

2026网络安全十大创新方向

Top Ten Innovative Technology Trends in Cybersecurity for 2026

2026

数说安全

AI安全创新从模型防护走向行动、身份、应用、供应链与基础设施



创新方向01：智能体运行安全与互联治理

推荐落地方案：

- 安泉数智-人工智能安全治理
- 奇安信-智盾AI智能体安全防护平台
- 三六零-360智能体安全防护与管理系统
- 悬镜安全-抵御 AI 智能体互联风险，构建可信智能体运行环境 | 问境 AIST
- 天融信-API安全审计系统

创新方向02：非人身份与智能体权限治理

推荐落地方案：

- 竹云科技-智能体全生命周期身份与权限治理 AIAM
- 格尔软件-AI大模型安全保险箱解决方案

创新方向03：Agentic SOC 安全运营自主闭环

推荐落地方案：

- 奇安信-XAgent 智能安全运营平台
- 微步在线-AI原生安全运营中心
- 三六零-仪天阵 AI时代的硅基安全防御团队
- 启明星辰-人工智能安全运营系统Agentic SOC
- 天融信-天问智防·智能安全运营中枢
- 安恒信息-AI 风险防御
- 睿安致远-Agentic SOC平台

创新方向04： AI自主安全研究与攻防验证

推荐落地方案：

- 悬镜安全-模拟攻防检验系统安全，提前阻断潜在漏洞风险 | 灵脉AI PTE
- 安恒信息-恒脑AI代码审计智能体
- 天融信-基于AI的自动化渗透测试系统

创新方向05： AI应用安全网关与运行防护

推荐落地方案：

- 奇安信-AI安全网关
- 三六零-AI安全卫士 企业级统一AI安全运营管理平台
- 绿盟科技-清风卫自身安全防护方案 AI UTM
- 天融信-大模型纵深防御体系

创新方向06： AI数字供应链与安全态势管理

推荐落地方案：

- 悬镜安全-洞悉数字供应链风险，实时掌握安全态势 | 源鉴 SCA

创新方向07：机密计算与可信AI推理

推荐落地方案：

- 蚂蚁密算-金融行业案例：提升银行资产质量的“数字风控官”

创新方向08： AI编码智能体与生成代码安全

推荐落地方案：

- 奇安信-QAgent Fabric 企业级安全可信 AI 研发基础设施
- 悬镜安全-勘破 AI 生成代码隐疾，闭环修复代码安全漏洞 | 灵脉 Code AI

创新方向09：生成内容真实性与溯源

推荐落地方案：

- 中科睿鉴-多模态内容真实性验证与全链路溯源方案

创新方向10：密码敏捷与抗量子迁移

推荐落地方案：

- 格尔软件-证券行业网上交易系统抗量子密码迁移方案
- 三未信安-SecQuan抗量子密码迁移平台

推荐方案无先后顺序。

智能体安全正在从模型输入输出防护，转向对任务规划、记忆、工具调用和动作执行的全过程控制。产品需在行动前完成动态判断，对MCP、A2A、Skill、工具权限和高风险操作实施准入、审批、阻断、回滚与审计。



核心能力

- 01 资产与行动链路发现
- 02 MCP/A2A/Skill治理
- 03 高风险动作准入审批
- 04 沙箱隔离、阻断与回滚
- 05 全过程审计

代表厂商（已具备相关产品或能力）





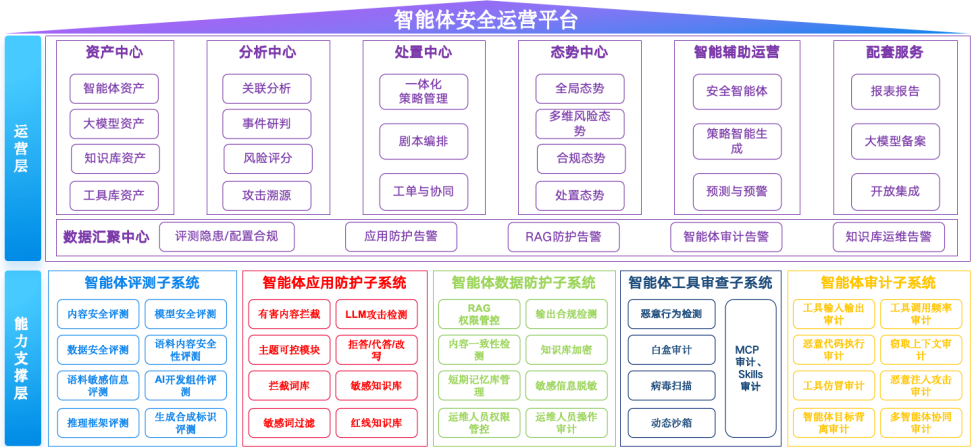
安泉数智成立于2023年，由浙江大学院士、教授、研究员和上市网络安全企业高管、核心技术人员创建，依托浙江大学区块链与数据安全全国重点实验室具有较强竞争力的前沿技术。具备“高校原始创新+产业工程实践”的双核优势。以“让智能更安全，让科技更向善”为使命，聚焦数据和人工智能安全领域，研发新一代数据安全和人工智能安全产品服务的国家级高新技术企业。以“成就客户、求是创新、至诚担当、奋斗共赢”为企业核心价值观，致力于成为全球领先的数智安全引领者。

方案概况

方案介绍：

面向政企单位在大模型、智能体及RAG知识库规模化应用中面临的内容违规、提示词攻击、敏感数据泄露、工具滥用、权限越界和审计缺失等AI 原生安全风险，方案打造“安全评测—应用防护—数据管控—工具审查—行为审计—安全运营”一体化原生安全防护体系。方案贯穿人工智能应用的全生命周期，提供“上线前风险评估、运行中实时拦截和事后可信审计处置”，帮助客户建立集 AI 资产摸底、风险感知、策略联动与事件响应于一体的集中化安全指挥中心。

方案示意图/拓扑图：



方案优势和用户价值

方案优势与特点：

- 全栈一体：集评测、防护、数据管控、工具审查、审计和运营于一体，打破单点防御壁垒，形成“监测-拦截-处置-进化”的全流程防护闭环。
- 全域覆盖：贯穿 AI 建设、部署与运行的全生命周期，全方位覆盖基座模型、知识库、智能体应用、API 工具及运行环境，消除防御死角。
- 精准防护：识别内容违规、越狱攻击、数据泄露、工具滥用和权限越界。
- 灵活易用：支持模块化组合、低侵入接入及私有化部署，适配不同业务场景。

用户价值：

- (1) 建立统一的AI资产台账和风险基线，及时发现未纳管大模型、智能体、知识库及工具资产，减少“影子AI”带来的安全盲区。
- (2) 实现“上线前测得清、运行中拦得住、上线后审得明”的常态化安全机制，实时化解内容合规、数据泄露及工具滥用风险，确保人工智能应用稳健运行。
- (3) 打通“监测告警—关联分析—策略联动—工单协同—审计追溯”的全链条运营协同，大幅提升响应与运维效率，轻松应对监管并满足企业合规要求。

典型客户或目标客户：

方案已应用于金融智能体客服实时风控防护、政务智能体办事大厅安全网关、企业智能体办公助手全链路行为审计、制造业智能体产线调度权限管控，以及航空智能体订票与客服系统实时内容过滤等智能体安全防护场景。



奇安信科技集团股份有限公司面向政企客户提供网络安全产品、解决方案与专业服务，覆盖终端、网络、云、数据与应用安全等领域。随着 AI 智能体规模化应用，Agent、MCP、Skills、Tools、模型等新型资产快速增长，并广泛运行于终端、Docker、Kubernetes 等环境，传统安全体系面临资产不可见、行为难监测、风险难关联等问题。为此，奇安信推出智盾 AI 智能体安全防护平台，通过统一探针实现智能体及相关资产的自动发现、适配与纳管，并持续监测资产、事件、会话及运行健康状态，帮助企业构建可见、可管、可控、可审计的 AI 智能体安全体系。

方案概况

方案介绍：

智盾AI智能体安全防护平台，面向AI编码、Agent运行等企业规模化AI应用场景，全面覆盖终端、Docker、Kubernetes等部署环境，依托插件、SDK、旁路采集多维度采集能力，自动发现、适配并统一纳管Agent、MCP、Skills、Tools等各类新型AI资产，持续监测资产变更、工具调用、会话交互及运行健康状态；结合会话上下文深度研判，精准识别提示词注入、越权执行、数据外泄等高危风险，实现风险关联分析、溯源定位与闭环处置，保障企业AI业务安全合规、稳定运行。

方案示意图：



方案优势和用户价值

方案优势与特点：

- 自动发现与纳管：覆盖终端、Docker、Kubernetes，自动发现影子 Agent 及 MCP、Skills、Tools、模型等资产。
- 执行防护：检测高危行为、命令、敏感文件和工具调用，按策略告警或阻断。
- 组件安全治理：检测 MCP、Skills、Tools 的投毒、篡改、异常外联及高风险调用。
- 上下文关联分析：关联会话、工具调用与执行结果，还原风险链路，支持告警与审计。

用户价值：

- 消除资产盲区：自动发现未知 Agent、影子 Agent 及 MCP、Skills、Tools、模型等 AI 资产。
- 降低业务风险：减少 Agent 误操作、敏感数据泄露及组件投毒对业务的影响。
- 提升处置效率：关联资产、告警与会话证据，快速定位异常行为及风险上下文。
- 灵活适配环境：覆盖终端、Docker、Kubernetes 等场景，按需启用防护、监测与审计。



360数字安全集团聚焦数字安全与AI安全，为政企客户提供实战导向的安全产品、服务与运营能力。

依托360近二十年积累的安全大数据、漏洞知识、攻防经验和专家能力，集团形成“看见+处置”数字安全能力体系，累计发现60个境外APT组织。面向智能体时代，集团坚持“以AI对抗AI”，以安全领域大模型和安全智能体蜂群为基础，一方面围绕大模型安全与智能体安全构建AI原生安全体系，另一方面推出360AI安全攻防系统图龙锋和自动化网络防御系统仪天阵，形成“主动发现+自动防御”的AI安全能力闭环。

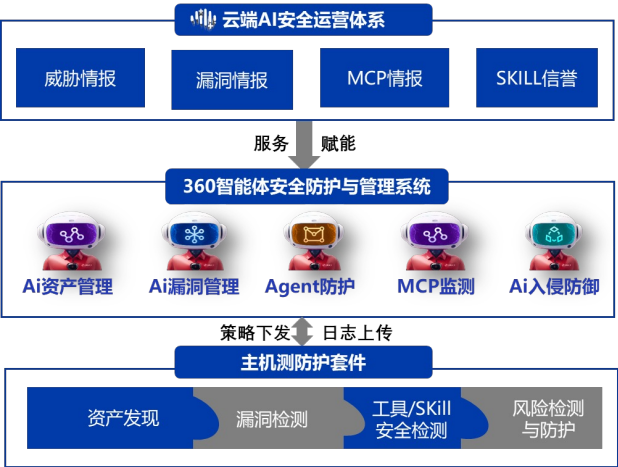
方案概

方案优势和用户价值

方案介绍：

360智能体安全防护与管理系统是AI Native的智能体运行时安全防护产品，系统围绕智能体资产发现与管理、智能体漏洞扫描与检测、入侵防御发现与拦截、MCP监测与防护、Agent安全防护、数据的备份恢复等核心能力，实现智能体环境安全可控、行为可审可管，为企业智能体多层次、立体化的安全防御屏障。

方案示意图/拓扑图：



方案优势与特点：

- (1) “主动扫描+深度检测”双引擎协同工作，发现、识别AI资产，消灭影子资产盲区。
- (2) 依托360云端 AI 运营与威胁情报能力，精准捕获AI资产漏洞与供应链风险，提升威胁发现效能。
- (3) 多层智能体运行防护，引入时静态扫描、事前意图识别、事中行为检测、事后行为审计进行Skill安全约束。
- (4) 智能体运行环境的安全防护，在防护智能体运行的安全同时，保护主机不被传统攻击所威胁。
- (5) 历史快照一键恢复，Agent改错文件、删错内容后，用户可以随时从多个历史版本中进行文件的一键恢复。

用户价值：

- (1) 解决客户“看得见”问题，摸清 AI 资产家底，精确到最小粒度，消除影子资产失控带来的安全风险问题。
- (2) 数据泄露风险识别，自动识别敏感数据外发、文件读取到API调用的上下链路行为，识别企业敏感数据外发风险。
- (2) 提高智能体安全运营效率，提供可视化、可追溯的安全运营能力，让智能体始终在人的管控之下工作。



悬镜安全源自北京大学“XMIRROR”网络安全技术研究团队，前瞻布局新一代数字供应链安全领域，先行构建“AI 原生安全 + 软件供应链安全 + AI 供应链安全情报”的治理体系。伴随 AI 智能体从对话助手演进为自主规划、调用工具、执行任务的数字劳动力，其安全边界随之扩展为模型、Agent、Skill、MCP、工具交织的复合体系。悬镜安全践行“以 AI 治理 AI”理念，依托问境 AIST 智能体 AI 原生安全治理平台与问境 AIDR智能体安全卫士，面向企业真实 AI 业务场景，构建智能体运行时安全与互联治理能力，帮助组织在 AI 业务规模化落地的同时，实现智能体行为可管控、风险可拦截、全链路可审计，护航 AI 业务安全稳定运行。

方案概况

方案介绍：

AI 智能体已深度赋能企业核心业务，亟需配套完成 AI 资产、运行行为、工具互联链路的安全管控。依托问境 AIST，通过主机 Agent + 网络嗅探双通道完成资产摸排，搭建包含Skills 安全审查在内的多模态运行时安全护栏，支持 SDK、网关、插桩轻量化接入异构环境。无需改造现有 AI 业务架构，保障业务连续运行，实现智能体行为管控、风险拦截、操作全链路追溯。

方案示意图：



方案优势和用户价值

方案优势与特点：

- 1. 双通道资产盘点：主机 Agent 结合网络嗅探识别全域 AI 资产，消除隐蔽资产盲区
- 2. 运行时安全护栏：防护输入输出及工具调用环节，内置Skills 安全审查能力，抵御提示词注入、Skill 组件恶意调用等 AI 原生风险
- 3. 互联链路治理：贯通模型-Skill-MCP-工具调用链路，收敛智能体跨组件互联风险
- 4. 业务零干扰接入：多形态轻量化部署，低开销、防护模式可切换，保障核心业务运行
- 5. 全链路审计追溯：留存智能体行为，异常事件还原现场，支撑风险闭环处置

用户价值：

- 1. 控资产：全域摸排 AI 资产，消除资产治理盲区，夯实智能体安全管控底座
- 2. 拦风险：运行时动态拦截 AI 原生威胁，依托Skills 安全审查识别拦截 Skill 组件恶意调用风险，降低越权操作、敏感数据泄露的业务隐患
- 3. 稳业务：安全策略弹性可配置，在开展防护的同时保障 AI 业务稳定连续运行
- 4. 达合规：自动输出 AI-BOM 资产清单与审计记录，支撑行业监管与合规核查工作
- 5. 促闭环：结合运行行为持续迭代防护策略，落地智能体安全常态化治理运营

典型客户或目标客户：

- 银行、证券、保险等金融机构
- 各级政务及数字化建设实施单位
- 能源、通信、车联网、工业互联网关基企业
- 大规模落地 AI 智能体业务的集团企业



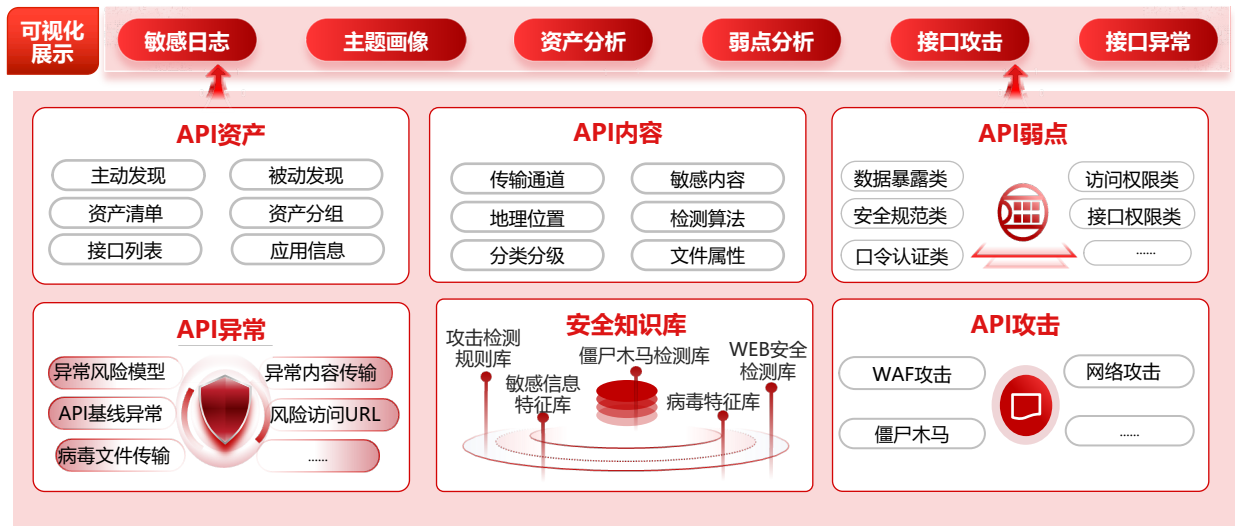
天融信（股票代码：002212）创始于1995年，是中国网络安全建设的中坚力量。在第四个“十年”发展期，公司围绕网络安全、智算云两大业务，聚焦AI安全防护、AI赋能安全、AI安全运营、AI基础设施建设四大方向，构建覆盖基础网络、工业互联网、物联网、车联网、卫星互联网、可信数据空间等全场景的产品、服务与解决方案，帮助全行业客户提升智能化安全防御水平、建设新一代智算基础设施，致力于成为中国领先的网络安全与智算云解决方案提供商，赋能千行百业数字化、智能化转型升级。

方案概况

方案介绍：

智能体（Agent）在运行过程中，通过大量API调用实现工具使用、数据获取与跨系统互联。API是智能体互联的核心通道，也是安全风险渗透的关键路径。天融信API安全审计系统将AI能力融入日志分析、系统研判、策略配置和安全处置等关键环节，构建“资产发现—内容检测—风险监测—可视分析—协同处置”全链路能力，将API安全从“被动防御”推向“主动智能”，为智能体互联提供全面的安全治理支撑。

方案示意图/拓扑图：



方案优势和用户价值

方案优势与特点：

- (1) API资产全面可视：自动发现全部API资产，精准识别“影子API”“僵尸API”等隐性资产，形成分类分级、责任人绑定的完整台账。
- (2) 接口访问精准管控：“用户-角色-API”权限绑定，实现精细化访问控制；支持自定义调用链序列，检测异常访问顺序，有效防范智能体越权调用。
- (3) 全维度风险监测：覆盖接口弱点检测（安全规范/权限控制/数据暴露等5大类）、异常检测（高频访问/撞库/数据爬取等）、威胁检测（SQL注入/XSS/僵尸木马等），实现“弱点+异常+威胁”三位一体防护。
- (4) 敏感内容深度审计：多维度检测API传输中的敏感信息泄露；全量日志留存+多维度检索+自动合规审计报告，满足法规要求。

用户价值：

- (1) 清互联资产底数：从API资产糊涂账到全可视、全掌控，消除智能体互联中的安全盲区；
- (2) 筑牢防护屏障：异常行为实时告警溯源+显性威胁提前阻断，保障核心数据在智能体互联中的安全；
- (3) 锚定合规要求：全量记录+精准追溯+自动报告，轻松应对监管审查，降低合规管理成本。

典型客户：已在政府、医疗卫生、税务、能源、交通、金融等行业规模化应用。

智能体正成为区别于自然人和普通服务账号的新型数字主体。治理需建立“用户—智能体—子智能体—工具”的动态委托链，明确代理对象、任务目的、有效时间、资源范围和责任归属，并支持短时凭证、最小权限与实时撤权。



动态委托链：权限随任务创建，随任务完成或风险变化而撤销

核心能力

- 01 智能体唯一身份与责任人
- 02 短时凭证与实时撤销
- 03 任务级最小权限
- 04 权限继承与委托治理
- 05 行动签名与审计

代表厂商（已具备相关产品或能力）





深圳竹云科技股份有限公司（简称“竹云”）是一家专注于数字身份管理与访问控制（IAM）核心基础软件及人工智能应用安全领域的高新技术企业，是国内IAM领域的中坚力量及国产化替代的深度实践者。公司拥有完全自主可控的国产化技术，构建了覆盖“人—组织—设备—应用—数据—AI智能体”全要素数字信任的产品矩阵，技术成果广泛应用于制造、能源、电力、航空、汽车、金融、政务等国家重点行业领域的数字化转型及人工智能应用创新与安全管控场景。

方案概况

方案介绍

针对企业规模化部署智能体引发的影子AI、混淆代理人、静态凭证泛滥、权限失控、数据泄露、权责无法溯源等高风险问题，构建AI智能体身份信任基础设施，解决AI智能体“看不见、信不过、管不到、控不住”四大难题；通过智能体资产发现、统一身份标识、动态凭证、最小权限授权、全链路审计能力，实现智能体全生命周期身份治理、权限管控与跨主体信任交互。

方案示意图



方案优势 and 用户价值

方案特点

- 端云融合：端侧（用户设备）内置智能体运行环境，实时监测影子AI，阻断异常访问请求；云侧（网络服务）基于智能体网关实现动态鉴权、应用和数据保护，端云协同综合研判。
- 身份权限推理图谱：基于可推理语义图谱，搭建覆盖人-设备-智能体-网络-应用-数据的六维对象模型；依托高性能实时推理计算引擎，实现实体关系推导、权限传递闭包、可达性分析等能力，为AI智能体提供确定性的推理与安全红线。
- 跨厂商兼容：兼容跨业务、跨厂商异构智能体，Agent、Skill等统一准入管控，覆盖备案申请、审批、授权、授信全流程，保障接入源头可信。

用户价值

- 可见：摸清智能体数量及智能体与人、资源间关联关系，实现AI资产与访问关系的透明化治理。
- 可信：管住智能体准入资质，实现来源可查、身份可验、设备可信，解决私装智能体和身份冒用等痛点。
- 可管：覆盖智能体注册-销毁全生命周期自动化管理，权限按需赋权、人-Agent权限联动。
- 可控：风险自动拦截、动态风控、实人兜底、全程存证，实现AI行为可约束、合规可举证。

目标客户

已规模化投产异构智能体，存在人-Agent或Agent-Agent多方调用，需管控智能体访问业务数据，并满足权限治理、风险及合规审计要求的企业。如大型央国企、金融机构、大型互联网&科技企业、大型制造集团及AI服务商等。



格尔软件股份有限公司是上交所主板上市的信息安全企业，3 次荣获国家科技进步二等奖。28 年来，格尔软件先后为 38 个国家部委、100 多家国企央企提供全栈全域的安全解决方案和专业化服务。2024 年，格尔软件在“身份认证”市场排名位列全国第二，荣获年度中国上市公司英华示范案例“A 股新质生产力价值奖”。2025 年，格尔软件承接阿尔及利亚某重要部 委数字信任体系建设项目，推动我国商用密码技术规模化出海。此外，格尔软件较早发布融合 PQC 的态势感知系统与量子 密码服务平台、抗量子视频安全解决方案等解决方案，较早推出 NGPKI 及抗量子混合证书解决方案及系列产品，较早完成自有密码产品体系 抗量子能力的全面升级，较早通过中国信通院 PQC 验证测试，获得抗 量子密码领域“上交会十大项目奖”和“中国网络安全与信息安 全产业年度优秀解决方案”。

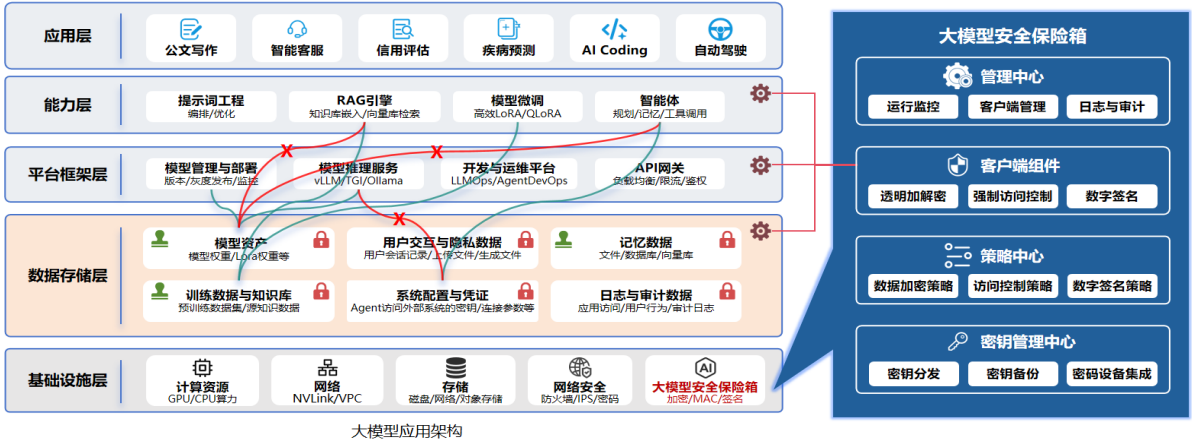
方案概况

方案介绍：

格尔AI大模型安全保险箱是专为AI核心资产打造的原生安全基础设施，旨在应对大模型时代“模型交付即失控”的安全困境。该方案直面模型权重泄露、敏感数据外泄、资产恶意篡改及Root权限越权四大痛点，将防护重心从传统的“网络管道”转移至“AI核心资产本体”。

产品通过三大核心技术机制构建闭环防护体系：加密为盾，在操作系统内核层实施透明加密，确保模型权重、知识库等落盘即密文，从根本上杜绝数据窃取；权控为锁，基于进程级强制访问控制，执行最小权限原则，精确管控进程对资产的访问，阻断非授权操作；可信为基，依托数字签名与完整性校验，为关键资产建立可信标识，防范投毒与篡改攻击。该方案可无缝嵌入异构算力环境，实现“业务零改造”部署，为金融、政务、能源等行业的AI应用提供从存储、访问到使用的全生命周期安全保障。

方案拓扑图：



方案优势 and 用户价值

方案优势与特点：

- 1. 业务零改造，开箱即用。无需修改训练、推理或知识库的任何代码，在内核层实现透明加解密，对应用与用户完全无感，零侵入集成。
- 2. 内核级强制访问控制，从底层杜绝越权。在操作系统内核层实施强制访问控制，只允许可信进程访问模型目录，即使拥有root权限也无法违规复制或窃取模型文件，彻底解决“上帝权限”滥用问题。
- 3. 高性能，GPU零损耗。加解密运算由硬件密码设备承载，对GPU训练与推理算力零占用，实测性能损耗低于5%，高强度安全与高效运行兼备。
- 4. 多级密钥保护，构筑高安全防线。采用“根密钥—保护密钥—文件密钥”三层架构，结合硬件安全模块（HSM）保护根密钥，即使服务器被攻破也无法获取明文数据。
- 5. 合规一步到位，生态广泛兼容。全面覆盖等保2.0、数据安全法、个保法及密评等合规要求；兼容 DeepSeek、通义千问、LLaMA等主流大模型，适配PyTorch、TensorFlow等框架及国产/开源操作系统与CPU架构。

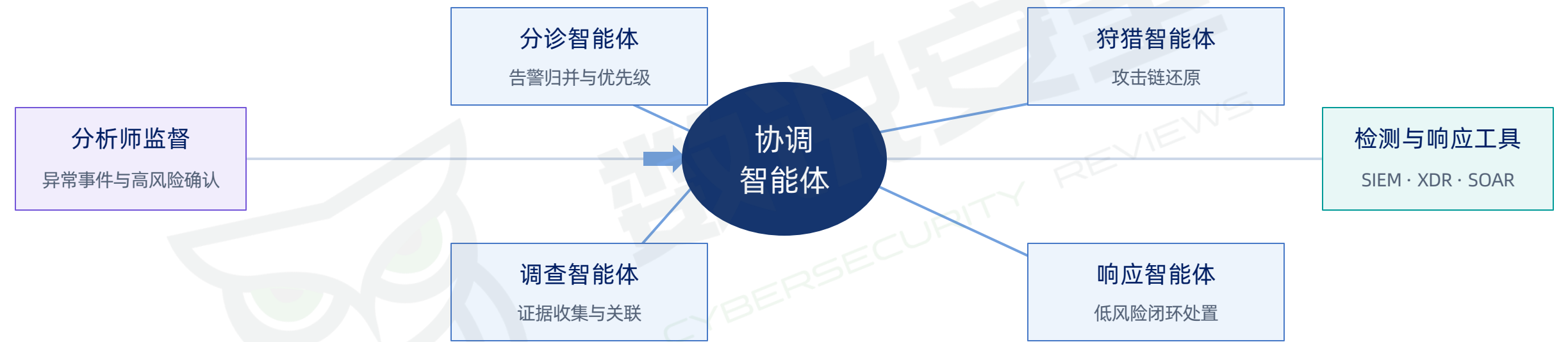
用户价值：

- 1. 打造了国内较早的证券期货业抗量子密码应用标杆案例（已于2025年上线）。
- 2. 解决了国际技术“卡脖子”风险，实现了核心技术自主可控。
- 3. 为证券行业从商用密码向抗量子密码迁移提供了可行路径与标准参考。

典型客户或目标客户应用场景：

- 1. 遵循《政务大模型安全规范》，保障数据安全与服务合规。
- 2. 保护内部规章制度、人事、财务等核心敏感信息。
- 3. 保护财务、市场等敏感数据，验证模型分析结果准确性。
- 4. 防止客户敏感信息泄露，确保回复合规礼貌。
- 5. 保护技术专利、核心代码等商业机密不泄露。
- 6. 确保内容符合广告法法规，规避品牌风险。

安全运营智能化创新不在于生成告警摘要，而在于多个专业智能体自主完成分诊、取证、关联调查、攻击链还原和部分低风险处置。安全分析师转向监督与异常事件处理，高风险动作仍保留人工确认。



区别于固定剧本：智能体可根据环境动态规划、选工具并调整调查路径

核心能力

- | | | |
|-------------|------------|------------|
| 01 多智能体任务规划 | 02 自动证据收集 | 03 攻击链关联还原 |
| 04 低风险闭环处置 | 05 高风险人工确认 | |

代表厂商（已具备相关产品或能力）





奇安信科技集团股份有限公司（以下简称奇安信，股票代码688561）成立于2014年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，在人员规模、收入规模和产品覆盖度上均位居行业头部。2019年，中国电子战略入股奇安信，奇安信成为网络安全“国家队”，迄今已完成91次国家重要活动网络安全保障任务，参与近千场实战攻防演习。作为网络安全领域重要参与者，奇安信将针对新技术下产生的新业态、新业务和新场景，继续为用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，助力实现“十五五”良好开局。

方案概况	方案优势和用户价值
方案介绍： XAgent，一个面向现代安全运营中心的多智能体自动化系统。它以最大化自主闭环运营为目标，可 7x24 小时不间断自主完成威胁检测、告警研判、事件调查及标准化处置响应等日常任务，从而极大地提升企业的安全运营效果。 自主闭环运营示意图：  QAX-GPT安全垂域大模型 通用大模型	方案优势与特点： （1）全面研判：秒级研判、零遗漏，准确率95%以上，告别告警疲劳。 （2）深度调查：分钟级溯源，深度调查攻击者留下的一切攻击痕迹。 （3）闭环响应：可联动奇安信及上百款第三方安全设备，实现生态级联动响应闭环。 （4）自主进化：从每一次任务中自我学习、改进，实现安全能力持续进化。 用户价值： （1）加速事件调查与响应：过去由分析师需要“数小时”才能完成的响应任务，XAgent 的智能体可在“分钟级”自主完成，最大化遏制风险扩散。 （2）自动化对抗AI攻击：XAgent 多智能体协同7x24小时永不停歇，持续对抗攻击者利用AI发起的自动化、规模化攻击。 （3）减少专家依赖：XAgent 智能体自主完成重复、低价值安全事件的闭环处置，降低对资深安全专家的依赖，让专家聚焦于高价值、高复杂性的安全任务。 目标客户： 金融、国企、央企、能源、政府、制造等



微步成立于2015年，是AI时代网络安全技术创新型企业，以实战导向的Agentic AI和处于行业前列的威胁情报TI为技术内核，提供覆盖“云、网、边、端”的新基础安全体系，通过新一代智慧安全运营平台、专家智能体和AI安全防护能力，帮助企业打造持续进化的自主智能安全。

方案概况	方案优势和用户价值
方案介绍： 微步 OneSOC是多智能体（Multi-Agent）架构打造的AI原生安全运营中心。微步OneSOC基于AI原生多Agent协同作战架构，可主动对告警进行智能研判，自动完成跨域多维关联取证，并实现秒级自动化响应与阻断。 微步OneSOC不是给SOC加上AI，而是用AI重新定义SOC，让AI真正走进安全运营，实现以AI对抗AI的新一代自主安全运营体系。 方案示意图： <pre>graph TD subgraph OneSOC_Cloud_Platform [OneSOC云端平台] AI_Agent[AI Agent 自动化安全运营] AI_Mapping[AI测绘 攻击面梳理] end subgraph Local_Broker [本地轻量Broker] Multi_Source[多源告警接入 告警日志汇聚] Cross_Device[跨设备联动调查处置 API/浏览器模拟接入] end Local_Broker -- "告警日志 加密、压缩上送" --> OneSOC_Cloud_Platform OneSOC_Cloud_Platform -- "调查/处置 指令下发" --> Local_Broker</pre>	方案优势与特点： （1）多Agent+人审协同作战。6大专精Agent覆盖研判→调查→处置全流程。自动跨设备协同调证，AI自主贯通，人仅审关键节点。（2）轻量化部署快速上线，本地仅部署轻量Broker，日志加密上送。云端承载AI运营与攻击面发现，已有建设零浪费。（3）开放生态功能模块化。100+设备预集成，支持STIX/TAXII/API标准化AgentHub自定义扩展，不绑定任何厂商。 用户价值： （1）多源设备集中研判。NDR、EDR等多品牌设备告警分散，设备老旧不统一，OneSOC统一接入后AI集中研判，告警压缩比超95%。（2）事件全流程自动化闭环。AI接入自主贯通从告警→研判→调查→处置的全链路，人工仅在关键节点审核。（3）安全运营团队AI化升级。不推翻已有SIEM/SOAR建设，轻量Broker接入现有设备。AI替代L1重复性研判，叠加智能运营能力。（4）攻防演练战时运营。演练/重保期间告警量暴增、值守人力透支。OneSOC多Agent协同7×24运转，AI动态编排替代预设固定剧本。（5）攻击面持续监控。替代传统的定期人工排查，7×24小时测绘暴露面，影子资产上线即感知。情报×画像×评分三轴融合，锁定致命风险。（6）安全知识体系构建与传承。向量知识库将历史案例沉淀为组织记忆，新人入职即继承团队实战经验。 典型客户： 国央企、智能制造、高科技、科研机构及高校等



360数字安全集团聚焦数字安全与AI安全，为政企客户提供实战导向的安全产品、服务与运营能力。

依托360近二十年积累的安全大数据、漏洞知识、攻防经验和专家能力，集团形成“看见+处置”数字安全能力体系，累计发现60个境外APT组织。面向智能体时代，集团坚持“以AI对抗AI”，以安全领域大模型和安全智能体蜂群为基础，一方面围绕大模型安全与智能体安全构建AI原生安全体系，另一方面推出360AI安全攻防系统图龙锋和自动化网络防御系统仪天阵，形成“主动发现+自动防御”的AI安全能力闭环。

方案概况

方案介绍：AI正在让攻击变得更快、成本更低、规模更大，依赖人工串联的防御方式难以跟上机器速度，安全运营必须走向自动化。面向这一结构性变化，**360仪天阵**将安全大模型、安全智能体、专业知识、Skill组织成**硅基安全防御团队**，把“人操作平台、串行推进任务”转变为“**人设定目标和边界、硅基安全专家自主推进协同**”，在受控边界内持续完成安全研判、处置与结果交付，实现自动防御。

方案示意图



新的范式不是再造一个平台，也不是简单增加人力，而是打造一支硅基安全防御团队。

方案优势 and 用户价值

方案优势与特点：

- (1) **以硅基安全团队重构安全运营主体：**从交付一套供人操作的平台，转向交付一支持续完成任务的AI专家团队；硅基专家负责理解、判断和动态调整，协同推进复杂任务直至交付。
- (2) **以目标驱动多智能体协同：**AI负责执行与交付，人负责目标、权限和关键审批，关键环节人在回路，过程全程可追踪、可审计。硅基专家自主围绕目标拆解任务、共享上下文、并行研判、补证与验证，直至输出可交付结果。
- (3) **轻量化架构加快方案落地：**不复制全量数据处理和平台功能，按任务获取必要线索、证据及能力；充分利旧已建设的安全设施。
- (4) **以360全栈安全智能技术体系构筑专业壁垒：**依托长期“AI+安全”实践，360形成专业模型判断、智能体协同、实战能力执行和企业级治理一体化的技术体系，将安全Know-how转化为稳定、可信、可规模复制的自动化防御能力。

用户价值：

- 01 让安全任务自动推进

从人工跨平台查询、派单和串行接力，转向硅基团队围绕目标持续协同，自主推进。
- 02 让人类专回归价值工作

仪天阵承担大量调查、证据整理和执行工作，人的精力聚焦复杂例外、风险决策和验收。
- 03 让已有安全投入持续增值

无需推到重建，保留已有SOC、数据和工具体系，较小改造实现AI重塑与能力放大。
- 04 让运营结果可信可控

统一沉淀结论、证据、动作和任务报告，通过人工审批、权限管控和审计留痕。



启明星辰信息技术集团股份有限公司成立于1996年，2010年在深交所中小板挂牌上市（股票代码：002439），2024年正式成为中国移动专责网信安全专业子公司，全面开启高质量可持续发展的新阶段。多年来，启明星辰始终以用户的需求为根本动力，将场景化安全思维融入到客户的实际业务环境中，不断地进行创新实践，帮助客户建立起完善的安全保障体系，逐渐成为政府、金融、能源、运营商、税务、交通、制造等企业级客户的重要合作伙伴。

方案概况

方案介绍：

启明星辰人工智能安全运营系统Agentic SOC依托AI原生架构，以多智能体联邦技术+自主决策中枢为核心，融合丰富的内置安全工具与第三方MCP标准化接入，实现从告警研判、事件调查、威胁狩猎到响应处置的全链路智能体自主协同赋能，驱动安全运营从“AI 辅助”向“AI 自主运营 + 人监督”的范式跃迁。

方案示意图/拓扑图：



方案优势和用户价值

方案优势与特点：

- (1) “自主”，主动识别运营目标需求，自动拆解任务及动态路径规划
- (2) “协同”，联邦式多智能体协同精准执行，100+ 步骤复杂流程稳定可控
- (3) “飞轮”，三大飞轮（生态×数智×效用）自驱加速，数据 + AI持续进化
- (4) “效能”，大模型负责深度推理、小模型扛高并发，研判深度与效率兼得
- (5) “生态”，200+内置安全工具+丰富的第三方MCP 标准化原子能力接入

用户价值：

- (1) AI 自主承担海量的告警研判、事件调查等高频重复运营任务，安全分析师从“操作员”升级为“审核员”，聚焦高级威胁与策略优化。
- (2) 运营经验持续沉淀为知识并反哺模型与策略，安全能力不随人员流动衰减，平台越用越强、越用越增值。

典型客户或目标客户：

山东移动、中移国际、中山市政数局、洛阳市大数据局、吉林银行、江苏国网、许昌市大数据局、移动云、广州烟草...



天融信（股票代码：002212）创始于1995年，是中国网络安全建设的中坚力量。在第四个“十年”发展期，公司围绕网络安全、智算云两大业务，聚焦AI安全防护、AI赋能安全、AI安全运营、AI基础设施建设四大方向，构建覆盖基础网络、工业互联网、物联网、车联网、卫星互联网、可信数据空间等全场景的产品、服务与解决方案，帮助全行业客户提升智能化安全防御水平、建设新一代智算基础设施，致力于成为中国领先的网络安全与智算云解决方案提供商，赋能千行百业数字化、智能化转型升级。

方案概况

方案优势和用户价值

方案介绍:

天融信天问大模型系统+态势感知系统构建智能安全运营中枢，为各类安全运营平台和安全设备联动赋能，构建更为智能化的安全运营防护体系，实现AI新型威胁防御、威胁情报自动分析、网络安全告警降噪等目标，提升日常安全运营效率。

方案示意图/拓扑图:



方案优势与特点:

- (1) “看得见”：威胁感知，快人一步。
天问大模型赋能安全运营平台，将威胁识别提升至第一瞬间，实现从事后追溯到实时感知的转变，让风险无所遁形。
- (2) “判的准”：精准研判、误报极低。
基于天问大模型的长周期学习与深层次训练，新型攻击、钓鱼邮件、可疑流量等场景均能精准识别，AI攻防场景准确率 > 95%。
- (3) “动的快”：智能协同，效能倍增。
内置数十种安全智能体，面对不同业务场景可协同联动。智能体可根据任务类型精准调配各类安全工具，形成高效闭环。

用户价值:

- (1) 海量告警降噪：智能体自动关联上下文、交叉验证，以高准确率过滤海量误报，大幅降低告警噪音。
- (2) 缩短响应时间：多智能体并行分析、调查将小时级排查压缩至分钟级，MTTR降低60%。
- (3) 加速威胁遏制：确认威胁后自动生成处置方案，人工确认后一键遏制。

典型客户: 政府、能源、金融、运营商、卫生、教育、大型央企等。



安恒信息技术股份有限公司（股票代码：688023）成立于2007年，于2019年科创板上市，是国内网络安全、数据安全和数据要素市场的重要参与者，也是国内积极推动以AI赋能传统网络安全、数据安全转型的典型企业代表。安恒信息以AI驱动产品服务革新，陆续推出安全智能体——恒脑，AI安服数字员工——安小龙，为业界树立AI应用标杆，自主研发了数据安全岛隐私计算平台、数由空间、数由器®连接器等明星产品，为数据安全流通、数据可信接入等数据基础设施建设场景中的难题提供了解决思路。

方案概况	方案优势和用户价值
方案介绍： 基于AI能力与风险防御六步闭环，构建漏洞监测、定向挖掘、渗透测试、仿真诱捕、漏洞治理与运营的风险防御体系；云端与本地协同、发现与验证并重、运营与治理闭环，帮助客户更高效发现漏洞、识别影响、验证风险并推动修复。 方案示意图	方案优势与特点： 1. 漏洞工厂云端监测与情报订阅：7×24 小时云端监测，覆盖全球漏洞情报，持续生产高质量漏洞数据，快速获取最新风险。 2. AI 代码审计定向挖洞：结合代码与 SBOM，AI 驱动定向挖掘，精准发现高危缺陷与潜在漏洞。 3. 安小龙自动渗透验证：自动化编排验证流程，快速确认漏洞可用性，降低人工成本，提升验证效率。 4. AI 蜜罐高仿真诱捕：多协议、多场景高仿真蜜罐，诱捕攻击者，捕获攻击链与 TTP。 5. 零日雷达资产漏洞关联 + 资产图谱暴露面科学治理：零日雷达关联资产与漏洞，洞察真实风险；资产图谱可视暴露面，科学制定治理策略。 用户价值： Ø 高效发现与影响识别：整合情报、代码与资产多源数据，AI 赋能全链路挖掘，快速发现漏洞并精准识别受影响资产与业务，全面掌握风险全景。 Ø 验证诱捕驱动精确修复：自动化验证确保风险真实可用，高仿真诱捕提升检测深度，基于资产图谱制定优先级修复策略，推动风险闭环治理，最大化安全投入回报。



睿安致远致力于AI赋能、数据+流程双轮驱动的Agentic SOC（自主化安全运营）平台，面向最终用户、厂商和安全服务商提供智能化、自动化、可快速按需定制的安全运营平台，帮助客户快速搭建属于自身的AI安全运营平台、产品与服务。

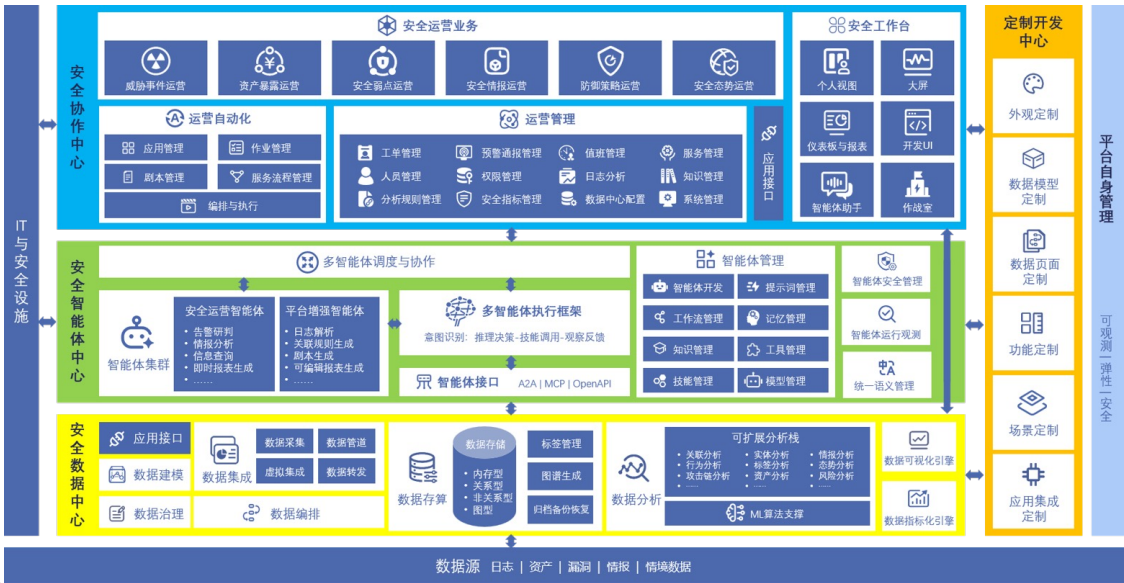
主创团队持续24年专注安全运营，完整参与国内SOC从1.0到3.0的发展演进过程，是国内SOC4.0（Agentic SOC）理念的提出者，2025年5月正式发布Agentic SOC平台产品MetaSec-SOP。

方案概况

方案介绍：

针对安全运营面临“人手紧、数据乱、效率低、定制难”的困局，睿安致远依托四大核心技术能力，推出Agentic SOC平台——MetaSec-SOP。该平台不仅通过开放式多智能体架构实现了安全运营工作的分级自主、可信运行和循环迭代，同时也提供AI就绪的安全运营平台数据底座、承载安全运营业务价值流的流程底座，以及低代码定制开发框架，真正实现人、智能体、运营工具和网络安全防御设施之间的自主化协同防御。

方案示意图



方案优势和用户价值

方案优势与特点：

- (1) 基于开放智能体的安全智能体中心：对接多种GenAI，采用多智能体协同、分级自主的模式，实现运营任务分级自主、可信运行、循环迭代。平台内置 MCP 服务器，支持平台内部以及外部第三方智能体调用接入；
- (2) 基于数据编织的安全数据中心：实现贯穿安全要素数据治理、集成、编排、分析、存储、分发、度量与呈现的数据架构重构，为运营自动化和AI化提供数据底座，全面激活数据价值；
- (3) 基于安全编排的安全协作中心：通过“双编排引擎+自主智能体”的组合，构建多级人机协同模式，实现安全运营人员工作的协作化、实战化、自动化；
- (4) 基于低代码技术的定制开发中心：依托平台自身的开放式架构，实现安全运营平台界面、数据模型、功能、场景等的低代码快速开发定制。

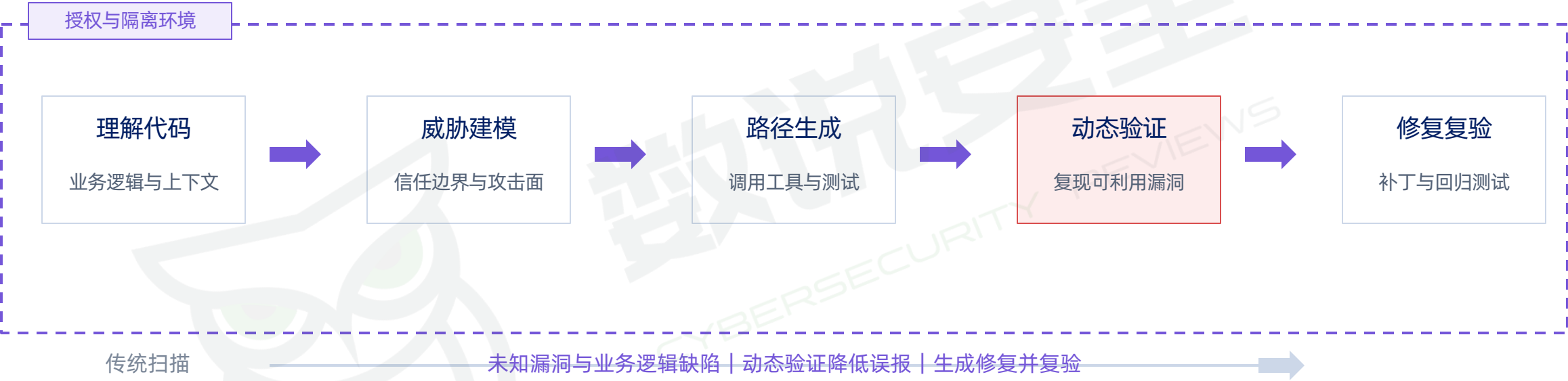
用户价值：

- (1) 释放数据价值：依托新一代安全数据架构，数据处理综合能效提升5倍；
- (2) 扩大运营规模：依托新一代流程驱动架构，运营流程执行效率提升10倍；
- (3) 提升运营效率：依托开放式智能体架构，运营自主化提效10倍；
- (4) 缩短定制周期：依托低代码开发技术，平均定制周期从2个月降到2周。

重点目标客户及合作伙伴：

金融、运营商、央国企数科公司及研究院、安全服务商、安全厂商等

AI正在从辅助生成测试报告，走向理解代码与业务逻辑、自主构建威胁模型、生成测试路径、调用工具验证漏洞、提出修复并复验效果的安全研究系统。价值核心是发现未知缺陷，并通过动态验证降低传统扫描误报。



核心能力

- | | | |
|--------------|--------------|------------|
| 01 代码理解与威胁建模 | 02 测试路径与工具调用 | 03 漏洞利用性验证 |
| 04 修复建议与补丁生成 | 05 隔离复验 | |

代表厂商（已具备相关产品或能力）





悬镜安全，起源于北京大学网络安全技术研究团队“XMIRROR”，前瞻布局新一代数字供应链安全，深耕**实战攻防与 DevSecOps 敏捷安全领域**。基于多年红队攻防实战积淀，率先落地多智能体驱动的 AI 自主威胁模拟技术，旗下**灵脉AI PTE 自动化渗透测试平台**是国内 AI 自动化攻防验证代表性产品，实现由单点漏洞扫描向完整攻击链仿真的技术代际升级。产品将专家级渗透经验转化为标准化安全算力，可联动软件供应链安全检测能力，兼顾业务系统与 AI 智能体攻防验证，助力企业落地“以攻促防”的主动防御体系，持续收敛全域攻击面。

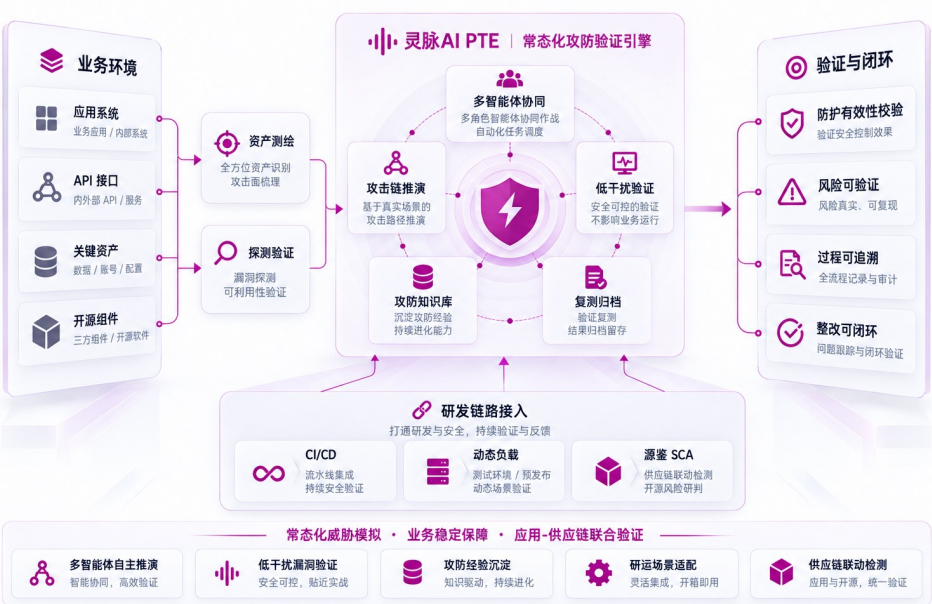
方案概况

方案优势和用户价值

方案介绍：

业务迭代加速，攻击趋向智能化、组合化，企业亟需常态化攻防验证能力。灵脉AI PTE 基于多智能体协同架构，复刻红队实战思维，完成资产测绘、探测验证、攻击链推演至复测归档全流程自主攻防验证；无缝嵌入 DevSecOps 研发链路，联动源鉴 SCA，将开源组件漏洞、投毒风险纳入攻防推演，保障业务稳定，开展常态化威胁模拟，校验防护有效性，实现风险可验证、过程可追溯、整改可闭环。

方案示意图：



方案优势与特点：

- 1. 多智能体自主推演：拆解渗透原子任务，模拟红队逻辑，自动生成攻击全景路径
- 2. 低干扰漏洞验证：无害 PoC 研判漏洞，压低误报，兼顾检测精度与业务稳定
- 3. 攻防经验结构化沉淀：沉淀专家渗透经验，搭建攻防知识库，实现能力复用
- 4. 研运场景深度适配：支持 CI/CD 接入、动态负载，覆盖研发、巡检、重保场景
- 5. 供应链联动检测：联动源鉴 SCA，推演开源风险，实现应用-供应链联合验证

用户价值：

- 1. 强实战：挖掘传统工具遗漏风险，核验防护拦截效果，消除入侵隐患
- 2. 提效能：承接重复渗透工作，压缩检测复测周期，减轻红队人力压力
- 3. 保稳定：动态调控检测负载，实现无扰动验证，规避扫描业务故障
- 4. 达合规：留存攻防完整证据，输出标准报告，支撑等保、演练、监管取证
- 5. 促闭环：贯通检测-分级-工单-复测全流程，落地以攻促防

典型客户或目标客户：

- 银行、证券、保险等金融机构
- 各级政府及数字化建设单位
- 能源、通信关键基础设施企业
- 具备大规模软件研发能力的集团企业



安恒信息技术股份有限公司（股票代码：688023）成立于2007年，于2019年科创板上市，是国内网络安全、数据安全和数据要素市场的重要参与者，也是国内积极推动以AI赋能传统网络安全、数据安全转型的典型企业代表。安恒信息以AI驱动产品服务革新，陆续推出安全智能体——恒脑，AI安服数字员工——安小龙，为业界树立AI应用标杆，自主研发了数据安全岛隐私计算平台、数由空间、数由器®连接器等明星产品，为数据安全流通、数据可信接入等数据基础设施建设场景中的难题提供了解决思路。

方案概况

方案介绍：

恒脑AI代码审计智能体被业界称为对标“Mythos”漏洞挖掘的中国方案，已在Windows、iOS、Linux、FreeBSD、Claude Code等重点项目及多个开源软件场景中开展漏洞分析。截至25年8月底，恒脑AI代码审计智能体累计分析漏洞超50000个，已分析出数百个0day漏洞，百余家客户单位参与试用体验，服务覆盖政府、金融、能源、教育等关键行业，破解传统 SAST 工具误报率高、难以挖掘 0day 与业务逻辑漏洞、深度审计高度依赖安全专家的行业痛点，可实现 7×24 小时无人值守自动化代码审计。

方案示意图/拓扑图：



方案优势和用户价值

方案优势与特点：

- 持续进化·无需干预：智能体具备自主学习与演进能力，一次部署即可持续提升审计能力，大幅降低人工维护成本。
- 灵活适配·开箱即用：无需改动核心系统，快速接入企业任意开发流程与安全策略，零摩擦落地。
- 五倍效率·并行破局：多智能体协同工作，大幅压缩代码审计周期，让安全团队从海量告警中解放，聚焦真正关键的高危漏洞。
- 自动验证·告别误报：内置标准化验证引擎，自动生成可执行的PoC，每条告警都经过实战化检验，精准可靠。

用户价值：

自动输出带证据链、分层修复方案的可视化审计报告，可对接 CI/CD 流水线，大幅降低人工审计成本，打破海外代码安全工具技术封锁，保障关键信息基础设施代码安全。

典型客户或目标客户：

政府、金融、能源、教育等关键行业



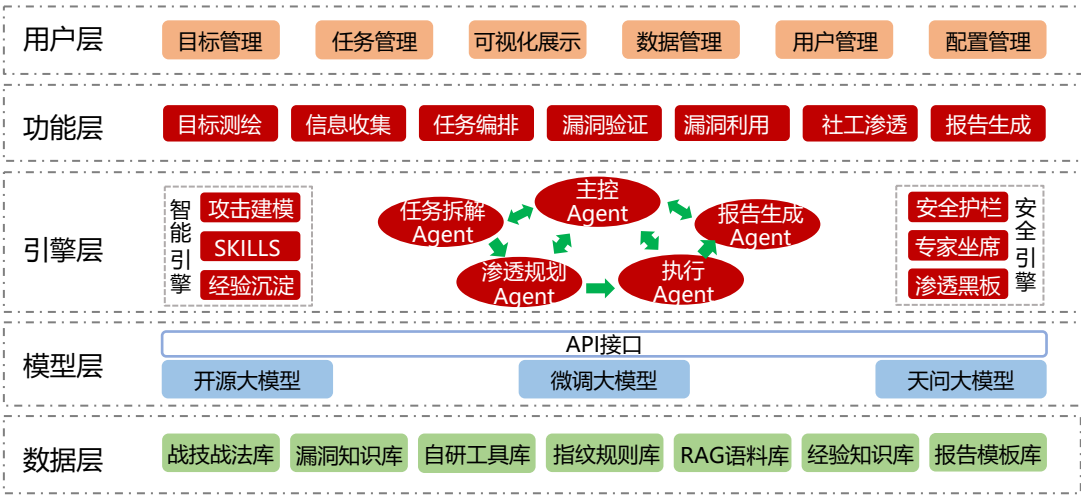
天融信（股票代码：002212）创始于1995年，是中国网络安全建设的中坚力量。在第四个“十年”发展期，公司围绕网络安全、智算云两大业务，聚焦AI安全防护、AI赋能安全、AI安全运营、AI基础设施建设四大方向，构建覆盖基础网络、工业互联网、物联网、车联网、卫星互联网、可信数据空间等全场景的产品、服务与解决方案，帮助全行业客户提升智能化安全防御水平、建设新一代智算基础设施，致力于成为中国领先的网络安全与智算云解决方案提供商，赋能千行百业数字化、智能化转型升级。

方案概况

方案介绍:

天融信基于AI的自动化渗透测试系统采用大模型、智能体等先进技术，结合动态威胁建模技术，构建了面向攻击链的智能体协作测试体系；引入渗透黑板和安全护栏技术，确保了智能体行为的安全、可靠和可控；支持专家坐席模式，由专家审批高风险操作，实现了自动化渗透测试过程的无害化；配备自研工具库，支持在实战中沉淀经验知识，补齐智能体的能力短板，增强智能体的漏洞检测能力。

方案功能与架构:



方案优势和用户价值

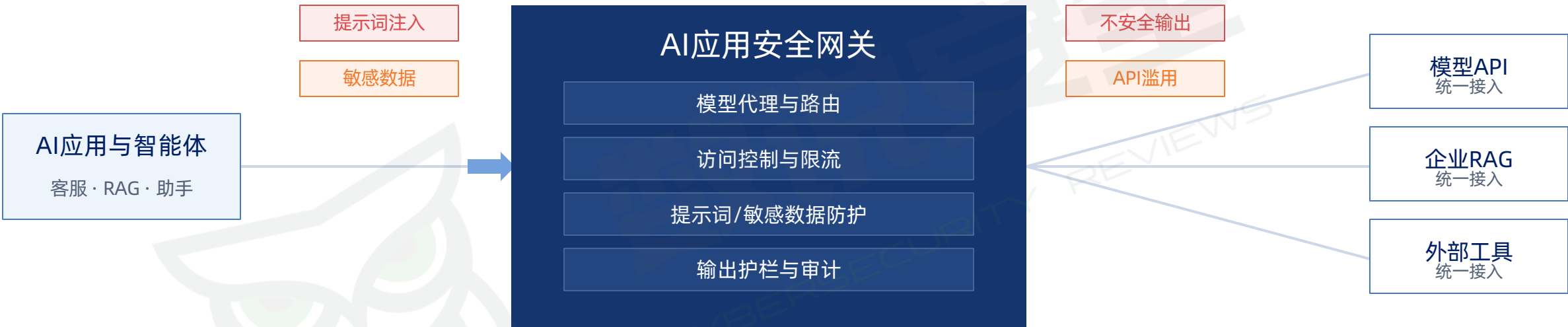
方案优势与特点:

- (1) **更全面**。依托AI驱动的动态规划和自适应探索机制，提高了对复合型、逻辑型漏洞的挖掘能力，降低了漏洞挖掘的漏报率。
- (2) **更准确**。支持基于智能体的自动化漏洞验证和利用，降低了漏洞输出的误报率。
- (3) **更安全**。安全护栏审核模型输出内容，专家坐席提供安全模式，渗透黑板控制智能体行为，渗透过程安全有保障。
- (4) **更专业**。配备自研工具库和SKILLS插件，支持实战经验自动本地沉淀，为客户提供更专业的安全服务。

用户价值:

- (1) **安全合规**。满足公安部令176号文要求，助力客户顺利通过监管部门检查。
- (2) **降本增效**。降低人工成本投入，提高渗透测试效率。
- (3) **能力建设**。补齐AI赋能的新型渗透测试能力，提升安全防护能力水平。
- (4) **风险规避**。风险前置防控，防患于未然，避免安全风险可能带来的损失。

企业接入多模型、智能体和外部知识后，需要在应用与模型之间建立统一安全控制面。AI安全网关将模型路由、访问控制、提示词攻击检测、敏感数据保护、输出护栏与审计整合到同一入口，并延伸到运行时防护。



统一控制面：在应用与模型之间实时检测、执行策略并留痕

核心能力

- 01 模型代理与智能路由
- 02 提示词注入与越狱防护
- 03 敏感数据识别脱敏
- 04 输出护栏与内容安全
- 05 运行监测与审计

代表厂商（已具备相关产品或能力）





奇安信是2025—2026年间国内传统网安头部厂商中AI战略重组幅度较大的一家：将原本分散在政企、金融、情报、代码卫士等业务集群的AI相关能力（攻防关键实验室、人工智能研究院、代码安全团队、数据安全与情报团队等）悉数划入新成立的独立“人工智能公司”，集中投入500人+，由集团高层亲自挂帅，以Q-GPT安全大模型为底座，向“智能安全”（AI赋能安全）与“安全智能”（AI自身安全）两个方向同时铺开。

方案概况	方案优势和用户价值
方案介绍： 奇安信AI安全网关部署在企业AI应用、Agent与大模型服务、MCP工具及业务系统之间，作为统一AI访问与调用控制入口，集中承接模型、MCP及Agent工具调用，提供统一接入、成本治理、条件路由、AI安全防护和全链路可观测能力，使企业AI调用可控、可管、可审计，支撑AI从分散试点走向规模化落地。 方案示意图/拓扑图：  一个入口，管住企业所有 AI 流量	方案优势与特点： (1) 专业AI安全护栏：规则引擎+安全小模型，覆盖敏感数据泄露、Prompt注入、违规内容等风险，支持告警、脱敏、阻断。 (2) 灵活智能路由：按语义类型、员工身份、模型属性、成本等动态选择调用路径，支持负载均衡与Fallback。 (3) 企业级高性能：面向生产级AI应用与Agent高频调用，支持高并发、高可用、低时延稳定运行。 (4) 统一治理可观测：统一身份与权限边界，持续记录模型、会话、工具、Token成本及关键执行链路。 用户价值： (1) 防泄密：数据外发前识别代码凭据、个人信息和业务敏感数据，按策略告警、脱敏或阻断，实现可发现、可控制、可追溯。 (2) 控成本：实时归因Token与成本，通过配额、限流、异常用量检测和语义缓存减少无效调用与资源浪费。 (3) 管权限、可审计：统一管理模型、MCP、工具和业务资源权限，完整记录关键调用链路，支撑安全调查、合规检查和责任追踪。 典型客户或目标客户： 中大型企业、小金融、国央企



360数字安全集团聚焦数字安全与AI安全，为政企客户提供实战导向的安全产品、服务与运营能力。

依托360近二十年积累的安全大数据、漏洞知识、攻防经验和专家能力，集团形成“看见+处置”数字安全能力体系，累计发现60个境外APT组织。面向智能体时代，集团坚持“以AI对抗AI”，以安全领域大模型和安全智能体蜂群为基础，一方面围绕大模型安全与智能体安全构建AI原生安全体系，另一方面推出360AI安全攻防系统图龙锋和自动化网络防御系统仪天阵，形成“主动发现+自动防御”的AI安全能力闭环。

方案概况

方案优势和用户价值

方案介绍： 360AI安全卫士方案系列以“端脑结合、以模治模、全链防护、体系协同”为核心设计思路，形成覆盖AI安全检测、AI安全防护、AI主机安全、AI安全运营管理等方向的方案体系。各模块共享垂域模型、工程化能力、异构智能体接入、云端全网情报和端侧安全积累，可独立部署，也可整体建设，组合形成企业统一的智能体安全控制面，实现“事前可见可评、事中可判可控、事后可溯可审”的运营闭环。

方案示意图：



- 方案优势与特点：**
- (1) “以模治模”的垂域安全模型群：面向提示攻击、恶意意图、数据泄露、多模态内容和工具调用等风险，形成多个可私有化部署的“以模治模”高精度、低成本专项模型。
 - (2) 贯穿事前、事中、事后的全链防护：覆盖上线前评估、运行中控制和事后溯源审计，实现风险可见、可判、可控、可追溯。
 - (3) 适配异构环境的低侵入接入：通过API、网关、SDK、日志等方式接入智能体防护业务流，完全从AI安全角度设计，不绑定特定的业务智能体框架。
 - (4) AI安全漏洞与云端全网情报，依托24万+漏洞、80万+检测规则、IoC信誉、恶意样本和攻击TTP情报，将风险转化为检测、防护与运营策略。
 - (5) 高性能工程化能力验证：已在360自有AI业务中验证，覆盖15万+智能体、2亿+用户和日均3000亿Token，沉淀互联网级智能体安全实践。

用户价值：

01 让智能体业务敢上线

通过观察、评估和逐步阻断的灰度治理，降低安全控制对业务上线和体验的影响。

02 让高风险行为可控制

在工具调用、敏感访问、数据外发前进行风险判定，支持脱敏、审批、代答和拦截。

03 让安全管理可审计

统一AI资产、依赖、告警、策略等，形成完整证据链，支持统一监管和分级治理。

04 让安全能力可扩展

不绑定单一模型或平台，从重点场景起步，逐步扩展至更多智能体、系统和组织。



绿盟科技集团股份有限公司（300369.SZ）是国内主要的企业级网络安全解决方案与服务提供商，深耕网络安全二十余年，产品与服务覆盖安全基础设施、云安全、数据安全、AI安全等方向，服务金融、运营商、能源、科教文卫等关键行业。公司前瞻布局AI自身安全赛道，推出“清风卫”系列AI安全产品，构建覆盖"模型安全、智能体安全、内容安全、数据安全"的下一代AI安全产品矩阵，致力于让每一家企业"安全地用AI、用安全的AI"。

方案概况

方案介绍：

AI-UTM是面向大模型与智能体时代的AI安全一体化网关。随着大模型、智能体（Agent）与MCP工具链在企业加速落地，模型滥用、提示词注入、敏感数据泄露、工具投毒、影子AI等新型风险不断涌现，传统网络安全边界难以覆盖AI流量。AI-UTM以网关形态串接在"用户—模型—工具"全链路，构建 A-F 六大能力域纵深防御体系：

能力域	名称	核心能力
A	资产与风险发现	AI资产测绘、风险暴露面分析、影子AI识别
B	安全围栏	模型输入输出安全，提示词注入/越权指令拦截
C	数据安全	敏感数据识别、阻断与脱敏，防入模/防出境
D	智能体与工具治理	MCP接入管控、Skills生命周期、工具投毒防护、能力边界收敛
E	访问控制	AI应用防火墙、用户与API访问控制、行为管控
F	审计与态感	全量审计回源、AI安全态势感知、合规报表

方案示意图/拓扑图：



方案优势和用户价值

方案优势与特点：

- (1) "全"：全栈AI资产覆盖。支持模型、智能体、MCP工具、提示词资产四类对象的自动测绘与风险发现，未知资产不遗漏，影子AI无处遁形。
- (2) "准"：语义级精准检测。安全围栏与AI-DLP采用语义理解引擎，精准识别提示词注入、敏感数据泄露等风险，误报率低、漏报可控。
- (3) "快"：毫秒级实时防护。网关串行部署检测时延毫秒级，策略分钟级下发，重大风险秒级阻断。
- (4) "深"：纵深防御体系。六大能力域层层递进，从输入围栏、数据防泄露到智能体治理，形成纵深防护、边界阻断的完整闭环。
- (5) "实"：可落地可闭环。内容可审计，策略可验证、事件可追溯、合规可举证，一套平台管住全部AI流量。

用户价值：

- (1) 面客AI：守住合规与品牌底线。建立输入—输出全链路安全围栏，拦截提示词注入、违规内容与敏感数据泄露，满足生成式AI服务合规与备案要求。
- (2) 内部AI：让员工"敢用、放心用"。收敛影子AI与滥用风险，敏感数据防外泄，全量审计可追溯，在赋能业务的同时守住安全底线。
- (3) 智能体与MCP：保障供应链安全。管控工具接入与Skills生命周期，防工具投毒与越权调用，支撑智能体规模化、安全化落地。
- (4) 运营提效：一套平台管住全部AI流量。统一策略中心+审计回源+处置联动，替代多套零散工具，降低安全运营成本、缩短事件响应时间。



天融信（股票代码：002212）创立于1995年，是中国网络安全建设的中坚力量。在第四个“十年”发展期，公司围绕网络安全、智算云两大业务，聚焦AI安全防护、AI赋能安全、AI安全运营、AI基础设施建设四大方向，构建覆盖基础网络、工业互联网、物联网、车联网、卫星互联网、可信数据空间等全场景的产品、服务与解决方案，帮助全行业客户提升智能化安全防护水平、建设新一代智算基础设施，致力于成为中国领先的网络安全与智算云解决方案提供商，赋能千行百业数字化、智能化转型升级。

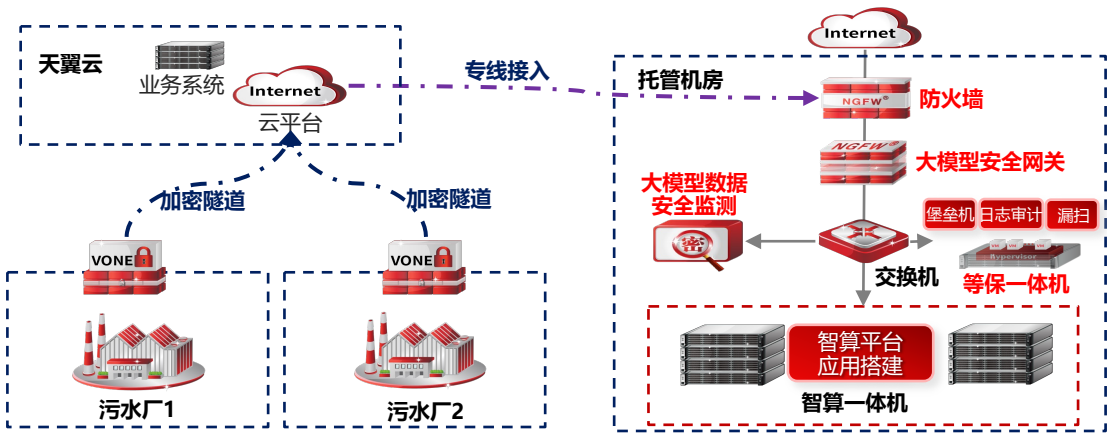
方案概况

方案优势和用户价值

方案介绍:

随着大模型技术走向规模化应用，传统网络安全边界被打破，提示注入、数据泄露、模型窃取等新型攻击手段层出不穷，单一防护手段难以应对。天融信结合大模型安全网关、大模型数据监测打造覆盖大模型全生命周期的一体化智能安全防护体系。大模型安全网关为大模型的输入输出通道提供实时安全防护，采用透明代理模式部署，无需改造现有业务，对所有进出大模型的流量进行实时检测与拦截。大模型数据安全监测系统旁路部署在网络中，对所有进出大模型的流量进行深度解析，实时分析并阻断可疑行为，形成“防护-监测-审计-处置”安全闭环，一站式满足行业安全合规要求。

方案示意图/拓扑图:



方案优势与特点:

- (1) AI主动防御，精准拦截各类攻击：快速识别并阻断各类AI恶意攻击流量，支持多模态深度感知防护，全面覆盖文本、图像、音视频交互场景。
- (2) 内容合规过滤：对大模型输出内容筛查管控，从输出侧规避合规风险、舆论风险，保障大模型输出内容合法合规。
- (3) 全生命周期风险防控，资产可视可控：覆盖大模型全生命周期风险监测，识别敏感数据泄露、各类AI攻击等安全风险，消除AI资产管控盲区，解决多模型、多Agent架构下资产混乱、底数不清、管控碎片化的问题。
- (4) 全链路审计溯源，赋能运维提效：支持各类安全事件快速溯源、精准定位，大幅降低人工运维成本，全方位提升企业AI安全治理运维效率。

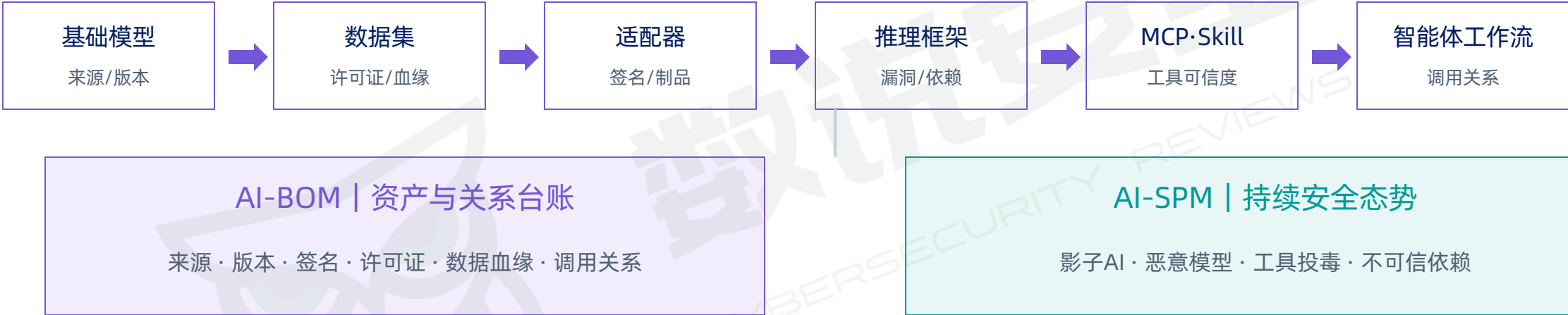
用户价值:

- (1) 避免用户敏感数据外泄风险，抵御提示词注入、供应链漏洞等攻击；保障用户大模型业务安全合规运行。
- (2) 满足合规监管标准，满足国家网信主管部门对生成式人工智能服务的安全要求。

典型客户:

政务、金融、医疗卫生、企业、能源、运营商、制造业等。

AI系统已扩展到基础模型、适配器、数据集、推理框架、MCP Server、Skill和智能体工作流。AI-BOM与AI-SPM需要持续发现这些资产，记录来源、版本、签名、许可证、血缘和调用关系，并识别影子AI与恶意依赖。



回答“企业正在使用哪些AI组件、从哪里来、是否可信”

核心能力

- | | | |
|------------------|---------------|------------|
| 01 AI资产发现与AI-BOM | 02 来源、签名与数据血缘 | 03 模型与制品扫描 |
| 04 影子AI持续发现 | 05 AI-SPM风险态势 | |

代表厂商（已具备相关产品或能力）





悬镜安全源自北京大学“XMIRROR”网络安全技术研究团队，前瞻布局新一代数字供应链安全领域，先行构建“AI 原生安全 + 软件供应链安全 + AI 供应链安全情报”的治理体系。在软件成分分析（SCA）领域，悬镜安全具备成熟完善的技术能力与行业落地实践，多次入选 Gartner、Forrester 权威报告 SCA 技术代表厂商；旗下源鉴 SCA 开源威胁管控平台产品市场应用规模位居行业前列，同步打造 OpenSCA 开源社区，沉淀深厚的开源技术生态。

方案概况

方案优势 and 用户价值

方案介绍:

企业业务高速迭代，研发广泛引入开源组件，对资产可视、风险处置、开源合规及AI制品安全管控提出更高诉求。方案依托源鉴SCA（开源风险治理）与夫子ASPM（安全态势感知），贯通研发交付链路，覆盖软件与AI模型多形态制品，提供资产盘点、风险研判、预警修复、审计追溯一体化能力，自动生成标准化SBOM。在保障研发迭代效率的同时，实现开源漏洞、许可证、供应链投毒风险常态化管控，依托云脉AI（供应链安全情报）达成风险可管、合规可审，支撑业务安全运营。

方案示意图:



方案优势与特点:

- 1. 全栈多引擎检测：覆盖多形态制品，可达性验证降误报，消除检测盲区
- 2. 标准化 SBOM 输出：兼容主流规范，资产可溯源，支撑审计举证
- 3. 情报驱动威胁预警：小时级感知 0-Day、组件投毒，快速定位受影响资产
- 4. 研发链路原生集成：对接 IDE/CI/CD/ 制品私服，安全左移，业务无侵入
- 5. 风险智能闭环处置：多维风险定级，输出修复策略，实现全流程闭环

用户价值:

- 1. 防风险：实现开源资产全局可视，完成漏洞闭环处置，统筹管控许可证、供应链投毒等各类供应链风险
- 2. 降成本：缩短风险处置周期，过滤无效告警，降低安全应急处置人力投入
- 3. 促合规：基于 SBOM 完整依赖链路，实现资产与许可证的系统化核查，输出可审计的合规凭证，支撑软件供应链监管审计落地
- 4. 常态化运营：摆脱被动应急救火模式，建立可持续的软件供应链安全工作机制

目标客户:

- 银行、证券、保险等金融机构
 - 能源、通信重点行业企业
- 政务数字化建设相关机构
 - 大规模软件研发的集团企业

大模型进入金融、医疗和企业知识库后，保护范围正从存储与传输中的数据延伸到计算使用中的提示词、响应、模型参数和知识。CPU/GPU可信执行环境、内存加密与远程证明，使用户能够验证推理是否运行在可信环境中。



从保护“存储中、传输中”延伸到保护“计算使用中”

核心能力

- | | | |
|------------------|---------------|---------|
| 01 CPU/GPU可信执行环境 | 02 使用中数据与密钥保护 | 03 远程证明 |
| 04 机密容器与推理 | 05 可信密钥释放 | |

代表厂商（已具备相关产品或能力）

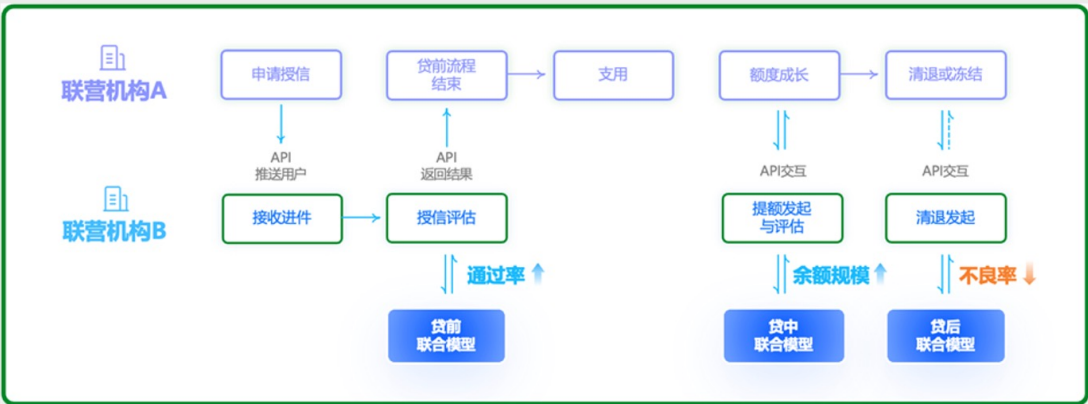
MISUAN
蚂蚁密算

火山引擎

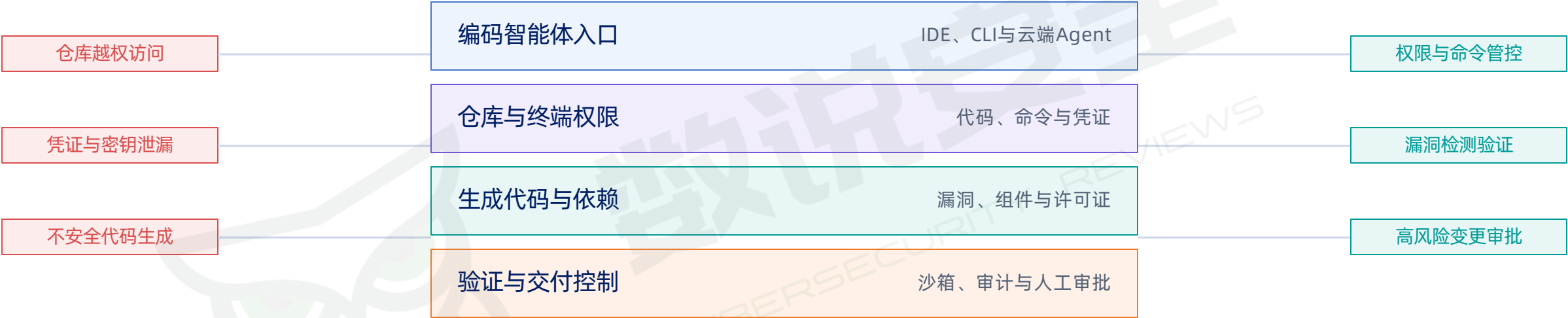
荆华密算



蚂蚁密算是蚂蚁集团旗下专注于数据要素可信流通与产业AI应用的全资子公司，致力于为AI时代构建安全可控的数据基础设施。公司基于密态计算核心技术，打造"可信智能Fabric"（Trusted Agent Fabric）架构，实现数据"可用不可见、可控可追溯"的全链路密态化保障，为产业AI变革铺设安全的"数据铁轨"。

方案概况	方案优势和用户价值
方案介绍： 在金融数字化转型过程中，数据已成为风险管理的核心要素，但跨机构数据协作的落地仍面临现实困难。某银行在推进零售贷款业务时发现，传统的跨机构数据共享方式存在两方面突出问题。一是数据在传输与流转过程中存在被截获或不当使用的安全风险，隐私保护压力较大。二是不同金融机构间的数据标准与格式存在差异，形成彼此割裂的数据体系，难以实现有效互联互通。如何在确保隐私安全的前提下打破数据壁垒，成为金融机构亟需解决的课题。 方案示意图/拓扑图： 	方案优势与特点： 利用密态计算技术联合开发了一套覆盖模型训练与推理全流程的风险评估解决方案。该方案采用分布式部署架构，打破传统数据集中汇聚的处理模式，确保双方原始数据始终保存在各自的管理域内，无需明文传输或向中心端汇集。在特征提取、模型推理等各个环节，系统均应用加密算法与密态计算技术，使得原始数据在“可用”的同时保持“不可见”，任何一方均无法获取另一方的原始信息，也无法通过对计算结果的反向推导还原原始数据。在此安全环境下，项目实现了浦发银行内部数据与合作伙伴提供的多维度外部数据的安全融合，构建起更全面的客户风险特征库。 用户价值： - 在风控精度方面，风险模型的KS值（Kolmogorov-Smirnov值，用于评估模型区分度）提升12%至23%，对信贷风险的识别与区分能力显著增强。 - 在信贷资源配置方面，项目累计识别出37万名低风险客户，相应增加授信额度80亿元，有效支持了对优质客户的精准服务。在风险拦截方面，项目成功识别超过14.5万名高风险客户，直接避免了约90亿元高风险贷款的发放，对银行资产安全起到了切实的保障作用。

编码智能体正在从代码补全走向读取仓库、执行终端、安装依赖和提交变更。安全控制需要同时治理“智能体如何工作”和“生成代码是否可信”，围绕仓库与终端权限、凭证保护、依赖选择、代码审计、沙箱验证和高风险变更审批形成闭环。



治理对象：编码智能体、代码仓库、终端命令、依赖组件与生成代码

核心能力

- 01 Agent资产与权限管理
- 02 仓库/终端/MCP管控
- 03 生成代码安全审计
- 04 依赖与SBOM治理
- 05 沙箱验证与变更审批

代表厂商（已具备相关产品或能力）





奇安信科技集团股份有限公司（股票代码 688561）成立于2014年，是中国主要的新一代企业级网络安全产品和服务提供商，在人员规模、收入规模与产品覆盖度上均位居行业头部。2019年中国电子战略入股后，奇安信成为网络安全“国家队”，迄今已完成百余次国家重要活动网络安全保障任务，参与近千场实战攻防演习。面对AI辅助编码从“个人提效”走向“组织级规模化交付”的趋势，以及企业在智能体权限、代码可信、供应链安全与审计追溯上的治理痛点，奇安信推出QAgent Fabric安全智能体研发框架。该方案已在奇安信研发体系中落地实践，实现交付周期缩短20%-30%、测试覆盖率≥80%、CI一次通过率≥90%、AI覆盖主要节点≥80%，并形成100+可复用的项目知识资产，把AI编码从个人工具升级为可管、可控、可审计的组织级能力。

方案概况	方案优势和用户价值
方案介绍： 奇安信 QAgent Fabric 是面向企业软件研发的 AI 研发基础设施，以“项目”为基本单元，统一连接代码、文档、需求、Issue、测试、环境、知识库和 CI/CD 系统，为编码智能体提供完整、持续、可控的项目上下文。 平台围绕“统一智能体入口、统一项目上下文、统一安全运行环境、统一研发工具链”构建能力，覆盖需求分析、方案设计、编码、测试、缺陷修复、代码提交和交付全过程。通过代码受控管理、Agent资产与权限管理、研发质量门禁、沙箱验证、过程审计和变更审批，实现研发过程可执行、可验证、可追溯、可治理。 方案示意图/拓扑图： 	方案优势与特点： 项目级安全管控：以项目为单元聚合代码、需求、文档、Issue、测试和环境信息，减少智能体因上下文割裂产生的错误。 研发安全闭环与质量门禁前移：贯通需求、设计、编码、测试全流程，在编码输出、依赖引入、代码提交关键节点，进行生成代码安全审计、高风险变更审批与质量合规检查。 代码与凭证受控管理：仓库访问最小授权，终端与 MCP 调用统一策略管控，凭证不落个人终端与提示词上下文；结合模型网关与审计，防外泄、防越权。 Loop研发闭环：支持“生成—构建—测试—发现问题—自动修复(授权范围内)—回归验证”的循环，高影响操作遵循变更审批，超出授权范围的高风险变更转人工审批，全程留痕。 企业级开放集成：通过API和MCP连接企业现有项目管理、代码仓库、测试、CI/CD及安全产品，避免替换已有研发体系。 用户价值： 研发提效：缩短需求分析、编码、测试和缺陷修复周期。 质量提升：通过过程门禁和自动化Loop，提高测试完整性和交付稳定性。 代码安全可控：降低源码落地个人终端、非受控模型调用和工具越权风险。 过程可度量：统一统计任务、工时、Token消耗、质量结果和交付过程，为项目成本、人效分析与安全合规审计提供依据。 适用客户： 适用于代码资产敏感、研发环境复杂、合规审计要求高，希望规模化引入AI研发能力的大型企业和组织，重点面向央国企、金融、能源、科研及网络安全等行业。



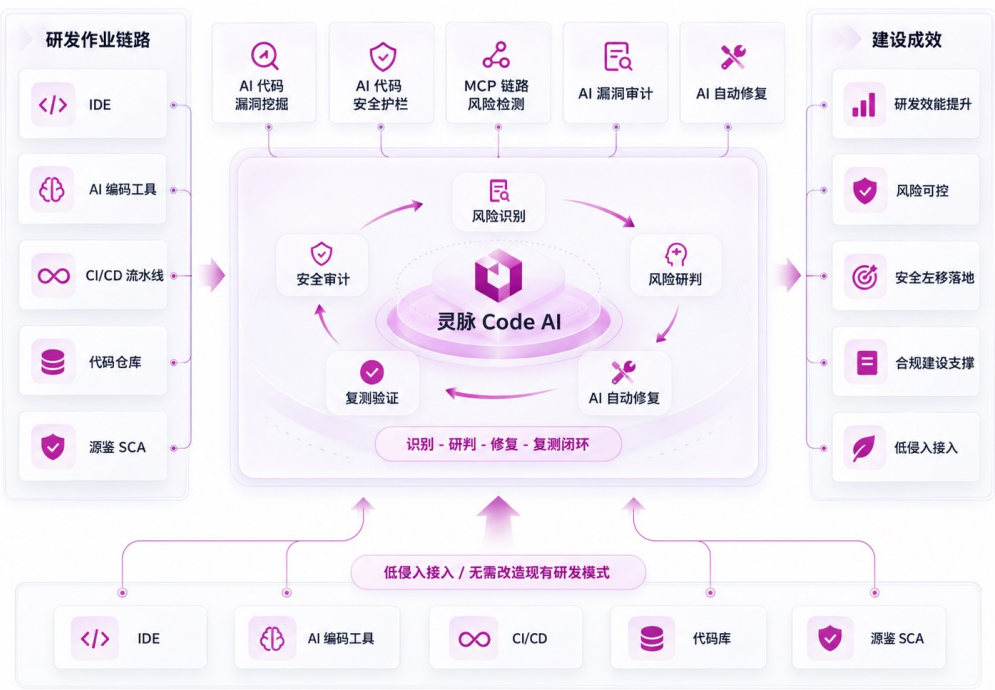
悬镜安全源自北京大学“XMIRROR”网络安全技术研究团队，前瞻布局新一代数字供应链安全领域，先行构建“AI 原生安全 + 软件供应链安全 + AI 供应链安全情报”的治理体系。伴随企业大规模落地 AI 辅助编码、AI Agent 开发模式，代码风险来源愈发复杂。悬镜安全聚焦数字供应链与 AI 原生安全赛道，打造灵脉 Code AI 代码安全智能体，践行“以 AI 治理 AI”理念，面向企业真实研发业务场景输出安全能力，助力组织在释放 AI 研发效能的同时，实现对 AI 生成代码、MCP 工具、AI 供应链安全风险的体系化管控。

方案概况

方案介绍：

AI编码助手与 AI Agent 已大规模落地软件研发，在显著加速业务交付的背景下，AI 代码、MCP 工具、AI 供应链的安全管控已成为企业必须补齐的建设环节。灵脉 Code AI 深度适配研发日常作业链路，低侵入接入 IDE、AI 编码工具、CI/CD 流水线，联动源鉴SCA构建风险识别-研判-修复-复测闭环。无需改造现有研发模式，落地安全左移，兼顾研发效能、风险管控与合规建设目标。

方案示意图：



方案优势和用户价值

方案优势与特点：

- 1. AI 代码漏洞挖掘：深挖AI生成代码与业务逻辑漏洞，减少无效告警，提供智能修复建议
- 2. AI 代码安全护栏：编码阶段实时拦截，阻断缺陷代码提交流入下游
- 3. MCP 链路风险检测：识别 Agent 工具投毒、越权访问，规避数据泄露风险
- 4. AI漏洞审计：批量AI审计和一键标注误报缺陷，大幅提高审查效率
- 5. AI自动修复：通过AI模型提供代码修复内容，降低人工修复的复杂度

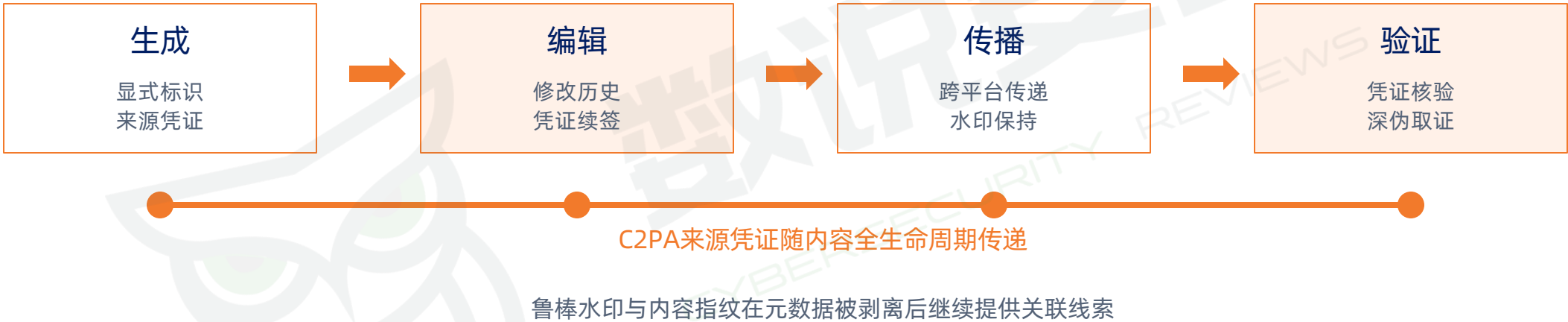
用户价值：

- 1. 控源头：编码环节拦截 AI 相关缺陷，降低线上安全事件风险
- 2. 提效能：减少告警甄别和整改人力，安全管控不拖慢版本迭代
- 3. 御新胁：覆盖 AI 编码、MCP 智能体风险，补齐传统工具能力短板
- 4. 强供应链：打通代码-组件-AI 模型风险，提前预警投毒、高危组件隐患
- 5. 达合规：输出报告与 SBOM/AI-BOM，支撑等保、AI 安全、开源合规审计
- 6. 促闭环：实现风险发现-修复-复测闭环，保障 AI 研发安全常态化

典型客户或目标客户：

- 银行、证券、保险等金融机构
- 各级政务部门及数字化建设单位
- 能源、通信、工业互联网关基企业
- 具备大规模 AI 自研能力的集团企业

生成内容治理正在从单点深伪检测，走向覆盖生成、编辑、传播和验证的真实性基础设施。显式标识、C2PA来源凭证、鲁棒水印、内容指纹和篡改检测需要协同工作，让内容来源、生成方式与修改历史可验证、可追溯。



核心能力

- 01 显式标识与C2PA凭证
- 02 鲁棒水印与内容指纹
- 03 编辑传播链追踪
- 04 标识篡改检测
- 05 深伪取证与核验

代表厂商（已具备相关产品或能力）





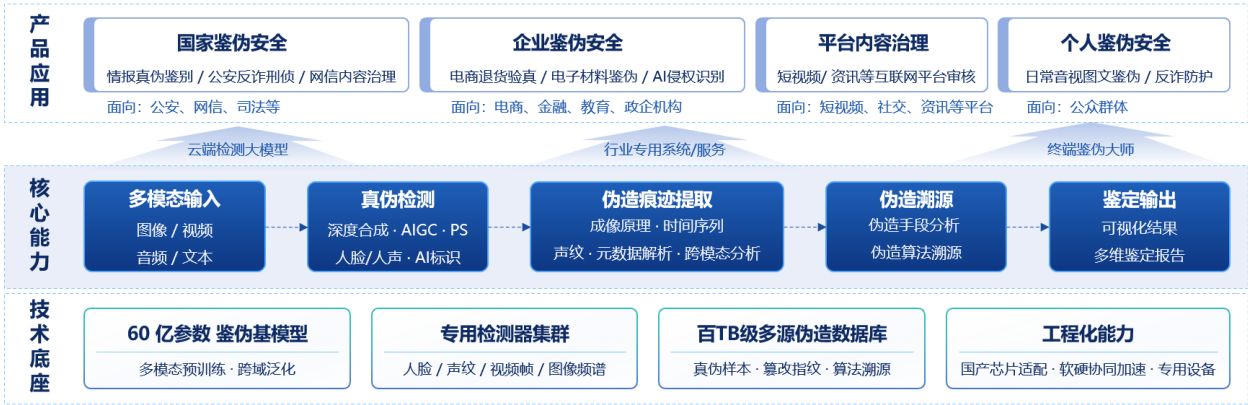
中科睿鉴秉持"用技术让世界更可信"使命，紧跟AI时代前沿，聚焦多模态伪造检测、生成式AI内容治理、大模型安全三大核心方向，搭建集数据、算力、模型于一体的AI安全能力底座，构建"检测—验证—溯源"全链路内容可信体系。面向国家监管、公共安全、行业治理、民生服务，提供深度鉴伪、内容溯源、AIGC合规标识、学术诚信治理等技术服务。公司深度服务于工信、公安、网信等部委，与三大电信运营商、联想、小米、快手等头部机构深度合作，终端鉴伪能力累计部署超5000万台，在新型反诈、AI内容风控、大模型安全等场景实战成效突出，持续筑牢AI时代可信内容安全底座。

方案概况

方案介绍：

中科睿鉴以深度鉴伪为核心引擎，面向音视图文全模态数据，构建"检测—验证—溯源"全链路技术体系，实现内容来源、生成方式与修改历史的可验证、可追溯。技术层面，深度鉴伪引擎覆盖深度伪造、AIGC生成、PS篡改、活体攻击等场景；融合C2PA来源凭证、内容指纹与篡改检测，多维交叉验证内容来源与修改历史；依靠数据指纹与动态特征库，实现伪造工具与算法溯源定位。治理模式上，云端部署鉴伪大模型支撑公域批量检测，服务国家安全；终端部署轻量化鉴伪能力兼顾防护与隐私，守护个人安全；面向金融、教育、通信、公安司法等行业提供专用检测服务，无缝对接业务系统。

方案示意图/拓扑图：



方案优势和用户价值

方案优势与特点：

- 全链路真实性治理：以深度鉴伪为核心，融合AI标识、C2PA来源凭证、内容指纹与篡改检测技术，构建了覆盖内容生成、编辑、传播、核验全环节的真实性验证基础设施，从单点深伪检测升级为全链路系统性治理。
- 快速迭代适配能力：云端基模型支持 600 余种检测方法、累计迭代 1000 余种模型版本，依托海量实战样本与少样本学习底座，短周期内可快速迭代并识别新型伪造手段、适配全新业务场景，结合对抗式数据生成平台形成技术飞轮。
- 国产化自主可控：具备硬件级检测能力，全面适配国产操作系统与国产主流芯片；团队深耕深度伪造检测领域，在多部委测评中综合指标表现优异，检出准确率稳定保持90%以上，已在公安、工信等国家级项目完成大量实战沉淀。

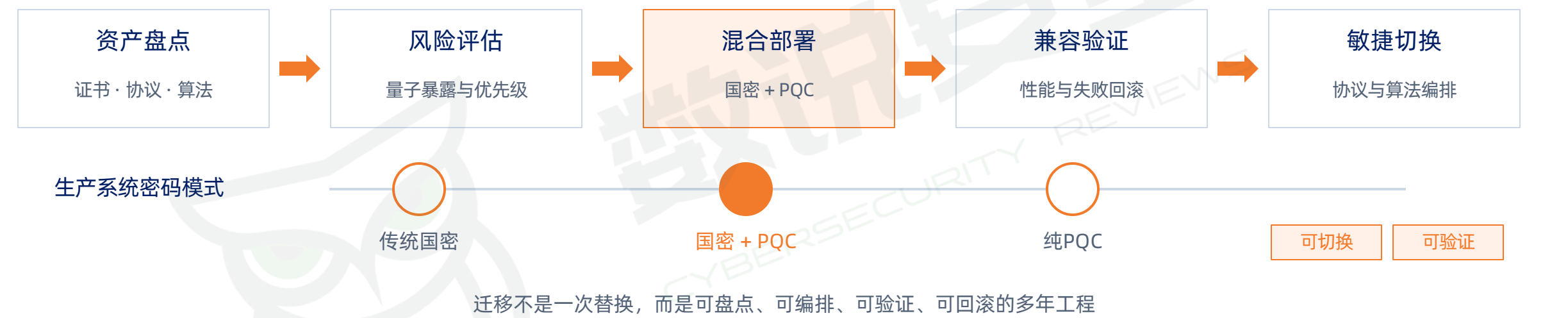
用户价值：

- 国家安全可信防护：为监管部门提供多模态内容真实性批量检测、全链路溯源研判能力，助力深度合成内容治理、网络风险排查，筑牢AI时代下的国家安全屏障。
- 企业安全权益保障：提供多行业、多模态的内容真实性验证方案，拦截 AI 换脸欺诈、虚假证据、AIGC违规生成等黑产风险，守护企业经营与业务合规安全。
- 个人用户安全防护：通过终端嵌入、国家反诈中心APP等渠道提供普惠鉴伪能力，对 AI 换脸、AI合成信息等诈骗风险提前预警，守护普通群众财产与信息安全。

典型客户或目标客户：

公安、网信、工信、司法、运营商、金融机构、终端厂商、高校、电商、个人用户等

抗量子密码的创新重点正在由算法研究转向工程迁移。企业需要先发现证书、协议、算法和密钥等密码资产，再开展风险评估、国密与PQC混合部署、协议升级、算法动态切换、兼容性验证和失败回滚。



核心能力

- 01 密码资产发现与CBOM
- 02 量子风险评估
- 03 国密+PQC混合部署
- 04 协议与证书升级
- 05 算法编排与失败回滚

代表厂商（已具备相关产品或能力）



股票代码：603232



三未信安



信安世纪



吉大正元



天融信 TOPSEC



格尔软件股份有限公司是上交所主板上市的信息安全企业，3 次荣获国家科技进步二等奖。28 年来，格尔软件先后为 38 个国家部委、100 多 家国企央企提供全栈全域的安全解决方案和专业化服务。2024 年，格尔软件在“身份认 证”市场排名位列全国第二，荣获年度中国上市公司英华示范案例“A 股新质生产力价值奖”。2025 年，格尔软件承接阿尔及利亚某重要部 委数字信任体系建设项目，推动我国商用密码技术规模化出海。此外，格尔软件较早发布融合 PQC 的态势感知系统与抗量子 密码服务平台、抗量子视频安全解决方案等解决方案，较早推出 NGPKI 及抗量子混合证书解决方案及系列产品，较早完成自有密码产品体系 抗量子能力的全面升级，较早通过中国信通院 PQC 验证测试，获得抗 量子密码领域“上交会十大项目奖”和“中国网络安全与信息安 全产业年度优秀解决方案”。

方案概况

方案介绍：

当前证券网上交易系统依赖的国密体系（SM2/3/4）已难以抵御未来量子计算的威胁。一旦量子计算机成熟，现有基于SM2的SSL VPN安全机制将面临被破解的风险，可能导致身份认证、访问控制及安全通信等安全机制失效，网上交易加密通信流量存在“先存储后破解”的前向安全风险，对国家金融安全构成严峻挑战。为此，格尔软件立足证券期货行业“高并发、低延时、强安全”的业务需求，基于《抗量子密码技术在证券业创新研究与应用》成果，制定以“平滑过渡、安全可控”为原则的实施方案。方案强调复用现有密码基础设施，实现向下兼容与资产利旧，降低改造与运维成本；并通过多节点部署与自动降级机制，确保系统在抗量子服务异常时可无缝回退至原有国密体系，保障业务连续稳定运行。

方案示意图/拓扑图：



方案优势和用户价值

方案优势与特点：

- 1. “稳”：创新“PQC+SSL VPN”混合模式与自动降级机制，抗量子服务异常时可无缝回退至原有国密体系，保障业务连续稳定，实现平滑迁移。
- 2. “安”：新建抗量子PKI基础设施，升级国密RA系统，有效抵御未来量子计算威胁，解决“先存储后破解”的前向安全风险，重塑网络空间信任链。
- 3. “快”：采用自主知识产权的抗量子算法，签名/验签性能较国外同类算法提升80%，满足证券期货行业“高并发、低延时”的业务需求。
- 4. “省”：复用现有国密密码机、协同签名等利旧设施，兼容原有国密证书，降低改造成本与运维复杂度，实现新旧体系融合与资产利旧。

用户价值：

- 1. 打造了国内较早的证券期货业抗量子密码应用标杆案例（已于2025年上线）。
- 2. 解决了国际技术“卡脖子”风险，实现了核心技术自主可控。
- 3. 为证券行业从商用密码向抗量子密码迁移提供了可行路径与标准参考。

典型客户或目标客户：

- 1. 金融证券期货业机构以及政务与能源这些关键领域



三未信安科技股份有限公司（688489）是国内主要的商用密码基础设施提供商，产品覆盖密码芯片、密码板卡、密码整机到密码系统的全栈体系，深耕金融、政务、能源等关键行业。SecQuan是公司面向抗量子密码迁移推出的战略级平台产品，致力于将抗量子密码从算法研究推进到工程化迁移落地。

方案概况	方案优势和用户价值
方案介绍： SecQuan抗量子密码迁移平台，贯通"发现—评估—规划—执行—验证"五步闭环，助力企业全面看清全网密码资产、科学评估量子脆弱性并排列迁移优先级、受控推进迁移动作、沉淀可证明的迁移结果，在量子计算成熟前构建可发现、可评估、可规划、可执行、可验证的完整抗量子迁移能力。 方案示意图/拓扑图： 从企业迁移的五个痛点出发，构建发现 → 评估 → 规划 → 执行 → 验证五步闭环 企业迁移痛点 资产看不见 应用 / 端口 / 证书 / 密钥分散，缺一底账 风险排不清 不知道哪些最脆弱、最该先迁 路径选不准 系统差异大，缺可执行迁移策略 执行改不稳 生产变更牵涉链路，中断 / 回滚难控 结果证不了 迁了哪些、风险降没降，缺审计证明 五步闭环 发现 评估 规划 执行 验证 SecQuan 治理闭环 把“看不见、排不清、选不准、改不稳、证不了”变成“可发现、可评估、可规划、可执行、可验证”	方案优势与特点： (1) "全", 全景密码资产底账，覆盖应用/端口/证书/密钥/密码库全要素 (2) "准", 量子脆弱性精准评估，结合迁移紧迫度科学排列优先级 (3) "稳", 观察→并行→切换三步渐进迁移，可监控可回退 (4) "融", NIST PQC+国密双标准兼容，复用既有HSM/KMS投资 (5) "证", 迁移全程可观察可审计，支撑密评与合规 用户价值： (1) 帮助企业建立密码资产"看清—排好—管住—证明"的治理能力，将"先存储后解密"风险窗口降至最低，掌握迁移主动权。 (2) 将抗量子迁移从单点算法替换升级为全过程可治理的工程化实践，避免"看不见、改不稳、证不了"的盲区，降低迁移成本与业务风险。 典型客户或目标客户： 金融行业（银行、证券、保险）、政府与公共事业、关键信息基础设施运营者、大型央企等密码资产分散、改造牵涉面广的中大型机构。



以数据为基础的网络安全产业研究平台

ssaq@geniuscybertech.com

2026
