有影攻击诱捕系统白皮书

元支点信息安全技术有限公司

版本：V4.0

发布日期：2026 年 4 月

公开范围：定向公开

版权声明

知识产权归属

本资料及相关产品（"元支点有路终端诱骗系统"，以下简称"本产品"或"本系统"）的所有内容，包括但不限于文字说明、技术架构图、界面截图、流程示意图、商标、标识及软件代码等，其知识产权均归北京元支点信息安全技术有限公司（以下简称"元支点"或"本公司"）所有，并受《中华人民共和国著作权法》《中华人民共和国商标法》《中华人民共和国专利法》《中华人民共和国网络安全法》《计算机软件保护条例》等相关法律法规及国际知识产权公约的保护。

使用限制

未经本公司事先书面许可，任何单位或个人不得以任何形式或方式（包括但不限于复制、修改、传播、展示、演示、转载、摘编、镜像、上载、下载、翻译、汇编、反向工程、反编译、反汇编等）使用、引用或传播本资料的全部或部分内容。未经授权的使用将被视为严重侵权行为，本公司保留依法追究其法律责任的权利。

商标声明

"元支点"及相关图形标识、产品名称等均为本公司的注册商标或商业标识。未经本公司书面授权，任何第三方不得擅自使用，否则本公司将依法追究相关法律责任。

资料更新

本公司保留随时修改、更新本资料内容的权利，恕不另行通知。最新版本以本公司官方发布渠道为准。

免责声明

资料性质与用途声明

本资料仅供本产品的技术说明、方案选型及项目决策参考之用，不构成任何投资、采购、技术实施或其他专业领域的最终建议。用户应结合自身网络环境、业务需求及合规要求，评估并确认本产品的适用性。

网络安全风险动态性声明

鉴于网络安全威胁的持续演化和攻防对抗的动态特性，本资料中所述的技术原理、产品功能、性能指标、部署方式及防护效果仅代表产品当前技术状态。本公司不承诺或保证本系统能够检测、拦截或预警所有已知或未知的安全威胁，亦不对因新型攻击手法、零日漏洞或不可抗力因素导致的安全事件作出绝对性效果承诺。

信息准确性声明

本公司在本资料编制过程中已尽最大努力确保所提供信息（包括但不限于产品技术参数、应用场景描述、部署案例数据等）的准确性与时效性，但不对其绝对完整性、准确性、及时性或适用性作出任何明示或暗示的担保。对于因信赖本资料信息而直接或间接导致的任何决策偏差、投资损失或其他后果，本公司不承担任何法律责任。

第三方内容与链接免责

本资料中可能引用或包含指向第三方网站、服务、产品或内容的链接。此类引用仅出于信息参考目的，不代表本公司对该等第三方内容的认可。本公司对第三方提供的内容、服务及其合法性、准确性、安全性不承担任何形式的审查义务或连带责任。用户访问或使用第三方内容的风险由其自行承担。

法律责任与合规使用声明

本产品为合法的网络安全主动防御工具，专供具备相应资质的企事业单位在自有网络环境中使用。用户须严格遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》及其他适用法律法规，不得将本产品用于任何非法侵入他人网络、干扰他人网络正常功能、窃取网络数据或实施其他危害网络安全的活动。因用户违规使用本产品而产生的任何法律后果、行政处罚或民事/刑事责任，均由用户自行承担，与本公司无关。

责任限制

在法律允许的最大范围内，本公司不对任何因使用或无法使用本产品或本资料而导致的直接、间接、附带、特殊、后果性或惩罚性损害（包括但不限于利润损失、数据丢失、业务中断、系统故障、商誉损害或其他经济损失）承担责任，即使本公司已被告知该等损害的可能性。

目录

前言

在数字化转型加速的今天，网络安全威胁呈现出高度智能化、持续化和隐蔽化的特征。攻击者不再满足于简单的边界突破，而是通过长期潜伏、横向移动、权限提升等手段，在内网中持续渗透，最终窃取核心数据或破坏关键业务。

传统的被动防御体系主要依赖边界防护和特征匹配，面对 APT（高级持续性威胁）、零日漏洞利用、AI 驱动的自动化攻击等新型威胁时，往往存在发现滞后、取证困难、溯源能力不足等问题。

有影攻击诱捕系统是元支点主动防御体系的核心产品，专注于内网横向移动阶段的主动感知与诱捕。通过构建真假融合的诱捕网络和隔离仿真环境，将攻击者从真实业务空间牵引到防守方预设的可控空间，实现攻击行为的早期暴露、持续观察和高价值取证。

本白皮书将全面介绍有影攻击诱捕系统的技术架构、核心能力、应用场景和客户价值，帮助读者深入理解主动防御理念在现代网络安全体系中的重要作用。

第一章 网络安全威胁演进与挑战

1.1 当前网络安全威胁态势

1.1.1 APT 攻击的长期潜伏特征

高级持续性威胁（APT）已成为当前网络安全的最大挑战之一。与传统攻击不同，APT 攻击具有以下特征：

- **长期潜伏**：攻击者可能在目标网络中潜伏数月甚至数年，持续收集情报
- **高度定制**：针对特定目标精心设计攻击路径和工具链
- **零日漏洞利用**：使用未公开的漏洞，传统基于特征库的防护手段难以识别
- **隐蔽性强**：攻击行为高度模拟正常业务流量，传统 IDS/IPS 难以有效检测

根据 Verizon 2025 年数据泄露调查报告，从攻击发生到被发现的平均时间为 **207 天**，而攻击者完成数据窃取平均只需要**数小时**。这种巨大的时间差，正是 APT 攻击得以成功的关键。

1.1.2 内网横向移动威胁

攻击者突破边界后，真正危险的往往不是单点入侵本身，而是随之而来的横向移动：

- **资产摸排**：通过扫描探测内网资产分布和网络拓扑
- **凭证窃取**：利用各种手段获取域控凭证、数据库密码等敏感信息
- **权限提升**：通过漏洞利用或配置缺陷获取更高权限
- **横向扩散**：从初始入口点逐步渗透到核心业务区域

在物理隔离的内网环境中，这种威胁尤为突出。由于缺乏外部威胁情报更新，传统边界防护设备对内网横向移动几乎无能为力。

1.1.3 AI 驱动的自动化攻击

随着人工智能技术的发展，攻击者开始利用 AI 技术提升攻击效率：

- **自动化横向移动**：AI 攻击代理可在内网中快速识别高价值目标，自动化执行横向渗透
- **智能化权限提升**：基于机器学习的攻击工具能够快速发现配置弱点和权限漏洞
- **低成本大规模试错**：在内网环境中，AI 可以低成本地对所有资产进行持续探测和攻击尝试
- **自适应攻击策略**：根据防御响应动态调整攻击路径和手法

这种"智能体对抗智能体"的攻防环境，对传统安全防护体系提出了全新挑战。

1.2 传统防护手段的局限性

1.2.1 边界防护的失效

传统安全架构以边界防护为核心，部署防火墙、IPS、WAF 等设备。然而：

- **边界模糊化**：云计算、移动办公、物联网等新技术使得网络边界日益模糊
- **内部威胁无力**：边界设备对内网横向移动无能为力
- **零信任缺失**：默认信任边界内的访问，缺乏持续验证机制

1.2.2 被动检测的滞后性

传统安全设备依赖已知特征匹配和规则引擎：

- **特征库依赖**：对未知威胁和零日攻击响应滞后
- **误报率高**：大量告警导致安全人员疲于应对，真正威胁被淹没

- **缺乏上下文**：单点告警难以还原完整攻击链路
- **人工研判压力大**：日志分析和事件关联高度依赖人工，在 APT 长期潜伏场景下难以及时发现

1.2.3 缺乏主动暴露攻击者的能力

现有安全体系以"防"为主，缺少主动诱捕和溯源取证能力：

- **被动等待**：只能等待攻击者触发已知规则
- **取证困难**：攻击发生后难以获取完整的攻击过程和证据
- **溯源能力弱**：无法有效追踪攻击者身份和意图
- **响应滞后**：从发现到处置的时间窗口过长

1.3 主动防御理念的兴起

面对上述挑战，网络安全防护理念正在从"被动防御"向"主动防御"转变：

被动防御：等待攻击发生 → 特征匹配 → 告警响应

主动防御：主动诱捕 → 持续观察 → 溯源取证 → 联动处置

主动防御的核心思想是：

1. **认知对抗**：通过欺骗和误导，破坏攻击者的决策基础
2. **主动暴露**：让攻击者在内网中"无声渗透"变得不可能
3. **可控观察**：将攻击行为引入隔离环境，持续观察而不打草惊蛇
4. **高价值取证**：获取完整的攻击链路和行为证据
5. **快速响应**：基于高置信度事件实现自动化联动处置

第二章 有影攻击诱捕系统概述

2.1 产品定位

有影攻击诱捕系统是元支点主动防御体系面向内网网络层的核心诱捕产品，聚焦攻击链中段的持续渗透阶段，通过构建真假融合的诱捕网络和隔离仿真环境，把攻击者从真实业务空间牵引到防守方预设的可控空间。

有影攻击诱捕系统系统采用管理平台+牵引器（探针）部署模式，管理账号具备三权分立能力，可实现对不同用户的账号的权限管控；牵引器（探针）支持软件及硬件形态部署，兼容海光、统信、龙芯、麒麟、兆芯等国产 CPU、操作系统。支持伪装 Telnet、Rdp、Samba、ssh 等系统服务；支持 MySQL、MongoDB、MariaDB 等数据库服务；支持 Shiro、Struts2、Tomcat、fastjson 等含特殊缺陷服务。单台设备蜜罐种类≥100 种，蜜罐传感器（软件探针）≥1000 个，支持同时运行 200 个以上蜜罐，设备日志保存≥6 个月。

有影攻击诱捕系统系统支持记录全过程蜜罐访问流量，支持以 PCAP 格式下载，管理节点和探针支持 v4/v6 双栈。

2.2 核心设计理念

2.2.1 真假融合

不依赖明显的"假目标"去吸引攻击者，而是在真实网络环境中投放高仿真诱饵资产、身份、共享信息和服务特征，让攻击者自然进入预设陷阱。

2.2.2 隔离承接

当攻击者触碰诱饵后，可将后续访问透明牵引至隔离仿真环境，在不影响真实业务的前提下，对攻击者后续命令、利用动作、凭证窃取和横向尝试进行持续观察。

2.2.3 低扰动接入

支持旁路 Trunk 模式接入核心交换或关键汇聚节点，无需大规模改造现网，支持跨 VLAN、跨网段诱捕覆盖，适配园区网、数据中心和复杂内网环境。

2.2.4 高价值取证

记录攻击者在内网阶段的扫描路径、会话行为、访问对象和操作链路，为溯源分析、攻击意图判断和复盘取证提供更完整的行为证据。系统具备自主研发的攻击请求语义分析引擎，可以感知攻击者对 Web 类服务蜜罐发起的攻击请求，并智能识别其 Payload 攻击类型和威胁等级。

2.3 解决的核心问题

问题	传统方案	有影方案
内网横向移动难以发现	依赖日志分析，发现滞后	主动诱捕，实时暴露
攻击行为取证不完整	碎片化日志，难以还原	完整录制攻击过程
无法区分正常与恶意访问	规则匹配，误报率高	任何触碰诱饵即为恶意
溯源能力不足	仅有 IP 地址等基础信息	多维度指纹提取和反制
影响业务连续性	阻断可能误伤业务	旁路部署，零业务影响

2.4 产品价值

有影的核心价值，在于让攻击者一旦进入内网，就不再拥有"无声渗透、自由试错"的空间：

- **把内网渗透行为前移暴露**：从"数月发现"压缩到"数分钟发现"
- **把后续攻击动作转入受控环境**：在隔离蜜网中持续观察，不打草惊蛇
- **把高风险事件沉淀为可研判、可取证、可闭环的完整攻击故事线**

在"智能体对抗智能体"的攻防环境中，有影负责让攻击者进入我们设计的战场。

第三章 系统架构与技术实现

3.1 系统架构设计

有影攻击诱捕系统采用分层架构设计，由**控制台、蜜网、蜜罐、流量牵引器（探针）**四部分组成。

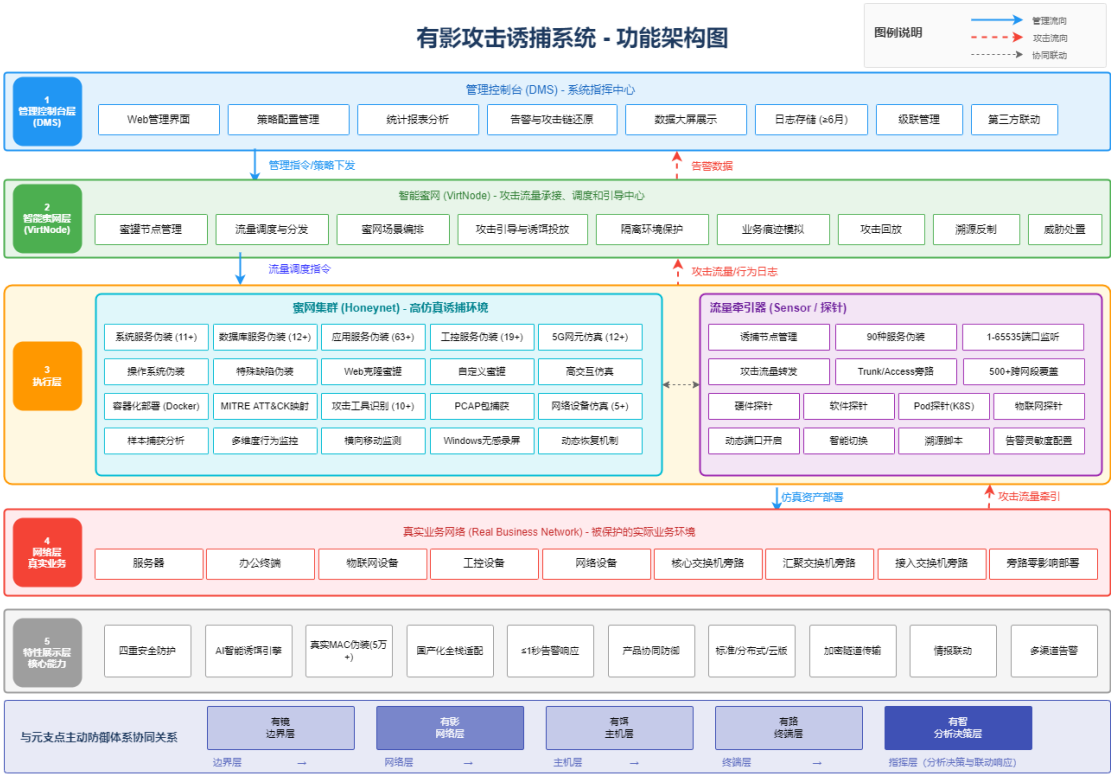


图 1 有影系统架构图

3.1.1 控制台（DMS）

管理控制台是系统的指挥中心，提供统一的管理界面和数据分析能力：

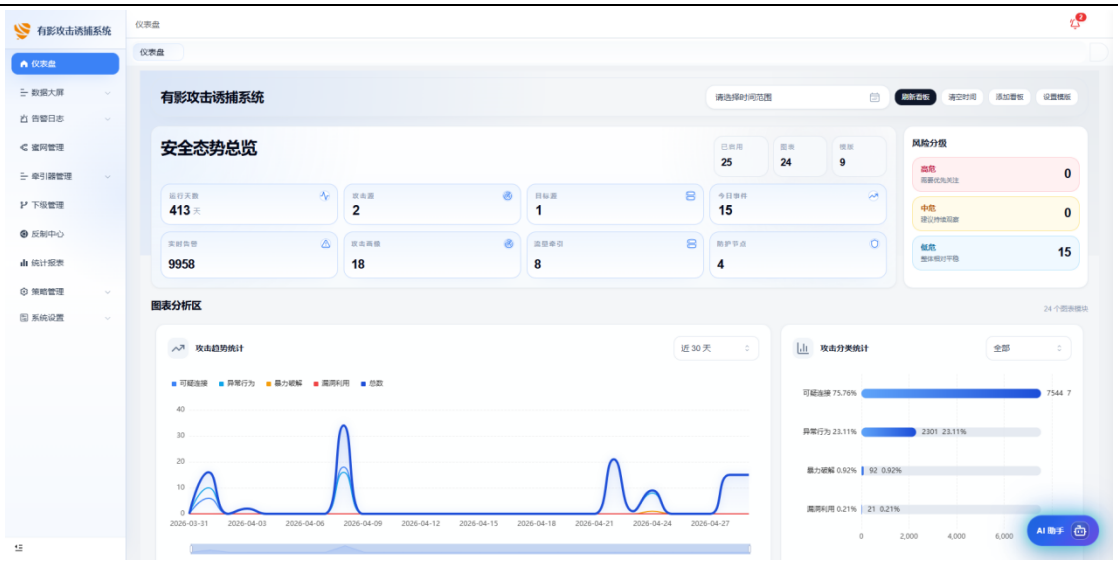


图 2 控制台系统截图

控制台 Web 界面截图

- **Web 管理界面**：B/S 架构，支持远程管理
- **策略配置**：诱捕场景、蜜罐配置、告警规则等
- **统计报表**：攻击趋势、威胁分析、周报月报等
- **告警分析**：实时告警、攻击链还原、溯源分析
- **数据大屏**：全局态势展示，支持指挥中心大屏投放

3.1.2 智能蜜网（VirtNode）

蜜网是攻击流量的承接和调度中心：

- **蜜罐节点管理**：统一管理和调度蜜罐资源
- **流量调度**：根据规则将攻击流量分发到不同蜜罐
- **场景编排**：支持自定义蜜网拓扑和业务关系
- **攻击引导**：通过诱饵投放引导攻击者行为
- **隔离保护**：确保蜜网与真实业务网络完全隔离

3.1.3 蜜罐集群（Honeypot）

蜜罐是与攻击者直接交互的仿真服务：

- **100+种蜜罐类型**：覆盖系统、数据库、应用、工控、5G 网元等
- **高交互仿真**：提供真实的服务响应和交互能力
- **行为记录**：完整记录攻击者的所有操作
- **动态恢复**：攻击后自动恢复初始状态，循环利用
- **容器化部署**：基于 Docker 容器，快速部署和扩展

3.1.4 流量牵引器（Sensor）

流量牵引器是部署在业务网络中的前置感知节点：

- **诱捕节点管理**：管理各网段的空闲 IP 地址，每个 IP 对应一个诱捕节点
- **服务伪装**：每个节点可开启 90 种不同类型的服务
- **威胁检测**：监听 1-65535 任意端口，感知所有攻击流量
- **流量转发**：将攻击流量通过管理口转发至蜜网
- **旁路部署**：Trunk 或 Access 模式接入交换机，对业务零影响
- **跨网段覆盖**：单台探针支持 500+跨网段、3000+诱捕节点部署

3.2 核心技术特性

3.2.1 四重安全防护机制

有影系统自身采用"容器+虚拟化+隔离环境+访问控制"四重防护，确保攻击者无法以蜜罐为跳板威胁内网安全：

1. **容器安全**：蜜罐运行在 Docker 容器中，资源隔离

2. **虚拟化安全**：基于 KVM 虚拟化技术，硬件级隔离

3. **隔离环境**：蜜网与真实业务网络完全隔离

4. **访问控制**：每一层都有严格的权限和访问控制

同时支持**逃逸检测**功能，实时监控攻击者试图逃离蜜罐的行为并告警。

3.2.2 AI 驱动的智能诱饵引擎

- **智能生成**：基于真实网络资产特征自动学习并生成高仿真虚拟资产诱饵
- **动态适配**：AI 自动跟踪真实业务资产变化，动态更新诱饵指纹特征
- **意图识别**：AI 辅助攻击意图分析与研判，自动识别攻击者行为模式
- **智能关联**：AI 驱动的攻击链关联分析，将碎片化攻击行为串联为完整攻击路径

3.2.3 真实 MAC 地址伪装

采用真实的 MAC 地址库（不少于 5 万条真实厂商 MAC 数据），不会被网络扫描和探测工具（如 Nmap）识别为蜜罐，大幅提升诱饵的真实性和欺骗性。

3.2.4 动态端口与智能切换

- **动态端口开启**：根据攻击情况自适应开启仿真端口，深度融入业务区域
- **智能切换**：自动化区分用户访问、攻击者嗅探和攻击者攻击等行为，实现真实系统和诱捕系统的动态切换

3.2.5 加密隧道传输

支持加密隧道模式，1-65535 的全端口流量可通过固定端口的隧道模式传输，进行攻击的隔离和保护，确保蜜网的安全性和网络策略的灵活性。

3.3 国产化适配能力

有影系统全面支持国产化生态，可兼容：

- **国产 CPU**：龙芯、飞腾、鲲鹏、海光
- **国产操作系统**：统信 UOS、麒麟、移动 BClinux、欧拉、龙蜥
- **国产数据库**：达梦 V8、人大金仓
- **国产中间件**：东方通 V7.0

同时支持仿真国产数据库服务，为国产化环境提供完整的诱捕能力。

第四章 核心功能详解

4.1 蜜罐伪装能力

有影系统提供丰富的高仿真蜜罐服务，覆盖企业内网常见资产类型，并可随产品迭代持续扩展。

4.1.1 系统服务伪装

支持常见系统协议的高交互仿真：

- **远程访问**：SSH、Telnet、RDP、VNC 等
- **文件传输**：FTP、SFTP、SMB、NFS 等
- **代理服务**：SOCKS、HTTP Proxy 等

- **其他服务**：DNS、Memcached、SIP、ADB 等

能够记录完整的异常访问日志，包括登录尝试、命令执行、文件操作等。

4.1.2 数据库服务伪装

支持主流数据库的高交互仿真：

- **关系型数据库**：MySQL、MSSQL、Oracle、PostgreSQL、人大金仓等
- **NoSQL 数据库**：Redis、MongoDB、Elasticsearch、Cassandra 等
- **消息队列**：MQTT、Kafka 等
- **其他**：InfluxDB、CouchDB 等

能够记录完整的数据库操作日志，包括增删改查、权限提升、数据导出等行为。

4.1.3 应用服务伪装

支持企业常见应用系统的仿真：

- **Web 应用**：Wiki、Apollo、BBS、Discuz、HRM、ECShop、Joomla 等
- **中间件**：Tomcat、WebLogic、JBoss、WebSphere 等
- **管理工具**：phpMyAdmin、Zabbix、Jenkins、Confluence 等
- **大数据平台**：Hadoop、Spark、Hive 等
- **企业应用**：OA、CRM、ERP、堡垒机（4A）、企业邮箱等
- **VPN 网关**：OpenVPN、IPSec VPN 等
- **其他**：Struts2、Spring Boot 等常见框架

4.1.4 工控服务伪装

针对工业控制系统提供专业的协议仿真：

- **电力行业**：IEC104、IEC61850、DNP3 等
- **通用工控**：Modbus TCP、S7、OPCUA、Bacnet 等
- **能源行业**：Kamstrup382 等
- **设备管理**：IPMI 等
- **其他**：支持自定义厂商名称、商品名称、产品名称等

能够捕获针对工控服务的攻击事件，如功能码、命令等关键信息。

4.1.5 5G 网元仿真

支持 5G 核心网网元的仿真，包括：

- AMF（接入和移动性管理功能）
- AUSF（认证服务器功能）
- NRF（网络存储功能）
- NSSF（网络切片选择功能）
- PCF（策略控制功能）
- SMF（会话管理功能）
- UDM（统一数据管理）
- UDR（统一数据存储）
- 其他

支持随 5G 网络安全防护需求持续扩展，适配更多核心网网元与业务接口场景。

4.1.6 操作系统伪装

支持多操作系统指纹伪装，通过扫描工具可识别出具体的操作系统版本：

- **Windows 系列**：XP、Vista、7、8、10、Server 2003/2008/2012/2016/2019 等
- **Linux 系列**：CentOS、Ubuntu、RedHat、SUSE12 等
- **国产操作系统**：Kylin、NeoKylin、UOS 等

支持定制开发，满足特殊场景需求。

4.1.7 网络设备仿真

支持常见网络设备的仿真：

- 打印机
- 路由器
- 交换机
- 防火墙
- 负载均衡器

4.1.8 特殊缺陷伪装

支持配置部署经典漏洞，吸引攻击者利用：

- **Web 漏洞**：Webshell、Struts2、Shiro、WebLogic、Fastjson 等
- **系统漏洞**：Shellshock、EternalBlue（永恒之蓝）等
- **应用漏洞**：Tomcat、Coremail、负载均衡等
- **设备漏洞**：NBR 路由器等

以时间线的方式记录完整的异常访问日志和漏洞利用过程。

4.1.9 蜜罐克隆与自定义

- **Web 克隆**：通过爬虫+代理获取网站资源，一键生成蜜罐服务
- **自定义蜜罐**：支持用户自行上传蜜罐模板，仿真门户、官网、办公 OA 等
- **证书预置**：支持预置自定义证书，实现 HTTP 转 HTTPS 协议访问
- **漏洞预置**：支持预置各种类型的安全漏洞，可被第三方扫描工具扫描发现

4.2 智能蜜网能力

4.2.1 全仿真网络构建

支持构建与用户真实业务网络配置相同的智能蜜网：

- **网络配置一致**：蜜网内资产可设置与真实业务相同的 IP、网段
- **业务类型相似**：模拟仿真与真实业务环境相同的资产类型
- **完全隔离**：与真实业务不产生任何冲突，不影响真实业务
- **资产类型丰富**：终端主机、网络设备、工控设备、安全设备、运维管理系统等

4.2.2 蜜网场景编排

支持蜜网场景自定义编排：

- **规则编排**：对蜜网内仿真资产进行规则编排
- **网络走向设计**：通过定义网络走向高度还原用户网络架构
- **多层次关系**：建立网络关系、业务架构层次关系、数据关系
- **拓扑可视化**：用图表形式展示蜜网架构、节点分布

4.2.3 业务痕迹模拟

支持模拟真实业务系统的运行痕迹：

- **网络流量模拟**：蜜网节点之间的网络流量
- **业务数据记录**：模拟业务系统的数据记录
- **访问记录**：模拟用户访问记录
- **用户活动记录**：模拟用户活动痕迹
- **操作记录**：模拟系统操作记录

这些业务痕迹信息大幅提升蜜网的真实性，让攻击者难以识别。

4.2.4 攻击引导与诱饵投放

支持在蜜网编排场景内投放多种欺骗诱饵：

- **反制诱饵**：伪造敏感文件，诱骗攻击者下载反制程序
- **系统诱饵**：浏览记录、登录密码、RDP 连接记录、域凭据等
- **文件诱饵**：Word、Excel、PPT 等办公文件
- **邮件诱饵**：钓鱼邮件，支持自定义内容和附件
- **凭证诱饵**：SSH 证书、数据库密码、API 密钥等

通过诱饵的欺骗内容，精准引导攻击者的行为，实现长时间驻留和高级持续性攻击的捕获。

4.2.5 蜜网集群与分级管控

支持构建集团级蜜网集群：

- **资源共享**：下级与总部共享智能蜜网资源

- **统一配置**：总部统一配置诱捕策略
- **分级权限管控**：支持多级权限管理
- **数据上报**：下级数据可上报至总部进行统一分析

4.3 诱捕探针能力

4.3.1 平台化管理

- **统一管控**：通过硬件/软件牵引器设备管理诱捕探针节点
- **即插即用**：牵引器平台支持分布式部署，自动注册到管理控制台
- **图形化界面**：支持图形化界面管理配置所有诱捕节点
- **多维度展示**：通过图表、表格、表单等形式展示诱捕探针数据

4.3.2 自动化部署

- **一键部署**：基于探测结果和智能算法，图形化界面一键自动化全网部署
- **非 Agent 模式**：无需在终端安装代理程序
- **自动探测**：自动探测网络内空闲 IP 地址，支持自定义探测周期
- **IP 防冲突**：支持 IP 防冲突功能，系统自动释放 IP 资源

4.3.3 多场景探针支持

- **标准探针**：部署在物理网络或虚拟化环境
- **Pod 探针**：以 Pod 形式部署在 Kubernetes 集群中，监测 K8S 集群攻击行为
- **物联网探针**：部署在物联网摄像头设备中，监测针对摄像头的攻击

4.3.4 探针覆盖能力

- **多网段支持**：单个物理探针可配置多个探针 IP（非 Agent 模式），覆盖多个网段、VLAN
- **大规模部署**：支持大规模诱捕节点和复杂跨网段场景部署
- **全端口监听**：支持全端口范围监听，且不限制端口数量
- **全流量感知**：感知所有攻击流量，记录全部接入探针网络流量的源地址、目的地址、源端口、目的端口、HTTP 头所有信息、URL、响应头等内容

4.3.5 智能特性

- **动态端口**：根据攻击情况自适应开启仿真端口
- **动态切换**：自动区分用户访问、攻击者嗅探和攻击者攻击，实现真实系统和诱捕系统的动态切换
- **溯源脚本**：支持在诱捕探针上设置攻击指纹溯源功能，自定义溯源脚本
- **流量转发**：支持将攻击连接请求推送到用户指定的服务器
- **告警灵敏度**：支持设置探针监测攻击的灵敏度，过滤不同攻击级别的日志

4.4 攻击分析能力

4.4.1 攻击事件记录

完整记录攻击事件的关键信息：

- **时间信息**：攻击时间、持续时间
- **源信息**：攻击源 IP、攻击源 MAC、攻击者操作系统
- **目标信息**：攻击目标 IP、被攻击服务、被攻击区域

- **攻击特征**：攻击方式、攻击阶段、攻击命令、攻击工具
- **威胁级别**：基于攻击行为自动评估威胁等级
- **真实信息**：真实 IP、真实源 MAC（穿透代理）

4.4.2 攻击回放

- **Windows 无感录屏**：完整录制攻击者在 Windows 蜜罐中的操作
- **Linux 命令回放**：对攻击者执行的命令进行回放
- **PCAP 包下载**：支持以 PCAP 格式下载攻击过程中的全部流量
- **样本捕获**：在攻击告警详情 Payload 中自动捕获分析攻击载荷样本

4.4.3 基于 MITRE ATT&CK 框架的攻击阶段分析

完整覆盖 MITRE ATT&CK 框架的全部 14 个战术阶段及 200+技术及子技术：

1. 侦察（Reconnaissance）
2. 资源开发（Resource Development）
3. 初始访问（Initial Access）
4. 执行（Execution）
5. 持久化（Persistence）
6. 权限提升（Privilege Escalation）
7. 防御规避（Defense Evasion）
8. 凭证访问（Credential Access）
9. 发现（Discovery）

10. 横向移动（Lateral Movement）

11. 收集（Collection）

12. 命令与控制（Command and Control）

13. 数据渗出（Exfiltration）

14. 影响（Impact）

以图表形式可视化展示攻击者在各个阶段的行为，帮助安全人员快速理解攻击意图。

4.4.4 横向移动监测

蜜网与真实环境隔离，可记录攻击者在多蜜罐间进行的横向移动，包括：

- 扫描探测行为
- 凭证尝试行为
- 服务利用行为
- 文件传输行为
- 权限提升行为

4.4.5 攻击工具识别

支持检测识别各种常见攻击工具：

- **扫描工具**：Nmap、Nessus、AWVS、AppScan、W3AF、RSAS、Netsparker、WebInspect、W13scan 等
- **漏洞利用工具**：SQLMap、Metasploit 等
- **Webshell 工具**：AntSword（蚁剑）、Behinder（冰蝎）、Godzilla（哥斯拉）、Cknife（菜刀）等

- **探测方式**：Null、Xmas、SYN、SSH、Curl 等

4.4.6 蜜罐内行为监控

全方位监控蜜罐内的各类行为：

- **进程监控**：监控和记录蜜罐内进程的变化
- **文件监控**：监控文件的新增、修改、删除，支持变更文件下载
- **系统登录监控**：监控系统登录，包括认证成功和认证失败
- **远程控制监控**：监控 RDP 连接，包括尝试连接、认证、启动图形桌面、断开等
- **网络监控**：监控端口监听、端口访问、数据传输等
- **服务监控**：监控服务的启动、停止、修改选项、安装等
- **本地账号监控**：监控用户账号和本地组的创建、启动、更改、重置、禁用、删除等
- **权限变更监控**：监控账号权限的调整、分配、撤销等
- **PowerShell 监控**：监控 PowerShell 脚本执行
- **注册表监控**：监控高危风险项的创建、删除、修改等
- **防火墙监控**：监控防火墙的开启、关闭、规则添加、修改、编辑等
- **日志清除监控**：监控系统日志、安全日志、应用程序日志的清除
- **计划任务监控**：监控计划任务的创建、修改、删除

4.5 溯源反制能力

4.5.1 攻击链溯源

以攻击链方式展现攻击者的入侵全过程：

- **完整操作记录**：查看攻击者完整的操作记录
- **攻击行为分类**：横向渗透、攻击扩散、密码破解、漏洞利用、木马上传等
- **攻击扩散拓扑**：以拓扑图形式展示攻击扩散情况，包含目标 IP、攻击类型、攻击手法等

4.5.2 攻击指纹提取

支持对攻击者指纹进行多维度提取：

- **网络指纹**：公网 IP、代理 IP、网络配置
- **社交账号信息**：QQ、WeChat、邮箱、GitHub、Gitee 等
- **硬件设备信息**：主机名称、MAC 地址、硬件配置
- **浏览器信息**：浏览器类型、版本、插件、历史记录
- **应用信息**：CS、Xshell、Navicat、Git 等应用的用户账号 ID

支持基于现有设备指纹进行设备指纹碰撞，反查攻击者的历史溯源信息，补充溯源信息。

4.5.3 情报联动

支持情报联动，能够自动化获取深度情报信息：

- 威胁情报库查询
- IP 信誉查询
- 域名信誉查询
- 文件哈希查询

4.5.4 反制能力

支持多种反制手段，获取攻击者更多信息：

反制诱饵：

- 支持上传自定义诱饵程序，引诱攻击者下载
- 诱饵通过反制程序添加花指令、多次编译、程序加壳等方式实现木马免杀

反制画像：

- 监控攻击者对蜜罐的入侵行为，并实现对攻击机器的反制
- 获取桌面文件、进程列表、设备硬件信息
- 文件上传下载、浏览器数据、网络配置、系统信息
- 桌面截屏、摄像头拍照
- 自定义命令执行

专项反制：

- **MySQL 反制**：监控 MySQL 服务入侵行为，读取攻击设备的主机名称、邮箱、微信 ID 等
- **Git 反制**：伪装 Git 源码泄漏缺陷，监控源码泄漏扫描和攻击行为
- **Goby 反制**：针对 Goby 扫描器的反制
- **Chrome 反制**：利用 Chrome 浏览器内核漏洞，获取攻击者主机权限
- **工具反制**：针对 AWVS、SQLMap、CobaltStrike 等安全工具的反制

4.5.5 威胁处置

- **一键加白**：支持对攻击 IP 进行右键一键加白处置

- **联动阻断**：与防火墙、交换机等设备联动，自动阻断攻击源
- **工单创建**：自动创建应急响应工单

4.6 可视化展示能力

4.6.1 数据大屏

支持数据大屏功能，适合指挥中心大屏投放：

图 3 有影数据大屏截图

- **攻击统计**：攻击总数量、攻击 IP 数量、被攻击传感器数量、被攻击服务数量
- **攻击趋势预测**：基于历史数据预测攻击趋势
- **攻击类型分布**：攻击类型、攻击服务的分布统计
- **告警排名**：高危告警、攻击源排名
- **实时攻击**：当前正在发生的实时攻击情况

4.6.2 仪表盘

图形化展示系统运行状态和攻击态势：

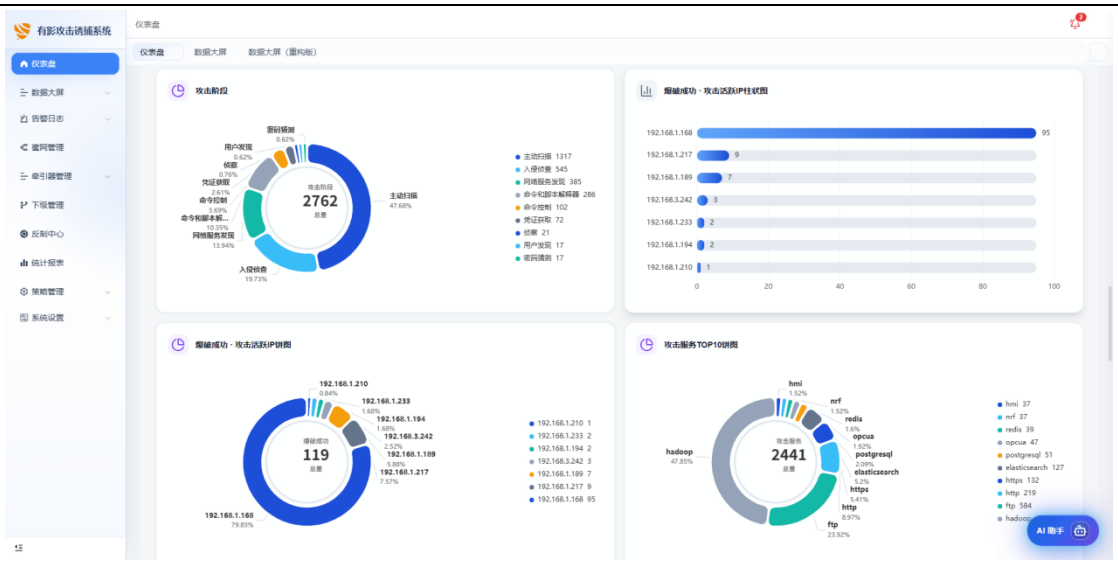


图 4 仪表盘界面截图

- **系统资源**：CPU、内存、磁盘使用情况
- **攻击事件**：攻击事件数量、攻击状态、攻击趋势
- **告警类型**：不同类型告警的分布
- **探针区域**：各区域探针的部署和告警情况
- **攻击画像**：攻击源画像、攻击目标画像
- **攻击排行**：攻击源 TOP、被攻击资产 TOP

支持 20+种攻击分析视图，支持视图自定义拖拽改变排版布局，支持自由组合分析视图保存为仪表盘模板。

4.6.3 攻击源分析

聚合攻击源信息，多维度分析：

- **攻击时间线**：攻击者的活动时间线
- **攻击扩散**：攻击扩散路径和范围

- **攻击目标**：攻击者关注的目标资产
- **攻击情报**：关联的威胁情报信息
- **攻击动作**：攻击者的具体操作动作

以图表形式呈现分析结果，支持攻击信息补充，支持按模块导出数据。

4.6.4 统计报表

支持威胁统计报表，按模板模块定制报表内容：

- **多维度统计**：攻击数量、攻击级别、攻击类别、攻击动作、攻击源 IP 等
- **多时间周期**：周报、月报、半年报、年报
- **定时生成**：支持定时生成报表功能
- **多格式导出**：支持 PDF、HTML、Word 导出格式

4.6.5 日志导出

支持以 JSON、CSV、LOG 和 XLS 格式导出告警类日志，方便与第三方系统对接。

4.7 系统管理能力

4.7.1 白名单管理

支持通过多维度设置白名单：

- **源 IP 白名单**：信任的源 IP 地址
- **源端口白名单**：特定的源端口
- **目标 IP 白名单**：特定的目标 IP
- **目标端口白名单**：特定的目标端口

- **协议白名单**：特定的协议类型
- **告警名称**：信任的告警名称

支持将用户扫描工具、测试机器等加入白名单，支持白名单导出 Excel、CSV、JSON 等格式。

4.7.2 级联管理

提供上下级多级管理功能：

- **统一管理**：对本地设备、下级设备以及异地设备进行统一管理监控
- **策略下发**：总部统一下发诱捕策略
- **数据上传**：下级数据上传总部进行统一分析
- **组织机构划分**：支持按组织机构划分系统用户和业务

4.7.3 资源监控

支持监控系统各组件的运行状态：

- **管理节点监控**：控制台的运行状态
- **蜜罐监控**：蜜罐的 CPU、内存、磁盘利用率
- **探针监控**：探针的运行状态和资源使用
- **远程操作**：支持蜜罐进行暂停、重启等操作

4.7.4 资产测绘

- **自定义网络 IP 资产**：支持上传 IP 文件自动解析
- **定时扫描**：创建定时任务自动扫描测绘网络资产

- **资产信息**：获取资产的网络、设备、主机、开放端口、开放服务等信息

4.7.5 告警联动

支持多渠道告警通知：

- **Syslog**：将日志同步到第三方服务器
- **邮件**：邮件告警通知
- **短信**：短信告警通知
- **Kafka**：通过 Kafka 消息队列推送
- **Webhook**：通过 Webhook 推送到第三方系统
- **即时通讯**：钉钉、飞书、企业微信等

告警信息包括攻击告警、蜜罐安全告警、ARP 欺骗、设备心跳和存储空间阈值。

4.7.6 第三方系统联动

- **开放 API 接口**：可与第三方平台进行二次开发
- **安全设备联动**：支持主机防御类、流量类、防火墙类等设备联动
- **数据关联**：接收第三方平台告警数据，可视化展示，分析关联数据绘制攻击链条

4.8 安全性保障

4.8.1 蜜罐安全

- **四重防护**：容器安全+虚拟化安全+隔离技术+访问控制
- **逃逸检测**：对试图逃离蜜罐的攻击者行为进行记录
- **网络阻断**：配置蜜罐是否可以外联

4.8.2 日志安全

- **加密存储**：日志以加密形式存储
- **长期保存**：最少保存 6 个月
- **备份机制**：支持日志数据存储发送到 FTP 进行备份

4.8.3 身份认证

- **证书认证**：支持通过证书进行强身份鉴别机制
- **三权分立**：支持管理员、操作员、审计员三种角色，分开管理，相互制约
- **3A 认证**：支持 Radius 认证登录和 LDAP 认证登录
- **密码策略**：支持首次登录修改密码、定期修改密码，可更改密码复杂度、锁定时间、页面超时等
- **账号锁定**：支持账号锁定策略，灵活设置账户锁定阈值、账户锁定时间
- **可信主机**：支持配置用于登录系统的可信任主机 IP 地址

4.8.4 系统备份

- **备份功能**：支持备份攻击告警日志、规则策略日志
- **远程备份**：发送到 FTP 远程备份
- **系统回滚**：支持系统备份回滚到某一时刻的状态

第五章 部署方案与应用场景

有影系统以旁路接入、分层布防和集中运营为主要部署原则，可根据客户网络规模、隔离边界、业务重要性和安全运营模式，灵活选择硬件一体机、分布式、云化等部署形态。

5.1 部署模式与接入方式

5.1.1 标准版

适用场景：中小型企业、单一园区网络、结构相对清晰的业务环境。

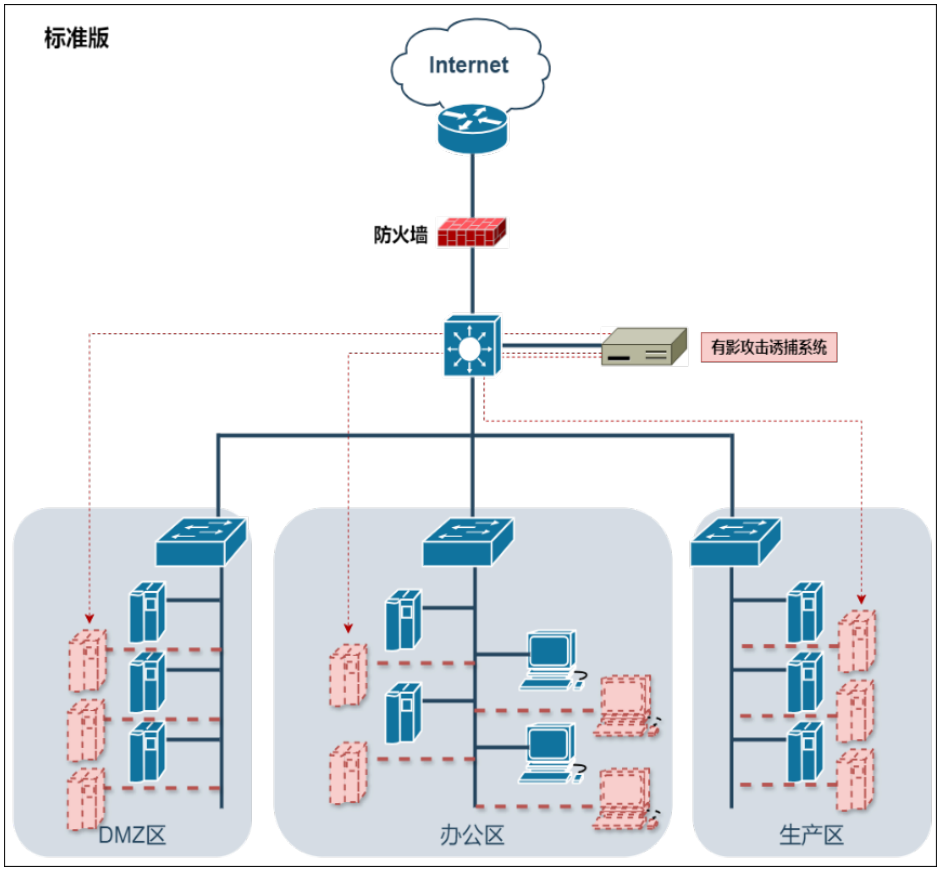


图 5 有影标准版部署示意图

架构特点：

- 单台硬件设备集成控制台、蜜网、蜜罐、牵引器等核心能力
- 采用旁路接入方式，无需改变现有网络拓扑结构
- 支持按管理、调试、入站等不同用途进行网口规划

部署要点：

- 可在核心或汇聚交换区域接入，实现跨 VLAN、跨网段监测

- 根据关键业务区和高价值资产位置配置诱捕策略
- 对现有业务系统运行无影响，便于快速上线和持续运营

5.1.2 分布式版

适用场景：大型企业、多数据中心、多网络隔离区域、跨地域分支机构。

架构特点：

- 通过中心控制台统一管理分布式牵引器和诱捕节点
- 牵引器可部署在不同隔离网络、业务区域或分支机构中
- 支持跨区域告警汇聚、策略下发和统一分析

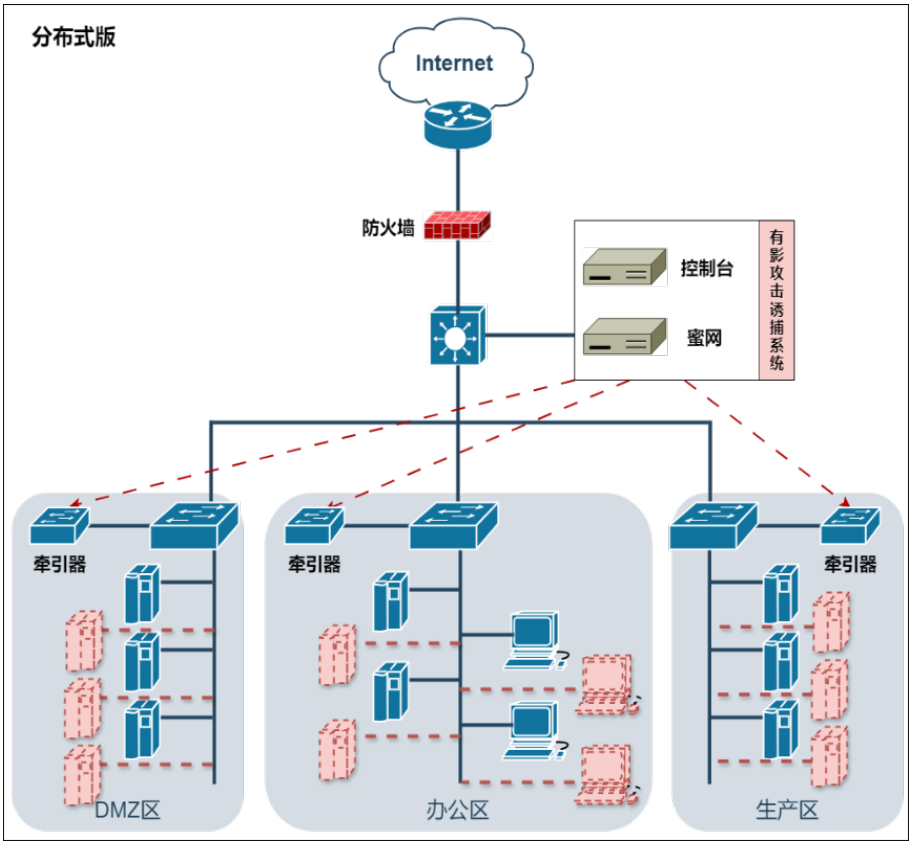


图 6 有影分布式版部署示意图

部署要点：

- 根据网络隔离边界和业务分区规划牵引器位置
- 控制台与牵引器之间建立受控、安全的数据交互关系
- 适合构建覆盖总部、分支、数据中心和专网环境的统一诱捕体系

5.1.3 云版部署

适用场景：私有云、公有云、混合云、虚拟化资源池等环境。

架构特点：

- 采用软件化形态部署，适配云上弹性资源和虚拟网络环境
- 支持跨云、混合云和多租户场景下的诱捕能力建设
- 可根据业务网段、租户边界和安全域灵活扩展牵引能力

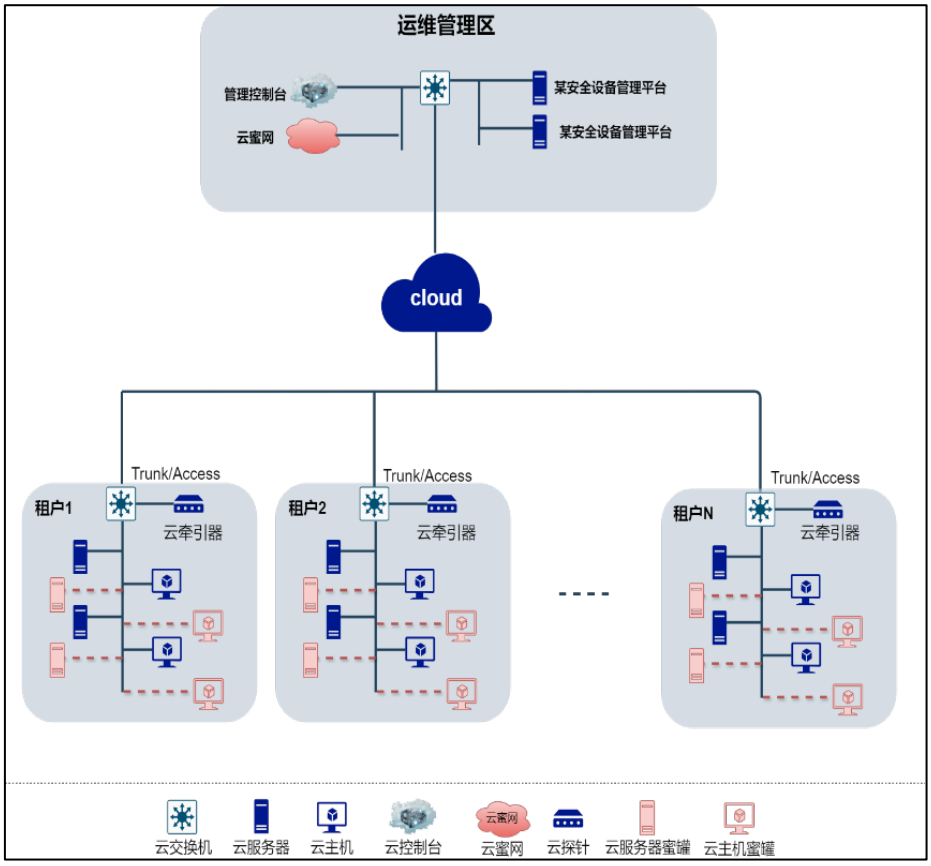


图 7 有影云版部署示意图

部署要点：

- 在关键云网络、核心业务 VPC/VNet 或重要租户区域部署牵引能力
- 根据云平台网络策略开放必要的受控访问关系
- 与云安全运营、日志分析和告警响应体系协同联动

5.1.4 旁路接入与部署位置

有影系统以旁路部署为主，对业务系统零侵入、低扰动，适合在不改变现网架构的前提下快速形成主动诱捕能力。

- **Access 模式：**适用于单一 VLAN 或特定业务区域的定向监测
- **Trunk 模式：**适用于多 VLAN、多网段环境下的统一覆盖
- **核心交换区旁路：**覆盖范围广，适合全网级威胁感知建设
- **汇聚交换区旁路：**适合对重点业务区、服务器区和办公区分域监测
- **接入交换区旁路：**适合高价值资产、敏感服务器或特定终端区域的精准布防
- **业务连续性保障：**关键场景可结合硬件 Bypass 等能力，降低设备异常对业务连续性的影响

5.2 场景化应用

有影系统的能力指标应与实际场景结合评估，重点关注诱捕节点承载、跨网段覆盖、告警响应、并发攻击承接、日志留存与平台联动等维度。面向公开材料，可将其概括为大规模覆盖、秒级发现、持续取证、统一运营和弹性扩展等能力。

5.2.1 园区网与内网横向移动感知

场景特点：园区网通常采用核心、汇聚、接入分层架构，办公终端、服务器、网络设备等资产类型丰富，人员和终端密集，攻击者突破边界后容易开展扫描探测和横向移动。

部署建议：

- 在核心交换区旁路部署牵引能力，形成全网基础覆盖
- 在关键业务区、服务器区和办公区按需增加诱捕密度
- 配置办公 OA、文件共享、数据库、远程访问等高仿真诱饵

应用价值：攻击者扫描或访问诱饵资产时即可触发高置信度告警，后续行为可被牵引至隔离蜜网持续观察，从而记录横向移动路径、攻击工具和操作手法，将内网威胁发现从被动等待转为主动暴露。

5.2.2 数据中心与核心业务区安全加固

场景特点：数据中心服务器密集、访问关系复杂，承载大量核心业务和敏感数据，是攻击者长期渗透和横向扩散的重点目标。

部署建议：

- 在数据中心核心或汇聚交换区域旁路接入牵引能力
- 构建高仿真的数据库、文件服务器、应用服务器等诱饵资产
- 在仿真业务中投放敏感文件、账号凭据、数据库表等诱饵内容
- 与有智等平台联动，结合访问基线识别异常访问模式

应用价值：一旦攻击者尝试探测核心业务区、访问异常数据库或进行数据导出，系统可快速告警并保留完整证据，帮助安全团队识别真实攻击意图，保护核心业务系统不被攻击者轻易定位。

5.2.3 工控网络安全防护

场景特点：工控网络对业务连续性要求极高，设备协议专用、系统生命周期长，传统安全设备往往难以充分识别工业协议和控制指令层面的异常行为。

部署建议：

- 采用旁路部署方式，确保对生产网络零影响
- 部署 Modbus、S7、OPCUA、IEC104 等工控协议蜜罐
- 仿真 PLC、HMI、SCADA 等典型工业设备与控制场景
- 监测扫描探测、漏洞利用、功能码调用和异常控制指令等行为

应用价值：在不影响生产系统稳定运行的前提下，及时发现针对工控设备和工业协议的攻击行为，记录攻击者操作意图，为事件处置、攻击溯源和后续加固提供依据。

5.2.4 物理隔离网络与高安全专网

场景特点：物理隔离网络通常资产固定、访问路径有限，但也面临内部威胁、违规接入、摆渡攻击和离线威胁情报更新滞后等风险。

部署建议：

- 结合固定资产和固定 IP 特征，建立高置信度诱饵策略
- 在关键服务器区、终端区和业务交换区域部署高密度诱饵
- 通过离线情报库和定期安全摆渡方式保持检测能力更新

应用价值：在访问关系相对稳定的专网环境中，任何触碰诱饵的行为都具有较高可疑度，有助于快速识别违规操作、内部探测和潜在攻击活动。

5.2.5 APT 攻击捕获与溯源

场景特点：APT 攻击者通常长期潜伏、低频操作、持续收集情报，传统基于规则和边界流量的检测方式难以及时发现其真实意图。

部署建议：

- 在蜜网中投放假域控、假数据库、假敏感文件等高价值诱饵
- 通过业务痕迹和诱饵内容引导攻击者进入隔离环境
- 完整记录攻击工具、攻击手法、攻击目标和操作路径
- 关联威胁情报和攻击指纹，支撑后续溯源分析

应用价值：通过主动构造攻击者感兴趣的目标，将长期潜伏行为转化为可观察、可取证、可研判的安全事件，为防护加固和情报生产提供高价值依据。

5.2.6 护网/重保期间快速加固

场景特点：护网、重保等关键时期，安全团队需要在短时间内提升内网发现能力、响应效率和攻击威慑力。

部署建议：

- 通过旁路方式快速上线，不改造现网、不影响业务
- 在关键业务区、高价值资产区和攻击高发路径部署高密度诱饵
- 配置高灵敏度告警策略，并与防火墙、交换机、SOC/SIEM 等系统联动
- 建立 7×24 小时监控、研判和处置流程

应用价值：快速提高攻击者的试探成本和暴露概率，为防守方争取响应时间，并将零散告警转化为可追查、可处置的闭环事件。

5.2.7 5G 网络安全防护

场景特点：5G 核心网网元开放接口多、协议复杂，面临扫描探测、接口滥用、协议攻击和新型漏洞利用等安全风险。

部署建议：

- 部署 AMF、AUSF、NRF、NSSF、PCF、SMF、UDM、UDR 等 5G 网元蜜罐
- 仿真核心网网元的服务接口、协议交互和业务访问特征
- 监测针对 5G 网元的扫描、漏洞利用、协议异常和攻击尝试

应用价值：为 5G 核心网提供专业化主动诱捕能力，帮助运营单位发现针对网元和接口的新型攻击行为，并沉淀 5G 网络安全威胁情报。

第六章 与元支点其他产品的协同

有影作为元支点主动防御体系的核心产品，与其他产品形成完整的纵深防御体系。

6.1 与有镜的协同

有镜：网络空间反测绘系统，负责边界层的入口伪装和测绘干扰

协同价值：

- **边界到内网的连续防线**：有镜负责边界误导，有影负责内网诱捕
- **数据互通**：有镜接收外部测绘信息并同步诱饵策略给有影
- **攻击链完整追踪**：从边界探测到内网渗透的完整攻击链路

典型场景：

攻击者通过有镜获取错误的资产信息 → 进入内网后触碰有影的诱饵 → 被牵引到隔离蜜网 → 完整记录攻击过程

6.2 与有路的协同

有路：终端诱骗系统，负责终端层和物联网层的本地触饵感知

协同价值：

- **网络层+终端层纵深防御**：有影覆盖网络层，有路覆盖终端层
- **攻击路径追踪**：终端触发告警后可引导至网络层蜜网
- **填补哑终端盲区**：有路覆盖物联网设备（摄像头、门禁、打印机等），有影覆盖网络流量

典型场景：

攻击者通过物联网设备进行侧翼渗透 → 有路在终端层触发告警 → 攻击者继续横向移动 → 触碰有影的网络层诱饵 → 被牵引到蜜网

6.3 与有饵的协同

有饵：主机威胁发现系统，负责服务器主机内部的威胁感知

协同价值：

- **主机层+网络层协同**：有饵在服务器内部触发高置信度发现，有影在网络层承接后续攻击
- **东西向流量监控**：有饵建立服务器间访问基线，有影监测异常横向流量
- **完整攻击链还原**：从主机入侵到网络横向移动的完整链路

典型场景：

攻击者入侵服务器 → 有饵检测到异常行为 → 攻击者尝试横向移动 → 触碰有影的诱饵 → 被牵引到蜜网持续观察

6.4 与有智的协同

有智：威胁分析决策平台，负责统一的威胁分析和联动响应

协同价值：

- **攻击链还原**：有智将有影捕获的碎片化攻击行为串联为完整攻击链
- **AI 研判**：有智基于 AI 进行攻击意图分析和真伪研判
- **联动响应**：有智统一编排响应策略，与防火墙、交换机等设备联动

典型场景：

有影捕获攻击事件 → 上报至有智 → 有智进行 AI 研判和攻击链还原 → 自动下发阻断策略 → 创建应急响应工单

6.5 完整防御体系

元支点主动防御体系形成"边界层+网络层+主机层+终端层+分析决策层"的完整纵深防御：

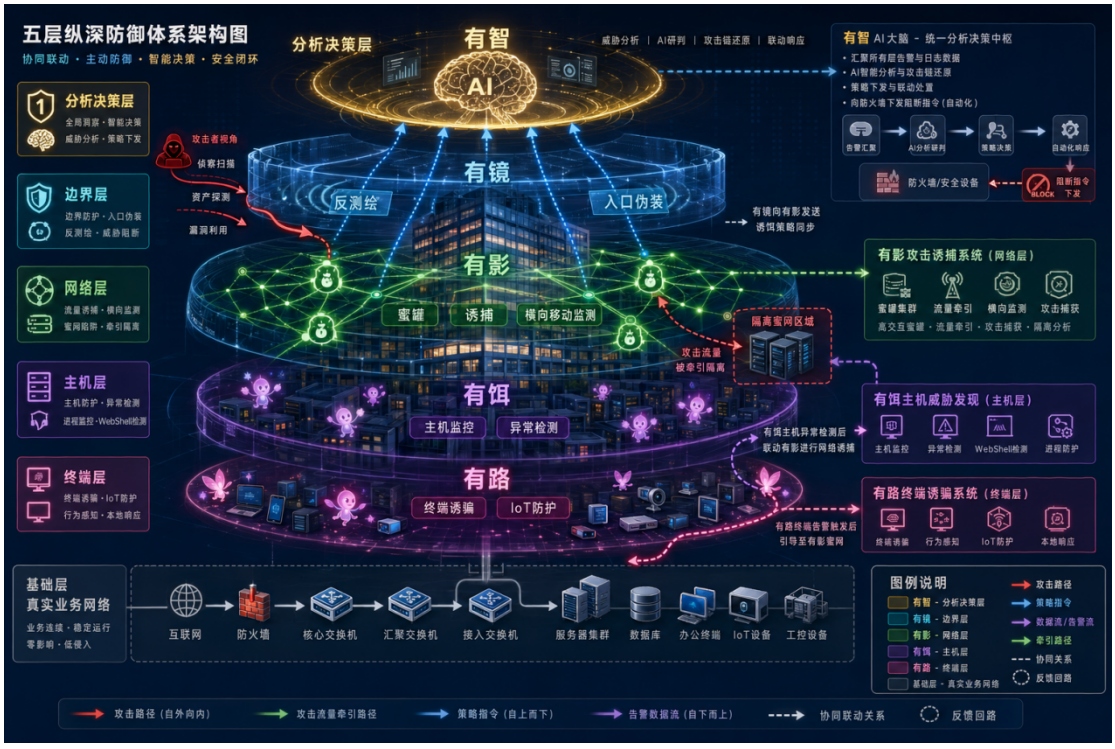


图 8 产品协同架构图

协同效果：

- **从入口到纵深的连续认知陷阱**
- **从发现到处置的完整闭环**
- **从碎片化告警到完整攻击故事线**

第七章 客户价值与实践案例

7.1 核心客户价值

有影系统的客户价值不只是新增一类检测工具，而是帮助安全团队把内网防护从“事后排查”推进到“主动发现、持续取证、联动处置”的运营模式。

7.1.1 威胁发现更早，告警更准

传统检测依赖规则、流量特征和人工研判，容易在低频潜伏、横向移动和内部探测阶段出现发现滞后。诱捕体系通过部署高仿真诱饵，将攻击者的扫描、访问、登录、利用等行为转化为高置信度告警。

价值体现：

- 将内网威胁发现从被动等待压缩到分钟级甚至秒级响应
- 降低低价值告警和误报噪声，让安全人员聚焦真实风险
- 为应急响应争取更早的研判和处置窗口

7.1.2 攻击过程可还原，证据可追溯

传统方案往往只能看到碎片化日志，难以回答攻击者“从哪里来、做了什么、想去哪”。有影在隔离蜜网中记录攻击者的访问路径、命令操作、工具特征、流量数据和攻击阶段，支撑攻击链还原与溯源分析。

价值体现：

- 获取完整攻击链路、攻击工具和 TTP 证据
- 支撑事件复盘、责任认定、溯源分析和防护加固
- 将一次告警沉淀为可复用的威胁情报和运营经验

7.1.3 部署低扰动，运营更轻量

有影以旁路接入为主，不改变现有网络拓扑，不影响核心业务连续性，适合在数据中心、专网、园区网、工控网络和云环境中快速上线。同时，系统通过高置信度告警、自动化研判和统一管理能力，降低日常运营压力。

价值体现：

- 快速形成主动防御能力，降低项目上线和改造风险
- 减少人工日志排查和重复研判工作
- 适配多区域、多网段、多安全域的统一运营要求

7.1.4 处置可联动，体系价值更强

有影可与元支点有镜、有路、有饵、有智等产品协同，也可对接防火墙、交换机、SOC、SIEM、短信网关、工单系统等第三方平台，将高置信度发现转化为可追查、可闭环的处置流程。

价值体现：

- 从单点告警升级为攻击链级别的整体研判
- 从人工通知升级为多平台联动处置
- 从孤立产品能力升级为主动防御体系能力

7.2 行业应用情况

有影攻击诱捕系统已在多个行业成功应用，服务客户超过 400 家：

7.2.1 政府行业

- **公安系统**：内网横向移动感知，护网期间快速加固
- **军队内网**：物理隔离环境下的 APT 攻击捕获
- **政务云**：云环境下的虚拟化部署

7.2.2 金融行业

- **银行数据中心**：核心业务区域的安全加固
- **证券交易系统**：高价值资产的重点防护

- **支付平台**：交易系统的横向移动监测

7.2.3 能源行业

- **电力调度中心**：工控网络安全防护
- **石油化工**：生产网络的安全监测
- **智能电网**：物联网设备的安全防护

7.2.4 运营商行业

- **5G 核心网**：5G 网元的安全防护
- **数据中心**：大规模服务器集群的安全监测
- **IDC 机房**：多租户环境的安全隔离

7.2.5 互联网行业

- **云服务提供商**：云环境下的安全防护
- **电商平台**：业务系统的安全加固
- **游戏公司**：防止游戏服务器被攻击

7.3 典型成功案例

案例一：某市公安机关专网主动防御体系规模化部署

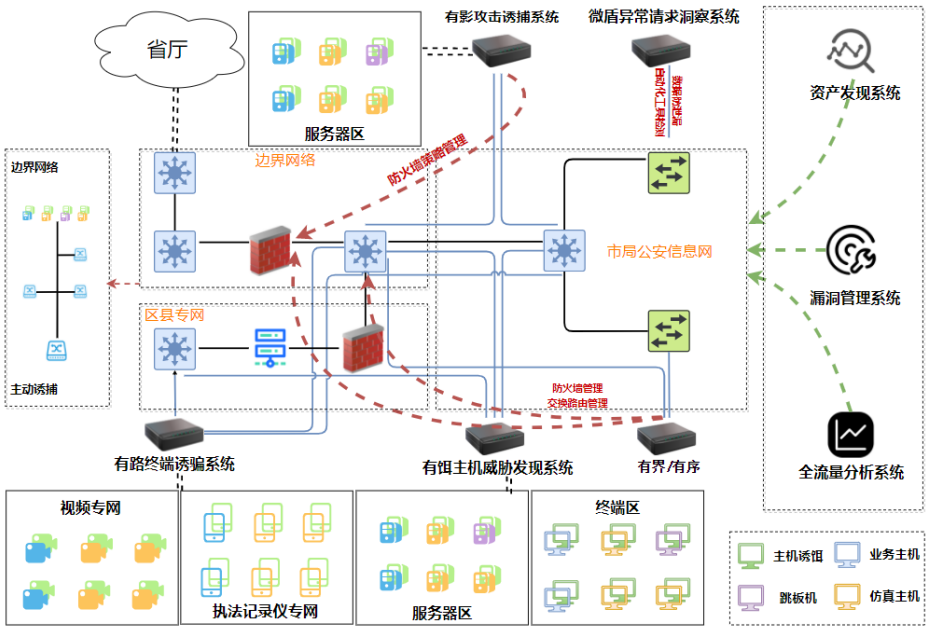
客户背景：

某市公安机关下辖公安信息网、视频专网等多张专网，涵盖 PC 终端、移动设备在内的大量联网资产，资产类型多样化导致攻击面不断扩大，安全缺口持续增长，传统防御技术难以满

足日益复杂的安全形势需要。同时，攻击手段日趋复杂隐蔽，监管合规要求与安全防护责任同步增加，亟需构建主动、全面的内网威胁感知能力。

部署方案：

- 覆盖全市范围内多场景复杂网络环境，包括市局、各区县分局、派出所、交警中队，以及看守所、车管所等各级公安单位
- 在 10000 余个终端投放部署感知诱饵，终端覆盖率≥90%
- 在 100 余台服务器部署威胁感知诱饵，服务器覆盖率≥95%
- 生成 25000 余个检测锚点，全面覆盖网络、主机、摄像头等各类业务场景
- 完成无处不在的陷阱和无死角的监控环境构建，初步形成网络违法行为的威慑力



实施效果：

- 在信息专网、视频专网等多网融合环境下实现主动诱捕能力的统一调度与协同
- 终端与服务器双重覆盖，消除传统安全盲区，有效应对从终端渗透到服务器横向移动的各类攻击路径

- 检测锚点覆盖网络协议层、主机层、应用层，形成立体化的威胁感知网络
- 依托该项目的成功实践，形成首个主动防御地方标准并已正式发布实施

客户评价：

"元支点主动安全防御体系在全市范围内的大规模部署，实现了多网融合场景下的威胁主动感知能力从零到一的突破。终端与服务端诱饵的高覆盖率让攻击者无处遁形，25000 余个检测锚点构建了真正无死角的监控网络。该项目不仅有效提升了全市公安机关的网络安全防护水平，更推动了首个主动防御地方标准的制定与发布，为公安行业网络安全建设树立了标杆。"

案例二：某银行数据中心横向移动监测

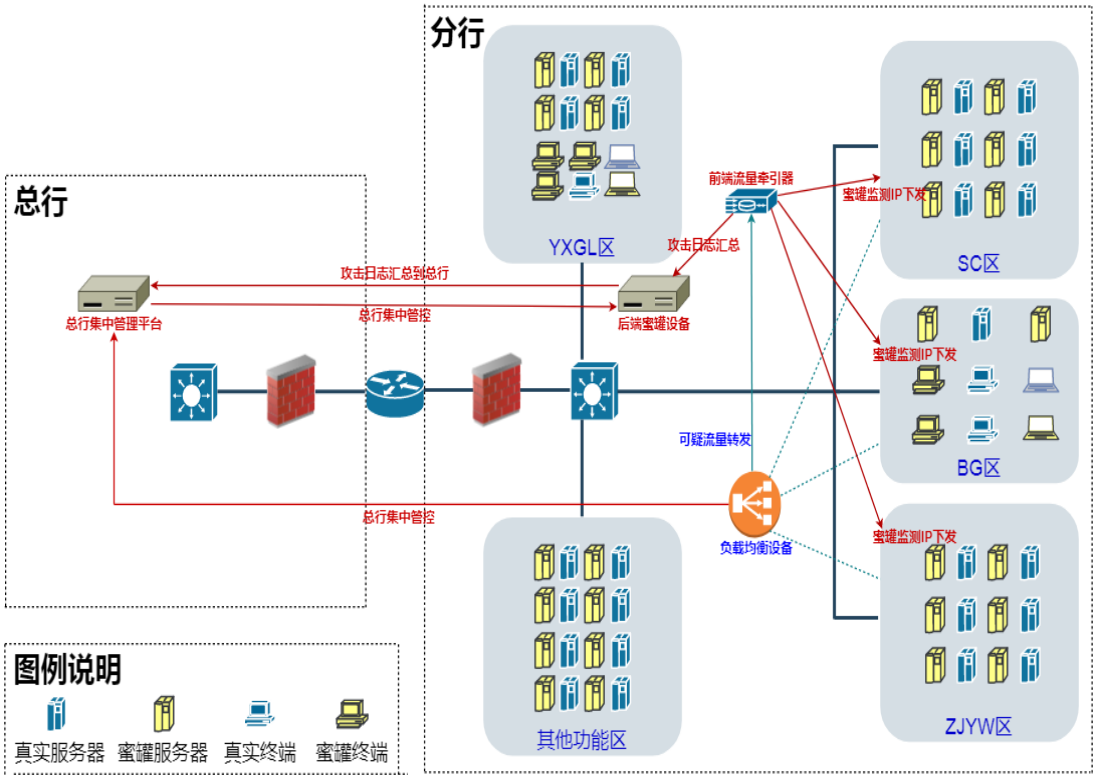
客户背景：

某大型银行网络环境复杂，覆盖总行、全国各省分行及海外分支机构，承载互联网公众服务、核心生产、办公运营等多类关键业务场景。随着数据中心规模持续扩大、跨区域互联互通日益频繁，攻击者一旦突破单点边界，极易借助横向移动渗透至核心业务系统，对全网安全运营与关键数据资产形成持续威胁。

部署方案：

- 在总行及全国 39 个分支行所有数据中心完成统一部署，覆盖全国各省分行、总行互联网公众服务区、DMZ 区、生产区、海外分行服务器区、办公区等 17 个重点区域
- 综合部署有影攻击诱捕系统、有饵主机威胁发现系统、有路终端诱骗系统，构建面向服务器与终端的一体化欺骗防御体系
- 全网平均每天运行约 10000 多个高仿真蜜罐，并部署约 10000 个检测诱饵（锚点），形成覆盖多区域、多层级、多类型资产的持续诱捕与监测能力

- 重要业务系统主机诱饵覆盖率超过 95%，终端诱饵覆盖率超过 90%，实现对关键资产和用户终端的高密度布防



实施效果：

- 仿真主机总数超过 1 万个，结合大规模检测诱饵投放，实现对全网横向移动、异常探测、资产试探等行为的无死角监控

- 有影、有饵、有路三大产品协同运行，显著增强了对攻击者侦察、渗透、横向扩散全过程的感知和取证能力，形成持续威慑

- 欺骗防御体系已成为该行检测响应的核心系统，并与态势感知平台、资源平台、短信网关等关键系统联动，建立起闭环处置机制

- 推动形成“响应及时、有告警必追查、有告警必处理”的新型安全运营流程与工作模式，显著提升安全团队对高风险事件的发现效率和响应质量

客户评价：

"元支点有影、有饵、有路产品在我行总行及全国分支数据中心的大规模部署，实现了从服务器到终端、从区域边界到核心业务系统的全方位覆盖。依托超过万个高仿真蜜罐和检测诱饵，我们真正建立了全网无死角的监控体系。该欺骗防御体系已经成为我行检测响应的核心支撑平台，并通过与多类安全和运维平台联动，推动形成了响应及时、告警必追查、告警必处理的常态化工作机制。"

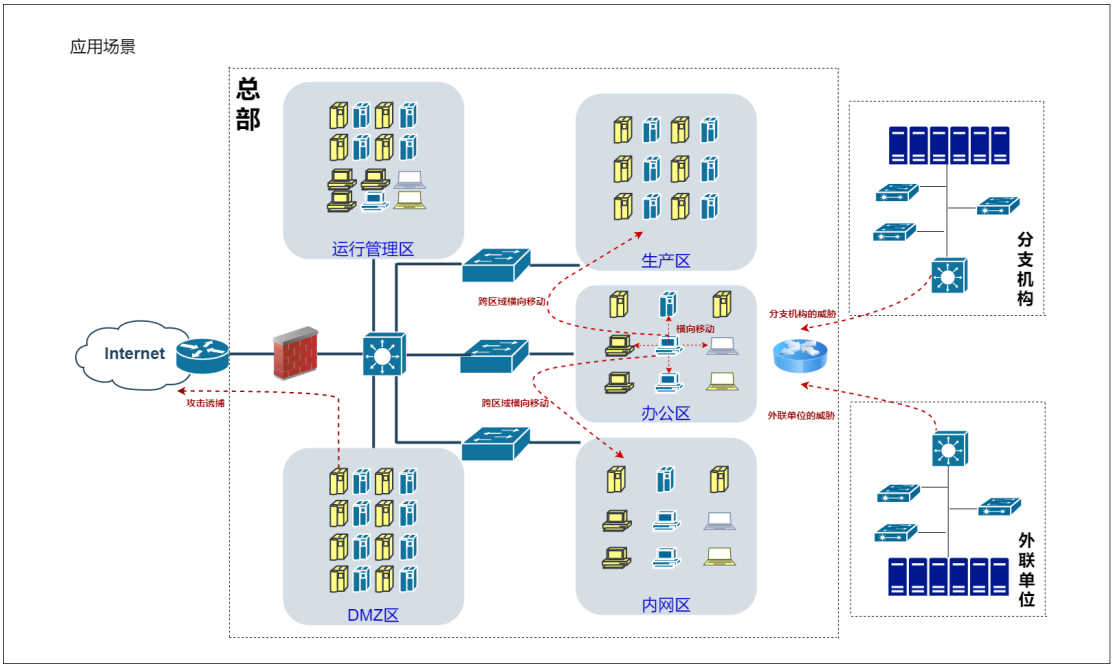
案例三：某电力公司工控网络安全防护

客户背景：

某省级电力公司调度中心，工控网络承载电网调度业务，对业务连续性要求极高。

部署方案：

- 旁路部署，确保对生产零影响
- 部署工控协议蜜罐（IEC104、Modbus、OPCUA 等）
- 仿真 PLC、RTU、SCADA 等工控设备



实施效果：

- 部署后 2 周，捕获到针对工控设备的扫描攻击
- 发现攻击者尝试利用工控协议漏洞进行攻击
- 完整记录攻击者发送的功能码和控制命令
- 及时阻断攻击，避免对电网调度系统的影响

客户评价：

"有影系统为我们的工控网络提供了专业的安全防护能力。系统部署对生产零影响，能够及时发现针对工控设备的攻击，是工控安全的重要补充。"

7.4 价值实现支撑能力

7.4.1 技术支撑

真假融合的高仿真能力

- **丰富蜜罐类型**：覆盖企业内网的各类资产
- **真实 MAC 地址**：基于真实厂商 MAC 数据进行伪装，不被扫描工具识别
- **动态适配**：AI 自动跟踪真实资产变化，动态更新诱饵特征
- **业务痕迹模拟**：模拟真实业务系统的运行痕迹

四重安全防护机制

- **容器+虚拟化+隔离+访问控制**：确保攻击者无法以蜜罐为跳板
- **逃逸检测**：实时监控攻击者试图逃离蜜罐的行为
- **加密隧道**：全端口流量通过加密隧道传输

AI 驱动的智能能力

- **智能诱饵生成**：基于真实资产特征自动生成诱饵
- **攻击意图识别**：AI 辅助攻击意图分析与研判
- **攻击链关联**：AI 驱动的攻击链关联分析
- **异常检测**：基于机器学习的异常行为检测

大规模部署能力

- **高密度诱捕节点承载**：支持非 Agent 方式的大规模诱捕能力建设
- **复杂网络覆盖**：支持跨网段、跨区域、跨安全域部署
- **并发攻击承接**：满足重保、演练和真实攻击场景下的持续取证需求

全面的国产化适配

- 支持国产 CPU、国产操作系统、国产数据库、国产中间件
- 可仿真国产数据库服务
- 满足国产化替代需求

7.4.2 服务支撑

全国服务网络

- 服务覆盖全国主要区域
- 提供"7×24"的邮件和"5×8"电话支持服务
- 专业技术团队提供便捷的服务

丰富的实施经验

- 服务客户覆盖多个重点行业
- 覆盖政府、金融、能源、运营商、互联网等多个行业
- 积累了丰富的复杂环境适配经验

持续的产品迭代

- 持续跟踪最新的攻击手法和威胁情报
- 定期更新蜜罐类型和检测规则
- 根据客户反馈持续优化产品功能

7.4.3 资质认证

- 计算机信息系统安全专用产品销售许可证
- 国家信息安全产品认证证书
- ISO 9001 质量管理体系认证
- ISO 27001 信息安全管理体系认证

第八章 总结与展望

8.1 产品总结

有影攻击诱捕系统是元支点主动防御体系的核心产品，专注于内网横向移动阶段的主动感知与诱捕。

核心能力：

- 真假融合的内网诱捕能力

- 隔离仿真环境承接
- 高价值行为取证
- 低扰动接入与跨网段覆盖

核心价值：

- 将威胁发现时间从"数月"压缩到"数分钟"
- 告警准确率接近 100%，大幅降低误报
- 获取完整的攻击链路和高价值情报
- 旁路部署，对业务零影响
- AI 自动化研判，降低运营成本 80%以上

应用场景：

- 内网横向移动感知
- APT 攻击捕获与溯源
- 护网/重保期间快速加固
- 数据中心安全加固
- 工控网络安全防护
- 5G 网络安全防护

协同价值：

与有镜、有路、有饵、有智形成完整的"边界层+网络层+主机层+终端层+分析决策层"纵深防御体系。

8.2 未来展望

8.2.1 技术演进方向

更智能的 AI 能力：

- 深度学习驱动的攻击意图预测
- 自适应的诱饵生成策略
- 更精准的攻击链还原

更丰富的蜜罐类型：

- 持续跟踪最新的应用系统和协议
- 支持更多国产化应用的仿真
- 支持用户自定义蜜罐的快速开发

更强大的反制能力：

- 针对新型攻击工具的反制
- 更隐蔽的反制手段
- 更丰富的溯源信息获取

8.2.2 应对 AI 驱动攻击的演进

随着 AI 技术在攻击领域的应用，有影系统将持续演进以应对新型威胁：

认知对抗：

- 通过制造"数据迷雾"，破坏 AI 攻击代理的决策基础
- 利用海量诱饵使 AI 进入"搜索空间爆炸"状态
- 消耗 AI 攻击代理的算力资源

智能体对抗智能体：

- 部署 AI 防御代理，与 AI 攻击代理进行实时对抗
- 动态调整诱饵策略，适应 AI 攻击代理的学习能力
- 预测 AI 攻击代理的下一步行动

8.2.3 产品生态建设

开放平台：

- 提供更丰富的 API 接口
- 支持第三方开发者开发自定义蜜罐
- 建立蜜罐模板市场

威胁情报共享：

- 建立威胁情报共享平台
- 与行业内其他安全厂商进行情报交换
- 为客户提供更全面的威胁情报

安全运营服务：

- 提供托管式安全运营服务
- 7×24 小时专业安全团队监控
- 定期安全评估和加固建议

8.3 结语

在数字化转型加速的今天，网络安全威胁呈现出高度智能化、持续化和隐蔽化的特征。传统的被动防御体系已经难以应对 APT 攻击、零日漏洞利用、AI 驱动的自动化攻击等新型威胁。

有影攻击诱捕系统代表了网络安全防护理念从"被动防御"向"主动防御"的转变。通过构建真假融合的诱捕网络和隔离仿真环境，有影让攻击者一旦进入内网，就不再拥有"无声渗透、自由试错"的空间。

在"智能体对抗智能体"的攻防环境中，有影负责让攻击者进入我们设计的战场。与有镜、有路、有饵、有智等产品协同，形成完整的纵深防御体系，实现从"被动防守"到"主动掌控"的能力升级。

元支点将持续投入研发，不断提升产品能力，为客户提供更专业、更智能、更高效的主动防御解决方案，助力客户构建面向未来的网络安全防护体系。

附录 A：术语表

术语	英文	解释
APT	Advanced Persistent Threat	高级持续性威胁，指长期潜伏在目标网络中的攻击
蜜罐	Honeypot	用于诱捕攻击者的仿真系统
蜜网	Honeynet	由多个蜜罐组成的网络环境
横向移动	Lateral Movement	攻击者在内网中从一个系统移动到另一个系统
零日漏洞	Zero-day Vulnerability	尚未公开或未被修复的安全漏洞
TTP	Tactics, Techniques, and Procedures	战术、技术和程序，描述攻击者的行为模式
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	MITRE 组织提出的攻击行为知识库
旁路部署	Bypass Deployment	不串联在网络链路中，而是从旁路监听流量
Trunk 模式	Trunk Mode	交换机端口模式，可传输多个 VLAN 的流量
Access 模式	Access Mode	交换机端口模式，只传输单个 VLAN 的流量