中国（香港）网络安全竞争力调研报告

(第一期)

（2026 年 3 月）

数世咨询
Digital World Consulting

中国（香港）网络安全竞争力调研报告

(第一期)

（2026 年 2 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

报告信息

报 告 方 向 ：产业研究

报 告 名 称 ：中国（香港）网络安全竞争力报告

报 告 编 号 ：DWC_20260301

主笔分析师：靳慧超 • 数世咨询-战略分析师

分 析 团 队 ：数世咨询 • 数字安全研究院

报 告 审 核 ：李少鹏 • 数世咨询-首席分析师

报告概述

本报告核心内容为数世咨询通过产业研究以及专业访谈所获得信息的总结与分析，聚焦香港网络安全产业现状及发展，是中国网络安全产业出海研究系列报告的一部分。

自 2022 年开始，数世咨询启动了中国网络安全产业出海调研与研究工作并为有关部门编制了一系列报告。本报告为首次公开发布的调研报告，是中国（香港）网络安全竞争力系列报告的第一期。

（一）调研说明

- **本次调研对象的选择标准**

✓ 在香港拥有合法经营资质，并且处于正常经营的中资网络安全企业
✓ 企业在香港已开展核心业务，并且拥有成功案例
✓ 主营产品具备自主知识产权，某一细分领域具备技术领先性

- **本调研报告推荐产品的选择标准**

✓ 主营产品已完成本地化改造
✓ 主营产品在功能与性能方面具备替换国际同类产品的能力
✓ 企业在香港拥有较为广泛的用户基础，且口碑较佳
✓ 企业在内地拥有广泛头部客户案例

（二）编制背景

香港作为我国对外开放的重要窗口和国际金融、贸易、航运中心，其网络安全不仅关乎本地社会稳定与经济繁荣，更直接关系到国家整体安全与发展大局。并且因其连通内外的特殊职能，具备国际化优势，可积极参与全球网络空间治理，是我国体现大国担当、彰显安全技术实力的最佳载体。

如何提升香港网络安全能力，关键在于强化网络治理能力和自主可控安全技术的应用。如何扩大我国安全技术影响力，关键在于争夺全球网络空间话语权和安全企业国际化业务的开拓。

本报告的核心目的，就是以第三方独立调研机构的身份，搭建香港和内地企业沟通的桥梁、疏通网络安全企业出海的路径，推广传播中国网络安全解决方案。并且通过对网络安全产业的洞察，助力政府部门及中资企业加快国产化替换进程，同时为外资企业安全合规建设提供第三方参考。

中资网络安全产业概况

（一）国产化替换

基于“一国两制”的制度优势，以及高度自由开放的经济体系、全球领先的金融与专业服务能力，香港成为了我国国际化程度最高的地区，也是国家连接全球、推动高水平对外开放的战略支点。因此，香港的政府部门、公共事业机构以及本地企业的业务系统绝大部分运行在外国品牌的 IT 设备和信息系统之上。

随着我国综合实力的不断攀升，尤其是中国式现代化进程的推进，中资品牌的信息系统逐渐具备了与国际品牌相同的功能、性能指标，甚至在许多方面具备创新性和领先性。通过经济、技术、政治等方面的综合考量，香港的政府部门、公共事业机构以及本地的企业正式拉开了国产化替换的序幕。近年来，由于全球地缘政治与经济形势的急剧变化，又加速了网络安全产品和服务的国产化替换进程。

第一批在香港开展核心业务的中资网络安全企业，以华为、深信服、山石网科等企业为代表，是中资网络安全产业的开路者，其经营时间都已超过了 10 年。2019 年前后，又一批中资网络安全企业陆续来到香港，走向了国际化发展的道路。2023 年起，更多的中资网络安全企业进军香港市场，在本地注册公司、招聘员工，正式接受香港客户严格的选择，助力国产化替换进程的顺利推进。

随着 2026 年 1 月 1 日《保护关键基础设施（电脑系统）条例》的正式实施，对于有意开展全球性业务的中资网络安全企业来说，可谓迎来了历史性机遇。相信随着更多的中资网络安全企业在香港开展业务，定会极大的加快国产化替换的进程，并且提高中资网络安全企业的全球影响力，充分彰显中国网络安全实力，使香港成为中资网络安全企业全球化发展的桥头堡。

（二）市场概况

据不完全统计，2025 年香港网络安全市场规模约为 343 Million USD，而中资网络安全企业所获份额尚未达到 10%，在 30Million USD 以下。由此可见，香港市场的增量空间巨大，对中资网络安全企业吸引力较强。同时在本次调研中，结合市场端表现以及自身经营情况来看，能否达到综合营收 1.5 Million USD 是衡量中资网络安全企业初步经营效果的关键指标。

现阶段，中资网络安全企业的客户群体基本集中在政府、公共事业、金融、运营商、互联网行业，其中绝大部分的国产化替换驱动力来自法规、政策、集团总部制度，同时叠加经济（性价比）因素的考量，还有一小部分来自于专项创新项目的定制需求。

在整体需求层面，香港网络安全市场集中在边界防护类、威胁检测类、终端管控类和数据防泄露等产品，以及安全规划、攻防演练等服务。绝大部分企业对网络安全工作的重要性具备较高认知，采购时均通过完整的产品性能、功能、业务需求匹配测试中的实际表现为最终评判标准。

2026 年开始，在以上产品的基础上，中资网络安全企业还会加大安全数据分析类、态势感知和 SaaS 化安全能力的推进速度，进一步加强中资网络安全企业在香港的综合竞争力。

（三）本地化改造

由于香港的全面国际化状态，为了顺利在香港开展核心业务，中资网络安全企业已经进行了产品、服务、经营模式的本地化改造。这不仅仅是简单的语言翻

译，而是 IT 文化、行业场景、商业规则的深度适配。

在 IT 文化适配方面 ，适应用户自主解决问题的需求以及在一线人员个人发展方面提供可靠保障：

- ✓ 升级技术文档，细化具体功能使用、操作步骤、故障排查等内容以支持用户自己解决问题
- ✓ 有效维持产品性能稳定、功能有效，避免用户因安全产品自身失效导致的安全责任
- ✓ 增加与独立第三方机构的交流、评测，帮助用户从客观角度了解产品真实技术能力，有效提高品牌认知度

在行业场景适配方面，设立总部研发专项支持，匹配 IT 基础设施环境和实际业务流程：

- ✓ 专业技术人员全力配合客户现场完整 POC，测试问题及时反馈
- ✓ 根据行业客户实际 IT 环境，升级产品适配国际主流信息系统
- ✓ 根据行业客户实际业务流程，改造安全架构、数据处理等功能细节
- ✓ 增加本地技术支持人员，响应用户即时需求

在商业合作适配方面，不同于内地“关系-价格-效能”的模式，而是以“效能-价格-关系”模式作为合作的准则：

- ✓ 摒弃过度宣传，宣发内容与产品、服务实际情况一致
- ✓ 重视客户隐私，严格遵守相关制度约束、商业规则
- ✓ 重视渠道伙伴与集成商的利益
- ✓ 重视一线人员的体验与建议
- ✓ 严格按照合约条款提供服务

国产化替换推荐

（一）可优先进行国产化替换的领域

网络安全领域进行国产化替换的意义在于统筹国内国际大局、充分发挥区域安全协同战略作用，以及加快构建新发展格局、稳步提升自主安全技术影响力。然而这样的替换进程并不是一蹴而就的，基于统筹发展与安全的核心理念，是要经过关键节点替换、并行运行验证、场景化替换、规模化替换等一系列不同阶段才能顺利完成的。

现阶段的香港网络安全环境，以《保护关键基础设施（电脑系统）条例》的实施为标志，正处于关键节点替换阶段。可优先进行国产化替换的网络安全场景具备如下特征：

- 标准化程度高，符合使用习惯

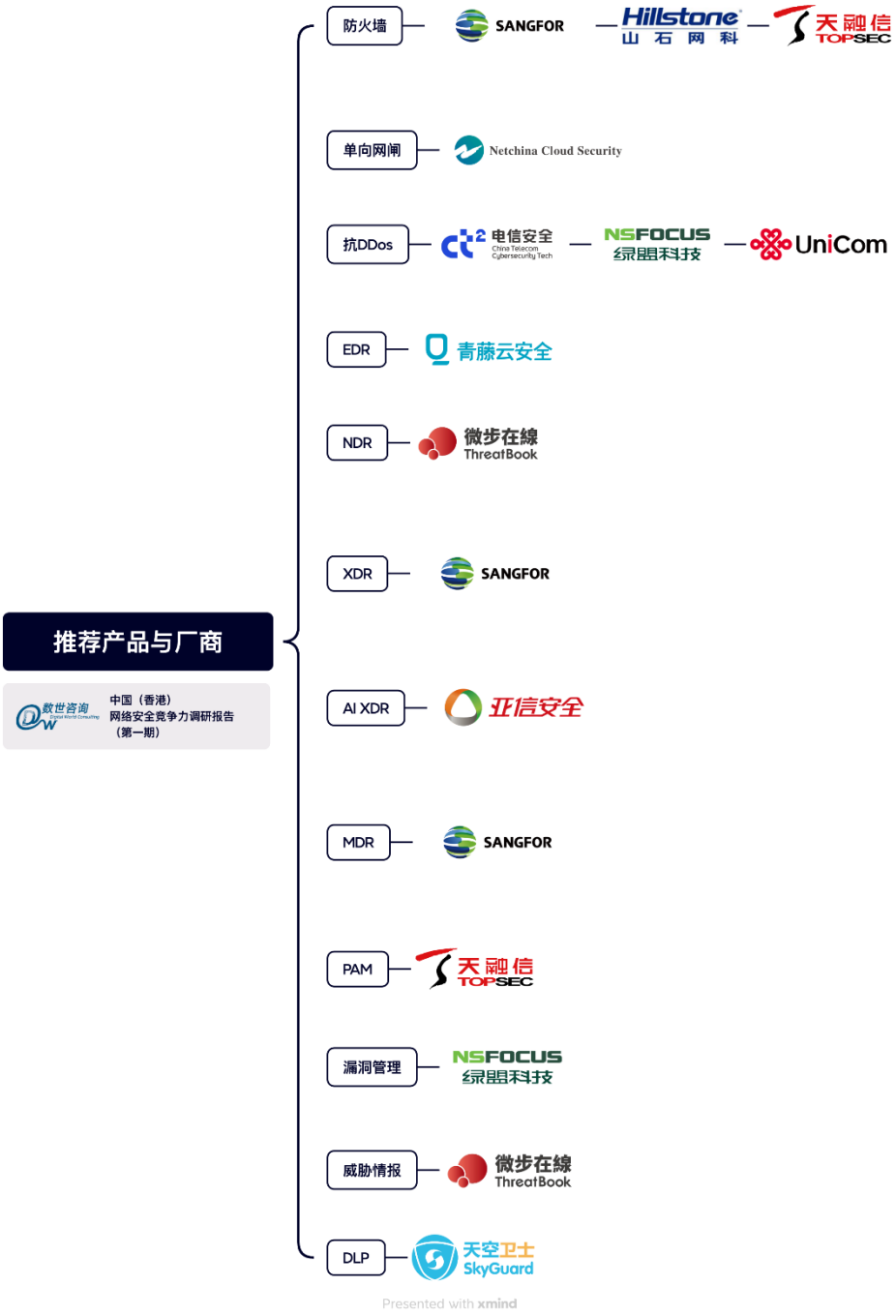
许多中资网络安全企业已开展多年国际化业务，具备全球化技术能力。它们的核心产品功能均可以适配国际标准要求，并且符合香港本地人员使用习惯。使用这类产品进行国产化替换，不产生额外的沟通和学习成本，可使香港本地用户在工作中无缝衔接。

- 内地成熟技术，具备推广价值

基于内地庞大的数字化市场，中资网络安全企业的技术能力，不仅可以覆盖全球绝大部分安全场景，而且还诞生了诸多特有的安全场景。一些在内地已经成熟应用在集团/总部企业的安全产品，凭借其实际应用价值以及集团/总部的制度要求，是进行国产化替换的不二选择。

（二）推荐产品与企业

基于香港本地网络安全市场现状并结合未来发展趋势，在可优先进行国产化替换的领域中，根据调研与评选的结果，特推荐以下产品与企业。



- 防火墙

SANGFOR

✓ 深信服

✓ 主要对标产品：**Fortinet** Fortigate

✓ 核心优势

能力	简介
原生的“全功能”集成	防火墙内直接内置了专业的 WAF（Web 应用防火墙）模块，并包含被动漏洞扫描技术。
更强的未知威胁检测	搭载了自研的 Engine Zero 人工智能引擎，利用深度学习模型进行静态和动态分析，对勒索病毒变种和未知木马的拦截率在实战中表现极佳（CyberRatings AAA 认证）。
内置“SOC Lite”可视化运维中心	将“安全运营中心（SOC）”的概念下沉到了防火墙控制台。它不仅显示流量报表，还会自动生成基于资产维度的风险评估和处置建议。
针对香港监管的合规与取证便利性	针对香港常见的日志留存和合规审计需求，深信服 NGFW 的本地存储和日志检索能力更优。它支持详细的应用行为审计（如社交媒体、网盘外发细节），并能一键生成符合合规要求的安全总结报告。
本地化的“专家级”技术支持	在香港拥有极其强大的原厂技术团队。在进行复杂的策略迁移、攻防演练或突发事件处置时，响应速度和沟通顺畅度极高。

Hillstone 山石网科

✓ 山石网科

✓ 主要对标产品：**Fortinet** Fortigate

✓ 核心优势

能力	简介

1U 设计	体积小，功耗低，具备高密度端口，提供最多 20 个 10GE 、4 个 100GE 光口、及多个扩展接口，采用 SSL 硬件解密引擎。
高端系列搭载硬件加速引擎	专注于较高流量场景下卸载 CPU 压力，整机最大性能可达 320Gbps，小包性能可达 140Gbps，报文转发延时可低至几微秒。
X 系列数据中心防火墙采用创新全分布式架构	搭配智能流量分配算法与资源管理算法专利技术，实现业务流量在多模块间的分布式高速处理，线性扩展并发、新建等系统性能。。
全面、智能的威胁检测与防护	内置高级威胁检测引擎，提供基于深度应用、协议检测和攻击原理分析的入侵防御技术。同时通过与云沙箱的联动，感知试图通过网页、电邮等方式入侵的恶意行为，从而进行未知防御检测。
网络地址转换端口复用技术	将单一 IP 地址可 NAT 的并发会话量最大提高 16 倍，有效缓解组织因地址资源有限而导致的访问受阻问题。
威胁情报集成	山石云瞻威胁情报中心联动，结合第三方情报提供“攻击前、攻击中、攻击后”的全生命周期安全防护。
智能、高效的策略运维	实现覆盖策略部署、管理、优化与运维全生命周期的智能运维和管理。
强大的网络适应性	支持 RIP、OSPF、IS-IS 和 BGP 等动态路由协议，可根据网络系统的运行情况自动调整动态路由表。此外，产品支持出站流量动态探测和入站流量 SmartDNS 等智能链路负载均衡功能，允许网络访问流量在多条链路上实现智能分担。

天融信 TOPSEC

✓ 天融信

- ✓ 主要对标产品：**Palo Alto** Next-Generation Firewalls、**CheckPoint** Next-Generation Firewalls
- ✓ 核心优势

能力	简介
全域安全能力	基于平台化能力，融合了网络安全、应用安全、Web 安全、数据安全相关的防护功能，提供网络探测响应、融合安全防护、高级威胁检测、资产安全分析和处置、攻击链可视等能力。
AI 检测防护	基于 AI 检测能力，对 DGA、隐蔽信道、恶意加密流量等高级威胁攻击进行实时检测防护。
云网端协同	基于云网端多元协同能力，提升了对网络资产和安全事件的感知分析能力，从而提升整网防护水平。
虚拟化云化	基于虚拟化和云化能力，适应新业务部署和应用场景，扩展边界防护范围。
深度资产安全	基于资产安全角度，深度提升网络资产风险和异常行为分析能力。
大模型安全防护	内置预训练安全检测模型，为大模型应用系统提供 AI 识别、大模型会话解析、应用及 API 防护、提示词注入防护、价值观内容过滤等防护能力，保障大模型应用的安全性、可控性。
智能管理安全运维	提供智能运维管理的一系列工具，包括安全监控、数据中心、安全中心、安全策略管理、集中管理、第三方管理接口等，帮助管理员全面掌握网络态势，实现自动化、可视化的安全运营。

- 单向网闸

Netchina Cloud Security

✓ 中网云安

✓ 主要对标产品：**Waterfall** Unidirectional Security Gateway、**ST Engineering** CyberTransporter

✓ 核心优势

能力	简介
物理单向传输	通过“双主机架构+光的单向传输特性”实现物理单向，确保数据的单向传输。
全面的业务支持	支持端口数据导入、POST 推送、KAFKA 代理等应用数据导入，支持包括 FTP/SAMBA 等协议的服务和文件同步。
文件同步机制	支持本地服务与外部导入两种文件传输模式，实现文件的单向同步传输。
数据库同步	持 Oracle、SQL Server、MySQL 等主流数据库的单向数据同步。
管理与监控能力	可选的独立管理/带内管理、接口自定义/图标化展示/按功能展示、SNMP 监控、NTP 校时、流量可视化及日志分级外发等功能。
高安全性增强	集成防病毒、抗扫描、抗攻击、ARP 绑定等安全组件，提高设备本身的安全性和业务数据的安全性。
良好的扩展能力	支持串联部署于网络边界，可与安全交换平台搭配构建单向或双单向安全边界。
易用与运维支持	提供配置向导、配置备份与恢复、邮件告警、在线抓包、多维度网络检测工具，简化运维管理。

- 抗 DDoS

电信安全
China Telecom
Cybersecurity Tech

✓ 电信安全

✓ 主要对标产品：**Radware** DDoS Protection、**AWS** Shield (Standard/Advanced)

✓ 核心优势

能力	简介
全网流量监测，全网监控	融合全网威胁情报，流量监测准，告警触发快，及时应对网络异常。
全球攻击防护	独有全球分布式 130+近源清洗节点，22T+防护容量，分布式架构应对大规模海量攻击。
全域分析溯源	基于中国电信运营商权威流量，可溯源精确到本地 IDC，不受虚假源 IP 地址的影响，可协助执法机关提供有公信力的溯源分析结果，助力客户强化网络。
多级联动	融合骨干网近源、IDC 近目的、国际关口局、城域网近端的多级组网架构联动，有效防御国内外的扫段、脉冲等混合攻击。
AI 画像	基于见微大模型，深度测绘僵尸网络，提取僵尸网络发起源控制端、被控主机、访问行为等信息，结合通过对僵尸网络样本的捕获、研判，逆向分析僵尸网络控制及技术手段生成学习模型库，对攻击发起者的恶意攻击行为生成画像数据。
云网边端一网统管	可与端侧云脉 SASE、边侧安全网关、网侧安全资源池等产品，采用 MSSP 态势服务平台形成模块化一网统管。

UniCom

✓ 联通国际

✓ 核心优势

能力	简介
攻击监测	基于多维度流量分析模型，实时监控联通网内流量异常，为用户提供 DDoS 攻击告警通知、流量趋势、流量异常分析、攻击溯源等信息。
流量清洗	通过调度部署于联通全网清洗节点的能力，对异常流量从攻击源头进行引流近源清洗并原路径回注，在联通骨干网层面领先一步缓解大流量 DDoS 攻击。
流量封堵	基于联通全网路由能力，对流向客户目标 IP 的某区域或全网区域流量进行阻断，避免客户互联网出口带宽拥塞导致其他未受攻击业务中断，保障客户整体带宽资源。
提供自服务平台	客户可通过联通 DDoS 攻击防护自服务平台自行提交清洗或者封堵防护任务，并进行任务防护参数配置，同时可以进行攻击防护任务、攻击报表的查看。
安全运营中心 SOC	提供全天候 24/7 的实时监控与不间断支持，包括普通话，粤语，英文。具备高度弹性，能够依据不同客户的特定需求，灵活提供定制化的安全运营服务。

NSFOCUS 绿盟科技

✓ 绿盟科技

✓ 主要对标产品：**NetScout** Arbor Sightline / Arbor Cloud、**Radware** Defense Pro / Cloud DDoS Protection Service

✓ 核心优势

能力	简介
针对 DDoS 专门设计的智能防御算法	多层次智能防御算法设计，同时具备静态过滤规则和动态防护算法，保证准确过滤 DDoS 攻击，将误防和漏防几率降到最低，有效应对复杂攻击。
满足全网、大流量攻击检测需求	具备 DFI/DPI 双栈检测技术，能同时满足运营商、IDC 行业的百 G 级流量检测需要，以及金融、政企行业的高精度，高时效性监测需要。
云端信誉库	与 NSFOCUS 的专业云端 NTI 数据进行联动,可以实现对攻击源 IP 的详情进行查看,并对僵尸主机一键过滤. NTI 平台整合了绿盟各个产品以及数据发掘团队发掘并验证的肉鸡攻击源,实现了智能清洗和简化操作的高效结合。
云地一体化防护	NSFOCUS 提供自建的 Cloud DPS 国际云清洗服务，具备 TB 级别防护能力。为本地清洗方案提供大流量清洗备援，帮助客户以最经济的投入形成立体化混合清洗方案，保障大规模攻击下的业务安全。
增值服务 Ready	为运营商、IDC、公有云等行业提供一体化增值运营平台，便于客户在增强 DDoS 防御能力的同时，通过为最终用户提供 DDoS 攻击防御增值服务来拓展新的业务模式。

- EDR

青藤云安全

青藤云安全

✓ 主要对标产品：**CROWDSTRIKE** EDR、**PALOALTO** EDR

✓ 核心优势

能力	简介
入侵检测、风险发现与响应能力高度一体化	在同一平台内实现入侵检测、漏洞扫描、补丁与弱口令检查、合规基线与自动化响应，避免多工具拼接，安全运营效率高于同类产品。
资产识别与风险可视化能力行业领先	可自动识别 180+ 资产类型、2000+ 行为与应用分类，并构建资产与风险关联关系图，支持风险溯源与攻击链分析。
Agent 轻量化设计，适合高性能与关键业务场景	Agent 资源占用低，可长期部署于数据库、交易系统、高并发服务器等核心业务环境，不影响业务性能。
通过超大规模生产环境验证	在单一客户环境中实现 30 万+ 主机的统一纳管与实时防护，具备成熟的大规模部署、集中管理与性能调度能力。
自动化响应与策略联动能力成熟	支持进程阻断、网络隔离、主机隔离、策略联动等自动化处置能力，可在大规模环境中减少人工干预。

● NDR

微步在線 ThreatBook

✓ 微步在线

✓ 主要对标产品：**Darktrace** NETWORK、**Trellix** NDR

✓ 核心优势

能力	简介
吞吐量与加密	支持 20Gbps 流量镜像，支持加密流量分析，加密通信识别率超过 99%。

精准检测	基于双向全流量检测，及微步业界领先的威胁情报、多维度的流量特征分析能力和特定场景的机器学习分析模型对攻击行为进行深度研判，自动化完成对攻击行为成功失败的判定，最大限度的减少告警“噪音”出现。此外基于对数百个 APT 组织的长期跟踪数据，及时准确地发现针对性攻击。
面向实战	可通过流量对攻击面进行全面梳理，从攻击者视角审视所有可能的攻击入口。包括智能识别 Web 及非 Web 登录入口，审计登录行为，检测弱口令、暴力破解等登录风险，发现业务 API 接口风险及上传接口等。采用非侵入式被动监听的方式不会对企业服务器和网络带宽带来压力和负担，帮助安全团队摸清家底。
响应闭环	具备有效性高达 99%的旁路阻断和联动第三方设备进行自动化联动能力，可有效缩短威胁响应时间，同时基于自动化进程取证，提升企业溯源能力，更好修复黑客攻击路径中暴露出的安全弱点。
可视化	可针对东西流量、内部资产风险可视化呈现，同时从防守视角、外部攻击视角、内部溯源视角、报警视角，全面可视化剖析威胁事件。

- XDR

✓ 深信服

✓ 主要对标产品：**Palo Alto** Cortex XSIAM

✓ 核心优势

能力	简介
极致的本地化服务与响应	在香港拥有极其深厚的本地服务团队。相比 XSIAM 依赖全球支持体系，深信服在香港的 Gartner 评分中，在“服务与支持”和“交付效率”上通常高于跨国品牌。
Security GPT 原生大模型能力	深度集成的 Security GPT 对中文及亚洲企业的办公语言环境理解更深。它能通过对话直接生成研判结论，而不仅是显示复杂的原始日志。
原生“端网”深融合的性能效率	许多香港企业已部署深信服的防火墙或终端等组件，XDR 能与这些原生组件实现零延迟的秒级联动。
直观的“业务视角”可视化 (Attack Storyline)	更侧重于攻击故事线（Storyline），能将琐碎的告警自动拼凑成逻辑清晰的攻击全过程，并直接关联到具体的业务资产。
更高的性价比与投资保护	XSIAM 作为“全家桶”方案，其存储成本和订阅费极高，深信服 XDR 提供了更灵活的部署模式（SaaS 或本地化），且对现有深信服设备的兼容性极强。

- AI XDR

✓ 亚信安全

✓ 主要对标产品：**CROWDSTRIKE** Falcon Insight XDR

✓ 核心优势

能力	简介
一点发现，全网处置	基于 AI 原生的数据驱动检测框架，深度融合云、网、边、端全域的数据采集与处置能力。当检测到一个微小异常点时，可自动关联扩展至客户全网资产，形成“全局威胁视野”，让威胁在扩散前被彻底拦截。在此基础上，威胁会在客户的允许下自动上传到云端威胁情报，

	真正实现“单点发现即全网联动处置”。
扩展检测，全面赋能	通过资产管理实现资产全生命周期清晰盘点，让企业安全“家底”一目了然；借助脆弱性识别这一安全“体检仪”，精准发现漏洞、弱口令、高危端口等防御短板；依托本地云查的海量本地恶意文件库，快速完成文件威胁比对分析；并通过本地情报（TI）沉淀自有威胁情报，强化原子级检测与分析能力。
多维联动，精准闭环	全面覆盖终端、IP、域名、文件、进程、启动项、服务、计划任务等多个处置点，构建“终端精准清除 + 网络全面拦截”的立体防御网。从威胁检测到多维度处置动作的联动执行，比传统安全平台的处置更加精准、更加精细化，更形成真正完整的安全闭环，确保威胁被彻底根除。
AI 增强，智能进化	借助 AI 技术实现安全运营智能化升级，不仅能提供数据查询统计、安全问答、告警 / 事件解读、资产解读、AI 降噪、辅助处置等多元能力，降低对人员专业能力的要求并大幅节约运营分析时间；还能通过归并、语义降噪、关联资产降噪、端网融合分析等一系列 AI 手段精准降噪，帮助安全团队从海量无效告警中解放，专注于关键攻击事件，显著降低运营成本。

- MDR

SANGFOR

✓ 深信服

✓ 主要对标产品：**Sophos** MDR

✓ 核心优势

能力	简介
交互式专家服务	深度集成了 Security GPT（安全大模型）。云端专家不仅提供研判结果，还能通过 AI 助手以自然语言即时回答用户的疑问。
更贴近香港客户的“本地化”专家值守	在香港设有专门的技术支持与安服团队。Sophos 的服务中心主要分布在欧美，存在一定的文化和时区惯性。
端网云深度联动的“闭环响应”能力	强在对自家“全家桶”（防火墙、EDR 等组件）的控制力。专家在云端发现威胁后，可以跨设备执行极其精准的联动阻断。
针对亚洲威胁环境的“主动猎捕”	威胁情报库（Threat Intelligence）对亚洲地区、尤其是大中华区特有的黑客组织、漏洞利用和定向攻击脚本有更深入的积累。
直观的“服务结果”可视化	提供非常符合管理层审美的运营可视化中心。它不仅展示拦截了多少病毒，还能量化“响应时效（MTTR）”和“业务风险趋势”。

- PAM / 堡垒机

✓ 天融信

✓ 主要对标产品：**CyberArk** PAM

✓ 核心优势

能力	简介
账号管理	包括主账号和从账号管理，主账号为用户账号，从账号为原 IT 系统帐号。通过主从账号的方式，将身份和授权分离开来，增强身份认证和系统授权的可靠性，从本质

	上解决帐号管理混乱问题，为认证、授权、审计提供保障。
身份认证	为提高访问安全性，系统提供高强度身份认证功能，支持本地认证与第三方认证服务器对接，如 AD 域、LDAP、Radius 等，另外支持 OTP 动态令牌、短信、UsbKey、数字证书、人脸识别等多种认证方式进行双因子强认证，保证身份可靠性。
集中授权	强调的“集中”是逻辑上的集中，而不是物理上的。系统提供统一的授权界面，不但可以做到基于应用边界的粗粒度授权，例如授权用户可以访问哪些资产，还可以做到基于应用内部的细粒度授权，例如限制用户的操作行为。
操作审计	将人员的操作记录为日志，管理人员可以在系统中查看相关的审计日志。操作审计主要审计人员的帐号管理、认证、账号分配情况、权限分配情况、账号使用（登录、资源访问、操作行为）等情况，所有操作有据可查。
自动改密	支持包括 Windows、linux/Unix、数据库及网络设备的自动改密。可以手动或周期性自动执行，密码复杂度支持自定义。通过自动改密，解决多资产、多账号的密码修改费时、费力和安全存储问题，在资产运行过程中实现无干预的定期批量改密，有效执行单位的强密码策略，落实安全管理制度，同时减轻管理员工作负担，提高资产安全性。

- 漏洞管理

✓ 绿盟科技

✓ 主要对标产品：**Tenable** Nessus Pro / Web App Scanning / Security Center / Vulnerability Management、**Qualys** Vulnerability Management (VMDR) / Web Application Scanning (WAS) / Compliance Solutions

✓ 核心优势

能力	简介
丰富的漏洞、配置知识库	支持扫描的漏洞数量超过 30 万条，涵盖各主流系统、数据库、应用，支持 CVE，CNVD，CNNVD 等国际及中国内地专业漏洞库。配置核查知识库提供 7 大类 60 多种产品 150 多个版本的系统的配置检查库，提供专业加固修补建议，以及多个行业的安全配置检查标准。
新 IT 资产全覆盖，全方位系统脆弱性发现	能够发现云计算、大数据、物联网、容器镜像、AI、大模型等新型 IT 资产的漏洞，以及传统系统漏洞，形成整体安全风险报告。
专业的云端情报支撑	依托绿盟威胁情报中心（NTI）多年的威胁情报运营，第一时间跟踪紧急漏洞的爆发，快速预警处置。
创新的漏洞处置优先级算法	基于威胁的多维度（热度、POC、恶意软件），基于业务的多维度（重要性、级别、是否防护）结合领先的算法重新定义漏洞处置优先级。
多源漏洞融合	支持各类异构厂商的扫描结果漏洞、渗透测试漏洞、外部通报、漏洞情报等多个维度的漏洞统一接入、融合分析、集中处置。

● 威胁情报

微步在線 ThreatBook

✓ 微步在线

✓ 主要对标产品：**Mandiant** Threat Intelligence、**RSA** FraudAction

✓ 核心优势

能力	简介
海量数据与高精准度	ATI 依托百亿级威胁样本库与千亿级基础设施数据；NGTIP 与 ATI 均实现 99.9% 的高精准度，确保情报置信度。
专业的 APT 与高级威胁追踪能力	核心能力源于微步情报局的研究成果，通过 ATI 与 NGTIP 输出，独家揭露大量 APT 组织、事件与零日漏洞。
本地化部署与云端服务的灵活交付	ATI（SaaS 及云 API）提供敏捷、可扩展的云端订阅与服务化接入。
强大的漏洞管理与预警能力	NGTIP 提供系统化的漏洞检测、处置及预警，依托平台对数百信源的实时监控与情报研究。
实时、多源的情报生产和更新体系	ATI 与 NGTIP 共享 3000+情报源及微步情报局独家研究成果、多语言报告构成的动态情报网络，支持报告级与小时级更新。
极大提升安全运营效率	NGTIP 通过高精准失陷情报，可直接为 SOC/SIEM 平台实现≥85% 的告警降噪，提升响应效率。
自动化数字风险暴露面监控与处置	DRPS 服务为中国境内外企业提供对仿冒 APP、网站、资产泄露等数字风险的 7x24 小时自动化监控与专业处置服务。

- DLP

天空卫士 SkyGuard

- ✓ 天空卫士
- ✓ 主要对标产品：**Forcepoint** DLP、**Symantec** DLP
- ✓ 核心优势

能力	简介
全维度海外生态兼容适配	极强的跨生态兼容能力，可与海外主流办公及系统生态无缝衔接，完美适配 Windows AD 域控管理、各类 Proxy 代理服务，能稳定兼容 M365 全系应用，保障邮件、文档协作、云端存储等核心办公场景顺畅运行。同时全面支持 MIP 信息保护功能，可实现数据加密、权限管控等安全操作，无需额外部署兼容插件或做系统改造，直接融入海外现有 IT 生态环境，保障跨生态业务协同无阻碍，适配海外办公及业务部署需求。
高标准全场景稳定运行	聚焦全链路稳定性，尤其针对终端设备的稳定表现做重点优化，大幅减少因设备故障、功能异常导致的业务中断。日常运行中可始终保持稳定输出，核心功能精准发挥作用，边缘功能无卡顿、闪退等问题，面对高负载、多任务并发等复杂场景仍能平稳运行，无需频繁运维排查，有效降低运维成本。
跨平台功能与体验高度一致	全面支持 Windows、MacOS、Linux 三大主流操作系统，实现多平台功能 1:1 同步覆盖，无平台差异化功能删减或功能降级，保障不同系统用户享受到同等的使用体验。同时搭载统一标准化配置界面，界面布局、操作逻辑、配置路径完全一致，用户在不同平台切换使用时，无需重新熟悉操作流程。
专业化高效能技术支持服务	构建完善的全流程技术支持体系，提供专业英文服务，适配海外用户及国际业务沟通需求。配套齐全的知识库（KB），涵盖常见问题、操作指南、故障排查等内容，方便用户自主查询解决问题；搭建高效工单系统，支持问题快速提交、进度实时追踪，保障问题闭环管理。

最佳实践

DIRECTORY

目 录

客户背景

作为国务院组成部门，下设22个机关司局和全国30个直属单位，业务规模庞大，部委信息中心在网络安全管理和监督方面承担着重大的责任和压力。特别是伴随着网络安全法正式施行，国家级攻防演练逐步扩大，网络安全建设进入深水区，实战攻防效果和运营响应效率成为更受关注的建设目标。

为了强化可内外协同、上下联动的主动监测预警能力、可对抗有组织攻击的纵深防御能力、可及时进行事件处置的应急响应能力建设，提升部委机关网络安全防护水平，建设方根据《中华人民共和国网络安全法》及部委网络安全顶层设计，将建设内容确定为六个方面，即

一、补充完善网络安全防御设施
二、建设网络安全威胁信息采集系统
三、建设网络安全大数据平台
四、建设网络安全威胁感知预警系统
五、建设网络安全决策指挥系统
六、系统集成

立项驱动因素 – 管理层面

确立“安全，实用”总基调，筑牢网络安全底线，推进智慧水利建设

合法合规角度	外部视角	内部视角	领导高度重视
			
《中华人民共和国网络安全法》第31条明确要求水利在内的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护；32条明确要求安全技术措施同步规划、同步建设、同步使用。	随着攻防新技术的发展和应用、未知威胁愈发普遍，0day漏洞频繁爆发，网络安全事件造成的影响力和破坏力持续加大，对组织的安全建设提出了更高要求。	具备“一点击破，全线失守”的特点，组织规模庞大，下属流域及各事业单位网络安全建设水平不一，IT信息资产尚未形成统一有效的盘点和监控。	部委党组高度重视网络安全，部领导在网信工作会议上明确指出：网络安全是底线，是一件不容商量的事，不论多难，也要千方百计地去消除隐患，并且要快。

立项驱动因素 – 技术层面

1、缺乏体系化的安全建设使得安全问题频发，现有技术工具无法为运营人员带来助力，反而让精力分散。主要表现在：

- 零散的安全设备看不清全局态势
- 内外环境快速变化频繁出现安全短板
- 海量安全日志让真实攻击难以定位

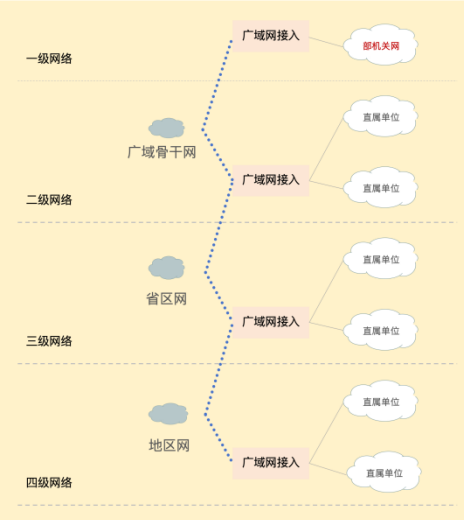
2、亡羊补牢式的被动安全运维并不是安全工作的初衷，同时运维工作量大、人员能力不足严重制约了运维效果。主要表现在：

- 运维被动响应并没有减少问题发生
- 每日的海量告警延缓了处置响应的时效性
- 人员能力差距导致无法提供有效的保障

3、仅仅停留在纸面的工作机制不清晰、不落地，运维工作执行不够规范，无法达成预期效果。主要表现在：

- 各部门的权责不清，工作推动困难
- 事件场景未分级分类，处置无依据
- 机制流程停留在纸面，执行效果差

需求分析



网络环境复杂，面临多层面的安全问题

（1）组织机制不健全
- ✓ 缺乏有效协同的运营机制

（2）信息资产不清晰
- ✓ 不能实时准确掌握资产的动态信息

（3）基础安全问题仍是重大隐患
- ✓ 缺乏适应业务场景的威胁发现、研判能力
- ✓ 异构的安全组件未能发挥1+1>2的效果

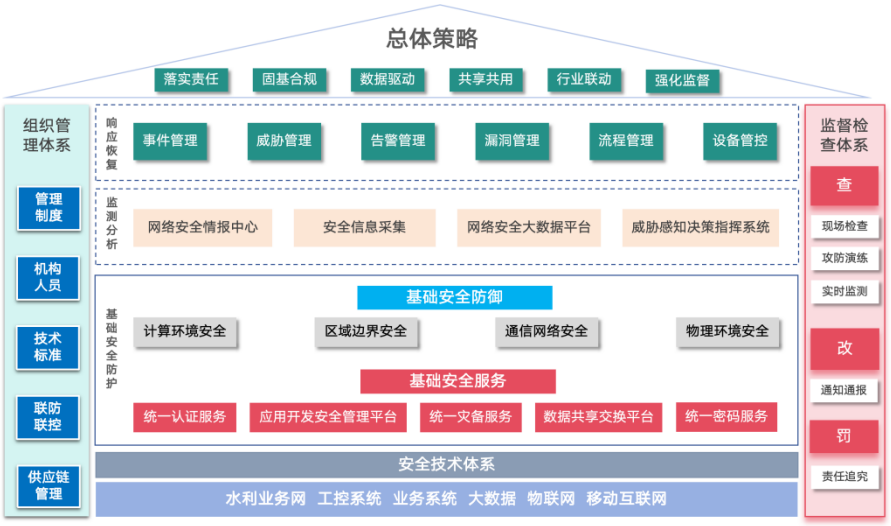
（4）行业短板问题突出
- ✓ 缺乏行业上下的联防联控

最终集中体现在，建设前运营工作繁重，但HW攻防实战成绩不佳

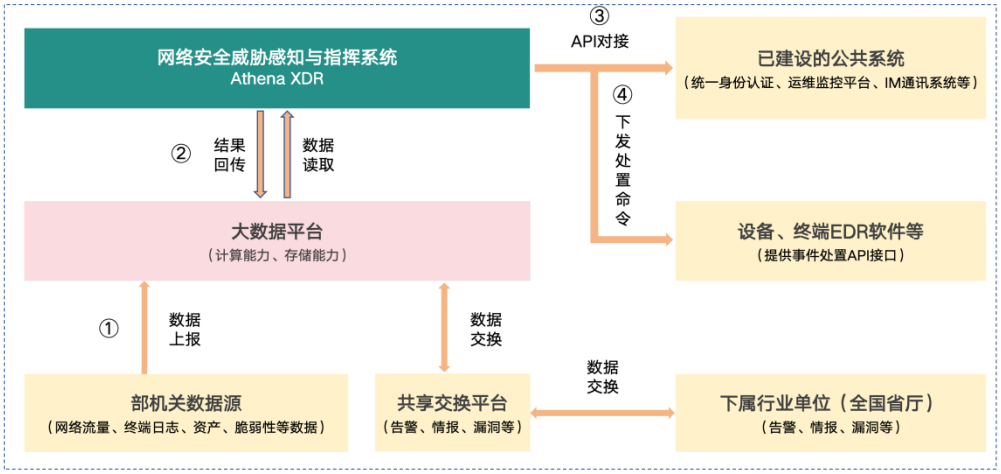

建设思路
数据驱动安全理念落地，平台补齐组件能力差距
优质的、完整的一手遥测数据 + 丰富的检测分析框架 -> 好的效果
资产、脆弱性、威胁集中汇聚，相互关联，统一运营
安全运营闭环，打通多人协作的响应处置流程
漏洞闭环管理流程
安全事件研判、遏制、处置闭环流程
全面管理资产，建设基本的出入库流程
系统开放性，能够支撑未来持续扩展与演进
标准数据集，标准检测框架，多源安全组件效果提升
开放API，灵活的数据接入、关联建模、SOAR剧本编排、联动组件对接、可视化扩展


DIRECTORY
目 录
01 建设背景
02 实践成果
03 效果总结

总体策略


总体策略
落实责任
固基合规
数据驱动
共享共用
行业联动
强化监督
组织管理体系
管理制度
机构人员
技术标准
联防联控
供应链管理
响应恢复
事件管理
威胁管理
告警管理
漏洞管理
流程管理
设备管控
监测分析
网络安全情报中心
安全信息采集
网络安全大数据平台
威胁感知决策指挥系统
基础安全防护
基础安全防御
计算环境安全
区域边界安全
通信网络安全
物理环境安全
基础安全服务
统一认证服务
应用开发安全管理平台
统一灾备服务
数据共享交换平台
统一密码服务
安全技术体系
水利业务网 工控系统 业务系统 大数据 物联网 移动互联网
监督检查体系
查
现场检查
攻防演练
实时监测
改
通知通报
罚
责任追究

平台架构


网络安全威胁感知与指挥系统
Athena XDR
③
API对接
已建设的公共系统
（统一身份认证、运维监控平台、IM通讯系统等）
④
下发处置命令
②
结果回传
数据读取
大数据平台
（计算能力、存储能力）
设备、终端EDR软件等
（提供事件处置API接口）
①
数据上报
数据交换
数据交换
部机关数据源
（网络流量、终端日志、资产、脆弱性等数据）
共享交换平台
（告警、情报、漏洞等）
下属行业单位（全国省厅）
（告警、情报、漏洞等）

DIRECTORY

目 录

效果总结：数据驱动安全

多源数据汇聚，XDR+GPT持续研判分析

威胁数据：

- 流量探针10+台，终端安全2套

资产数据：

- SIP、EDR、白帽汇、画方等多种设备

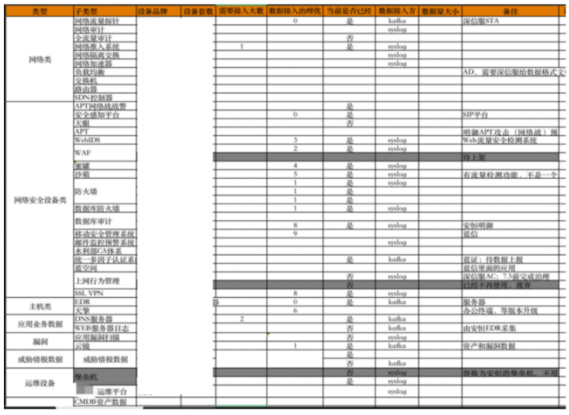
脆弱性数据：

- 漏洞管理系统，云镜、小智等

组件联动：

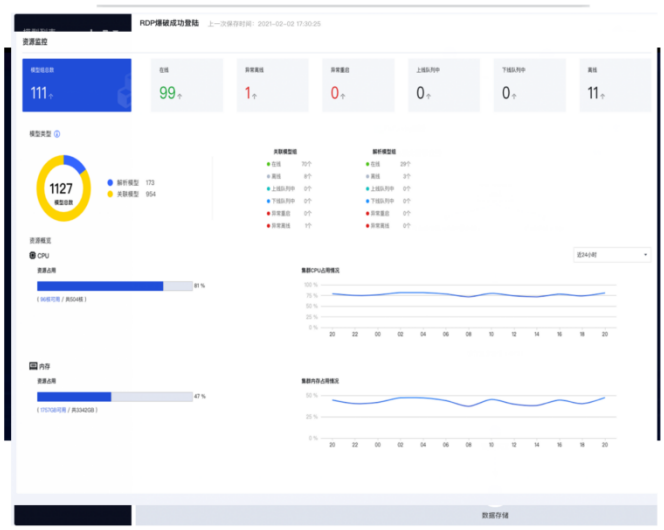
- 自建大数据平台、集中管控平台、蓝信、准入、邮件、短信等多种组件

共计接入数据源20多类、70多台设备/系统



效果总结：检测效果提升

- 基于安全数据治理能力，为安全运营工作构建统一运营界面
- 通过清晰的人员岗位设置及运营流程机制，结合自动化剧本的构建，将原有需要数据小时完成处置的工作提升到1小时内
- 通过运营团队威胁挖掘帮助部委发现多项潜藏攻击，并基于攻击路径分析修复了安全短板
- 构建100+威胁模型匹配高级威胁，同时为部里及下级单位提供检测能力支撑，同时实现海量告警降噪



安全效果效率全面提升，行业联防联控初见成效

围绕网络安全威胁和脆弱性，依托深信服XDR+GPT方案，建立起网络安全联防联控机制，逐步实现“一处预警、处处设防，一处威胁、处处处置”的目标。仅2022年，行业共享威胁预警5000多次，联合处置70多起高危网络安全攻击。

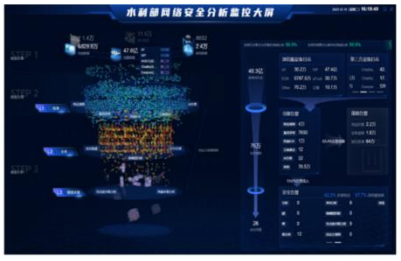
建设前	建设后
防护300+重要信息系统，使用30+个安全设备	每天只登陆1个平台，完成安全监控与分析
日均安全告警数量千万级	自动研判准确分类，日均100条内精准安全事件
告警处理平均闭环时间5小时以上	处置闭环平均耗时30分钟左右
缺少多源异构数据分析能力和APT攻击发现能力	XDR+GPT双引擎，提升威胁发现和研判分析能力
安全运营效率不高，驻场需求大，难以保障7*24	安全GPT加持，1人驻场+远端支持足以应对日常威胁运营

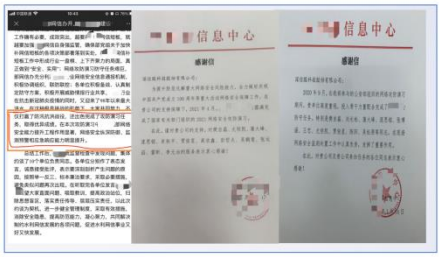
国家级攻防演戏持续第六年优异

2023年水利网信（数字孪生水利）

水利行业在网络攻防实战演习中再创佳绩

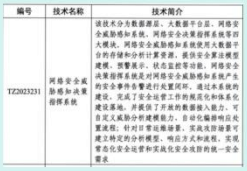
2023年，水利行业参演单位数量历年最多，覆盖全部水利关键信息基础设施运营者，长江委、黄委、海委、水利报社、浙江、江西、湖北、宁夏、深圳、大连等组织开展专项攻防演练。水利部在国家级网络攻防实战演习中连续第6年获“优异”最高等次，水利部信息中心、南水北调中线公司、长江委、海委、湖北组建水利行业攻击队，第一次作为攻击方参演，多项技战法入选优秀技战法汇编。





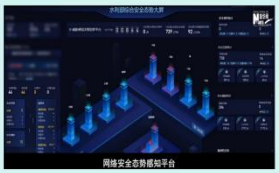
信息来源：http://www.mwr.gov.cn/ztpd/2024ztbd/slwxszlsslsjdspx23/jggs/

项目成果及行业认可情况



编号	技术名称	技术简介
TZ2023231	网络安全威胁感知决策指挥系统	该技术分为数据源层、大数据平台层、网络安全威胁感知系统、网络安全决策指挥系统四大模块。网络安全决策指挥系统使用大数据平台的存储和分析计算资源，提供安全算法模型建模、预警展示、状态监控等功能。网络安全决策指挥系统是对网络安全威胁感知系统产生的安全事件告警进行处置闭环，通过本系统的建设，完成了安全运营工作的规范化和体系化建设落地，并提供了开放的数据接入能力，可自定义威胁分析建模能力，自动化编排响应处置流程；针对日常运维场景，实现流程场景可建立特定的分析模型，响应方式和流程，实现常态化安全运营和实战化安全攻防的统一安全需求

《水利先进实用技术重点推广指导目录》2023年度



数字化转型先行者 | 从治水到“智”水-水利部态势感知大屏展示（新华网）

网络安全技术应用试点
水利部信息中心联合

CSO 二十大杰出安全项目
水利部网络安全威胁与决策指挥系统

7	关键信息基础设施（水利）网络安全关键技术与应用	水利部信息中心、河海大学、深信服科技股份有限公司、[redacted]公司、[redacted]公司、[redacted]公司	付静、詹全忠、张潮、许峰、钱峰、周维续、谢文君、杨旭、吕鑫、沈智镇、陈岚、邹希、范宇楠、古亮、殷悦

水利部信息中心、河海大学、深信服科技股份有限公司等公司共同参与完成的：“关键信息基础设施（水利）网络安全关键技术与应用”入选2022年度大禹水利科学技术奖拟授奖名单一等奖。

4	AI大模型深度赋能，建立数据安全智能防线	水利部信息中心	水利部信息中心、深信服科技股份有限公司

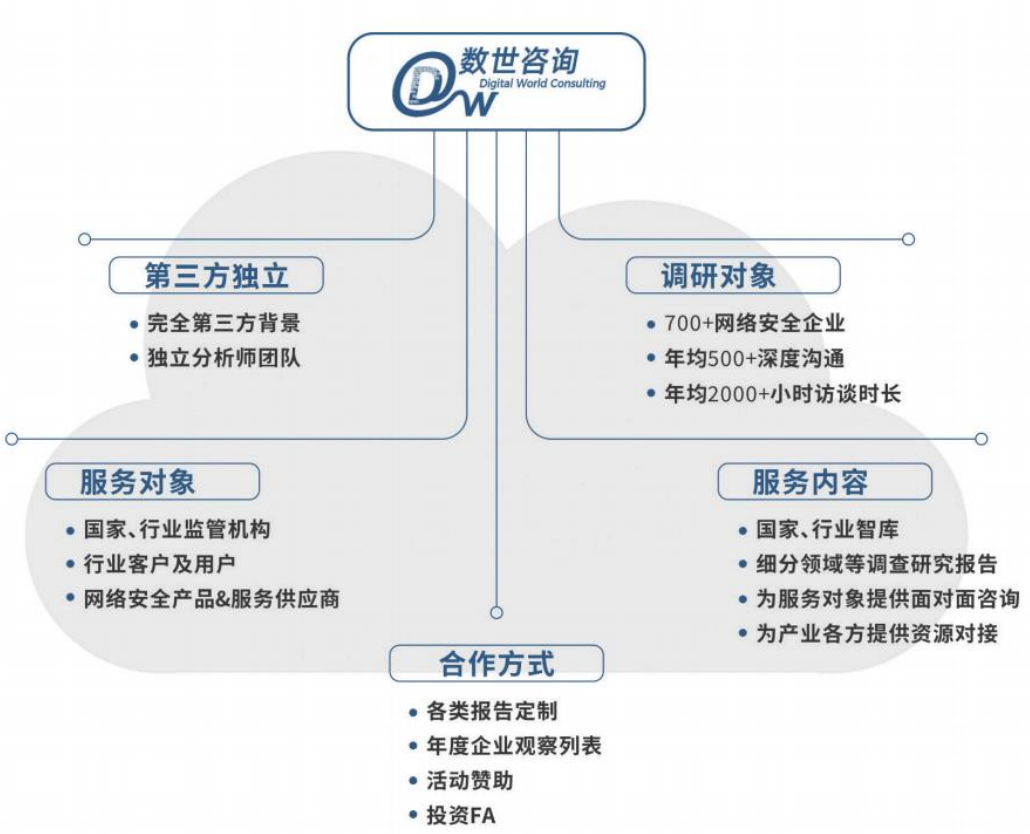
入选《数字孪生水利建设典型名录》

主笔分析师信息

靳慧超（Anatole Jin）
数世咨询 • 战略分析师
16601182683（微信同号）
添加时请注明“公司-姓名”

曾就职于神州数码集团-安全 BG、启明星辰集团-战略咨询中心、360 集团-城市产业事业部，主要负责安全咨询、规划等工作

现任数世咨询战略分析师/合伙人
负责战略规划、产业咨询等工作，研究方向为数据安全、AI 安全、软件供应链安全、安全运营



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