JUMING 聚铭
让安全更简单

聚铭安全产品

EASIER WAY FOR SECURITY

累计服务10000+政企客户

聚铭铭察高级威胁检测系统

(iATD)

聚铭网络
www.juminfo.com

聚铭铭察高级威胁检测系统

聚铭铭察高级威胁检测系统（简称：iATD），以旁路方式接入网络，能够实时对网络环境中的 APT 进行监测及反制。通过对网络流量深度识别、解析、检测，挖掘已知及未知威胁，精确定位攻击来源；通过多维分析取证技术及第三方异构设备联动技术，实现智能化程度高、及时性强的未知威胁研判及反制。为客户在高级威胁入侵时，及时察觉，及时止损。

产品功能示意

1 行业现状

① 未知威胁层出不穷

1、零日漏洞公开叫卖，高级逃逸躲避手段日新月异；

2、黑客使用 WormGPT 的人工智能工具进行钓鱼和 BEC 邮件攻击，未知威胁激增。

② APT 挑战安全极限

1、手段组合，长期潜伏，迂回渗透，无孔不入；

2、对整个安全体系构成全面、长期、艰巨的挑战。

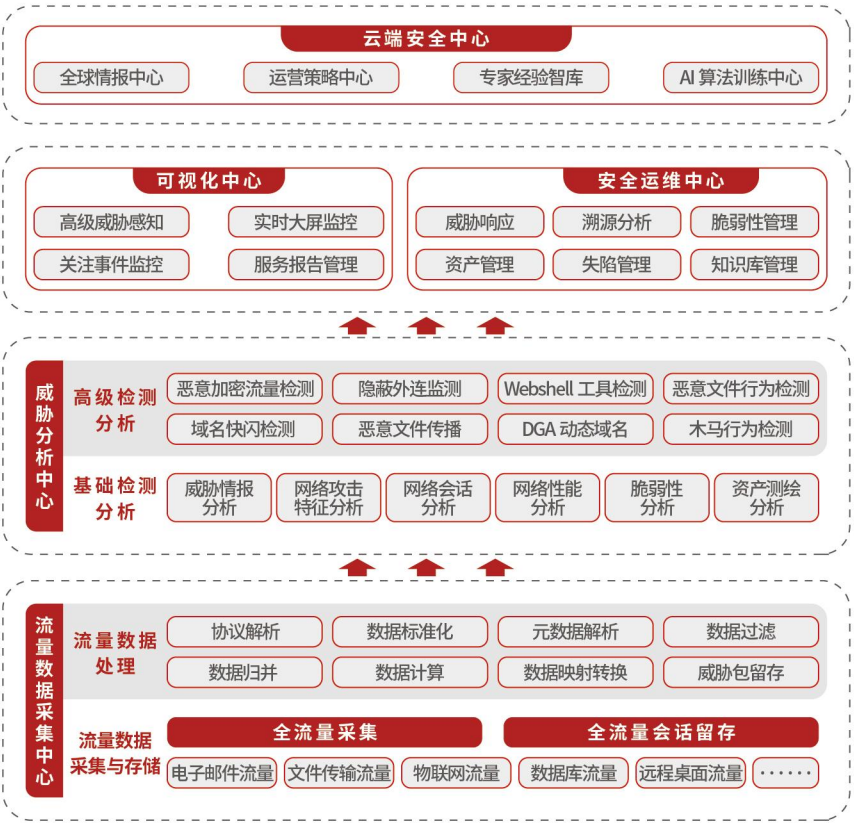
③ 被动防御疲于奔命

1、日常无法提前预防，只能被动响应；

2、高级威胁对抗发现、研判工作对人员能力要求高；

3、遭受攻击后人工响应效率低，难以有效防护。

2 系统架构



3 核心功能

资产及供应链安全测绘

通过持续对资产及供应链的深度测绘，不断地识别新的潜在风险，从而可对未知威胁做好提前预防。

高级威胁深度检测

针对 0day 漏洞利用、攻击绕行、隐蔽信道、恶意加密流量等高级威胁行为，采用AI机器学习及动态行为检测技术，实现对高级威胁深度检测。

高级威胁精准研判

基于全流量会话及威胁数据包留存技术，结合语义识别及威胁攻击链自动生成能力，对高级威胁行为进行精准研判。

万能联动响应

不受第三方设备API限制，可智能化完成第三方设备的对接，对防火墙、EDR等设备实现万能联动，及时完成对未知威胁的反制。

高级威胁实名溯源

针对DHCP场景中发现的未知威胁，可实名追溯攻击链上的各个设备，定位攻击源和被攻击目标的实名账号。

4 产品优势

未知威胁精准检测、回溯、取证

千余种应用协议深度还原，全流量留存，无死角回溯。通过结合行为模型、AI算法、攻击研判及取证等技术，提高未知威胁检出准确率。

智能 AI 检测技术

结合威胁样本生成算法模型，针对恶意加密流量（专利技术）、隐蔽外连、DGA、域名快闪攻击等进行智能AI分析，挖掘潜在威胁，提升对未知威胁检测效果。

多态高性能恶意文件行为检测技术

支持200余种文件还原及检测，采用多态高性能恶意文件行为检测技术，每天可完成15万个恶意文件的行为检测。

干预反制 多维联动智能布防

内置众多异构设备联动，基于模块化万能联动技术，半小时内完成定制设备适配，通过场景策略，实现智能布防。

5 产品价值

NO.1 高级威胁事前预防

结合供应链测绘、暴露面测绘、未知威胁检测等技术，持续识别新的潜在风险，及时做好提前预防。

NO.2 高级威胁事中快速响应

针对勒索软件、僵木蠕软件、0day 漏洞攻击等未知威胁攻击，通过第三方安全设备联动，实时完成对未知威胁的反制。

NO.3 事后威胁回溯完善防御体系

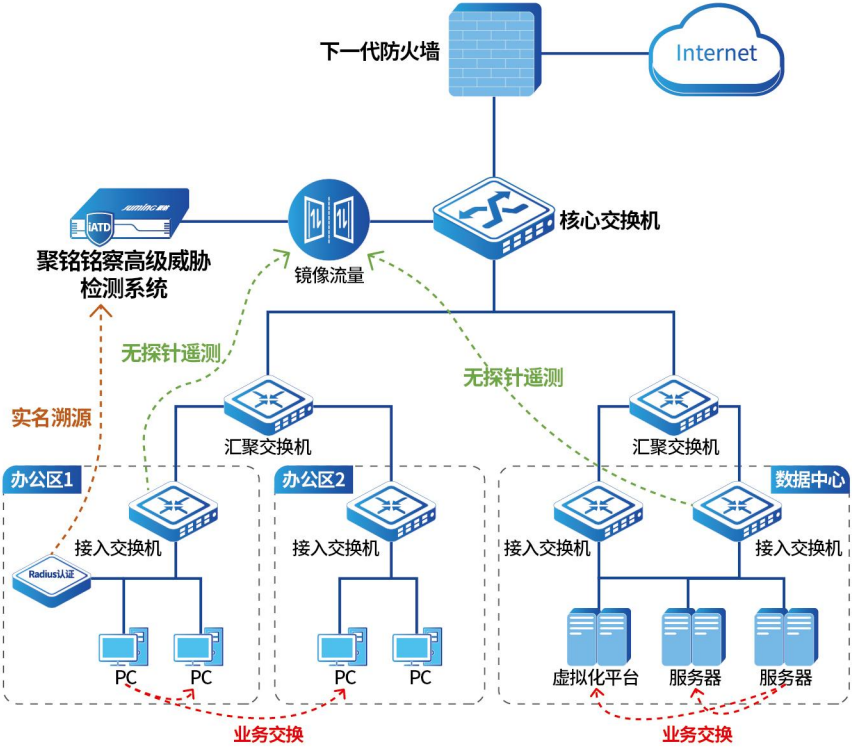
高级威胁发生后，实名回溯发生过的网络攻击行为，分析攻击路径、受感染面和信息泄露状况。协助用户升级和完善网络威胁防御体系，确保安全防护的稳固与高效。

NO.4 满足新等保的合规要求

满足新等保 2.0 对网络攻击检测和分析要求，特别是针对新型网络攻击和 APT 攻击。

6 部署方式

聚铭铭察高级威胁检测系统设备标准配置一个管理口，N 个监听口（N 由实际配置决定），其中管理口用于设备控制、系统访问等；监听口与交换机镜像口相连，铭察高级威胁检测系统设备通过监听口接收交换机镜像流量，实现流量采集功能，部署方式如图所示：



聚铭 Juminc

聚铭订阅号

荣获国家发明专利20余项
通过【ISO9001质量管理体系认证】【ISO27001信息安全管理体系认证】
【ISO20000信息技术服务管理体系认证】
【ISO14001环境管理体系认证】【ISO45001职业健康安全管理体系认证】
【CCRC信息安全风险评估服务资质认证】【CCRC信息安全应急处理服务资质认证】

公司地址：江苏省南京市雨花台区软件大道180号南京大数据产业基地7栋4层
电话：025-52205520　　传真：025-52205565
全国统一服务热线：400-1158-400　　公司官网：www.juminfo.com