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

聚铭网络流量智能分析审计系统

(iNFA)

聚铭网络

www.juminfo.com

聚铭网络流量智能分析审计系统

聚铭网络流量智能分析审计系统（简称：iNFA）是全流量智能化审计专家。该产品是以全流量还原为基础，结合失陷分析、网络攻击检测、威胁情报分析、异常流量行为挖掘、文件检测、网络质量检测等技术，对全网流量实时进行威胁感知、可疑流量分析，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

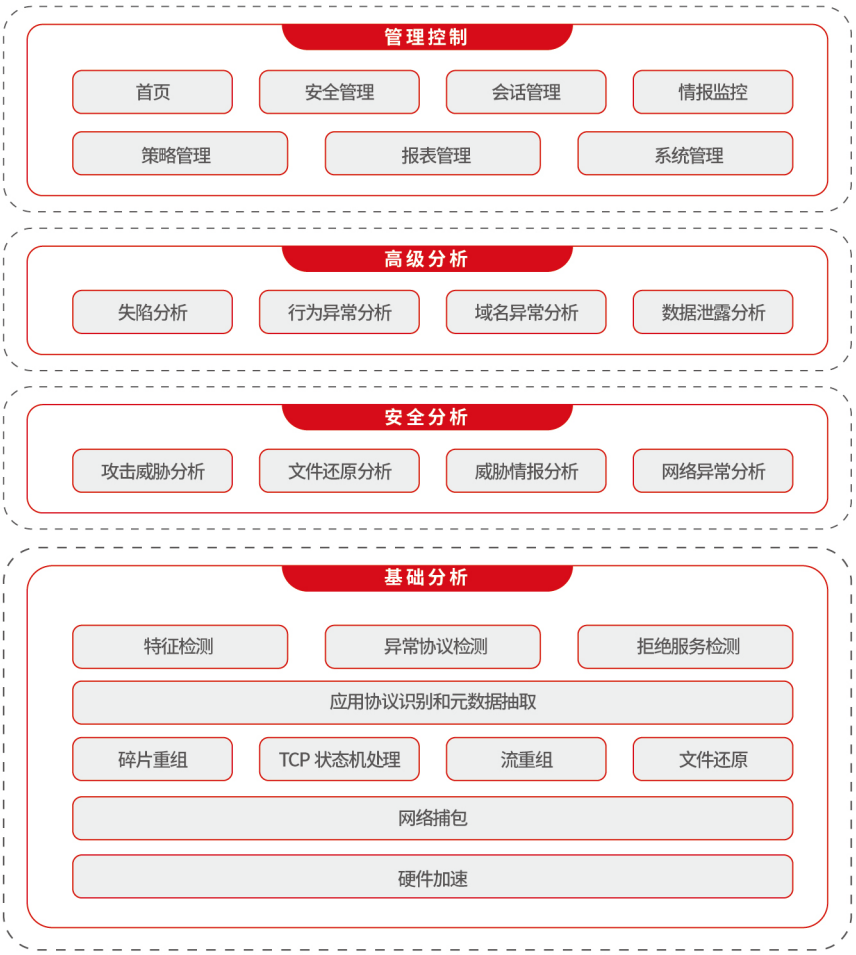
1 行业现状

信息化建设的同时，威胁总数和威胁形式不断增加，
威胁态势复杂多变，隐蔽能力强，难以发现和分析

1. 传统的安全设备及产品都是基于已知规则进行检测，无法应对未知的威胁
2. 传统的安全设备无法保存全流量数据，在入侵发生后，无法做到完整的溯源取证和损失评估
3. 达不到合规要求

现状分析

2 系统架构


管理控制
首页
安全管理
会话管理
情报监控
策略管理
报表管理
系统管理
高级分析
失陷分析
行为异常分析
域名异常分析
数据泄露分析
安全分析
攻击威胁分析
文件还原分析
威胁情报分析
网络异常分析
基础分析
特征检测
异常协议检测
拒绝服务检测
应用协议识别和元数据抽取
碎片重组
TCP 状态机处理
流重组
文件还原
网络捕包
硬件加速

3 核心功能


安全态势感知
威胁情报分析
威胁检测
安全事件分析
工控协议指令级深度解析
应用协议深度识别
网络会话分析

4 产品优势

全流量智能化审计

包括流量采集、数据分析、攻击检测、文件检测、威胁情报检测、异常行为检测等六大处理引擎，通过对全流量进行采集和分析，有效保证用户终端的安全。

混合精准情报

融合多家情报，提升情报的精准度。

灵活的部署方式

旁路SPAN及TAP部署方式，不改变用户现有网络架构和网络配置。

5 技术优势

网络全流量 实时采集匹配

iNFA采用零拷贝、全程无锁化技术处理网络流量数据包，而且充分利用CPU向量化指令，对各类模式进行识别或匹配，故即使在超大流量情况下，系统也能实时采集。

支持千余种应用协议解析

精确解析 HTTP、DNS、TLS、数据库、FTP、Telnet、邮件、即时通讯等千余种应用协议，同时对 Modbus、IEC、EthernetIP/CIP、OPC、OPCUA、MMS/S7Common 等工控协议实现了指令级解析。

AI 技术行为分析

采用AI技术及大数据技术，内置威胁样本数据，对应用协议所包含的源数据及识别后的会话数据实时留存、实时分析，挖掘可疑的流量行为，提升未知威胁检测效果。

内置威胁检测规则库

本地恶意特征检测规则 500W+；漏洞利用检测规则 4000+；Web 应用检测规则 5000+。

文件静态检测搭配动态行为分析

文件静态检测：防病毒检测、威胁情报检测、防泄密检测。文件动态检测：注册表分析、进程分析、网络分析、恶意释放文件等。支持提取攻击的完整样本，并提供样本的下载能力。

失陷定性分析

通过安全情报技术、大数据技术、AI技术进行安全分析，结合Kill-Chain理论对失陷主机进行定性分析，还原完整攻击轨迹，极大提升运维效率。

6 产品价值

NO.1

可有效检测外部攻击、外连威胁、内部非法连接、网络会话模式异常等安全威胁，全面提示企事业单位安全防御水平。

NO.2

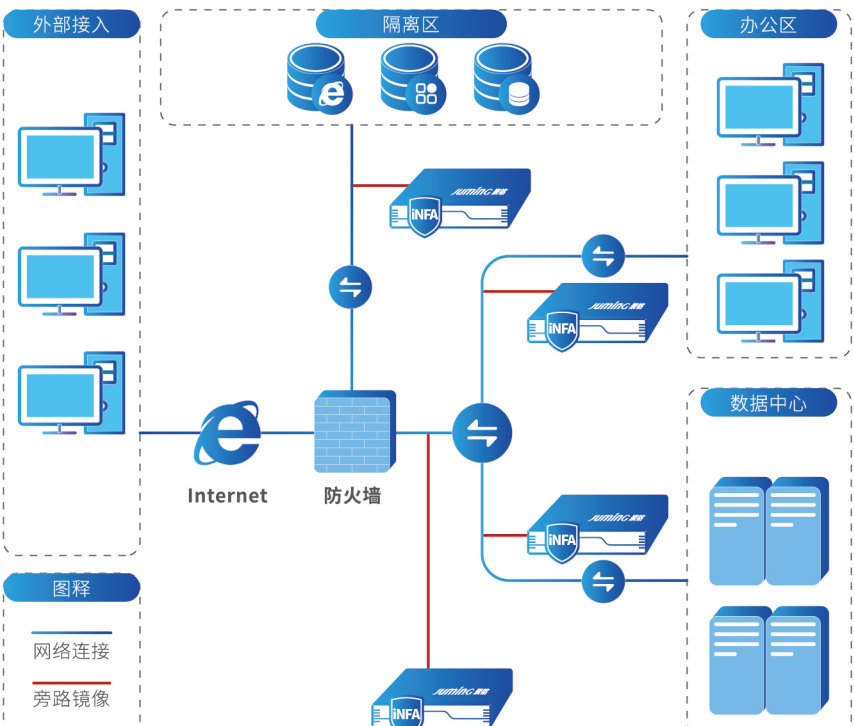
入侵行为发生后，通过大数据检索技术可以快速进行精准溯源分析，为客户实施安全加固提供有力的策略支撑。

NO.3

满足《网络安全法》、等保2.0等法律法规对安全合规的要求。

1 部署方式

聚铭网络流量智能分析审计系统(iNFA)采用旁路 SPAN 部署方式和 TAP 部署方式，两种部署方式均不会改变用户现有网络架构和网络配置，且不会对用户现有的生产业务或应用产生任何影响；设备部署的示意图如下：



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】【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】

北京总部：北京市海淀区丹棱街18号创富大厦9层
南京总部：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：010-82666399 / 025-52205520　　传真：010-82669679 / 025-52205565
全国统一服务热线：400-1158-400　　公司官网：www.juminfo.com