

哨云景御安全管理平台

AI 原生安全运营

无代理架构实现全域资产可见
AI 智能体驱动自动排查与响应
覆盖云、主机、容器与 AI 全场景

产品介绍



让 AI 创新建立在安全之上

资产看得全 · 风险判得快 · 危险控得住 · 过程查得清

哨云科技

SYSENTRY.CLOUD · 2026

AI 让攻击更快，也让行为更难看清

攻击自动化压缩防护窗口，智能体开始读文件、执行命令和调用工具，传统安全逐步失效



攻击自动化，窗口被压缩

AI 让黑客的攻击速度远超人工响应

- AI 降低漏洞利用、钓鱼投递、横向移动的技术门槛，攻击链从"天级"压缩到"分钟级"
- 传统运营靠人工排查漏洞、核对资产、编写报告，一个 CVE 应急往往需要数小时甚至数天
- **核心矛盾：**不是看不到告警，而是**人工排查速度跟不上攻击自动化速度**



行为变化，安全逐步失效

智能体开始代人操作，传统工具看不懂

- 智能体会读取代码/文件、执行命令、通过 MCP 调用外部工具——传统 EDR/防火墙只能看到进程和域名
- 影子 AI 泛滥：员工自行安装的智能体、Skill、MCP 插件不在资产台账内，"看不见、管不住、审不了"
- **核心矛盾：**安全管控需从"管进程"升级到"管 AI 的每一步操作"

攻击在加速，行为在变化——安全运营必须从"人工驱动"走向"AI 原生"

让 AI 安全从被动防守走向主动运营

以自动排查、实时防护、全程审计三项能力，建立可持续的 AI 安全运营体系

01

自动排查

AI 原生安全运营

- **无代理巡检：**无需逐台安装，持续发现资产与风险
- **分钟级应急：**输入公告，自动完成影响面排查
- **替代人工：**从发现、分析到报告，全流程自动化

02

实时防护

AI 全生命链防护

- **资产发现：**识别模型、智能体、Skill、MCP 及供应链
- **风险检测：**发现投毒、配置错误、漏洞等 AI 风险
- **执行前阻断：**敏感操作执行前审计或阻断，形成闭环

03

全程审计

AI 会话观测与审计

- **无代理采集：**无需插桩，获取完整会话与工具调用
- **意图识别：**基于上下文分析 AI 的安全意图变化
- **危险操作：**标记读取、写入、执行、外发、提权等行为

三项能力共用一套资产台账、策略体系和响应入口，不是产品拼凑，而是一体化平台

一套平台，统一管理所有资产

统一管理中心 + 四大产品模块，无代理与安全客户端两种接入方式协同工作



核心技术：无代理架构（对标 Wiz / 微软 Defender / Orca Security）+ AI 智能体驱动分析 + MCP 标准协议集成
支持本地化部署与 SaaS 交付，两种接入方式在同一管理中心协同工作

国内首个无代理云安全、实时防护与 AI 安全一体化运营平台

01

让安全运营摆脱人力瓶颈

无代理技术解决覆盖问题，AI 智研承担排查、分析和报告编制

安全运营 70% 的时间花在资产盘点、漏洞排查、应急响应和报告编写等重复劳动上。哨云景御用**无代理 + AI 智能体**替代人工排查，让安全人员从“执行者”升级为“决策者”。

本章节将依次介绍：无代理自动排查 · AI 智研分钟级应急 · MCP 能力集成 · 多云资产与风险检测

从 “人肉排查” 到 “AI 自动解决”——安全运营的范式转变

让资产与风险无处隐藏

无需逐台安装客户端，持续发现云资产、配置、权限、漏洞、暴露面和攻击路径

1 API 驱动发现

持续读取云账户中的计算、网络、存储、数据库、身份对象，同步周期最短数分钟级

2 只读快照分析

对虚拟机磁盘、容器镜像、文件存储创建临时只读快照，在隔离环境检测漏洞和恶意软件

3 跨服务关联

结合配置、日志、权限、网络关系识别暴露面和可利用路径，如公开存储桶 + 过度权限角色

4 会话数据采集

通过云平台日志和流量镜像，采集 AI 会话与工具调用数据，无需在业务侧插桩

无代理 vs 传统有代理

有代理：需逐台安装 Agent，容器/Serverless 覆盖难，存在性能开销和盲区，部署周期长

无代理：通过云 API + 快照实现全覆盖，对业务零影响，部署即开即用，无维护成本

核心价值：解决安全运营从 0 到 1 的可见性问题——先有完整资产台账，才有准确风险判断

技术边界：不发探测包、不做网络爆破，所有检测负载在云连接器侧，对业务系统零侵入

无代理架构实现全域资产可见——覆盖全、部署快、零侵入、无盲区

把应急响应压缩到分钟级

输入安全公告后，自动理解影响条件、匹配资产并生成响应建议；典型场景 1 分钟形成初稿

传统应急流程（数小时 ~ 数天）

安全工程师读公告 → 人工核对资产 → 逐台确认版本 → 判断是否暴露
→ 编写影响面报告 → 分派整改

AI 智研流程（典型场景 1 分钟）

输入公告/CVE → AI 自动解析影响条件 → 全量资产匹配 → 上下文研判暴露面 → 生成响应建议初稿

1 读懂公告

输入安全公告原文或 CVE 编号，
AI 自动解析受影响产品、版本、
漏洞类型和利用条件

2 自动比对资产

与平台已纳管的产品、版本、主机、
容器镜像、Java/Python 类库全
量比对，秒级完成匹配

3 上下文研判

检查是否公网暴露、是否有攻击路
径、是否有缓解配置，明确区分"
已确认"和"待验证"

4 生成报告

1 分钟内输出影响范围、证据
链、处置建议和优先级，可直
接分派整改或导出报告

AI 智研不仅自动分析，而且会驱动应急响应的整体过程

构建企业自己的 AI 原生安全能力

通过 MCP 将平台能力集成到企业运营平台和智能体体系，使安全能力可被企业 AI 直接调用



安全运营智能体

企业安全运营助手可直接调用哨云的资产查询和风险检测能力，无需切换系统、无需人工导出数据。

价值：安全人员用自然语言即可完成资产盘点和风险排查。

SIEM / SOAR 联动

SIEM/SOAR 触发告警时，自动调用哨云做影响面排查和资产匹配，把告警到响应串成自动化流程。

价值：告警响应从"人工转单"变成"自动闭环"。

企业 AI 助手集成

企业内部 AI 助手可同时访问知识库和哨云实时安全数据，员工提问时自动关联安全状态和风险信息。

价值：安全能力从"专业工具"变成"普惠服务"。

哨云不只是独立平台，更能成为企业安全运营体系的能力底座

统一多云安全，降低运营复杂度

统一盘点公有云、私有云、虚拟化、容器和主机资产，并自动确定高风险问题的处理顺序

多云资产统一检测

通过云连接器接入的环境包括：

公有云

阿里 · 腾讯 · 华为 · 火山 · 天翼 · AWS

专有云 / 云栈

天翼混合云 · 飞天 · TCE · Stack · H3C

虚拟化 / 超融合

FusionCompute
e · OpenStack · ZStack

容器 / 主机

K8s · Docker · Linux · Windows

资产类型：计算、网络、存储、数据库、身份、软件供应链（镜像/类库/包）

发现方式：API 持续同步 + 只读快照分析，无需在业务侧安装任何软件

全维度风险检测

四大检测领域，统一进入风险响应队列：

攻击面管理

公网暴露 · 端口 · 证书 · 域名

漏洞管理

CVE · 镜像漏洞 · 类库漏洞 · 配置缺陷

身份与配置

过度权限 · 密钥泄露 · 配置错误

威胁与入侵

恶意软件 · 异常行为 · 入侵痕迹

合规检测：覆盖等保 2.0、CIS 基线、云平台最佳实践，自动生成合规报告

响应管理：所有风险统一进入队列，按优先级分派，关闭前必须确认和复测

一套平台统一管控多云、终端及AI的资产与风险——消除多工具切换与统计维度差异带来的偏差

02

让安全跟上 AI 的每一步

覆盖 AI 资产发现、风险检测、执行前防护和使用过程审计

智能体引入后，用户的行为变了——AI 开始读文件、执行命令、调用工具。安全必须从“管进程”升级到“管 AI 的每一步操作”，沿着 AI 应用的全生命周期构建防护闭环。

本章节将依次介绍：AI-SPM 资产与风险检测 · AI 实时防护 · AI 审计（上下文分析优势）

AI 全生命链防护——从资产到会话，每一步都看得见、管得住、审得清

看清每一项 AI 资产与风险

发现模型、智能体、Skill、MCP 和开源组件，识别影子 AI、错误配置和供应链风险

AI 资产全景发现

大模型

本地部署模型
API 调用模型
微调模型

智能体

企业智能体
员工自建 Agent
第三方 Agent

Skill / MCP

自定义 Skill
MCP 服务端
外部工具插件

影子 AI 发现

通过网络流量、DNS 日志、API 调用记录，自动发现员工自行安装的智能体、Skill 和 MCP 插件，建立完整的 AI 资产台账，解决"看不见、管不住、审不了"的影子 AI 问题。

AI 风险检测

供应链投毒

检测恶意 Skill、被篡改的 MCP 服务端、包含后门的开源组件

配置错误

发现过度权限、密钥硬编码、未授权网络访问、数据泄露风险

漏洞与缺陷

检测模型漏洞、Prompt 注入风险、智能体逻辑缺陷和已知 CVE

AI-SPM：AI 时代的安全态势管理——从资产发现到风险处置全覆盖

让风险止于执行之前

在敏感数据读取、危险命令、凭据使用、网络访问和外部工具调用执行前进行审计或阻断

五类高危操作管控

敏感数据读取

客户数据、源代码、密钥文件、内部文档读取前审计或阻断

危险命令执行

rm -rf、格式化、提权、批量删除、系统配置修改等高危命令

凭据使用管控

API Key、数据库密码、云平台密钥的使用范围和频率限制

网络访问

外网访问、特定域名限制

外部工具调用

MCP 工具、第三方 API 白名单

两种管控模式

审计模式

记录操作但不阻断
适用于观察期和低风险

阻断模式

执行前直接拦截
适用于高危操作和合规要求

核心价值

- **事前防护**：在操作执行前拦截，而非事后追溯，避免数据泄露和系统破坏
- **细粒度策略**：按智能体、用户、场景配置不同管控策略，兼顾安全与效率
- **无缝集成**：通过安全客户端和 MCP 拦截器实现，无需修改 AI 应用代码

从"事后审计"到"事前阻断"——让 AI 的每一步操作都在安全管控之内

看懂上下文，才能看准 AI 风险

对比只分析输入输出的大模型防火墙，突出完整会话、工具参数、执行结果和实际影响分析

LLM 防火墙（传统方案）

只能看到模型的输入和输出，看不到中间过程

- **只能分析文本：**基于关键词和语义匹配判断输入输出是否包含敏感内容
- **看不到工具调用：**智能体调用了什么工具、传了什么参数、返回了什么结果，完全不可见
- **看不到执行过程：**AI 是否读取了敏感文件、是否执行了危险命令、是否访问了外网，无法感知
- **无法判断意图：**同一句话在不同上下文中风险完全不同，单轮分析容易误判和漏判
- **事后追溯难：**出了问题只能看到输入输出，无法还原完整的操作链路和影响范围

哨云 AI 审计（完整上下文）

记录完整会话、工具调用、执行结果和实际影响

- **完整会话记录：**记录多轮对话的完整上下文，理解 AI 的真实意图和决策过程
- **工具调用留痕：**记录每次 MCP/API 调用的工具名、参数、返回值和执行耗时
- **执行结果可见：**AI 读取了什么文件、执行了什么命令、修改了什么配置，全部可追溯
- **上下文意图分析：**结合完整会话判断操作意图，区分正常操作和异常行为，大幅降低误判率
- **影响范围评估：**出问题时可快速还原操作链路，评估数据泄露范围和系统影响

AI 审计的核心优势：不是看 AI 说了什么，而是看 AI 做了什么、为什么做、造成了什么影响

03

让每一次 AI 行为有迹可循

完整记录 AI 对话和工具调用，为排查、复盘、协作与合规提供依据

AI 会话观测与审计是提升组织效率的关键。哨云景御通过**无代理方式**实现无盲区的会话采集，记录 AI 的完整对话、工具调用、参数和执行结果，让每一次 AI 行为都可追溯、可分析、可审计。

本章节将依次介绍：无代理会话采集 · 安全意图分析 · 危险命令操作识别

AI 会话观测与审计——让 AI 的每一步操作都看得见、说得清、查得到

更低成本，看全 AI 会话

无代理方式减少客户端部署和维护；安全客户端补充物理机、办公终端、边缘设备及实时防护场景

无代理会话采集（主流方式）

通过云平台日志、流量镜像和 API 调用记录采集会话

- **零部署成本：**无需在 AI 应用和智能体中安装任何插件或 SDK，接入即用
- **无盲区覆盖：**覆盖所有云主机、容器、Serverless 函数和 AI 服务，包括员工自建的影子 AI
- **零性能影响：**采集在云连接器侧完成，不占用业务系统的 CPU、内存和网络资源
- **低维护成本：**无需逐台升级客户端、无需处理兼容性问题，运维成本降低 80% 以上
- **完整数据：**采集完整的对话内容、工具调用、参数、返回值和执行结果，不丢失上下文

安全客户端（补充方式）

面向无代理无法覆盖的场景，提供端侧深度防护

物理机与裸金属服务器

无云平台 API 可调用，需客户端直接采集进程和网络数据

办公终端与员工设备

员工在本地运行的 AI 工具和智能体，需端侧采集和管控

边缘设备与实时防护场景

需要在操作执行前实时阻断的场景，客户端提供更低延迟

无代理为主、客户端为辅——用最低成本实现最完整的 AI 会话覆盖

让 AI 行为可理解、风险可判断

自动识别读取、写入、执行、删除、联网、外发、凭据和提权行为，发现危险命令及意图变化

八类 AI 行为自动识别

读取

敏感文件
客户数据

写入

文件修改
配置变更

执行

命令执行
脚本运行

删除

批量删除
数据清除

联网

外网访问
异常连接

外发

数据外传
邮件/API

凭据

密钥使用
密码获取

提权

权限提升
越权操作

安全意图分析

- 基于完整会话上下文，分析 AI 每一步操作的真实意图
- 区分正常操作（如查询数据）和异常行为（如批量导出）
- 识别意图突变：从"辅助分析"转向"主动操作"的关键节点

危险命令与操作识别

- **系统命令**：rm -rf、格式化、批量杀进程、修改系统配置
- **数据操作**：批量导出、数据库删除、全量下载、加密勒索
- **网络行为**：端口扫描、横向移动、反向 Shell、C2 通信
- **凭据操作**：密码抓取、密钥导出、Token 窃取、权限提升

从 "记录行为" 到 "理解意图"——让 AI 的每一步操作都可理解、可判断、可预警

让 AI 创新建立在安全之上

哨云景御安全管理平台 · AI 原生安全运营

资产看得全

无代理架构实现全域资产可见
云、主机、容器、AI 全覆盖
无盲区、无遗漏

风险判得快

AI 智研 1 分钟完成应急排查
自动分析公告、匹配资产
生成响应建议初稿

危险控得住

执行前审计或阻断高危操作
敏感数据、危险命令管控
从事后追溯到事前防护

过程查得清

完整会话与工具调用留痕
上下文意图分析
可追溯、可复盘、可合规

一套平台，三大能力，覆盖 AI 时代安全运营完整闭环

AI 原生安全运营 · AI 全生命链防护 · AI 会话观测与审计

哨云科技 · 让 AI 创新建立在安全之上

SYSENTRY.CLOUD · 无代理云安全 · 实时防护 · AI 安全一体化运营