ISC.AI 2025
创新性案例

目录

CONTENTS

安全智变，AI赋能新力场

—— ISC.AI 2025 创新百强评选活动

在全球数字经济与智能化浪潮持续演进的背景下，人工智能正以前所未有的速度重塑产业形态、业务模式与生产力结构。进入 2025 年，AI 的应用已从局部试点迈向规模化、体系化落地阶段，逐步演变为支撑企业运营、产业升级与社会治理的重要基础能力。

普华永道在其发布的《2026 年全球数字信任洞察（Global Digital Trust Insights 2026）》报告中指出，人工智能已跃居企业网络安全与技术投资议程首位，近 50% 的受访组织明确表示，正在将 AI 作为提升网络防御能力与风险治理水平的核心技术支撑。与此同时，Gitnux 行业统计研究显示，超过 60% 的网络安全预算已被专门投入至 AI 工具与智能防护系统的研发与部署中，并预测 AI 驱动的安全解决方案在未来几年内有望协助阻断 90% 以上的网络攻击行为。

然而，技术红利释放的同时，安全风险亦在加速演化。据 TechRadar 发布的《AI powering a dramatic surge in cyber threats》相关数据显示，借助 AI 的自动化威胁扫描规模已达到每秒 36,000 次，攻击呈现出高度自动化与规模化趋势。埃森哲发布的全球安全调研进一步指出，90% 的企业尚未为 AI 驱动的安全挑战做好充分准备，36% 的安全与技术负责人认为 AI 安全发展速度已超过组织现有防护能力。

这些数字不仅反映了技术创新本身所带来的防护压力，更深刻揭示出一个现实问题：在智能化浪潮下，安全防护体系若无法与 AI 技术协同演进，原本应释放的“技术红利”反而可能转化为新的系统性风险源。

正是在这一背景下，数字安全与智能体技术的融合创新，成为全球范围内的核心议题。无论是在产业界、学术界，还是在监管与治理层面，围绕“AI 如何赋能安全、如何以安全护航 AI”的探索正在持续深化。以中国为例，“AI 赋能网络风险防控”已逐步成为行业共识，多场国家级会议与行业论坛聚焦如何通过 AI 技术提升安全事件的实时感知能力、风险预测能力与防御体系的智能化水平。在产业实践层面，国内安全企业相继推出多种基于 AI 大模型的安全产品与解决方案，覆盖智能告警分析、自动化威胁响应、动态渗透测试与防护等多个环节，充分体现了 AI 技术在安全运营与攻防对抗中的关键价值。

基于此，本届 ISC.AI 2025 创新百强评选活动将主题确定为“安全智变，AI 赋能新立场”，旨在回应智能时代数字安全发展的两大核心命题：

一是，安全已不再是单一的防御问题，而是需要构建具备智能感知、动态演进与协同对抗能力的综合安全体系；

二是，AI 不再只是提升效率的生产力工具，而正成为新一代安全体系的动力引擎与战略支撑点。

在智能化发展的“双刃剑”效应日益凸显的当下，“AI 赋能安全”已不再停留在理念层面，而是成为产业与商业实践中的现实命题。正是在这一关键节点上，启动并持续推进数字安全创新百强评选，具有鲜明的时代意义与现实价值。

本次评选活动立足全国范围，聚焦数字安全与 AI 融合发展的前沿实践，对具有代表性的创新案例进行系统筛选、专业评估与集中展示，力求真实反映行业发展趋势与创新成果。通过评选与案例集的形成，我们希望逐步构建：

- 一个能够客观呈现技术突破与创新价值的**“灯塔案例库”**；
- 一个促进产学研用深度联动、推动跨界协同的生态交流空间；
- 一个加速智能安全技术规模化落地、助力产业融合发展的实践平台。

在评选过程中，评审视角不仅关注技术本身的先进性，更强调创新成果在真实业务场景中的应用价值、落地能力与行业普适性。典型的安全与 AI 融合创新，既包括智能威胁检测、自动化响应、数据安全治理等传统安全能力的智能化升级，也涵盖利用 AI 提升安全运营效率、构建安全智能体体系、推进自主可控安全系统建设等更具前瞻性的探索方向。

以往届成果为例，根据 ISC.AI 发布的前期案例洞察报告显示，2024 年数字安全创新百强案例已呈现出多项清晰的发展趋势：从基于安全大模型构建安全智能体，到依托 AI 实现跨域 XDR 协同防御，再到智能化威胁狩猎与自动化防御体系的系统化建设，安全创新正由单点技术突破向整体解决方案演进，并逐渐成为政策制定、产业投入与技术布局的重要参考依据。

更为重要的是，安全创新早已超越单纯的技术范畴，成为衡量产业竞争力与国家数字治理能力的重要组成部分。在我国推进数字经济与智能化转型的过程中，网络安全与 AI 安全持续上升为经济社会稳定运行的基础性力量。《网络安全法》《数据安全法》《生成式人工智能服务管理办法》等一系列法律法规的出台，既体现了对技术发展趋势的积极回应，也为“如何安全、可控、负责任地应用 AI”明确了制度方向。

因此，通过本次评选活动与案例报告的发布，我们期望进一步实现以下目标：

- 汇聚行业共识：推动安全与AI深度融合成为产业发展的广泛共识；
- 激发生态创新：以典型案例引导企业与科研机构持续探索智能安全新模式；
- 促进产业协同：强化政府、资本、企业与高校之间的协作联动；
- 提升风险应对能力：增强组织与行业对AI安全风险的识别、评估与实战防护水平。

总体而言，“安全智变，AI 赋能新立场”不仅是本届评选活动的主题概括，更是数字安全产业在智能时代的战略指引。它既回应了时代带来的挑战，也明确了技术与实践的演进方向，为行业在不确定性加剧的环境中实现稳健发展提供了清晰的行动框架。

本报告将围绕上述主题，系统呈现入选的创新案例，从应用场景、技术架构与行业影响等多个维度进行深入解析，力求为政府主管部门、产业界、研究机构及广大从业者提供具有前瞻视野与实践价值的参考样本。

360安全智能体“以模治模”解决AI安全问题

案例提供方：360数字安全

案例背景：

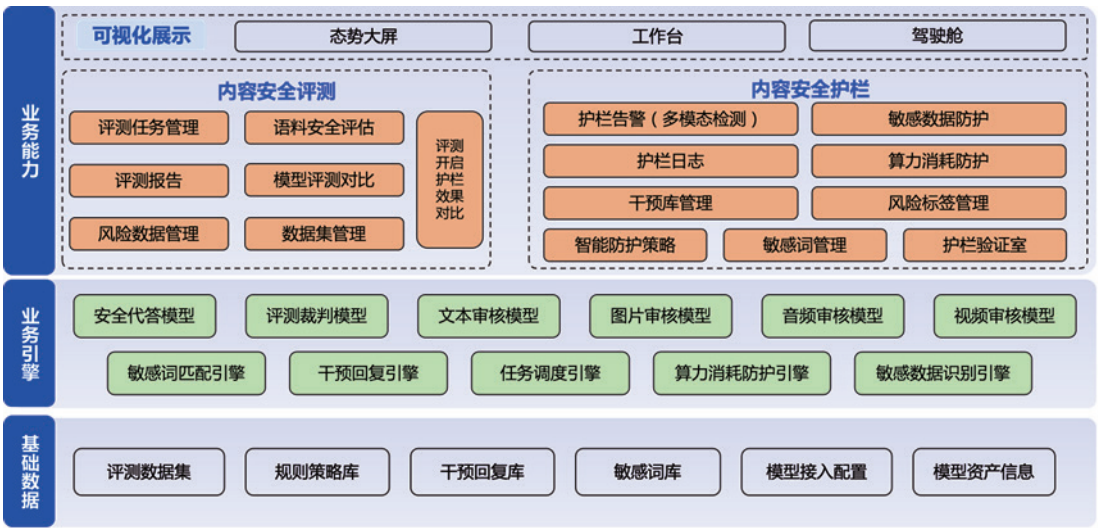
《关于深入实施“人工智能 +”行动的意见》明确指出，人工智能已成为驱动经济社会高质量发展的关键引擎，推动各行业领域智能化转型已然成为不可逆转的时代大势。与此同时，《意见》着重强调，安全保障能力是智能化应用落地的八大基础支撑之一，这一定位深刻凸显了 AI 安全在“人工智能 +”行动中的基础性、保障性地位。内容安全直接关系到企业智能化的合规性与社会价值，一旦内容失控，不仅直接危害社会安全、触碰法律红线，更会彻底摧毁 AI 系统的信任根基。因此，内容安全成为 AI 安全治理必须攻克的首要命题。

内容安全作为大模型安全的核心环节，直接关系到企业智能化的合规性与社会价值。随着大模型生成内容的规模化应用，内容安全风险已成为行业突出隐患：一方面，大模型别有用心者被诱导后可能生成虚假信息、暴力色情、歧视性言论等有害内容，若流入公共领域，将引发舆论混乱、损害用户权益，危害意识形态安全，甚至可能导致数据、技术泄露等风险，导致企业核心竞争力直线下降；另一方面，企业在利用大模型开展、政务咨询、内容创作、客户服务时，若内容存在合规风险，可能面临监管处罚、品牌声誉受损等风险。

在此背景下，市场对大模型内容安全防护产品的需求愈发迫切：企业亟需能够实时拦截有害内容、确保生成内容合规的工具，政府及监管部门也需要通过专业产品实现对大模型内容输出的有效监管，保障“人工智能 +”背景下内容生态的安全、健康与有序，内容安全成为 AI 安全治理必须攻克的首要命题。

解决方案：

360 大模型卫士兼具大模型内容测评与大模型内容护栏双重核心能力，专注大模型内容安全防护。基于“以模治模”、“以测促防”的设计理念，提供智能判定机制、风险内容检测、敏感问题代答、内容安全测评等关键技术，提供“自动化、高准确率、低成本”的内容安全评测和全链路内容安全防护能力，实现“输入输出内容安全，大模型价值观对齐”的防护目标，帮助企业筑牢大模型内容安全防线，实现技术价值与社会责任的统一。



事前评测：通过百万级风险题库与裁判大模型，在模型上线前与运行过程中实施系统性安全评测，主动评测业务模型在针对违规提问、诱导提问等方面输出内容的安全性，实现“风险前移、以测促防”。

事中防护：融合传统静态匹配与 AI 动态泛化识别能力，构建五道安全防线，针对算力消耗、违规输入、对抗性提示词攻击、敏感数据泄露等风险行为展开实时防护，并智能调用安全代答大模型对风险查询生成向善合规应答，兼顾 AI 应用安全与用户体验。

事后迭代：基于实际风险处置数据，持续优化防护策略与题库，及时新增新型攻击模式的检测规则，推动安全防护能力螺旋式提升。

核心技术路线：

风险检测大模型：专攻内容风险与攻击手段识别，精准捕捉隐喻违规、复杂诱导等隐蔽风险，囊括 100+ 内容安全风险类目，保证召回率的前提下，风险检测准确率高达 90% 以上；相比传统规则匹配式方案，产品检测精准度遥遥领先，显著提升内容安全管理的深度和广度。基于检测到的风险内容的分类，在不同的业务上配置不同的策略，给出不同的分级处置建议。

安全代答大模型：聚焦敏感问题合规回应，通过安全预训练、监督微调、强化学习、RAG 增强等专项训练加持后，能够将裸模型安全评分（百分制，越高即越安全）从 78 提升至 96 以上，实现用一个“安全向善”的大模型专门对敏感问题进行安全代答，减少大模型输出内容安全风险，更好地平衡用户体验和安全性。

评测裁判大模型:专用于评估 AI 生成内容是否安全，能够对 AI 输出的文本进行自动化的安全性判断与评分，涵盖多种风险类型，如涉政、暴力、色情、歧视、虚假陈述、价值观偏差、敏感信息暴露等，判定结果人工一致率 95% 以上。

红蓝对抗大模型：专用于自动化构建动态内容安全评估数据集，通过多维度攻击体系构建与动态样本生成机制实现突破，确保评测任务持续紧贴前沿攻击策略与风险热点，以动态、智能的评估方式构建可持续演进的安全评测体系。

创新性与价值：

技术价值：突破大模型内容安全防控技术瓶颈，填补行业空白。本项目创新性提出“以模治模”的技术理念，通过专项训练评测裁判大模型、风险检测大模型、安全代答大模型，借助安全大模型的语义识别、智能分类、风险泛化识别、内容生成等能力，应对业务大模型针对敏感输入无防护、违规输出缺审核的问题，填补了当前大模型内容安全领域的技术空白，提供可落地的技术范式。

管理价值：构建大模型内容安全标准化运营体系，降低企业管理成本。提供“评测 - 防护 - 优化”的一体化能力，打破传统“分散式管理”的弊端：从模型上线前的风险评估，到运行中的实时拦截，再到事后的策略优化，全流程数据互通、策略联动，无需在多系统间切换即可完成风险闭环管理。不仅减少了安全团队的沟通成本与操作复杂度，还能通过全局风险视图快速定位高优先级问题，显著提升内容安全管理的系统性与效率。

合规价值：助力企业落实监管侧内容安全合规要求，规避监管风险。将复杂、模糊的法律条文，转化为简单、清晰、自动化的技术流程。通过产品内置的合规性评测体系与实时防护机制，可覆盖监管对大模型应用的合规要求：在模型备案阶段快速完成自评估并生成合规报告，提升备案通过效率；在日常运营中自动拦截违规内容、输出合规回复，避免因内容不合规引发监管处罚、品牌声誉受损等问题，让企业在合法合规的框架内安全开展 AI 业务，将合规成本从不可控的人力开销，转变为可预期的技术投资。

社会价值：保障大模型内容生态安全，支撑“人工智能 +”行动健康发展。从行业层面，通过输出标准化的内容安全解决方案，推动大模型行业建立内容安全准入门槛与运营规范，促进行业良性竞争；从社会层面，产品可有效拦截虚假信息、暴力色情、歧视性言论等有害内容，防止其通过社交平台、短视频等渠道扩散，维护意识形态安全与公共利益，保障用户权益；同时，通过解决内容安全这一核心障碍，为“人工智能 +”行动在政务、医疗、教育等关键领域的深度应用扫清障碍，助力智能化转型真正实现“安全落地、价值落地”。

应用效果：

案例一：360 自有 AI 业务实践

在 360 自有 AI 大模型业务实践中，日均守护 1.5 万卡算力集群、3000P+ 算力及数十条核心 AI 业务链路，为业务稳定运行筑牢安全防线。在内容安全方面，通过部署 360 大模型卫士，可将开源大模型安全性提升 10-30%。

案例二：守护东博会 AI 应用内容安全向善

第 22 届中国 - 东盟博览会在会展中深度融合人工智能技术，设有重要活动、智慧餐饮、智慧物流等 19 项 AI 服务，以提升会展体验，需要持续守护 AI 服务内容安全向善。360 大模型卫士在会议前期先后经历两轮攻防演练实测，成为内容安全防护主力系统，在会议开展期间，精准识别用户输入与 AI 输出中的各类风险，准确率超 95%，累计拦截恶意请求 117 次，识别攻击行为 571 次，代答可疑请求 790 次。

案例三：支撑某监管部门监管备案大模型内容安全

某市 WXB 需履行对已备案生成式人工智能服务内容安全监管职责，利用 360 大模型卫士接入 8 个备案大模型，完成 100+ 检查，积累专项评测数据集超 100 万条，形成扎实的数据支持与决策依据。

经验总结：

首创“以模护模”理念，破解传统防护失效难题。技术路线的核心是颠覆传统安全思路。基于关键词、规则等传统方式无法有效防御由 AI 驱动的新型、语义层面的攻击。为此，360 首创“以模护模、以测促防”的设计理念。产品架构并非单一模型，而是由风险检测、安全代答、评测裁判等多个专业大模型构成的立体防护体系，用 AI 的思路去解决 AI 自身的安全问题。这一设计理念从根本上破解了“传统安全手段在新威胁面前失效”的难题。面对复杂的提示词攻击、内容合规风险和模型“幻觉”等问题，该体系能够进行智能、精准的语义理解和风险判定，实现了从被动防御到主动、智能防御的范式转变。

激活存量安全数据资产，破解高质量语料稀缺难题。充分利用 360 二十年积累的核心资产，将全球独有的样本库、威胁图谱、漏洞库、攻防技战术知识等海量、高质量的安全大数据，作为训练安全大模型的核心语料。同时，结合搜索引擎沉淀的海量合规数据，为模型构建了扎实的数据支撑。此举成功破解了 AI 领域最关键的“高质量、专业化训练数据稀缺”的难题。它解决了模型训练的“冷启动”问题，确保我们的安全大模型从诞生之初就由真实世界的攻防数据“喂养”长大，这是其具备实战能力、保障高准确性的根本原因。

风险情报驱动的数字供应链安全治理实践

案例提供方：悬镜安全

案例背景：

随着电信行业数字化转型深入推进与软件技术栈的日益复杂，软件从需求设计、组件选型、开发测试到部署运维的全流程中，数字供应链已广泛涉及大量第三方供应商，涵盖上下游众多主体、海量第三方组件与许可证，逐渐形成一个复杂交织的软件供应链体系。随着供应链环节的不断延伸，安全风险点持续增多，其重要性愈发凸显。当前主要痛点集中体现在供应链资产“看不清、管不全”、漏洞风险“响应慢、控不住”、供应商与组件准入“缺手段、难闭环”等方面。为此，企业亟需构建一套与自身高速研发节奏相匹配的、具备主动免疫能力的数字供应链安全治理体系，其核心需求包括：

1. 风险情报驱动的漏洞智能响应与闭环管控：建立多源风险情报聚合引擎，整合全球开源漏洞库（NVD、CVE）、通信行业风险情报、软件供应链投毒数据等，实现漏洞情报的实时同步与智能分析；
2. 供应链资产全链路可视化与精准管理：针对在研与在运项目，实现软件物料清单（SBOM）的自动生成与动态管理，覆盖开源组件、第三方 SDK、软件包等依赖项，并进行多层传递依赖关系的深度解析；
3. 供应商与组件制品安全准入生态协同：建立供应商安全准入评估体系，对外部合作伙伴实施安全能力分级管理，要求交付的组件包、容器镜像等制品通过自动化安全检测，包括组件漏洞扫描、许可证合规分析、恶意组件检测等环节。

关键挑战：

在推进电信行业在推进数字供应链安全治理实践中，电信行业主要面临软件成分解析、数据整合、漏洞情报利用等多维挑战：

挑战一：复杂异构技术栈下的软件成分精准解析。电信行业软件研发涉及多种技术形态与海量第三方组件，组件依赖层级深，关系复杂，传统软件成分分析（SCA）工具难以有效识别深层依赖依赖，导致供应链资产可视性不足。

挑战二：二进制、固件漏洞的精准识别与防护。硬件固件作为设备核心组成部分，其规模和复杂度不断上升，来源和更新记录往往缺乏透明度，传统供应链检测工具通常无法有效识别固件和二进制组件中存在的漏洞，也难以给出有效防护方案。

挑战三：多源供应链安全数据异构数据整合。供应链安全数据分散在多个独立的系统，如 SCA 工具、漏洞库、日志平台、供应商自评估系统等，缺乏统一的数据治理框架，导致难以汇聚分析并形成全局、可视化风险画像。

挑战四：海量、碎片化漏洞情报的有效利用。安全团队需要监控包括 NVD、CNVD、CNVD、GitHub 安全公告、开源社区、商业情报源在内的数十个信息渠道，面临严重信息过载。同时，各渠道漏洞描述与影响评估标准不

统一，进一步加强情报运营与决策难度。

解决方案：

为系统化应对电信行业在数字供应链安全治理中面临的挑战与核心需求，本方案以悬镜安全数字供应链安全治理能力为核心，结合其创新的“XSBOM 供应链情报运营数据”云端服务能力，构建了一套“云端情报驱动、本地精准管控、生态协同治理”的一体化、主动式数字供应链安全解决方案。

一、方案具体实施策略包括以下几个方面

1. 多模态资产采集：

① . 源代码与构建制品分析：在 CI/CD 流水线的代码仓库与应用服务器中部署应用监测探针，对应用组件进行自动化解析和代码指纹识别，构建初步的软件成分清单。

② . 二进制与固件深度解析：针对二进制文件、设备固件等“黑盒”资产，采用二进制成分分析引擎进行逆向分析与漏洞特征识别，有效发现其中隐含的第三方库、编译器版本、潜在漏洞特征片段，弥补传统 SCA 工具在此类资产上的检测盲区。

③ . 容器与云原生制品扫描：对 Docker 镜像进行分层扫描，识别各层引入的软件包、配置文件和敏感信息，构建完整的镜像 SBOM，实现云原生环境资产可视化。

2. 动态 SBOM 与资产关系图谱构建：

基于采集到的组件数据，自动生成可追溯、可更新的动态软件物料清单，并利用图谱生成技术，构建“项目 -> 应用 -> 组件 / 库”的立体化资产关系图谱，当发现某个组件存在漏洞时，可一键定位所有受影响的上层应用，实现影响范围精准研判。

3. 多源情报聚合与智能关联：

平台持续从云端情报服务拉取经过预处理的、标准化的漏洞情报流，结合资产上下文、风险上下文、供应链上下文进行综合分析，一旦新增风险情报触达，内置的关联引擎将立即将其与本地 SBOM 资产库进行比对，快速定位风险影响范围，支撑精准响应。

4. 供应商安全准入与生态协同：

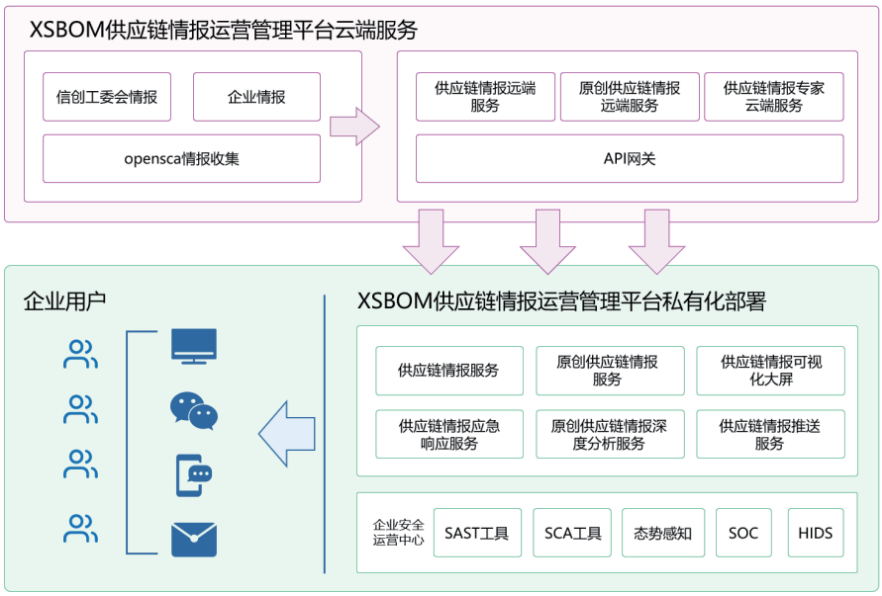
结合“XSBOM 供应链风险情报”及 SCA 检测能力，为外部供应商提供一个安全交付入口，实现组件制品自动化安全检测、安全评估与闭环等服务，通过对供应商交付的软件包、SDK、容器镜像扫描，并结合供应链情报服务，可检查漏洞、许可证合规性及潜在恶意代码，并将供应商的软件、组件质量（漏洞数量、修复及时性）纳入其安全能力分级体系，与后续合作挂钩，形成管理闭环。

5. 可视化风险运营与事件处置：

提供供应链情报可视化大屏，实时呈现软件资产全景、软件资产总数、风险组件分布、高危漏洞趋势、供应商安全指数等关键指标，当发生重大组件漏洞事件时，平台自动聚合受影响资产清单、漏洞详情、修复方案（如官方补丁链接、热修复补丁）、内部相关责任人，实现安全供应链事件一站式研判与处置。

二、方案技术架构

本方案的技术架构严格遵循“数据采集 - 分析 - 决策 - 执行 - 反馈”的安全运营闭环逻辑，该方案旨在将外部的、动态的风险情报与内部的、静态的资产信息、动态的研发流程深度整合，构建“看见风险、分析风险、管控风险、运营风险”的闭环治理能力。如下图所示：



1. 云端智能情报中枢（驱动层）

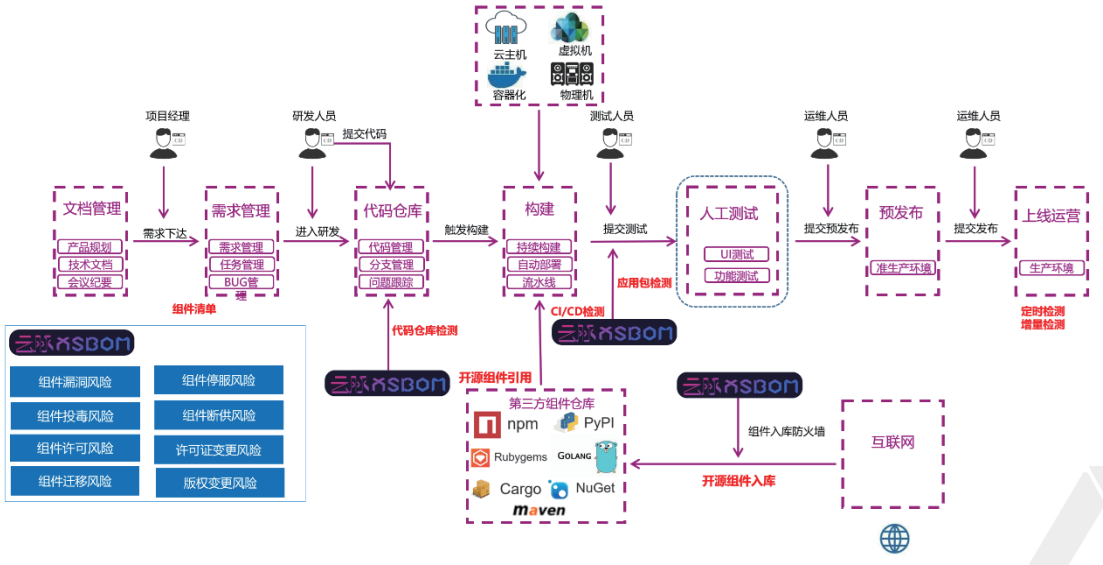
云端智能情报中枢作为方案的“智慧大脑”，该中枢基于 XSBOM 供应链情报运营管理平台云端服务，汇聚 NVD、CNNVD、CNVD 等权威漏洞库，以及信创渠道等专项情报、企业情报、OpenSCA 开源社区情报等多源信息。通过主动监控与深度挖掘，对开源项目进行持续监控，挖掘潜在风险与投毒攻击事件，形成具有前瞻性的原创供应链情报。该层不直接接触企业敏感资产数据，而是专注于海量、多源威胁情报的聚合、分析、挖掘与标准化推送，实现与企业的云端联防联控。

2. 本地私有化治理平台（管控层）

在企业内部数据中心私有化部署“数字供应链安全治理平台”，该平台作为方案的“神经中枢与执行终端”，负责企业内部的资产清点、风险分析、流程管控和运营协同职责，接收云端下发的精准风险情报，并与本地资产、流程数据结合，执行具体的安全策略。并通过加密 API 通道与云端情报中枢保持情报同步，并生成的标准化 SBOM，与云端进行情报匹配，云端通过情报智能分析，将处置方案和防护推送企业安全运营中心，触发自动化响应流程。

创新性与优势：

悬镜安全的“风险情报驱动的数字供应链安全治理实践”方案，在技术与治理模式上实现了双重创新，有效突破了传统方案的局限，为应对数字供应链安全挑战提供了系统性的解决框架。其核心创新性与优势具体如下图所示：



一、技术创新性优势

1. 多模态资产采集与全栈解析能力，突破传统工具局限

传统软件成分分析 (SCA) 工具往往局限于源代码与已知组件的识别，对二进制文件、固件等”黑盒”资产以及深层次的依赖关系难以解析。而悬镜安全的方案创新性地采用多模态资产采集技术，生成源码组件成分分析、代码成分溯源分析、制品成分二进制分析、AI 模型安全扫描、容器镜像成分扫描、运行时成分动态追踪及开源供应链安全情报预警分析七大核心引擎，实现了从软件到硬件、从应用到底层的全栈资产可视，实现了供应链安全全栈解析能力。

2. 云端智能情报中枢与本地治理平台协同，实现高效联防联控

传统方案中企业依赖企业自身进行静态、滞后的情报收集与分析，难以应对快速演变的供应链威胁。本项目构建了“云端智能情报中枢 + 本地私有化治理平台”的协同架构，云端专注多源情报的聚合、挖掘与标准化推送；本地平台负责资产管控与策略执行。二者通过加密通道实时同步，形成了“情报驱动、精准下发、快速响应”的主动防御闭环，大幅提升整体防御效率和协同能力。

3.AI 驱动的智能关联分析，提升风险治理精准度

面对海量、碎片化的漏洞情报和复杂的资产数据，传统的人工分析方式效率低、易遗漏且容易出错。本方案引入 AI 智能算法，实现了智能关联分析与风险优先级排序。

二、治理模式创新优势

1. 动态 SBOM 与资产关系图谱，实现全链路可视化治理

传统方案中，企业往往缺乏对软件供应链资产的全面、动态管理，导致资产“看不清、管不全”。该项目通过生成动态 SBOM 和构建资产关系图谱，实现了全链路可视化治理。当特定组件出现风险时，可一键穿透定位所有受影响资产，变被动响应为主动洞察，从根本上解决了资产“看不清、管不全”的痛点。

2. 供应商安全准入与生态协同，构建闭环治理体系

传统供应商管理缺乏将安全要求嵌入合作流程的有效手段。本方案建立了集自动化检测、安全评估与能力分级于一体的供应商准入体系。通过统一的安全交付入口，对供应商提供的制品进行漏洞、合规、恶意代码等自动化检测，并将结果量化为供应商安全评级，与后续合作挂钩，从而将安全治理从内部延伸至生态伙伴，实现了从准入到退出的全程闭环管理。

3. 供应链风险可视化运营，提升应急响应能力

传统风险展示分散，不利于快速决策与协同处置。本方案提供的可视化运营大屏，集成了资产态势、风险分布、漏洞趋势及供应商指数等关键指标，呈现全局供应链安全视图。在发生重大漏洞事件时，平台能自动聚合受影响清单、修复方案与责任人员，实现“情报 - 资产 - 处置 - 责任人”的一站式联动，极大提升了应急响应速度与协同处置能力。

本方案通过技术创新与治理模式重塑，构建了“看见、分析、管控、运营”的持续治理闭环，不仅系统性解决了电信行业供应链安全的核心痛点，其“情报驱动、协同治理”的理念与可落地的架构，也为其他面临类似挑战的行业提供了具有高度参考价值与实践意义的范本。

应用效果：

一、实际应用效果

资产全面可视化：该方案在实际应用效果中，实现了运营效率与供应链安全能力双重提升，平台已完成企业数百个核心在研与在运项目的自动化资产清点，生成了覆盖源码、容器镜像、二进制固件的统一化软件物料清单（SBOM）资产库，首次实现了数字供应链资产的资产图谱可视化，实现了从“看不见”到“全看清”的根本转变。

应急响应效率飞跃：在应对开源组件漏洞事件中，通过“云端情报 + 本地关联”的智能模式，并结合平台资产关系图谱，将影响范围分析与定位时间从过去的“数天至数周”缩短至“30 分钟以内”，应急响应效率提升超过 95%，彻底告别了“大海捞针”式的被动排查。

二、客户评价

该方案获得客户安全团队的高度认可，电信行业安全部门负责人评价：本方案使我们拥有了清晰的供应链

资产地图和雷达，该方案不仅是一套技术平台，更是将供应链安全能力深度融入到我们软件研发体系的血脉中，为我们在数字化时代的快速、安全创新，构筑了坚实的供应链安全底座。

三、经济效益

方案的实施带来了切实可量化的经济收益与风险成本节约：

直接成本节约：通过自动化资产管理与风险处置，每年为企业在供应链安全运维上节约人力成本超百万元；供应商准入流程的线上化与标准化，显著降低了第三方审计与协同沟通成本。

风险风本规避：通过“安全左移”与源头管控，在研发早期即拦截大量风险，避免了问题流入生产环境后可能引发的巨额紧急修复费用、业务中断损失及潜在的数据泄露合规罚款，实现了从被动补救到主动投资回报的转变。

经验总结：

本项目为电信行业构建了数字供应链安全主动免疫体系的先行实践，不仅取得了显著成效，也在过程中遇到了一些问题和可优化的方面，包括：

1. 历史遗留系统与“黑盒”资产的治理难题

在全面资产清点过程中，部分服役多年的核心系统因文档缺失、源码不可得或采用特殊架构，成为成分分析的难点。针对此类资产，未来将计划引入更先进的二进制软件基因图谱技术，逐步提升全面性与覆盖精度。

2. 安全运营数据的深度价值挖掘待加强

平台积累了海量的资产、漏洞、修复过程数据，但目前主要应用于风险处置和基础报表，在预测性分析、安全效能度量方面还有巨大潜力可挖。下一阶段将利用机器学习模型，自动分析漏洞趋势，预测特定技术栈的风险热点，实现精准改进。

某头部制造企业防勒索“主动免疫”体系建设与实战应用案例

案例提供方：思而听

案例背景：

该客户是国内离散行业的大型制造企业，在全国拥有 5 大生产基地，其核心命脉在于 MES 生产执行和 ERP 系统。在数字化转型过程中，客户面临最棘手的问题就是核心业务如 ERP 和 MES 系统对网络依赖极高：生产线上大量工控终端仍运行在 Windows 7 甚至 XP 等老旧系统上，因兼容性限制无法安装补丁。

在当前的 RaaS（勒索软件即服务）攻击大环境下，传统杀毒软件对不断变异的 Mallox、LockBit 等家族几乎失去拦截能力。一旦感染，按照传统的“离线备份 + 全盘恢复”流程，停工周期起步就是几天甚至几周，而该企业每停产一天，直接损失就高达数百万人民币，业务连续性保障压力极大。

关键挑战：

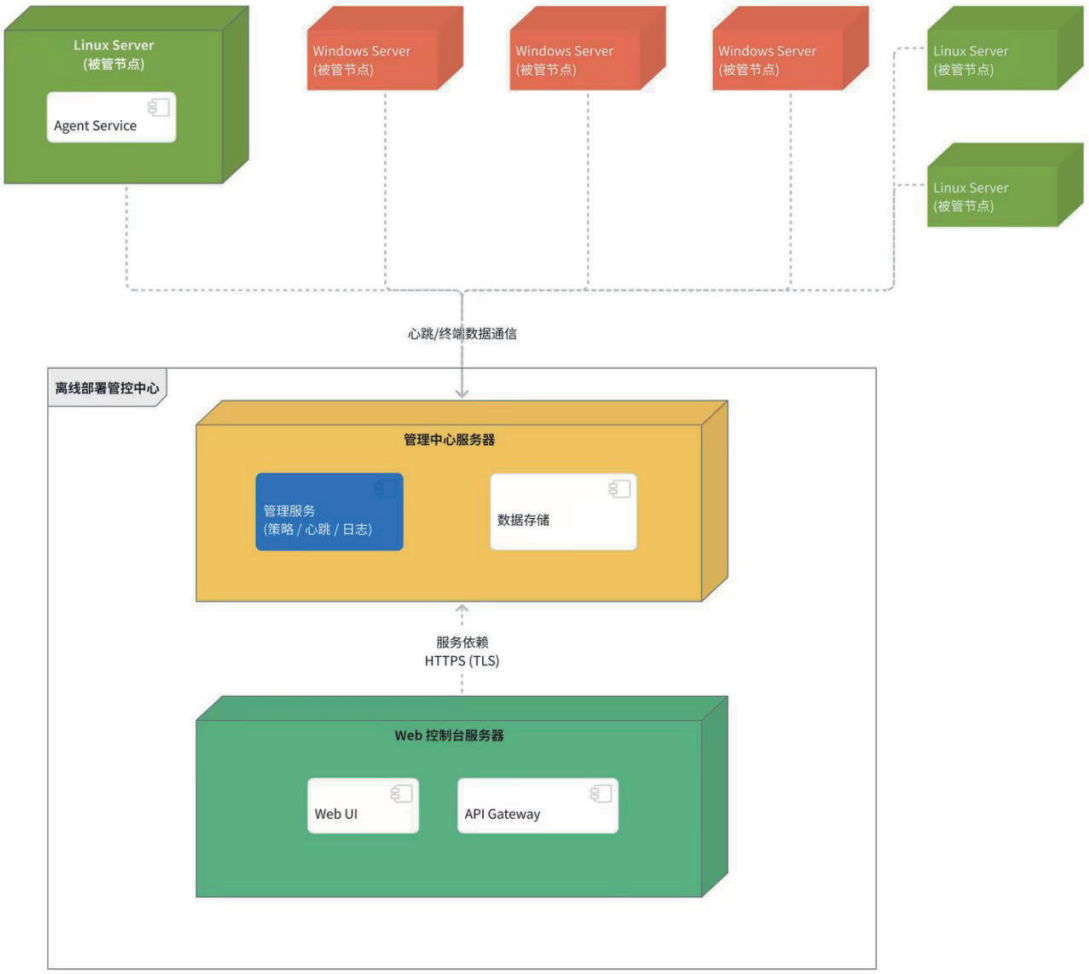
在现实当中，该企业面临的挑战极具代表性。首先是攻击响应的“黄金时间”被极度压缩，新型勒索病毒从系统入侵到核心数据完成加密，整个过程往往在几分钟内就结束，留给运维人员人工排查的窗口期几乎为零。其次是极其苛刻的资源限制，老旧工控机性能薄弱，任何高占用的安全插件都会导致生产程序卡顿甚至崩溃导致生产指令延迟甚至停工。最后，面对黑客“加密 + 数据泄露”的双重勒索手段，客户不仅需要防住加密，更需要在极端情况下能实现快速恢复产线运作，避免陷入支付高额赎金的被动境地。

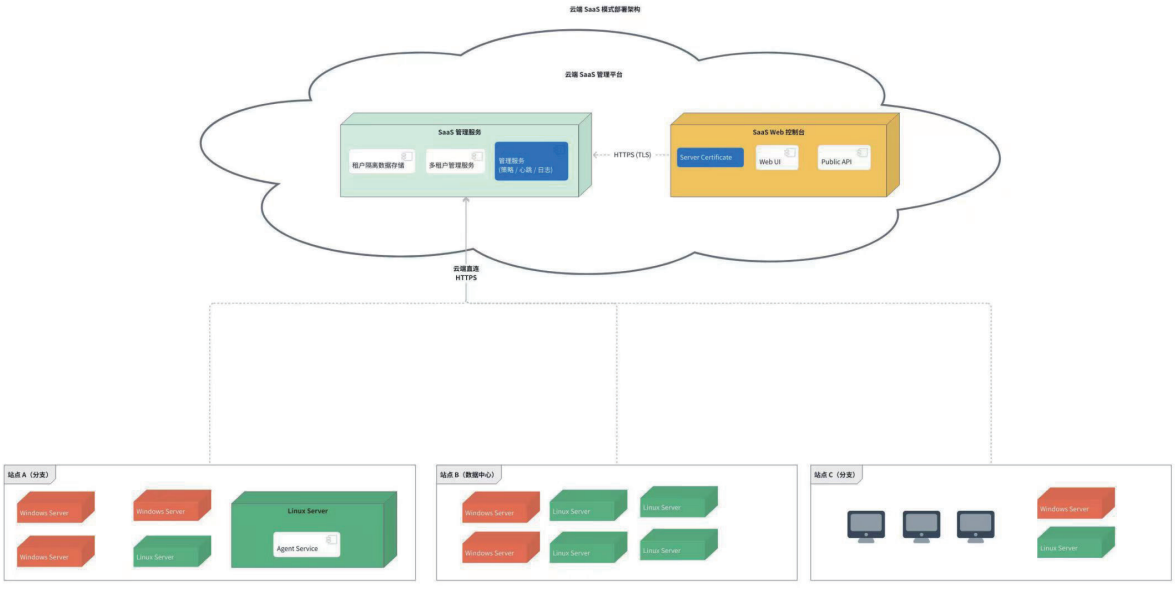
解决方案：

为达到企业需求，我们对本项目实施了以“SAR 防勒索 AI 疫苗”为核心的主动免疫体系。不同于传统的勒索病毒黑名单比对，该方案在内核驱动层直接注入轻量化的行为识别引擎，重点针对勒索病毒绕不开的文件改写操作进行微隔离。其核心杀手锏是“内存密钥拦截技术”：在病毒调用加密算法的关键瞬间，SAR 能实时截获内存中生成的临时密钥并加密上报。同时，我们在客户内网全量部署了“诱饵文件陷阱”，一旦有进程触碰这些诱饵，系统会判定为恶意攻击，会立即触发进程熔断和网络隔离策略，实现毫秒级的自动止损。

在实施策略上，我们采取了“先演练后部署”的闭环模式。首先利用思而听勒索病毒演练平台，对客户现有的防线进行了一次全方位的模拟“体检”，根据发现的短板动态调整疫苗策略。此外，Solar 安全团队提供 7×24 小时的 MDR 托管监测与响应服务，结合自动化告警与人工逆向分析，确保在病毒运行初期即可完成威胁闭环。这种“技术平台 + 专家服务”的模式，改变了以往单纯依赖防火墙的被动防御局面，实现了从入口管控到数据保护的全链路覆盖。

SAR离线部署架构图


Linux Server
(被管节点)
Agent Service
Windows Server
(被管节点)
Windows Server
(被管节点)
Windows Server
(被管节点)
Linux Server
(被管节点)
Linux Server
(被管节点)
心跳/终端数据通信
离线部署管控中心
管理中心服务器
管理服务
(策略 / 心跳 / 日志)
数据存储
服务依赖
HTTPS (TLS)
Web 控制台服务器
Web UI
API Gateway


云端 SaaS 模式部署架构
云端 SaaS 管理平台
SaaS 管理服务
相户隔离数据存储
多租户管理服务
管理服务
(策略 / 心跳 / 日志)
HTTPS (TLS)
SaaS Web 控制台
Server Certificate
Web UI
Public API
云端直连
HTTPS
站点 A（分支）
Windows Server
Windows Server
Windows Server
Linux Server
Linux Server
Agent Service
站点 B（数据中心）
Windows Server
Linux Server
Linux Server
Windows Server
Linux Server
Linux Server
站点 C（分支）
Windows Server
Linux Server

创新性与优势：

这套方案最核心的创新点在于从“已知检测”转向了“主动免疫”。传统安全产品在面对 0-day 漏洞或未知变种时往往由于缺乏指纹而失效，而 SAR 疫苗关注的是加密逻辑这一本质特征，从而实现了“主动免疫”。此外还有一个优势是它的极致轻量化：Agent 在运行时的 CPU 占用率常年控制在 1% 以内，内存消耗不足 50MB。在遭受大规模攻击压力测试时，资源波动也极其轻微，完美适配了计算资源极度受限的工业控制终端。

此外，这一方案颠覆了传统的数据恢复手段。大多数企业的应急响应预案都依赖于备份，但备份恢复的 RTO（恢复时间目标）往往无法承受。SAR 通过前期捕获的内存密钥，可以实现原地解密被锁文件。这种“不依赖备份、不支付赎金”的恢复逻辑，把原本需要按天计算的恢复周期压缩到了分钟级，成功率接近 99.8%，这在目前的防勒索市场上具有极强的技术壁垒，真正做到了让企业“无惧加密”。

应用效果：

项目上线至今，成功为该企业拦截了多次针对性的勒索渗透攻击。在一次针对 LockBit 3.0 变种的实战拦截中，SAR 系统在病毒加密前 1.2 秒内精准锁定异常行为并阻断，保护了数 TB 的核心生产图纸数据。

从实际应用效益看，该方案将客户遭遇攻击后的数据恢复周期从传统的 21 天大幅缩短至分钟级，业务连续性保障能力提升了 95% 以上。客户评价称，该方案在不影响生产效能的前提下，提供了“最后一道防线”的保护性，这种保护性显著降低了企业在网络安全方面的隐性投入成本。此外，该案例被新华网等主流媒体深度报道，被公认为制造业数字安全防护的创新标杆。

经验总结：

通过本项目，我们意识到在复杂的制造环境下，单一的安全产品难以应对体系化攻击，必须通过“病毒演练 +AI 疫苗”的模式实现防御前置。项目实施中发现，部分离散终端的防护缺失仍是内网最薄弱的跳板，未来应进一步强化“端网联动”的自动化响应深度。同时，持续优化的 AI 归属研判算法将是下一步的重点，旨在通过自动化逆向溯源，不仅要“防得住”，更要能“追得深”，实现安全治理的可持续闭环。

基于AI大模型智能驱动的天懋资产监测与边界内联检查控制系统

案例提供方：天懋信息

案例背景：

专网边界作为专网的第一道安全防线，安全防护能力建设非常重要。实施专网边界监管目的是为了防止因网络边界的缺陷，或专网存在不受控网络边界，导致入侵攻击和内部信息外泄等安全事件的发生。专网边界负责团队需采取各类技术手段识别专网与外部可以或可能通信的网络边界，并对网络边界进行有效的安全管控。

现行专网安全监管体系下的边界安全管理在实践中已暴露出诸如覆盖面不全、适应性不强、弹性扩展能力不足、安全事件感知与响应滞后等问题；在政企数字化转型过程中因业务设计和应用创新的参与度不高，导致既有业务迭代和新型应用成为网络边界安全管理的监管盲区的问题；缺乏对擅自部署的违规网络边界特别是以逃避监管为目的设计的违规网络边界设施、设备和应用的发现和处置的技术手段。

传统的安全分析工具往往依赖于规则库和特征匹配，难以应对新型攻击和未知威胁，在专网业务场景中对异常流量检测、异常行为识别、资产类型识别等新型、未知风险检测的准确率和时效性亟待提升。同时从客户场景看监管视野存在“盲区”，对于蓄意规避监管，经合规路径实施违规操作、私搭乱建跨网通道并对外发布资源、不安全的互联网远程穿透访问等专网边界防护薄弱环节，在专网网络暴露面和通联关系收敛监管上缺乏行之有效的解决方案。

关键挑战：

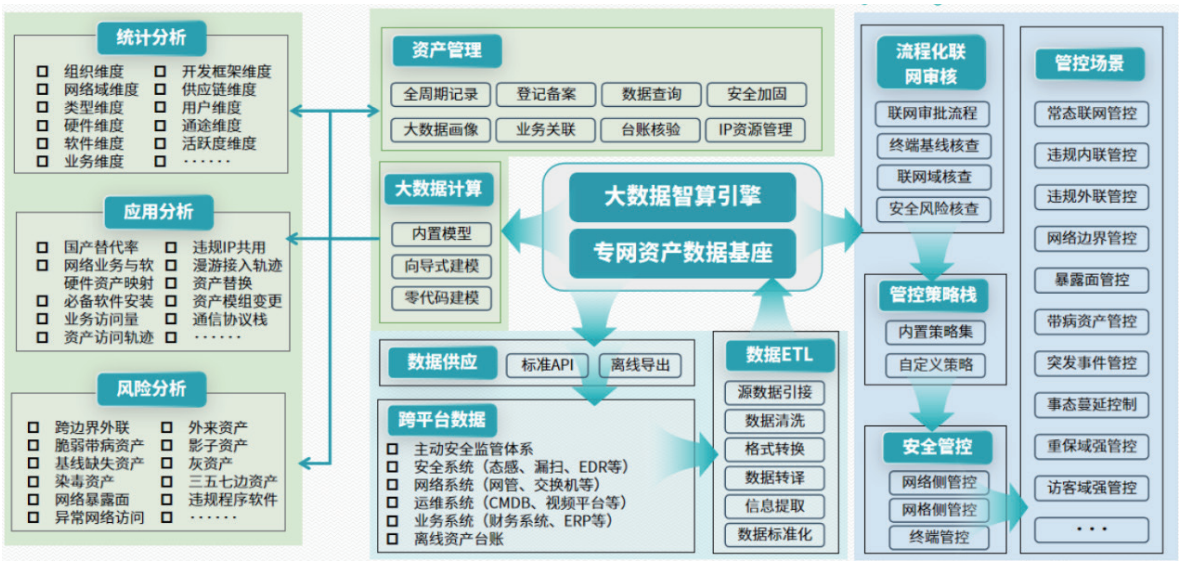
近年来，随着国家、政府大力推进了“智慧城市”、“平安城市”、“天网工程”、“雪亮工程”等视频监控系统的建设，逐渐形成了覆盖整个城市和乡镇的视频监控网络，有力地促进了各项公安业务的开展，但视频网的安全问题也日益凸显出来。为了整治视频网安全问题，公安部从 2020 年开始加大了对视频网的安全检查与考核，将违规外联、非授权边界设备、资产准确率、资产脆弱性（包括：弱口令、漏洞）等问题作为重点考核点，推动省市县视频网安全建设，提升视频网主动安全能力，实时感知边界安全风险、及时监管资产安全状况、主动处置安全隐患，全面保障视频网的安全。

同时，公安部下发的“关于加强公安视频监控安全管理工作的通知”（以下简称：通知）中，对公安视频图像网（以下简称：视频网）从提高安全管理认识、加强技术防护措施、健全安全管理制度、开展安全风险隐患排查等四个方向提出了要求。随后发布的“公安视频图像信息系统安全技术要求 第 4 部分：安全管理平台”明确了安全监测包括：资产识别、漏洞检测、弱口令检测、边界完整性检测、网络空间测绘的需求。

解决方案：

1. 解决方案组成

天懋信息基于对 AI 驱动网络安全产品智能升级的深刻洞察和理解，自主研发打造的一系列以“TINDAE(天懋网络数据智能分析引擎)”为核心的专网边界安全系列产品及解决方案，可从资产安全、空间测绘边界安全、网内攻击、信令安全、违规行为、多维数据取证、联合防控等维度提供主动安全监测与分析，构建网络空间纵深防护体系。



基于 AI 大模型智能驱动的资产监测与边界内联检查控制系统整体解决方案图

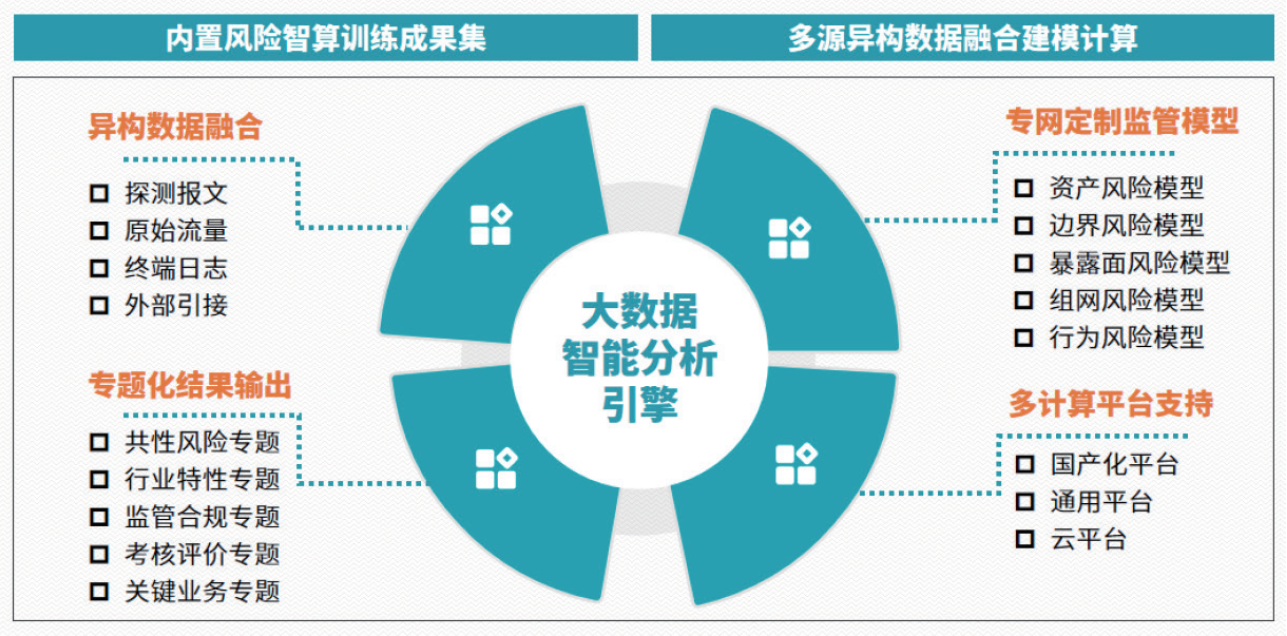
主动安全监测类产品：以安全监测为核心，贴合专网数字化业务安全保护与运维实战，减少海量数据干扰，主旨从宏观到微观层面的全域监控与智能研判能力。可实现百万级联网端点网络空间地理测绘和全网域通联关系可视化，支持挂图作战；对专网应用场景中的违规内联资产、违规共用 IP、违规挪网资产、违规数字资产和资产脆弱性等提供实时预警、精确定位及跨系统联动防控。

指挥与管理类产品：以数据治理为核心，主旨构建一个集成化的网络资产指挥中心，实现多源数据的融合、清洗与动态监控，保障资产生命周期的全面管理与运营安全。针对不同目标数据特性，平台支持通过模型配置数据条件、数据内容融合优先级等方式。为专题分析作数据集合准备，以所需分析结果为导向，支持分析多类数据模型后得到所需分析结果。

网络防控类产品：以事件处置与响应为核心，面向新一代联网资产监管模式，适配超大规模专网至局部网络辖区不同规模网络资产监管需求。自动构建资产台账，让资产联网可管可控；采用智能值守主动监管模式，支持网络、网格、终端三层管控措施，对网络设备的统一管理与控制；实现自动化的安全响应与处置，强化对核心数据与资源的保护。

2. 方案引入大数据智能分析引擎

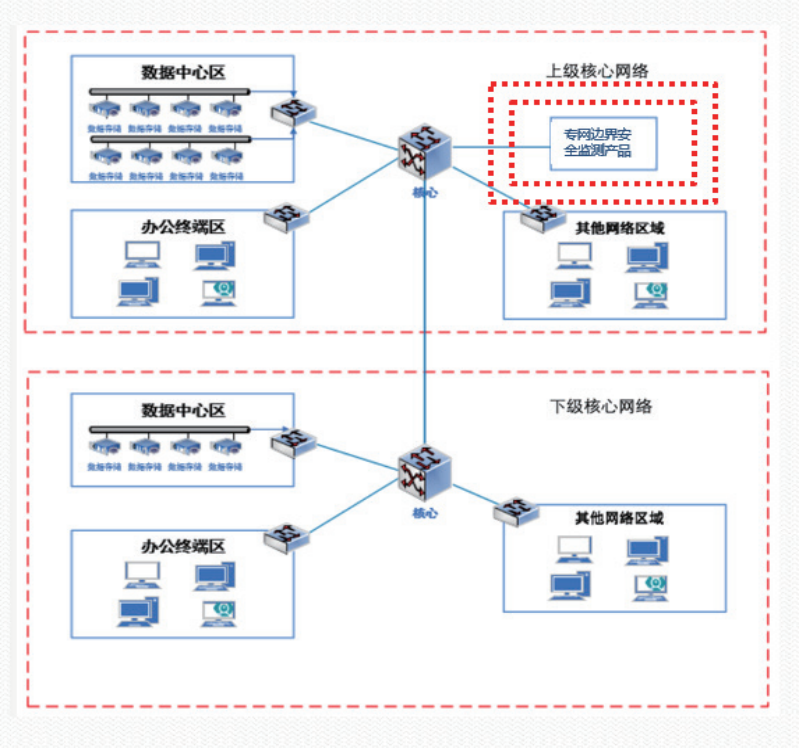
目前产品体系已全面接入 AI 大模型，在异常行为检测、资产识别、知识图谱的实体、关系智能抽取等多个关键技术应用场景，从各行业专网的业务特性和安全监管要求出发，以 AI 大模型构建更加智能、高效的网络安全防护体系，助力公安、政府、军队等行业的专网边界安全监管高质量发展。



大数据智能分析引擎核心能力

3. 方案部署形态

天懋信息专网安全 AI 大模型产品和解决方案，通过管理平台与末梢传感器的模式部署，采用多种非侵入手段，包括核心镜像、主动探测以及传感器探针等技术，以实体行为分析模式感知专网环境安全风险，实时监测违规内外联、私建网中网、不受控跨网通道、未备案边界平台等破坏网络边界完整性的行为，敏锐感知网络攻击、病毒传播等高风险行为，并自动化对网络安全事件取证和联动防控，建立“边界监测 - 攻击分析 - 资产管控”等多个维度的监管能力，实现对专网全方位安全监控，保障外联终端安全接入和访问控制，有效提升面临的各方面威胁和对应的安全防护手段，实现事前预防、事中阻断、事后溯源的全过程防护，以集中、可视化呈现专网内安全隐患及威胁情况，有效保障专网安全、稳定、高效运行。



资产监测与边界内联检查控制产品部署图（旁路部署 支持分级管理）

创新性与优势：

在公检法司和政企部委客户的专网边界安全项目中，引入 AI 大模型智能驱动的资产监测与边界内联检查控制解决方案，与以往方案相比，效果上有显著提升：

1. 提供更加精准的资产识别能力，实现更加强大网络空间测绘能力

结合 DeepSeek 深度推理技术、数据融合技术以及行为分析算法，动态分析设备行为模式。

2. 增强异常 / 虚假 / 伪造资产识别检测能力，助力资产管理“零盲区”

依靠 DeepSeek 推理分析模型，结合多源数据深度分析与模式识别技术，通过资产监控和异常检测算法，快速识别虚假或恶意资产；并基于多层次的规则引擎与自适应学习技术，实现异常模式的准确推断，自动生成封堵策略。

3. 增强资产暴露面精准分析和定位能力，构建更完整的边界安全防线

充分融合漏洞挖掘、风险评估模块和 DeepSeek 推理分析能力，依托资产库与漏洞数据库为每个资产生成实时的脆弱性评分，基于行为分析技术预测潜在的脆弱性风险。

4. 增强异常流量的智能分析与识别能力，让未知威胁“无处遁形”

结合 DeepSeek 强大的大数据分析能力和流量模式识别技术，通过深度学习算法训练模型，识别各类流量

异常类型，筛查不符合常规流量模式的异常行为，进而精准定位攻击源与攻击路径，提升对新型攻击的预测和防御能力。

5. 新增外联设备的排查定位分析能力，产品核心能力再升级

凭借 DeepSeek 的推理分析能力实现自动化识别与追踪各类外联设备的接入行为，并对外联设备的安全性进行实时分析，快速锁定潜在安全隐患，实现对违规行为的精准排查和实时分析。

6. 新增对话式智能互动入口，打造 7*24 小时在线的智能客服

借助 DeepSeek 模型在自然语言理解和生成上的强大能力，新增对话式智能互动入口，快速响应用户需求，提供专业支持与帮助，确保用户能够快速获取系统状态、资产安全评估和处理建议。

应用效果：

基于 AI 大模型智能驱动的资产监测与边界内联检查控制系统采用多维远程监测技术与网络末梢风险感知技术，可实时监测全网边界防护安全，及时发现违规外联行为，准确定位网中网，感知边界设备，实现网络边界安全防护的有效监管，提升网络安全的纵深防御能力。

1. 全域集成非侵入式监控

多种非侵入式技术构建一个跨领域的全局监控网络 , 确保每个操作环节的安全数据都能在不干扰正常业务的情况下进行实时采集和分析。

2. 前瞻性威胁感知与精准预警

依托先进的人工智能与大数据分析技术，系统能够精准捕捉潜在威胁，提供实时的风险预警。

3. 深度学习驱动的智能异常检测

结合深度学习与模式识别技术，快速分析大量复杂数据，精准识别出潜在的安全异常。

4. 自适应多层动态策略调节

自适应的多层次、细颗粒度的策略自适应调节机制，能够根据网络环境调整监测策略，确保对未来威胁的高度敏感与快速反应。

经验总结：

新时期的专网安全建设能力亟需加快与 AI、平台生态、行业场景深度融合，形成更加智能的安全防护体系，以高效和准确的专网安全监测技术赋能网络边界安全管理，理清全网网络边界底数，明确其所处的网络空间位置，进而掌握跨边界交互的具体情况和落实安全管理措施；记录网络边界运行和服务状态，帮助管理者掌握网络边界安全形式，发现各类私自搭建的不受控网络边界和跨边界交互行为，为快速响应和处置安全风险提供数据支撑。

陕西科技大学校园网出口防火墙升级改造项目

案例提供方：山石网科

案例背景：

陕西科技大学是位于十三朝古都西安的一所公办全日制普通高等学校，以轻工为特色，是陕西省人民政府与中国轻工业联合会、中国轻工集团公司共建的省部共建高校。涵盖工学、理学、艺术学等多学科的省属重点大学，现有全日制在校师生生 2.9 万余人。校园网作为学校教学、科研、管理和师生日常生活的核心基础设施，已实现全校教学区、办公区、宿舍区、家属区等区域的全覆盖，当前校园网出口带宽超过 30Gbps，连接各类终端设备超 2 万台，支撑着在线教学平台、科研数据传输、教务管理系统、校园一卡通等关键业务系统的稳定运行。

近年来，随着学校数字化转型加速，智慧教学、远程科研协作、高清视频会议等应用场景日益普及，师生对网络的带宽、稳定性和安全性提出了更高要求。同时，网络攻击手段持续迭代，勒索病毒、数据泄露、DDoS 攻击等安全威胁频发，原有校园网出口防火墙在性能支撑、安全防护、运维管理等方面逐渐暴露出短板，已难以满足教学科研核心业务的稳定运行需求，亟需通过升级改造构建高效、安全、智能的校园网出口防护体系。

关键挑战：

（一）性能瓶颈制约业务效率

原有防火墙设备设计吞吐量较低，难以匹配当前出口带宽需求。在每日两个用网集中时段——上午教学类应用访问密集期、晚间宿舍区数据传输高峰期，设备处理能力跟不上，导致网络延迟明显升高，丢包现象增多，在线教学视频播放卡顿、科研大文件传输中途断开等情况时有发生。仅今年上半年，就收到多起相关反馈，对教学科研工作造成一定干扰。

（二）接口规格落后，无法适配高速网络环境

原防火墙接口规格有限，主要配备常规速率与少量较高阶速率端口，暂不支持更高速率的新型接口，因此无法直接对接运营商新开通的大带宽上行链路，导致出口带宽未能充分发挥效能。同时，现有接口的数量与类型灵活性不足，难以按需扩容或调整，限制了后续网络架构升级以及多云互联等新业务场景的部署空间，如不及时优化，可能影响校园网整体数字化升级的步伐。

（三）安全防护能力不足，存在数据泄露风险

原有设备在威胁检测与防御方面智能化程度不高，主要依靠静态策略和特征库来识别风险，对勒索软件、APT 攻击、零日漏洞这类新型高级威胁的捕捉能力偏弱。过去一学年曾出现若干起成功渗透的情况，导致部分科研数据外泄，教务系统也出现过短暂受影响，既对学校科研成果的安全带来隐患，也干扰了日常教学管理的平稳运行，存在较明显的数据安全与业务连续性风险。

（四）运维管理复杂，故障处置效率低

传统防火墙策略配置主要靠命令行操作，策略条目数量较多，管理起来费时费力，而且缺少直观的流量可视化和行为分析手段，遇到问题时排查定位往往要花很长时间。复杂的运维方式让网络故障难以及时处置，容易让业务受影响的时间拉长，同时也推高了运维的人力投入。

解决方案：

本项目核心采用山石网科 ASIC 架构国产化防火墙，构建“高性能支撑 + 全维度防护 + 可视化运维”的校园网出口防护体系，具体实施策略如下：

1、高性能接口与硬件加速配置：选用支持多种高速接口的山石防火墙设备，配备涵盖高阶、中高阶及常用速率的全系列接口模块，其中主力接口直接对接运营商大带宽上行链路，同时预留可插卡扩展槽位以便后续灵活扩容。借助山石网科自研 ASIC 安全专用芯片实现硬件级加速，将流量转发、策略匹配、SSL 加密解密等核心任务从通用处理器卸载至专用芯片，达到较高的防火墙吞吐性能与充足的并发连接能力，能够充分满足当前出口带宽需求，并为未来带宽升级留出宽裕空间。

2、全栈智能安全防护部署：集成多层级安全防护功能，构建“边界防护 + 威胁检测 + 精准阻断”的安全体系。

3、可视化安全策略优化：可按教学区、宿舍区、办公区等不同区域维度统计流量分布，帮助精准发现高带宽占用业务；提供策略自动优化功能，通过智能分析冗余或冲突的策略，自动给出优化建议，减少人工介入；同时配备全图形化的业务流排障操作界面，取代传统命令行配置，显著降低运维门槛。

4、分阶段实施与割接策略：为避免改造过程对核心业务造成影响，采用“先并行运行、后平滑割接”的实施流程。第一阶段完成新设备部署与配置调试，将新防火墙与原有设备并行接入网络，验证性能与安全策略的有效性；第二阶段分时段切换流量，先将非核心业务流量切至新设备，运行一段时间无异常后，再于非高峰时段逐步迁移其他业务；第三阶段持续监控一段时间，优化安全策略与流量配置，最终完成旧设备下线。

创新性与优势：

ASIC 硬件加速突破性能瓶颈，性价比远超传统方案：

相较于传统软件架构防火墙或通用 x86 架构防火墙，本方案采用山石网科自研 ASIC 安全专用芯片实现硬件级加速，在性能提升与资源占用优化上形成双重优势。传统架构在复杂流量环境下易出现明显性能衰减，而 ASIC 防火墙实现吞吐性能约 3 倍提升，小包性能媲美大包；新建连接数提升约 2.5 倍，IPsec VPN 性能提升约 2 倍，彻底突破传统设备的算力瓶颈。

时延方面，ASIC 防火墙可将处理时延稳定控制在 ≤ 4.8 微秒，相比传统防火墙数十微秒的水平降幅超 80%，完美适配实时交互业务场景对超低延时的需求。硬件加速还显著降低设备功耗，单台设备能耗较传统方案降低超 40%，全年可节省可观电费，节能效果显著。

针对传统防火墙高速接口数量受限的痛点，ASIC 防火墙全系标配更多万兆接口，并支持 100G 高速接口扩展，为高带宽组网提供坚实基础。同时，与传统架构在高负载下 CPU 占用率飙升不同，ASIC 芯片承担主要数据面负载，确保系统在高吞吐场景下仍保持低 CPU 占用率和稳定运行，为业务连续性提供可靠保障。

2、AI 驱动的智能威胁防御，防护能力更全面精准：区别于传统防火墙依赖静态特征库的被动防护模式，本方案内置 AI 检测模型与行为分析引擎，具备“主动识别未知威胁”的核心优势。通过对校园网历史流量数据训练，模型可较精准地识别勒索软件、挖矿木马等新型恶意程序的行为特征，即便面对零日漏洞攻击，也能借助异常行为分析提前预警，威胁识别率相比传统方案明显提升。同时，AI 引擎可自动学习校园网正常业务流量特征，减少误报情况，测试中误报率保持在很低水平，避免因过度防护影响正常教学科研业务。

3、可视化业务流展示实现运维降本增效，管理模式更智能：相较于传统防火墙与命令行相结合的运维模式，本方案实现三方面提升：一是策略管理更智能，传统方案需多名专业运维人员耗费较长时间梳理大量策略，本平台可在很短时间内完成策略分析与优化建议生成，策略优化效率显著提高；二是故障定位更精准，借助流量可视化与事件关联分析，可将故障定位时间从以往较长周期缩短到很短时间，大幅提升处置效率；三是管理权限更精细，支持按角色分配运维权限，实现多部门多维协同管理，避免权限集中带来的操作风险。

4、弹性扩展架构适配未来演进，可持续性更强：本方案采用模块化设计与冗余配置，具备很强的弹性扩展能力。接口层面，预留的可插卡扩展槽位可根据未来带宽升级需要，快速新增高速接口模块，支持校园网出口带宽从当前水平平滑升级到更高规格；功能层面，可通过软件授权快速开启终端安全管理等新功能，更好适配智慧校园建设的新需求。

应用效果：

1、性能指标显著提升，核心业务体验优化：项目上线后，校园网出口网络性能得到明显改善。网络平均延迟从改造前的较高水平降至更低范围，高峰时段也能保持稳定低延迟；丢包率大幅下降，基本消除了在线教学视频卡顿、科研大文件传输中断的问题。出口带宽利用率明显提高，运营商大带宽上行链路资源得以充分利用，在开学高峰与考试季等重要时段，未发生因网络性能导致的教学科研业务中断，相关投诉量较改造前明显减少。

2、安全防护成效显著，安全事件大幅减少：依托智能安全防护体系的有效运行，校园网整体防护能力明显增强。上线以来，成功阻断多起各类网络攻击，包括多次较大流量的 DDoS 攻击、若干次勒索软件渗透尝试以及不少科研数据异常外联行为，安全事件发生频率较改造前显著降低。未再出现科研数据外泄、教务系统中断等安全事故，学校数据安全等级保护测评结果提升至更高等级，信息化办公室获评网络安全先进称号。

3、运维效率提升，经济效益明显：可视化数据流的应用在不同阶段有效降低了运维成本。策略管理耗时较改造前明显缩短，原本需要较长时间完成的策略梳理，现在能在很短时间内完成；故障平均修复时间大幅压缩，运维人员工作量有所减轻。同时，硬件加速带来的节能效果与接口直连减少的中间设备投入，使每年可额外节省运营成本，综合经济效益较为突出。

4、客户评价与行业认可：项目成果获得学校师生与管理方的高度肯定，作为典型案例进行交流分享，为

省内同类高校校园网升级改造提供了可借鉴的参考，具备较好的行业推广价值。改造后的网络架构顺利支撑了冬季学期大量在线课程的稳定运行，覆盖众多在校生，师生网络满意度调查显示好评率很高。

经验总结：

一是新旧设备割接风险控制问题，初期担心核心业务受影响，通过制定“分阶段割接方案”，先安排一段并行运行测试期，充分验证策略有效性与设备兼容性，最终实现割接过程中核心业务无中断。

二是运营商链路对接协调问题，因运营商大带宽链路调试周期偏长，通过提前与运营商建立专项对接机制，安排技术人员现场协同调试，确保链路与设备同步达到可用状态。

中粮期货零信任安全体系与无界办公项目

案例提供方：亿格云

案例背景：

客户概况：中粮期货作为中粮资本核心子公司，聚焦农业产业链金融服务，业务覆盖期货经纪、风险管理、资产管理等领域，服务超 2000 家机构客户及数万个人投资者。随着数字化转型加速，业务场景向跨境交易、智能投研、云端协同延伸，传统安全架构难以应对多端接入、数据流动泛化及新型 APT 攻击威胁。

核心痛点：

安全边界模糊：远程办公与多分支混合接入办公导致网络边界瓦解，暴露面扩大。

动态风险失控：业务系统频繁迭代，终端安全风险发生无法阻断风险蔓延业务。

合规压力剧增：等保监管趋严，需满足《等级保护 3 级》《个人信息保护法》及期货行业合规要求。

用户体验割裂：多系统独立认证导致操作繁琐，影响业务效率和员工体验。

用户需求：构建“互联网零信任 + 内网准入”安全底座，实现“人 - 设备 - 应用 - 数据”全链路可信访问，支撑业务敏捷扩展。

关键挑战：

1、技术挑战：

异构系统兼容性差（自研交易系统、第三方合作平台、云服务并存）。

动态风险感知能力不足，缺乏实时威胁狩猎机制。

2、业务挑战：

高频交易场景下，安全策略需兼顾低延迟与高可靠性。

业务人员流动需平衡合规性与业务连续性。

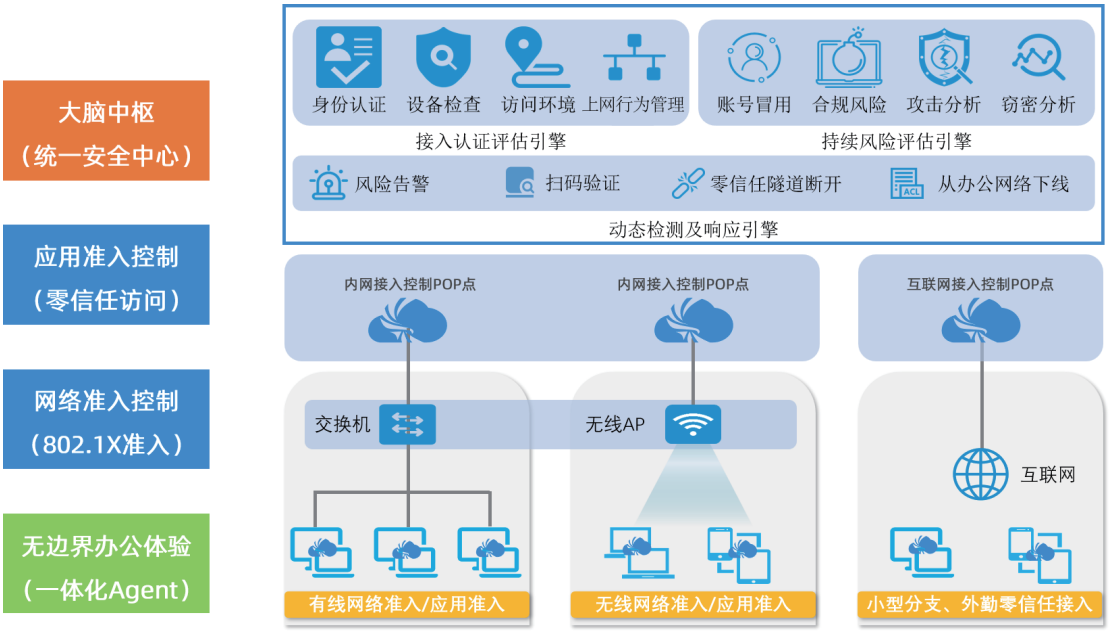
3、风险分析：

若安全架构升级失败，可能导致员工无法访问核心业务，造成重大经济损失。

合规漏洞可能引发监管处罚及品牌声誉受损。

解决方案：

无界办公核心技术架构：



身份中台：基于零信任和准入的动态身份认证（对接企微打通身份和扫码认证，并联动上网行为管理准入，提供更好认证体验）。

策略引擎：AI 驱动的实时风险评估（流量异常检测、行为分析）。

微隔离：软件定义边界（SDP）+ 网络切片技术。

数据安全：数据传输、存储均采用强加密手段。

创新性与优势：

维度	传统方案	本方案
安全模型	静态边界防护	动态信任评估，根据用户、设备数据+安全风险+数据风险维度的动态持续安全评估和自动处置。
性能损耗	防火墙深度检测导致延迟≥50ms	微隔离架构延迟≤5ms
管理复杂度	多系统独立策略	统一管控平台、统一策略编排和管理
合规能力	人工审计为主	自动化合规报告生成

核心优势：

智能动态防御：基于用户行为画像和基于属性的访问控制模型的实时权限调整，阻断横向渗透攻击。

无感化体验：单点登录（SSO）+ 自适应认证（互联网零信任、内网准入）+ 上网行为管理联动，用户操作步骤减少 80%。

生态协同：开放 API 接口，与微步、深信服等厂商威胁情报和上网行为管理联动。

应用效果：

安全效能提升：

形成终端纵深防御能力，安全风险和数据风险在终端联动阻断，防止风险蔓延。

2025 年用户终端安全风险攻击次数同比提升 300%，零安全事故。

业务系统 0 暴露，避免直接攻击业务系统。

业务支撑能力：

支持中粮期货 300 员工无界办公，系统可用率达 99.99%。

助力新业务快速上线和安全访问。

经济效益：

年度安全运维成本降低 40%。

因安全事件导致的业务中断损失归零。

经验总结：

实施难点：

遗留系统改造：部分老旧交易系统接口不兼容，需定制开发适配。

员工适应性：初期因操作习惯改变导致部分业务部门抵触。

优化方向：

AI 模型迭代：引入联邦学习技术，提升跨机构威胁情报共享效率。

用户体验：开发轻量化管理控制台，实现策略配置自动化率 90%+。

未来智安AI智能体安全运营平台助力某运营商构建全流程智能闭环运营体系

案例提供方：未来智安

案例背景：

运营商面临 5G 发展和网络复杂性增加带来的数据孤岛、低效运营和缺乏闭环优化等挑战，亟需引入 AI 智能体平台，构建自动化运营新体系。

运营商运营痛点与挑战

数据孤岛与碎片化运营：运营商内部系统复杂，数据分散，导致难以形成统一、高效的全局视图和协同运营。

传统运营效率低下：许多运营流程（如故障处理、业务保障、客户服务）仍依赖大量人工干预，效率提升困难，响应速度慢。

业务发展与网络复杂性增加：随着 5G、云计算等新业务的发展，网络复杂度剧增，传统运营模式难以快速适应。

缺乏闭环优化能力：难以将“监测 - 分析 - 决策 - 执行 - 反馈”的运营流程高效地串联起来，无法实现持续的自我学习和优化。

引入 AI 智能体平台的需求

构建自动化、智能化运营体系：迫切需要引入 AI 技术，特别是 AI 智能体的能力，实现运营流程的端到端自动化。

实现全流程的智能闭环：希望通过 AI 智能体平台，将分散的运营环节整合，打通数据、流程和系统，实现真正的“智能闭环运营”。

提升运营效率和服务质量：利用 AI 的决策和执行能力，快速识别并解决问题，从而降低运营成本，提升客户体验和业务保障能力。

关键挑战：

一是安全威胁复杂化带来的识别与响应风险。运营商网络覆盖 5G 核心网、云资源池、专线专网及大量边缘节点，攻击路径呈现多阶段、跨域、低频隐蔽特征。传统基于规则和单点检测的手段难以理解攻击上下文，易出现漏报、误判，存在高风险事件无法及时发现和处置的隐患。

二是告警规模失控引发的运营效率与稳定性风险。多安全设备并行运行，日均产生海量告警，重复、无效告警占比高。安全人员需频繁进行人工筛选、关联和判断，分析周期长、响应滞后，关键事件易被淹没，直接

影响网络与业务连续性。

三是运营流程割裂导致的闭环失效风险。检测、分析、处置、复盘分散在不同系统和团队之间，缺乏统一的流程编排和状态跟踪机制，事件处置依赖人工协调，难以形成“发现—研判—响应—优化”的闭环运营，运营成果不可量化、不可沉淀。

四是人力依赖度过高带来的可持续运营风险。安全运营高度依赖专家经验，新技术、新攻击不断出现，人员培训和经验复制成本高，一旦人员流动或业务高峰叠加，容易出现能力断层，制约安全运营规模化和长期稳定运行。

五是合规与监管要求提升带来的管理风险。监管部门对运营商在安全可视化、处置可追溯性、责任界定等方面提出更高要求。传统运营模式难以实现全过程留痕和效果量化，存在审计支撑不足、合规风险难以评估的问题。

解决方案：

数据整合与治理：针对运营商数据孤岛和多源异构的挑战，平台采用 AI 数据湖底座作为解决方案。它通过“实时 + 批量”双引擎，对终端、网络、云等多源数据进行高效采集、清洗和标准化处理，从而打破数据壁垒，为后续的智能分析奠定基础。

告警降噪与精准研判：针对海量告警导致的“告警疲劳”和误报率高的问题，平台创新性地使用了大小模型融合降噪技术。具体而言，利用 XGBoost 小模型进行快速、高置信度的误报过滤，再结合大模型（如 DeepSeek、千问）对复杂告警上下文进行深度解析和研判。该方案使告警降噪率高达 99% 以上，有效解决了行业痛点。

协同自动化处置与闭环：针对运营流程碎片化和缺乏高效闭环能力的难题，平台构建了多智能体架构。该架构包含 10 余类专业的智能体（如资产监测、处置响应等），通过智能体管理引擎实现高效协同作战，全面覆盖 IPDRR（识别、保护、检测、响应、恢复）流程。这种机制通过零代码创建自定义智能体，显著提升了平台的流程适配性。

快速响应与模型动态进化：为应对新型威胁和 0-day 漏洞，平台构建了动态进化能力。该解决方案建立了“威胁情报 - 实战数据 - 模型优化”的闭环机制，实时同步 CVE 漏洞库和 APT 组织情报，并通过人机协同复核持续优化模型精度，确保攻击识别率稳定提升至 95%，实现对未知威胁的快速响应。

工具集成与低代码定制：为解决传统工具集成复杂、自动化剧本开发门槛高的问题，平台利用 MCP 工具生态和 SOAR 自动化响应模块。通过标准化接口集成了 2000 多类工具，并提供拖拽式的剧本编排功能，实现了低代码定制。这一创新大大降低了自动化流程的开发难度，将部署周期缩短了 60%。

创新性与优势：

一是架构创新，“1+4+N”一体化架构打破数据与工具壁垒，通过统一数据底座整合多源信息，四大引擎提供核心动力，N 个专项场景适配不同行业需求，解决传统安全产品“碎片化”问题，实现全流程协同运营。

二是智能体协同机制，创新打造多智能体分层协作体系，支持零代码创建自定义智能体，可根据业务需求灵活配置功能，实现“即插即用”，较同类产品的单一智能体模式，适配性提升 300%，已在运营商场景落地 7 个专用智能体，覆盖 IPDRR 全流程。

三是大小模型融合降噪技术，通过 XGBoost 小模型快速过滤高置信误报，大模型深度解析复杂告警上下文，结合 BERT 语义匹配与历史数据比对，实现 99% 以上的告警降噪率，较传统规则引擎误报率降低 90%，解决行业“告警疲劳”痛点。

四是动态进化能力，构建“威胁情报 - 实战数据 - 模型优化”闭环，实时同步 CVE 漏洞库、APT 组织情报，通过人机协同复核持续优化模型精度，攻击识别率从 85% 提升至 95%，可快速响应 0-day 漏洞、未知变种等新型威胁。

五是低代码定制与生态开放，通过 MCP 工具市场支持第三方工具快速接入，提供拖拽式剧本编排功能，非专业人员也可定制自动化流程，较同类产品的高门槛开发模式，部署周期缩短 60%，已形成覆盖检测、取证、处置的完整工具生态。

应用效果：

运营效率方面，AI 自动化处置覆盖 90% 常规安全事件，告警数据压缩 90% 以上，安全人员研判效率提升 100 倍；某省级运营商应用后，日常运营效率提升 60%，重大活动保障期间威胁处置时间从 2 小时缩短至 15 分钟，漏洞自查效率提升 60%。

人力成本优化上，7×24 小时智能值守替代人工夜班，减少 70% 的重复性劳动，使安全人员聚焦高级威胁狩猎；通过专家经验沉淀复用，新员工培养周期从 6 个月缩短至 1 个月，有效缓解行业人才缺口压力，某能源企业安全团队人均效能提升 3 倍。

风险防控层面，高级威胁检出率达 97%，资产纳管覆盖率从传统 65% 提升至 99%，漏洞处置周期从 30 天压缩至 3 天；在运营商场景中，成功解决 15% 攻击链漏判问题，误封事件减少 12%，保障核心业务连续性。

商业价值上，平台帮助用户满足工信部、网信办等监管考核要求，获得合规加分；在运营商集团内部已申报优秀案例推广，具备跨行业复制能力；

应用生态方面，已覆盖政府、金融、能源、制造业、互联网等多个行业，服务客户包括省级运营商、大型能源企业等标杆用户，形成“产品 + 服务 + 生态”的良性循环，工具市场持续扩充，第三方开发者生态逐步完善。

经验总结：

运营商网络架构复杂、业务线多样，不同部门对安全运营目标和关注重点存在差异。项目初期，未来智安在需求梳理与场景抽象上投入较多时间，用于统一对威胁优先级、处置标准及运营指标的认知。后续可通过标准化场景模板和行业最佳实践库，进一步提升前期对齐效率。

基于安全大脑的网络安全智能中心平台

案例提供方：金睛云华

案例背景：

某企业长期服务于国家关键基础设施及大中型企业等高安全等级网络场景，客户业务系统规模大、网络结构复杂、数据类型多样，对安全的连续性、可靠性和自主可控要求极高。随着云计算、数据中心和办公网的深度融合，网络边界不断模糊，攻击手段呈现出多阶段、隐蔽化和自动化趋势，传统基于规则和单一特征的安全检测方式已难以满足实际防护需求。

在现有安全运营中，客户普遍面临三方面痛点：一是安全数据来源分散，日志、流量、终端和业务数据难以统一关联分析，导致威胁发现滞后；二是告警数量庞大、误报率高，安全人员长期陷入人工分析与处置，运营效率和响应速度不足；三是针对加密流量、未知威胁和高级持续性攻击（APT）的识别能力有限，难以形成持续、闭环的安全运营能力。

基于上述背景，客户迫切需要建设一套以多模态威胁检测和“安全运营安全大脑”为核心的新一代网络安全系统：通过引入生成式 AI 和人工智能大模型，融合流量、行为、日志和上下文等多源数据，实现对复杂威胁的精准识别与智能研判；同时提升安全运营的自动化与协同能力，减少对人工经验的依赖，为本地数据中心、云计算平台及办公网络提供统一、智能、高效的安全支撑，全面增强关键基础设施的网络安全检测与运营保障能力。

关键挑战：

客户面临的首要挑战来自安全数据规模与复杂度的急剧上升。一方面，网络环境中部署了大量异构安全设备和业务系统所产生的日志与流量数据呈指数级增长，日均数据量可达 TB 甚至 PB 级。如此海量的数据对采集、存储、计算和实时分析能力提出了极高要求，传统办法难以及时发现潜在威胁。

另一方面，现有安全管理与监测系统多为分散建设，缺乏统一的架构与数据标准，不同系统之间难以实现有效联动，形成明显的“信息孤岛”，导致攻击行为无法被完整还原为清晰的攻击链。对于具有多阶段、长潜伏期特征的高级持续性攻击（APT），这种割裂式的防护模式极易造成漏报与误判，放大关键基础设施被持续渗透和横向扩散的风险。

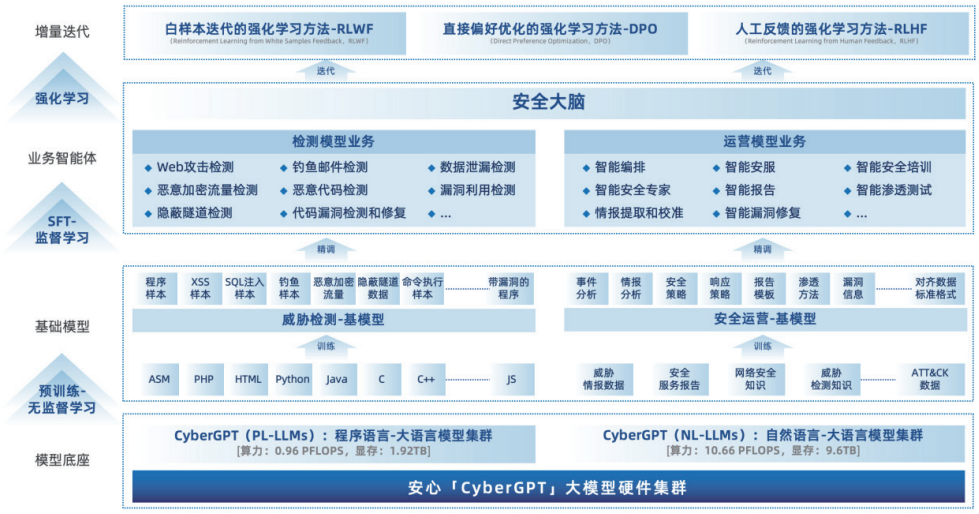
解决方案：

本项目以“内置安全大脑的网络安全智能中心平台”为核心目标，构建可对接主流 SOC / SIEM / 态势感知 / 日志审计平台的 AISecOps 解决方案，支撑 7×24 小时无人值守的智能安全运营模式，实现检测、研判、处置和运营的全流程闭环。

在模型层面，方案以 Qwen3 大模型作为统一模型底座，结合网络安全领域特性进行深度定制。通过分层

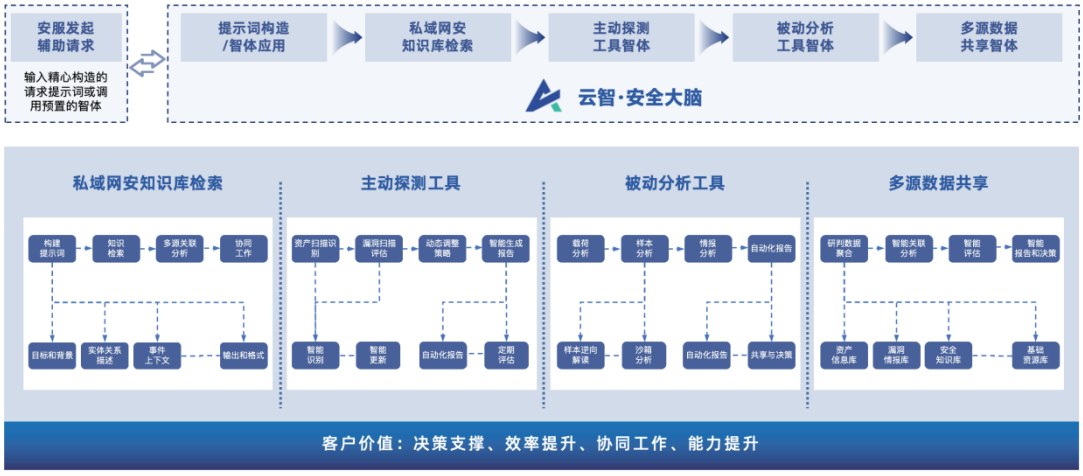
递进式训练策略，首先利用大规模通用与安全语料完成预训练，构建稳定、广泛的基础认知能力；随后通过 SFT（监督式微调）对安全检测、运营研判等关键任务进行精准适配；在此基础上，引入 DPO（直接偏好优化的强化学习）、RLHF（基于人工反馈的强化学习）/RLWF（基于白样本反馈的强化学习）等强化学习机制，持续优化模型在真实安全场景中的决策质量与稳定性，使模型能够不断贴合用户实际网络环境与白样本特征，实现长期可演进。

训练框架图如下：



在能力层面，方案通过检测智能体与运营智能体的协同设计，实现“检测即研判、研判即运营”。检测智能体聚焦于多模态威胁感知，覆盖 Web 攻击、恶意加密流量、隐蔽隧道、数据泄露与漏洞利用等核心风险场景，提升对未知与高级威胁的发现能力；运营智能体则面向安全运营全流程，提供智能编排、专家级研判、情报提取与校准、智能安服、自动化报告、漏洞修复、钓鱼邮件与恶意代码检测、代码安全修复、智能培训与渗透测试等能力，构建全生命周期的安全运营支撑体系。

安全运营智能体工作流程：



创新性与优势：

本方案以“多模态威胁检测 + 安全运营安全大脑”为核心，通过检测大模型、降噪 / 运营大模型与分层智能降噪体系的协同创新，构建面向未来的新一代智能安全能力。

在威胁检测层面，方案创新性地构建了面向网络安全的检测大模型。该模型采用大规模、任务无关的预训练架构，覆盖 ASM、C/C++、Java、SQL、PCAP 等 32 类程序与协议语言，基于近 1 亿不重复程序文件进行预训练，显著增强模型对程序语义、协议行为和攻击模式的理解能力。在此基础上，融合多年积累的 50 余类攻击样本库进行迁移学习与精调，使模型具备对真实攻击的高精度识别能力。同时，通过增量学习持续吸收用户侧白样本特征，动态适配不同业务环境，避免模型老化；结合模型压缩技术，在保证检测效果的前提下降低算力与部署成本，满足国防、政务及大型企业对自主可控与规模化部署的要求。

在安全运营层面，方案引入降噪大模型 / 运营大模型，通过更大参数规模模型，并结合 ChatGPT-o1、DeepSeek-R1 等模型进行高维特征提取与知识蒸馏，显著提升告警降噪和高级威胁发现能力。运营大模型通过“二次预训练—精调—对齐”的系统化训练流程，在应对 APT、零日漏洞和多阶段攻击时，具备更强的识别、预测与推理能力。在智能研判方面，平台融合资产、漏洞、威胁情报、原始流量等多源数据，结合 GraphRAG 技术，实现跨域关联分析与可解释推理，自动生成事件摘要、攻击路径解析、证据链和处置建议，输出完整、可追溯的攻击链报告，大幅提升研判效率与决策质量。

在告警治理方面，方案提出分层智能降噪（L0/L1/L2）机制。L0 层通过日志过滤、相同链接与载荷相似性聚合、ATT&CK 场景关联等方式，快速压缩约 50% 的初始告警；L1 层引入亿级参数的威胁检测大模型，对告警载荷进行深度语义分析，进一步剔除低价值告警；L2 层则调用运营大模型，对边界告警和潜在高级威胁进行上下文级研判，最终从海量噪声中精准锁定真正的高危攻击。该体系可在秒级完成告警降噪与分级，显著降低人工分析负担，避免关键威胁被淹没。

应用效果：

在实际应用中，业务处理时长从小时级缩短至分钟级，降噪率达 98%，综合运维成本降低 60%。

从客户评价来看，用户普遍认为该系统在复杂网络环境下具备较强的适应性和可解释性，攻击链与证据链展示增强了对研判结果的信任度，降低了对个人经验的依赖，有效缓解了安全人员的压力。系统在保障自主可控和稳定运行的同时，提升了安全管理的专业化和规范化水平。

在经济效益方面，通过告警降噪和运营自动化，安全团队效率显著提升。同时，重大安全事件风险的降低，减少了潜在的业务中断、数据泄露和合规处罚成本。综合来看，该方案在提升安全能力的同时，实现了可量化的运营降本和风险控制价值，具备良好的推广和复制意义。

经验总结：

在项目实施过程中，围绕多模态威胁检测与安全运营安全大脑的建设，团队积累了较为成熟的实践经验。

面对不断演化的攻击手段和业务变化，模型的持续迭代能力至关重要。项目实践表明，增量学习与持续精调是保障检测准确性的关键，但仍需进一步完善模型评估和优化机制，确保系统长期稳定、高效运行。

易安联零信任一体化办公终端安全项目

案例提供方：易安联

案例背景：

某省通信服务有限公司 2007 年成立，业务覆盖通信工程、智慧城市等多领域。因数字化转型，其面临网络边界模糊、云上资产暴露面扩大、终端管控缺失、身份认证不足、访问控制低效等安全挑战，亟需构建零信任安全防护体系，保障多场景下的身份、终端、数据等安全。

关键挑战：

1. 互联网的飞速发展突破了业务常规的时间和空间限制，移动化、碎片化的访问方式导致网络边界变得模糊，使得该公司的网络安全防护边界容易被泛化。

2. 大量业务大规模向云上迁移，应用系统不断增加和累积，导致企业资产在互联网上的攻击暴露面不断扩大，对现有安全体系造成了识别不了、监管不到、控制不全、分析不足等诸多新风险。

3. 终端数量巨大且缺少安全管控，无法实时掌握全网所有终端系统的安全态势，甚至基本的硬件配置和软件信息都无法获取，也就无法进行管理和管控。

4. 日益繁多的业务系统使得管理和访问变得更加困难，传统的基于账户和凭证的访问方式已无法确保身份的可信度。

5. 公司各地市公司、专业公司人员众多，各种不同角色的用户、不同访问途径、不同的业务系统、不同类型的终端交织下，传统基于网络层的访问控制策略显得不够灵活，通常还存在授予的权限比较宽泛，容易造成违规访问、越权访问等事件，并且运维管理成本增高。

解决方案：

基于零信任安全理念，易安联为该公司构建 1 个零信任安全运营体系，3 大基础平台：零信任可信接入平台、移动安全工作平台、终端管控平台，实现 8 大安全能力：可信身份管理能力、终端环境感知能力、暴露面收敛能力、最小化授权能力、基于业务的准入控制能力、数据管控能力、移动安全接入能力、动态策略编排能力，强化内网纵深防御能力，整体能力架构如图所示：

创新性与优势：

易安联零信任一体化办公终端安全是集身份认证、网络接入、防病毒、终端威胁检测、漏洞修复、终端管控、网络访问控制、安全空间等融合的全方位终端安全解决方案。基于零信任架构，该方案全面覆盖身份认证、终端防护、访问控制和数据安全等多维度防护，为企业提供一站式、高效、安全的终端安全防护能力。具备以下核心优势：

1. 病毒防护：守住第一道防线

高效病毒查杀：通过本地病毒库与云查杀结合，能够精准检测并拦截病毒、木马、勒索软件等威胁；

实时更新病毒库：定期更新病毒库和查杀引擎，确保第一时间应对最新威胁，让终端始终保持安全状态；

深度清理功能：快速消除潜在风险文件，及时恢复终端运行安全，为设备运行提供安全保障。

2. 终端威胁检测：快速检测与处置威胁

实时威胁监控：监测终端运行的每一个进程和操作，快速识别异常行为，及时预警；

快速溯源与处置:在威胁发生后,提供详细的安全事件日志记录,协助管理员快速定位问题根源并采取行动;

响应机制：内置威胁响应规则，实时识别并快速预警，有效降低事件扩散风险。

3. 网络接入：为每台终端划定安全界限

安全基线检查：设备接入前，需通过操作系统、杀毒软件、补丁等多项安全基线合规性检查，确保接入设备符合企业安全要求；

动态准入策略：根据安全状态、用户角色、地理位置等策略因子动态调整访问权限，确保安全性与灵活性兼得；

网络准入与业务准入结合：结合网络准入与业务准入，为企业提供无缝的安全接入体验。

应用效果：

构建“零信任”动态可信业务访问控制能力：参考零信任思想，遵循“持续信任评估、动态访问控制”原则，通过网络隐身、持续验证、细粒度动态访问控制等功能，收敛网络暴露面，降低漏洞被利用的机率，阻止潜在攻击。与 4A 整合联动，实现对用户身份的统一管理和认证，确保身份可信，保障业务接入和访问的安全。

构建全网智能化安全监测与威胁发现能力：终端安全态势感知，包括终端环境感知、终端安全事件检测与响应（EDR）、轻量级 DLP 等功能，可应对终端不同层面的安全威胁，满足终端安全、可信、合规要求。

构建全网智能化应急处置能力：以“零信任安全大脑”为核心，整合联动安全审计中心和安全应急处置中心，实现多方协同，在统一的安全环境里执行一致的安全策略，构建基于零信任的一体化主动安全防御体系，发挥最大的安全防护效能。

零代码策略编排扩展能力：使得公司在半天时间内就完成集团公司关于通行字管理要求，并通过零信任策略进行自动化管理。这得益于零信任平台的高级策略编排能力，无需厂家的研发介入，即可快速 DIY 想要的安全策略。

经验总结：

本项目在成果示范推广方面具有广阔的前景和价值空间，具体包括以下几个方面：

通信行业示范效应：作为通信行业在零信任安全领域的代表性成果，项目的成功实施和取得的显著成果将在整个行业内产生示范效应。其利用产品高级策略中心及可自主编排满足通信行业安全规范的策略，其他企业和机构将受到启发，看到零信任安全方案在信息安全保护方面的价值和优势，积极借鉴和推广这一先进经验，加强自身的安全防护能力。

创新解决方案提供商的角色：基于本项目的实施经验和成果，该客户有望在零信任安全领域成为创新解决方案的提供商。通过将项目的技术和实践经验转化为商业化的产品和服务，公司可以向其他各行各业提供定制化的零信任安全解决方案，满足不同行业的安全需求，并为企业提供增值服务，进一步提升公司的竞争力和市场份额。

市场需求的增长与扩展：随着 5G、互联网、云计算等技术的快速发展，对安全的需求日益增长。不仅金融、政府、高校等传统行业对零信任安全的需求迫切，而且制造业、医疗健康、物流等新兴行业也迅速意识到了信息安全的重要性。本项目的示范推广有望满足多样化行业的安全需求，拓展市场空间，实现商业增长。

纬将扩展检测响应平台建设项目

案例提供方：经纬信安

案例背景：

（一）客户基本情况

本项目服务客户覆盖政府机关、金融机构、通信运营商、能源电力、交通物流、医疗教育、科研院所等多个关键行业，客户普遍具备业务规模大、资产类型复杂、数据价值高、网络环境异构化等特点，对网络安全防护的全面性、实时性、智能性及合规性有严格要求。

（二）客户面临的痛点

传统安全防护体系碎片化严重，孤立的安全工具无法关联网络、终端、云环境等多源数据，形成“数据孤岛”，难以洞察威胁全貌，对高级持续威胁（APT）、零日漏洞攻击、复杂多向量攻击等新型威胁防御能力不足；

安全事件检测依赖人工分析，异常检测阈值固定，误报率、漏报率较高，且无法快速适配网络环境变化与威胁形态演进；

安全响应流程繁琐，多依赖人工手动操作，响应迟缓，难以在威胁扩散前完成处置，导致安全事件影响范围扩大；

安全运营效率低下，大量重复性工作占用安全团队精力，无法聚焦高风险事件处置，同时面临合规审计压力，缺乏标准化、可追溯的安全报告与运营流程；

企业资产动态变化，新增设备、应用频繁，传统防护方案难以实现全方位、自适应的安全覆盖。

（三）用户需求

需构建一体化安全运营平台，打破数据孤岛，实现多源异构数据的整合与关联分析，全面覆盖网络、终端、云环境的威胁检测；

要求具备智能检测与分析能力，能够自适应网络环境变化，精准识别新型威胁，降低误报率，提升威胁研判效率；

需实现安全事件的自动化响应与流程编排，缩短响应时间，减少人工干预，保障关键业务连续性；

希望通过智能决策辅助工具，基于海量数据生成科学的威胁报告与处置建议，优化安全策略制定与资源配置；

满足行业合规要求，提供可追溯、标准化的安全运营记录与报告；

支持灵活部署模式，适配不同 IT 架构，同时具备国产化、自主可控能力，保障数据安全与主权。

关键挑战：

（一）技术挑战

多源数据整合难度大：客户网络环境中存在网络流量、系统日志、用户行为、威胁情报等异构数据，格式不一、来源分散，需解决数据清洗、标准化及冲突修正问题，确保数据质量；

威胁检测精准度要求高：新型威胁不断涌现，攻击手法隐蔽多变，需突破传统规则检测局限，实现对未知威胁、变种威胁的精准识别，同时避免过度检测导致的误报；

自动化响应适配性复杂：不同客户的 IT 架构、业务流程、安全策略存在差异，需实现自动化响应剧本的灵活适配，同时平衡安全处置与业务连续性，避免误操作影响正常业务；

大模型落地适配难题：需将大模型技术与安全业务深度融合，解决模型训练数据针对性不足、实时性要求高、决策建议可落地性等问题。

（二）风险分析

安全风险：若威胁检测不及时或响应迟缓，可能导致客户核心数据泄露、业务系统瘫痪，引发重大经济损失与声誉损害；

合规风险：若无法满足行业合规标准，客户可能面临监管处罚，影响业务开展；

适配风险：不同客户的国产化软硬件生态差异较大，适配不当可能导致平台稳定性不足，影响防护效果；

运营风险：客户安全团队技能水平参差不齐，若平台操作复杂度高或缺乏自适应体验，可能导致功能利用率低，无法充分发挥平台价值。

解决方案：

（一）核心技术架构

平台采用五层架构设计，深度融合 XDR、SOAR 与 AI 大模型技术，构建全流程自适应安全运营体系，架构如下：

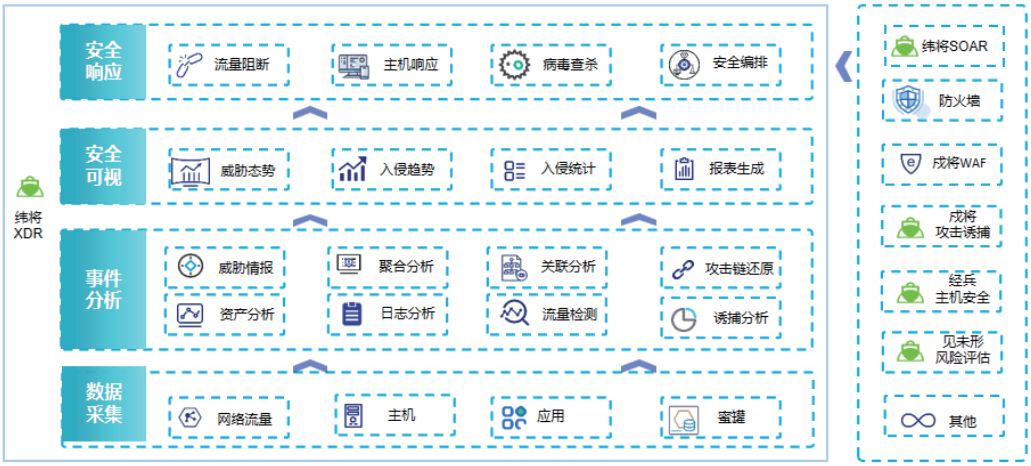
数据采集与整合层：部署网络流量探针、终端传感器、云平台连接器等采集器，智能识别新增设备、应用及数据格式变化，动态调整采集策略；通过数据清洗、标准化及关联分析，将多源异构数据整合为统一格式存入安全数据湖，针对数据冲突自动启动自适应算法，依据可信度、时效性完成数据修正与融合。

XDR 检测与分析层：融合无监督学习、图神经网络等 AI 算法，基于网络流量波动与用户行为变化自动调整检测阈值及参数，精准识别 DDoS 攻击、内部横向移动等异常行为；通过图神经网络构建自适应安全知识图谱，持续融入新威胁关系与资产关联信息，还原攻击路径、定位威胁源头。

SOAR 自动化响应层：基于预设安全剧本与工作流，实现安全事件自动化响应，可根据事件态势、业务需求及资源情况实时调整响应策略；通过 API 接口与第三方设备、系统无缝集成，自适应匹配不同设备的接口规范与协议，实现跨平台协同响应。

大模型 AI 赋能层：引入大模型技术对海量安全数据深度分析，自动解析复杂告警并提取关键信息，实时优化告警解析算法；动态生成威胁报告与处置建议，预测潜在风险并自动优化预测模型参数；构建全面的安全知识图谱，为威胁分析与溯源提供知识支撑。

可视化与决策层：提供直观交互的可视化界面，根据用户操作习惯、关注重点及态势紧急程度自动调整布局与展示内容；内置智能决策辅助工具，依据事件动态、用户反馈及企业安全目标自适应优化决策算法。



（二）核心功能实施策略

多源威胁检测实施：整合 NDR、EDR 等技术，全面覆盖网络、终端、云环境威胁检测；针对网络威胁实时监测流量模式，识别 DDoS 攻击、端口扫描等；通过终端传感器监控进程异常、文件篡改等事件；结合云平台数据检测云服务滥用、数据泄露风险。

智能威胁分析实施：运用 AI 算法与大模型技术，通过异常检测算法减少误报，利用机器学习模型对威胁分类分级；借助大模型自然语言处理能力解析安全日志与告警信息，提取关键威胁情报。

自动化响应处置实施：预定义覆盖常见威胁场景的安全剧本，检测到威胁后自动执行隔离设备、阻断连接、应急修复等动作；支持客户自定义剧本，适配个性化业务需求；通过与第三方安全设备联动，扩大防护范围。

安全编排与协同实施：将威胁检测、分析、响应、报告等环节自动化编排，形成闭环运营流程；通过 API 接口与业务系统集成，实现安全与业务深度融合。

自适应安全运营实施：全流程动态适配网络环境、威胁形态及业务需求，包括动态调整采集策略、优化检测模型参数、自适应响应剧本、个性化可视化展示等。

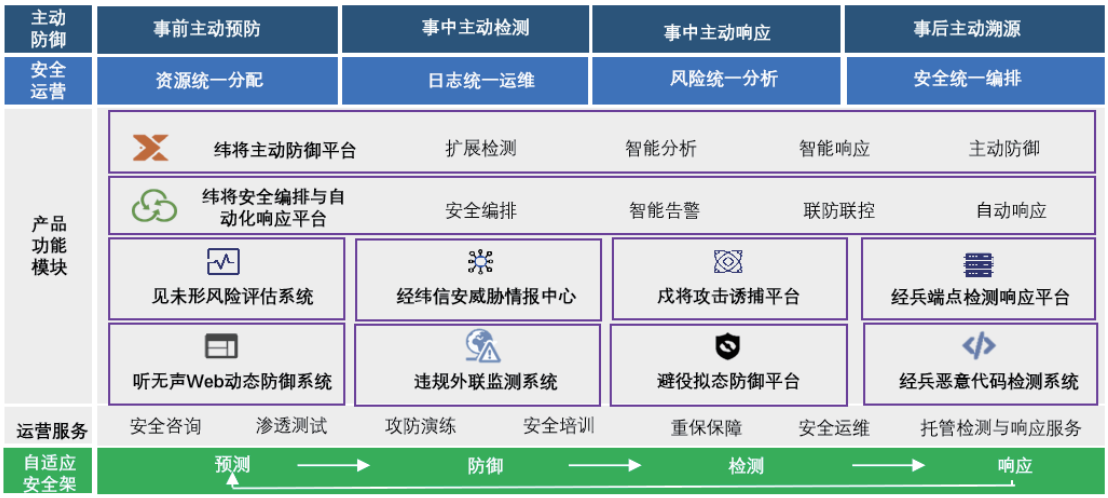
（三）部署模式选择

本地部署：针对数据安全与隐私要求严格的客户，部署在企业内部数据中心，确保数据本地存储与处理，满足数据主权与合规需求；

云部署：以 SaaS 模式部署在云端，企业通过浏览器即可访问，无需复杂本地部署与维护，降低中小客户与分支机构的运营成本；

混合部署：核心数据与关键业务部署在本地，非关键业务与数据存储在云端，通过安全网络连接实现本地与云端数据同步与协同，兼顾安全性与灵活性。

创新性与优势：



（一）核心创新点

自适应全流程安全运营：突破传统安全平台固定配置局限，实现采集策略、检测模型、响应剧本、可视化展示的全流程动态自适应，可根据网络环境变化、威胁形态演进及业务需求实时优化，无需人工频繁调整。

XDR+SOAR+AI 大模型深度融合：并非简单叠加三项技术，而是实现技术间的协同联动——XDR 提供全面数据支撑，SOAR 实现流程自动化落地，大模型提升智能分析与决策能力，形成“数据 - 分析 - 响应 - 决策”的闭环赋能。

国产化自主可控生态适配：已与统信软件 UOS、飞腾、龙芯、兆芯、银河麒麟等主流国产芯片及操作系统完成适配互认证，拥有 100 多项国家发明专利与软著，提供自主可控的主动防御解决方案，满足关键行业国产化替代需求。

安全知识图谱动态演进：基于大模型的知识抽取与图谱构建能力，自动整合新增威胁情报、资产关联信息，实现知识图谱的实时更新，持续提升威胁溯源与分析能力。

相比传统 / 同类方案的优势

对比维度	传统方案/同类方案	本项目方案
数据处理能力	孤立工具无法整合多源数据，数据利用率低	打破数据孤岛，整合网络、终端、云多源数据，数据处理能力≥15000EPS
威胁检测效果	依赖固定规则，对未知威胁识别能力弱，误报率高	AI算法+大模型赋能，自适应调整检测参数，未知威胁识别率提升60%以上，误报率降低50%
响应效率	人工响应为主，平均响应时间数小时	自动化响应+协同联动，平均响应时间缩短至分钟级，响应效率提升90%
适配灵活性	部署模式单一，难以适配异构IT架构	支持本地、云、混合三种部署模式，适配国产化生态与复杂IT环境
运营体验	操作复杂，需专业人员维护	界面自适应用户习惯，决策辅助工具降低操作门槛，安全团队工作效率提升70%
合规支撑	缺乏标准化报告，合规适配性差	生成符合GDPR、等保2.0等标准的安全报告，合规通过率100%

应用效果：

（一）实际应用效果

安全防护能力显著提升：平台已在政府、金融、能源、交通等多个行业落地应用，成功防范多起 APT 攻击、零日漏洞利用及勒索病毒攻击，某能源客户部署后，网络安全事件发生率下降 85%，核心数据泄露风险为零；

安全运营效率大幅优化：通过 SOAR 自动化响应与大模型智能辅助，客户安全团队的重复性工作减少 75%，威胁研判时间从平均 4 小时缩短至 30 分钟内，某大型银行客户的安全运营人力成本降低 40%；

合规需求全面满足：平台生成的标准化安全报告与运营记录，帮助客户顺利通过等保 2.0、GDPR 等合规审计，某政府客户在年度合规检查中获得优秀评级；

国产化适配效果良好：已在多个关键行业的国产化项目中成功部署，与国产软硬件生态兼容稳定，运行故障率低于 0.5%，满足自主可控要求。

（二）客户评价

中央网信办在重大活动网络安全专项服务中，对平台的威胁检测精准度与响应速度给予书面表扬，称其“为重大活动网络安全保障提供了坚实支撑”；

国家电网相关负责人评价：“纬将扩展检测响应平台实现了电网系统多源安全数据的统一管理与智能分析，自动化响应能力有效保障了电力业务连续性，是电网安全运营的核心支撑工具”；

广发银行反馈：“平台大幅降低了我们的安全运营成本，大模型提供的决策建议贴合金融行业场景，误报率远低于同类产品，帮助我们快速聚焦高风险事件”。

（三）经济效益与荣誉认可

经济效益：累计为客户减少安全事件直接经济损失超 10 亿元，降低安全运营成本平均达 35%-50%；

荣誉认可：项目荣获江苏省优秀实践案例第一名、2023 年江苏省信息技术应用创新优秀应用示范案例、2024 网络安全“金帽子”年度优秀政务行业解决方案、2024 全球数字经济大会 - 年度数据安全体系建设优秀实践案例等多项行业权威奖项;连续收录于《中国网络安全发展蓝皮书》,技术实力与应用效果获得行业广泛认可。

经验总结：

（一）项目实施过程中遇到的问题

部分客户的 legacy 系统接口不标准，导致数据采集适配难度大，影响数据整合的完整性与实时性；

不同行业客户的威胁场景差异显著，大模型初期对小众行业威胁的识别精度不足；

部分客户安全团队对自动化响应的信任度较低，倾向于人工干预，导致自动化功能利用率未达预期；

国产化生态中部分小众软硬件产品适配工作量大，需投入额外资源进行定制化开发。

（二）可优化的方面

技术优化：深化数据采集层的接口适配能力，开发更灵活的通用接口适配方案，提升对 legacy 系统与小众软硬件的兼容度;加强大模型的行业定制化训练，引入各行业专属威胁数据集，提升小众场景威胁识别精度;

产品优化：推出轻量化自动化响应剧本配置工具，降低客户自定义剧本的门槛；增加自动化响应效果模拟功能，提升客户对自动化处置的信任度；

生态优化：扩大国产化适配范围，与更多小众国产芯片、操作系统及第三方安全设备完成互认证，构建更完善的生态体系；

服务优化：加强客户培训与驻场指导，提供行业专属的运营方法论，提升客户安全团队的平台操作能力与自动化运营意识。

政务大模型合规与服务能力一体化测评系统建设项目

案例提供方：赛宁网安

案例背景：

省级政务服务管理局，负责统筹全省政务数字化建设，计划在 2026 年推广政务大模型（覆盖政务咨询、审批辅助、政策解读等场景），已试点部署 2 款政务大模型（省级通用版、民生服务专项版）。

面临的痛点：

1、政务大模型缺乏统一测评标准：

不同部门（民政 / 税务）对大模型的“政策准确性、数据保密性”要求不统一，测评流程混乱；

2、人工测评效率极低：

单大模型全场景测评需 1 个月，无法支撑全省 16 个地市的试点推广节奏；

3、合规风险高：

政务数据涉及公众隐私、行政机密，现有测评无法覆盖“数据脱敏、内容安全”等政务专属合规要求。

关键挑战：

1、政务场景特殊性：

需覆盖“政策解读准确性、审批流程合规性”等政务专属场景，测评题库需贴合行政业务逻辑；

2、数据安全风险高：

测评过程需接触政务敏感数据（如企业注册信息、民生补贴数据），需同时满足《政务数据安全管理办法》《个人信息保护法》；

3、多部门协同难：

全省 16 个地市的政务需求差异大，测评系统需适配不同部门的个性化指标，同时保证结果的统一性。

解决方案：

1、政务场景测评体系搭建：

在“测评对象管理”新增“政务大模型”分类，关联不同场景（咨询 / 审批 / 解读）；

在“测评题库集”构建“政务专属题库”：含政策合规库（如减税政策解读准确性）、数据安全库（如敏感数

据脱敏检测）、服务能力库（如审批流程辅助效率）。

2、安全合规测评落地：

通过“测评智能体”对接政务云平台，模拟公众咨询、企业审批等真实场景，自动执行测评任务；

调用“测评工具集”的“政务数据脱敏检测工具”“内容合规审查工具”，确保测评过程数据安全。

3、多部门适配与报告输出：

在“测评策略管理”中配置“部门个性化指标模板”（如税务部门侧重政策准确性）；

通过“测评报告管理”生成“全省统一合规结论 + 部门个性化服务得分”的双维度报告。

创新性与优势：

政务专属测评体系：相比通用 AI 测评，首次将“政务政策准确性、行政流程合规性”纳入核心指标，贴合政务场景需求；

安全与效率兼顾：测评周期从 1 个月缩短至 72 小时，同时实现测评过程“数据零泄露”，满足政务安全要求；

多部门协同适配：支持部门个性化指标与全省统一标准结合，解决政务系统“分散与统一难平衡”的痛点。

应用效果：

实际应用效果：已完成 2 款政务大模型的全省试点测评，政策解读准确率从人工测试的 81% 提升至 96%，数据脱敏合规率达 100%；

客户评价：“系统解决了政务大模型推广的合规与效率瓶颈，让智能政务服务既安全又好用”；

社会效益与经济效益：政务咨询人工客服压力降低 40%，企业审批辅助效率提升 35%，每年节省政务服务人力成本约 800 万元。

经验总结：

遇到的问题：初期部分地市的小众政策（如地方专项补贴）未纳入题库，导致测评结果覆盖不全；

可优化方面：后续需增加“地市政策题库自动更新接口”，联动各地市政务系统同步最新政策，提升测评的全面性。

云脑安全智能体平台建设项目

案例提供方：云起无垠

案例背景：

本案例客户为政企及关键信息基础设施单位，业务系统体量大、研发周期长、安全要求高。在长期安全建设过程中，客户一方面积累了大量与漏洞治理相关的安全知识资产，包括安全规范、漏洞分析报告、历史研判结论、整改经验及审计材料；另一方面也持续开展代码漏洞检测与安全测试工作，使用了多种静态分析和检测工具。然而在实际运行中，这两类能力长期处于割裂状态：安全知识难以在漏洞检测与研判过程中被有效调用，而漏洞检测结果又无法系统性沉淀为可复用的知识资产，导致同类问题反复出现、研判高度依赖个人经验。客户希望构建一个以知识为核心驱动力、以漏洞检测为核心应用场景的统一平台，实现安全知识与漏洞检测能力的深度融合，支撑安全治理能力的持续提升。

关键挑战：

客户在推进安全能力升级过程中，面临的核心挑战集中体现在知识与漏洞检测两个层面。在知识场景中，安全知识来源广泛、结构不统一，既包括文本类制度与报告，也包括与具体漏洞强相关的研判结论和代码片段，传统文档管理和搜索方式难以满足复杂问题下的快速调用需求。在漏洞检测场景中，虽然检测工具能够输出大量结果，但误报比例较高，研判过程依赖人工经验，且研判结论往往停留在项目层面，难以复用。此外，检测、研判、修复和复测之间缺乏统一的知识支撑和证据链管理，导致漏洞治理流程难以形成可持续优化的闭环。这些问题共同制约了安全知识价值的释放和漏洞检测效率的提升。

解决方案：

针对上述问题，云脑安全智能体平台以“知识驱动的漏洞治理”为核心设计理念，构建统一的安全智能平台。在知识场景中，平台通过安全智库能力，将客户内部的制度文件、漏洞分析报告、历史研判结论及外部安全研究成果进行统一纳管，并通过对话式交互方式，使安全知识能够在具体问题分析和漏洞研判过程中被直接调用。在漏洞检测场景中，平台并不简单替代原有检测工具，而是作为智能研判中枢，对多工具检测结果进行统一解析，并结合代码上下文和已有知识进行综合研判，输出高可信度的漏洞结论和修复建议。同时，平台将研判过程中的关键结论和证据反向沉淀为知识资产，持续丰富企业安全知识体系，形成“知识支撑检测、检测反哺知识”的正向循环。

创新性与优势：

云脑安全智能体平台的创新性，体现在其打破了传统安全建设中“知识系统”和“检测系统”相互独立的模式，实现了两者的深度融合。在知识场景中，平台不再将知识视为静态参考资料，而是通过智能体能力，使安全知识能够在漏洞检测和研判过程中主动参与分析，显著提升知识的使用频率和价值密度。在漏洞检测场景中，平台通过知识增强的研判机制，对检测结果进行上下文理解和经验校正，使误报率下降约 30%–50%，有

效漏洞命中率显著提升。相较于单纯依赖规则或模型的检测方式，云脑通过持续积累研判知识，使检测能力具备“越用越准”的演进特征，形成难以被简单复制的长期竞争优势。

应用效果：

云脑安全智能体平台在实际应用中，在知识利用效率和漏洞治理效率两个方面均取得了显著成效。在知识场景中，安全人员在进行漏洞分析、审计支撑和方案制定时，相关资料和历史结论的检索与复用效率提升约 2–3 倍，对个人经验的依赖明显降低。在漏洞检测场景中，通过知识增强研判机制，人工研判工作量平均减少约 50%，高风险漏洞的识别和确认速度显著提升，截至目前已成功发现零日漏洞上百个，其中有 10 余个漏洞已经申请 CVE 编号。同时，研判结论和修复经验被持续沉淀为可复用知识，为后续项目提供直接参考，减少同类漏洞重复出现的概率。整体来看，平台有效提升了客户在漏洞检测与治理过程中的质量、效率与可持续性，显著增强了安全能力的长期价值。

经验总结：

未来，云脑安全智能体平台将持续围绕“安全能力智能化、体系化和可持续演进”三大方向进行规划与建设。在技术层面，平台将进一步强化多智能体协同与任务编排能力，使安全知识获取、威胁情报分析、漏洞发现与研判等能力不再孤立运行，而是以智能工作流的形式自动协作，逐步实现从“人工触发”向“智能驱动”的安全作业模式演进。同时，云脑将持续深化安全垂直大模型对企业上下文的理解能力，通过引入更多真实业务场景数据和反馈机制，不断提升研判准确性、修复建议的可执行性以及整体决策质量。

在产品能力演进方面，云脑平台将从当前的“智能辅助”阶段，逐步迈向“安全中枢与决策引擎”阶段。通过持续完善安全指标体系、趋势分析与可视化能力，平台将能够为管理层提供长期、量化、可追溯的安全态势洞察，支撑安全投入评估、风险趋势判断和治理策略优化。在研发安全与安全运营场景中，平台也将进一步加强与企业现有流程和工具链的深度融合，推动安全能力向前置、自动化和常态化发展。

从行业视角来看，云脑安全智能体平台致力于构建可复制、可推广的安全智能化建设范式。通过模块化智能体能力和统一平台底座，云脑可根据不同行业和组织规模灵活组合与扩展，支持政企、关键信息基础设施及高安全要求行业的长期演进需求。未来，云脑将持续探索安全大模型与智能体技术在更多安全场景中的应用边界，推动安全治理从“被动响应”向“主动预防”和“智能决策”转型，为行业提供具有前瞻性和示范价值的安全智能化解决方案。

总结

人工智能正以前所未有的速度重塑技术体系、产业结构与组织形态。从大模型能力跃迁到智能体加速落地，AI 已从“赋能工具”转变为深度嵌入业务流程与生产系统的关键变量。在这一过程中，数字安全不再只是保障信息系统稳定运行的基础设施，而正逐步演进为支撑智能系统可信运转、推动新质生产力释放的核心能力。

通过对 ISC.AI 2025 第六届数字安全创新百强评选入选案例的系统梳理与分析，可以清晰看到一个共识正在形成：安全正在发生“智变”，而 AI 正在成为重构安全能力边界与价值形态的关键驱动力。

一、从被动防护到内生安全，安全能力加速前置化、体系化

在本届创新百强案例中，安全能力已不再局限于事后响应或外围防护，而是深度融入数据治理、模型训练、智能体决策与业务执行全过程。无论是面向大模型的数据安全与隐私保护，还是围绕智能体运行环境构建的实时风险感知与策略联动机制，均体现出安全能力从“外挂式防御”向“内生式架构”的转变。

多项案例显示，企业正在通过安全大模型、安全智能体等新形态，将安全能力嵌入业务逻辑本身，使其成为智能系统的“默认属性”。这种转变不仅提升了风险防控的及时性与准确性，也显著降低了智能化场景下的运维复杂度，为规模化落地奠定了基础。

二、AI 驱动安全能力跃迁，攻防关系正在被重塑

评选案例同时反映出，AI 对数字安全的影响是双向且深刻的。一方面，攻击手段正在加速智能化，自动化漏洞挖掘、生成式钓鱼、深度伪造等威胁不断突破传统防护体系的能力边界；另一方面，AI 也正在成为安全防御侧最具决定性的技术杠杆。

在入选案例中，AI 已广泛应用于威胁检测、行为分析、风险预测与自动化响应等场景，通过模型推理与持续学习显著提升安全系统对复杂威胁的识别能力。部分案例已实现从“人机协同”向“智能体自主处置”的演进，初步展现出安全运营模式在智能时代的全新形态。

三、场景牵引创新，数字安全加速向产业纵深渗透

本届百强案例覆盖金融、能源、制造、政务、交通、互联网等多个关键行业，充分体现出数字安全创新正在从通用能力建设走向深度场景适配。安全不再以“统一方案”简单复制，而是围绕行业业务逻辑、数据特征与风险结构进行精细化设计。

在工业互联网、物联网等场景中，安全能力正与实时控制、边缘计算和智能决策高度耦合，成为保障关键基础设施安全运行的重要组成部分。这一趋势表明，数字安全正在加速融入实体经济主战场，成为推动产业智能化升级不可或缺的底座能力。

四、生态共建成为共识，安全创新进入协同发展阶段

从评选结构与案例分布来看，数字安全创新已不再是单一企业或单点技术的突破，而是产学研用多方协同的系统性成果。本届评选汇聚安全企业、AI 技术厂商、行业用户、科研机构与资本力量，反映出安全创新正在形成更加开放、多元、协同的生态格局。

尤其是在安全大模型与智能体安全领域，多数入选案例均体现出跨领域协作特征，通过开放平台、联合研发与场景共创，加速技术成熟与规模化应用。这种生态化发展模式，将成为未来数字安全持续演进的重要支撑。

五、以“安全智变”回应时代命题，构建 AI 时代的新安全立场

综合本届数字安全创新百强评选成果可以看出，“安全智变，AI 赋能新立场”并非口号，而是一场正在发生的结构性变革。安全的角色正在从“成本项”转变为“能力项”，从“保障系统运行”升级为“支撑智能决策与价值创造”。

本报告所呈现的创新案例，既是对当前实践成果的阶段性总结，也为未来发展提供了可参考的路径样本。随着智能体进一步走向自治与协同，数字安全必将持续演进，其核心使命将不止于防范风险，更在于构建可信、可控、可持续的智能未来。

ISC.AI 将持续以评选与研究为抓手，推动数字安全与人工智能在更高层次实现融合发展，助力构建安全、韧性与创新并重的智能时代新生态。