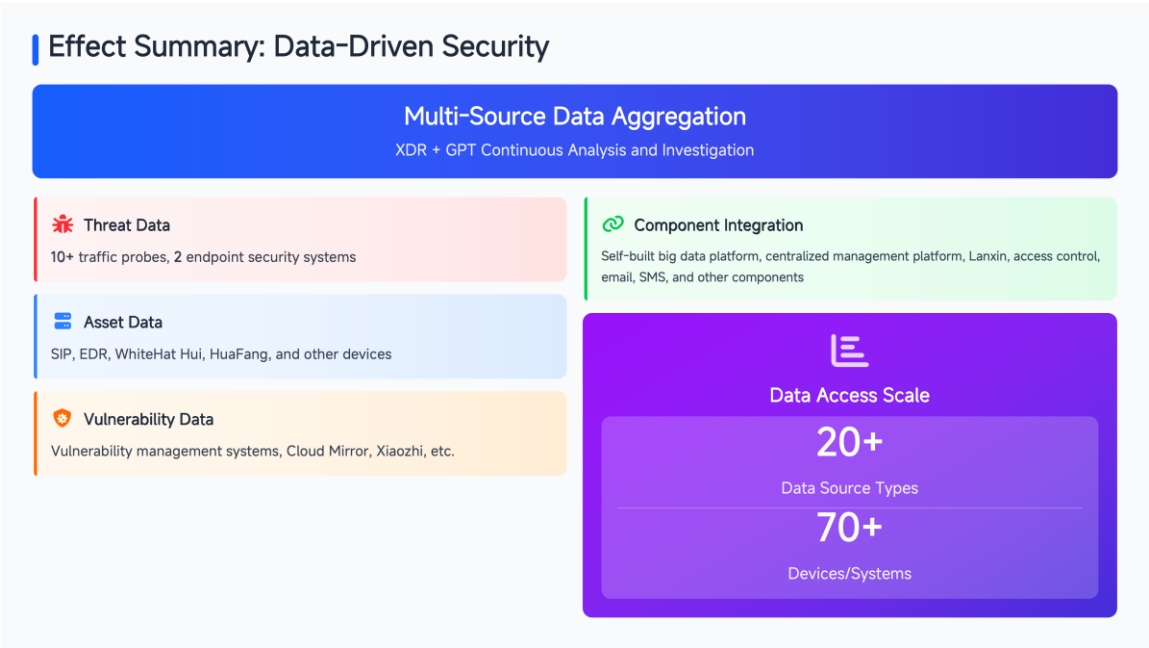
Provide detection capability support for the ministry and subordinate units while achieving massive alert noise reduction

Unified Operations Interface

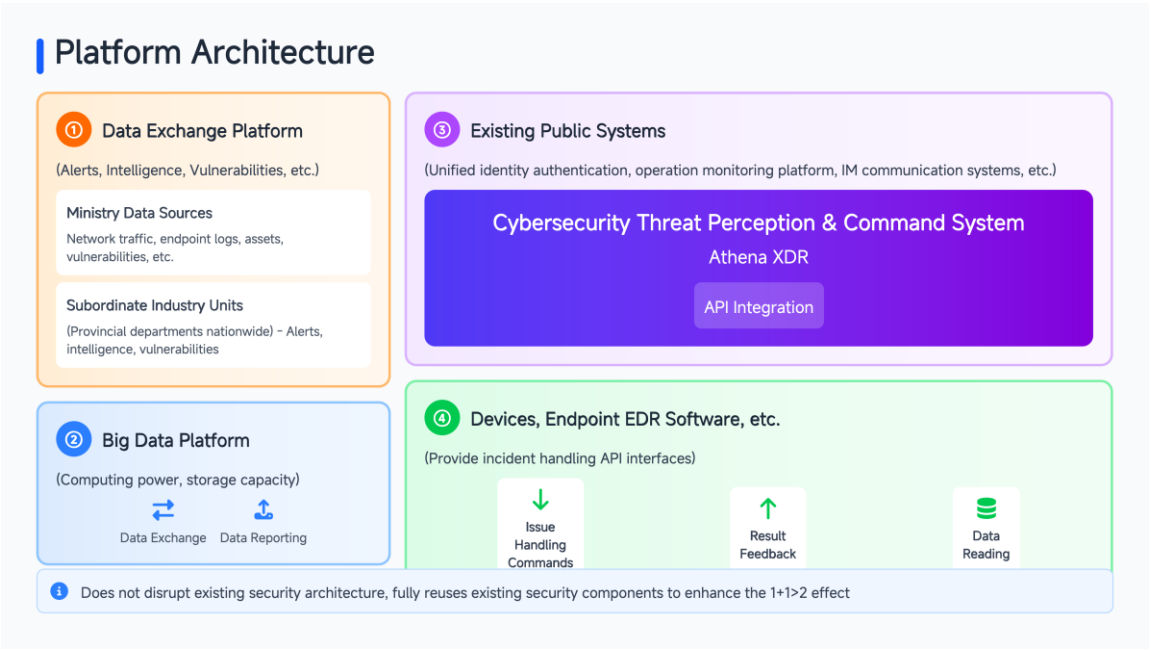
Clear Role Definitions

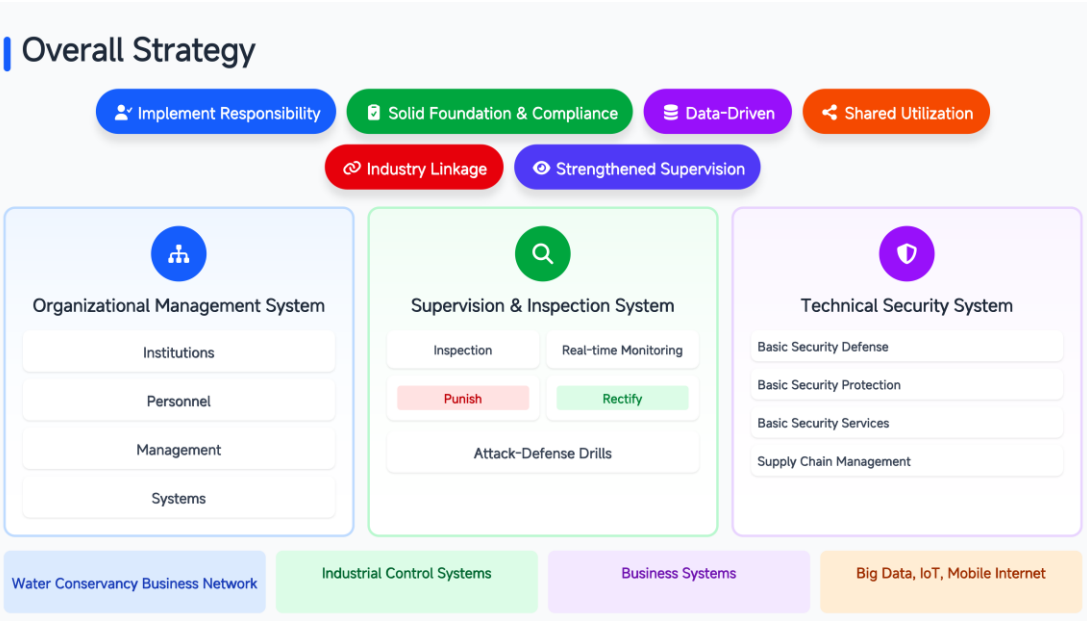
Automated Playbooks

Alert Noise Reduction


Effect Summary: Data-Driven Security
Multi-Source Data Aggregation
XDR + GPT Continuous Analysis and Investigation
Threat Data
10+ traffic probes, 2 endpoint security systems
Asset Data
SIP, EDR, WhiteHat Hui, HuaFang, and other devices
Vulnerability Data
Vulnerability management systems, Cloud Mirror, Xiaozhi, etc.
Component Integration
Self-built big data platform, centralized management platform, Lanxin, access control, email, SMS, and other components
Data Access Scale
20+
Data Source Types
70+
Devices/Systems


XDR BENCHMARK CASE
Ministry of Water Resources
01
Construction Background
02
Practical Achievements
03
Effect Summary
DIRECTORY


Platform Architecture
① Data Exchange Platform
(Alerts, Intelligence, Vulnerabilities, etc.)
Ministry Data Sources
Network traffic, endpoint logs, assets, vulnerabilities, etc.
Subordinate Industry Units
(Provincial departments nationwide) - Alerts, intelligence, vulnerabilities
③ Existing Public Systems
(Unified identity authentication, operation monitoring platform, IM communication systems, etc.)
Cybersecurity Threat Perception & Command System
Athena XDR
API Integration
② Big Data Platform
(Computing power, storage capacity)
Data Exchange
Data Reporting
④ Devices, Endpoint EDR Software, etc.
(Provide incident handling API interfaces)
Issue Handling Commands
Result Feedback
Data Reading
Does not disrupt existing security architecture, fully reuses existing security components to enhance the 1+1>2 effect


Overall Strategy
Implement Responsibility
Solid Foundation & Compliance
Data-Driven
Shared Utilization
Industry Linkage
Strengthened Supervision
Organizational Management System
Institutions
Personnel
Management
Systems
Supervision & Inspection System
Inspection
Real-time Monitoring
Punish
Rectify
Attack-Defense Drills
Technical Security System
Basic Security Defense
Basic Security Protection
Basic Security Services
Supply Chain Management
Water Conservancy Business Network
Industrial Control Systems
Business Systems
Big Data, IoT, Mobile Internet

Lead Analyst Information

Jin Huichao (Anatole Jin)

DWC-Strategic Analyst

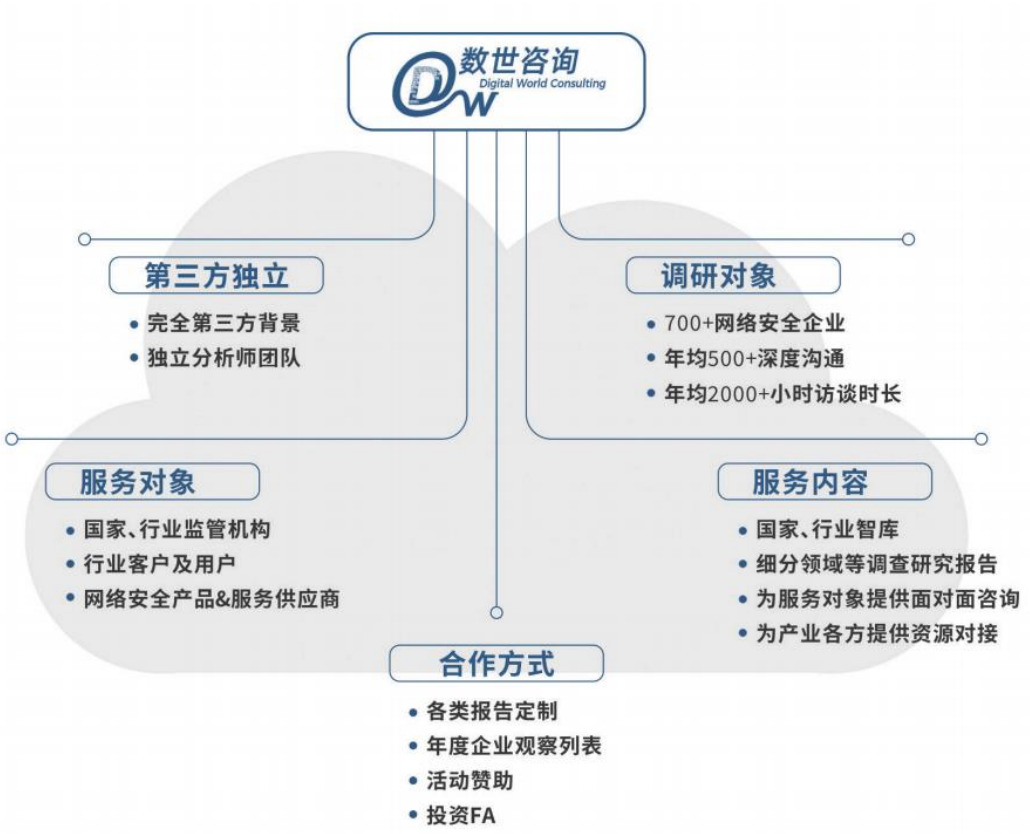
+86 16601182683 (WeChat)

Please add with note "Company-Name"

Previously worked at Digital China Group - Security BG, Venustech Group - Strategy Consulting Center, and 360 Group - City Industry Business Division, primarily responsible for security consulting and planning work.

Current position: Strategic Analyst/Partner at DWC

Responsible for strategic planning and industry consulting; research directions include data security, AI security, software supply chain security, and security operations



北京数字世界咨询有限公司（以下简称“数世咨询”）是国内数字化领域独立第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全100强》、《中国数字安全产业年度报告》等业内影响力巨大的公开报告。同时，还为监督机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，以及150余家网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动、投资对接，安全产品与企业推荐，企业资源整合等

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区天鼎218文化金融园东外110号 网安小酒馆
官方网站：www.dwcon.cn
联系邮箱：dw@dwcon.cn

小酒馆

数世咨询
Digital World Consulting

数字安全领域独立第三方调研机构