

juminc 聚铭
| 让安全更简单 |



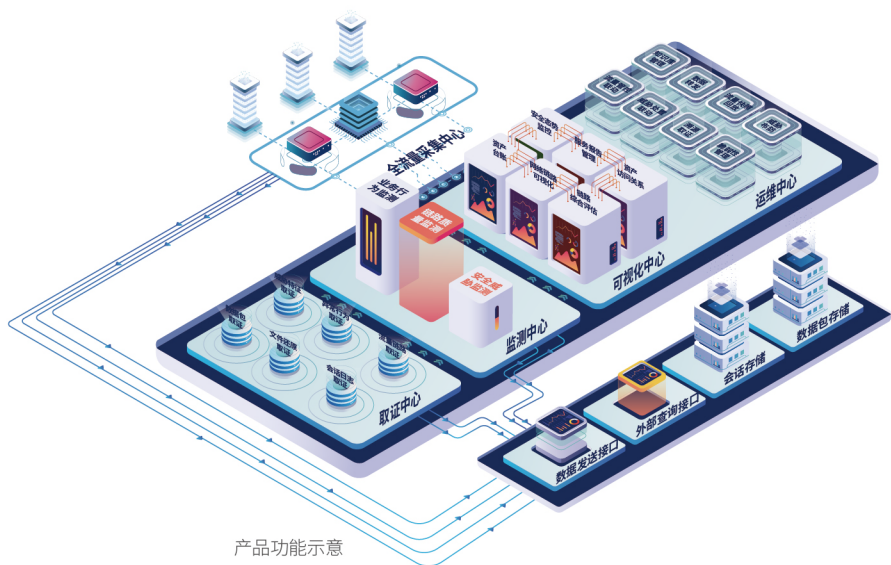
累计服务10000+政企客户

聚铭铭溯全流量 回溯取证系统 (iNTF)

聚铭网络
www.juminfo.com

聚铭铭溯全流量回溯取证系统

聚铭铭溯全流量回溯取证系统(iNTF)，以旁路方式接入网络，对网络流量数据全量接入、解析、检测、存储，具备对历史数据进行回溯取证能力，使网络分析突破时间的限制，当发生网络链路故障、业务访问异常、网络威胁等各类问题后，能够及时对故障发生时的网络链路指标、应用访问行为、网络安全事件上下文进行完整还原，从而定位问题根因，帮助用户解决网络中的各类问题。



产品功能示意



行业现状

① 安全检测类产品回溯取证能力缺失

- 安全设备误报多，每天成千上万条安全事件，缺乏价值数据，无法分析研判；
- 安全设备检测规则的滞后性，大量威胁难以及时发现，事后无法回溯验证。

② 多分支及业务扩容网络安全建设成本高

- 建设扩容，数据监测需要部署大量高性能探针，建设成本巨大；
- 分支机构数据回传，专线带宽也面临着巨大的挑战。

③ 链路质量问题，造成业务瘫痪，难以排障

- 互联网访问经常卡顿，网络故障难定位；
- 业务系统访问无响应，业务异常难诊断。

④ 故障人工处置，分秒必争

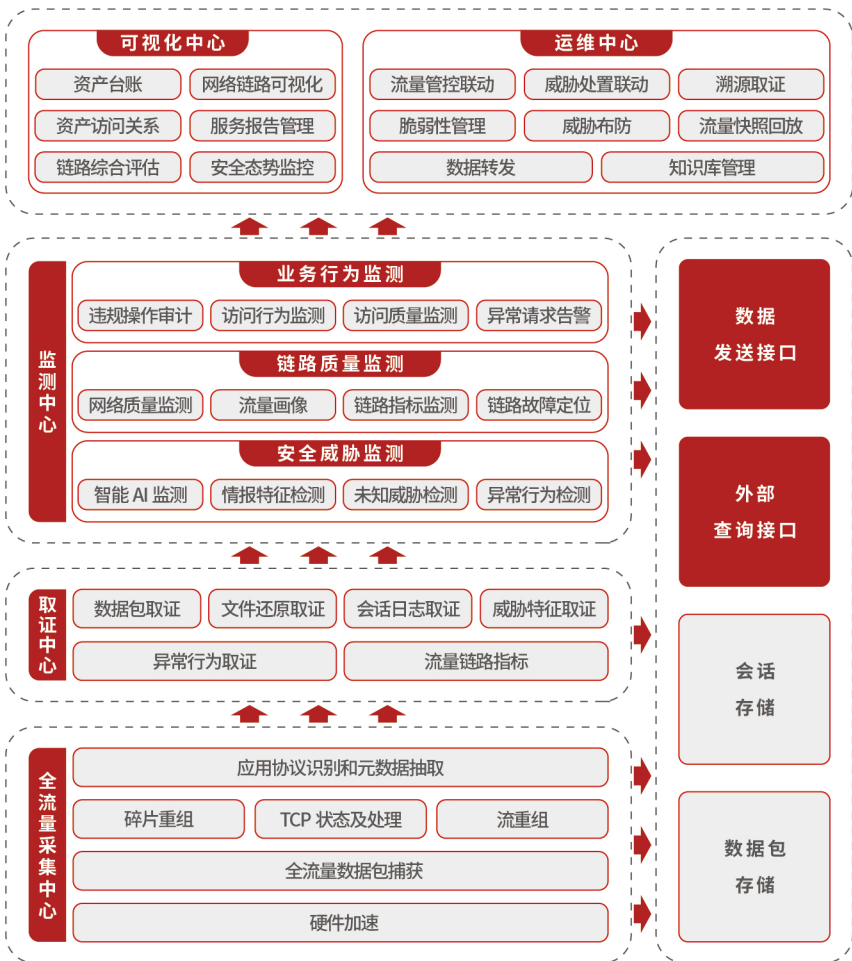
- 遭受网络威胁，难以及时阻断威胁扩散，容易造成数据泄露、勒索事故；
- 链路故障，难以及时流量管控，疏通链路瓶颈，造成业务长时间瘫痪。

⑤ 红蓝对抗及日常被监管通报压力大

- 家底不清、资产间的访问关系混乱，易被通报；
- 对抗期间被动挨打，无法回溯取证、反制阻断。



系统架构



核心功能



全流量采集
及精准解析



全流量
回溯及取证



实时
数据转发



业务故障监测
及智能自愈



资产及
服务测绘



产品优势



多维度流量快照，纵深检索，快速回溯及分析

系统针对流量数据进行分层快照，留存流量链路指标、威胁上下文、网络会话日志、还原文件、原始数据包多种维度数据，便于遇到故障时，多维度数据纵向关联分析，快速定位问题原因。



流量遥测汇聚及压缩技术，大幅降低安全设备建设成本

全量采集东西向网络流量，无需部署大量探针或代理，并对采集的流量进行清洗及裁剪，定向转发给其他安全设备，从而大幅降低安全设备建设成本、运维成本。



万能异构联动响应

不受第三方设备API限制，可智能化完成第三方设备的对接，实现阻断设备、流控设备联动，自动完成网络威胁、拥塞等故障治理。



弹性扩容，无带宽负担

通过分布式部署，对于新建分支机构、网络扩容等场景，增加分布式节点，节点自带独立分析能力，无需网络流量回传，不会对专网造成负担。



产品价值

NO.1 降低业务扩容对网络安全建设成本的负担

实时数据分发，对流量可筛选、压缩，减轻下游安全设备负载，无需大量建设探针，减少安全设备建设投入。

NO.2 异构共享，以流量数据价值，赋能原有安全基建

提供开放的 API、支持价值数据回放等多种方式为第三方异构设备提供原始数据服务，便于安全设备实现威胁取证、检测策略验证、攻击过程复盘等场景，提升自建安全生态整体能力。

NO.3 网络安全、链路排障及智能自愈，减轻人工压力

针对网络安全、链路故障，能够自动识别与抑制，通过联动异构设备，实现阻断、流控，及时解决链路及安全事故。

NO.4 满足新等保的合规要求

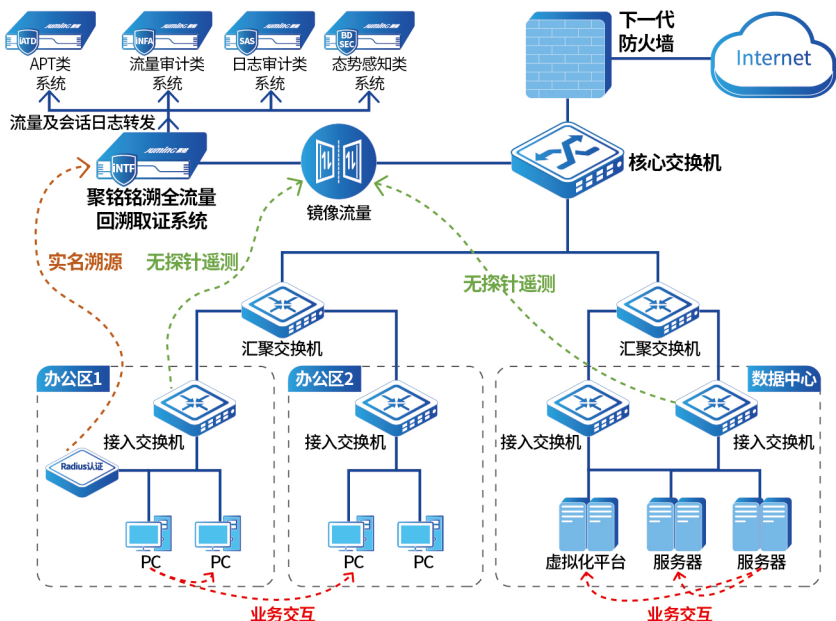
满足新等保 2.0 对网络攻击检测和分析要求。

6

部署方式

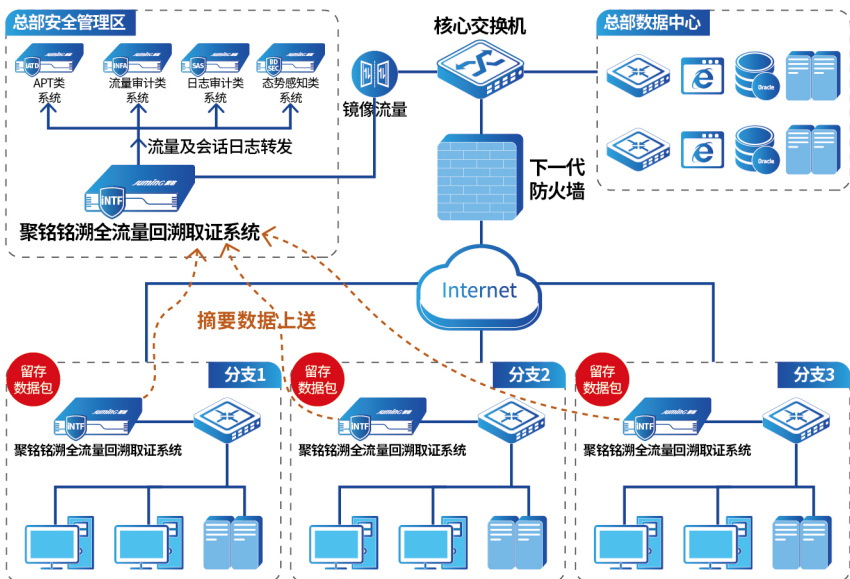
1、一体机部署

聚铭铭溯全流量回溯取证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），其中管理口与交换机或电脑相连，用于设备控制、系统访问等；监听口与交换机镜像口相连，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：



2、分布式部署

聚铭铭溯全流量回溯取证系统，对于需要进行分支机构统一管控的单位，可以在分支单位部署独立全流量回溯取证节点，无需通过专网进行网络流量回传，不会对专网造成负担。常规部署图如图所示：



聚铭 JuminG



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