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

聚铭威胁检测系统
(TDS)

聚铭网络
www.juminfo.com

聚铭威胁检测系统

聚铭威胁检测系统具有国际领先的威胁检测引擎，支持包括扫描探测、拒绝服务攻击、漏洞利用、WEB 攻击、SQL 注入等入侵威胁检测；支持包括游戏、P2P、广告、炒股等违规通信检测；支持包括木马、矿机、勒索软件在内的恶意软件通信检测；结合高精准 IOC 智能检测技术与 CTI 主动溯源追踪技术，对潜在网络威胁进行猎捕溯源；另外系统内置了基于 Kill-Chain 技术的失陷分析、网络威胁态势感知两大安全分析模型，帮助用户聚焦网络威胁点，大大降低安全运维成本。聚铭威胁检测系统是企业提升网络威胁检测水平的有力武器。同时，也是满足国家等保测评、网络安全法及行业安全规范的最佳解决方案。

产品功能示意

行业现状

企业内部系统安全问题容易被忽略，无法适应当前日益严峻的安全形势。

大多安全产品基于已知规则库进行检测，对被加密或者被做了免杀处理的数据无能为力。

现状分析

1 2 3 4

威胁攻击手段日益复杂多变，隐蔽能力强，难以发现和分析。

达不到合规性要求。

2 系统架构

管理控制

首页 | 威胁分析 | 会话分析

策略管理 | 报表管理 | 系统管理

高级分析

失陷分析 | 网络威胁态势感知 | 情报溯源

威胁检测

攻击威胁检测 | 违规通信检测 | 威胁情报检测 | 网络质量检测

基础接入

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

网络捕包

硬件加速

3 核心功能

- 网络攻击检测
- 违规通信检测
- 恶意软件通讯检测
- 威胁情报分析
- 失陷分析
- 网络威胁态势感知分析

4 产品优势

混合精准情报

融合多家情报，提升情报的精准度。

全面的威胁检测

包括漏洞利用、WEB攻击、SQL注入等入侵威胁检测，游戏、P2P、广告、炒股等违规通信检测，木马、矿机、勒索软件在内的恶意软件通信检测。

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。

联动响应

联动手段多样，包括阻断、取证等，提升处置效率，降低人工投入。

5 技术优势

高速的网络抓包及模式匹配技术

TDS有独有的智能协议识别技术，可高速、准确识别上千种应用，检测各种协议伪装行为。系统可充分利用CPU向量化指令对各类模式进行识别匹配，保证整体处理无延迟。

精准多样的攻击检测规则

TDS内置多种网络攻击检测策略，可对一般网络攻击、明文传输、过期系统或软件、木马、隐蔽通道、电子加密货币活动、勒索软件、数据库攻击等进行精准检测。

及时精准的威胁情报

TDS能够实时检测僵尸网络、C&C节点、木马回连、垃圾邮件、钓鱼节点、扫描节点、恶意软件等威胁IP、URL、文件HASH，并支持情报详情的追踪溯源，精准呈现威胁情报详细信息。

全面、精准分析

在安全情报、大数据技术、AI技术进行安全分析的基础上，结合Kill-Chain技术实时精准发现资产安全失陷，除此之外还包括统计分析、行为关联分析、溯源分析等。

6 产品价值

NO.1

全面检测感知各类网络攻击、违规通信、恶意连接等威胁并及时响应处理，保障信息系统安全运行。

NO.2

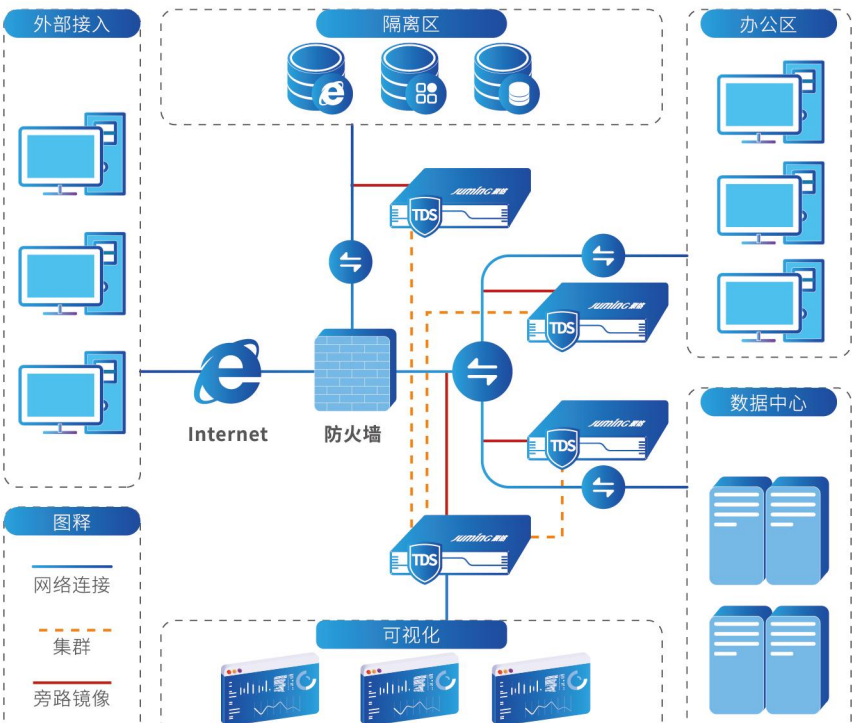
将安全问题聚焦于设备，减少运维工作量。

NO.3

满足《网络安全法》、等保2.0等法律法规对网络数据审计的要求。

部署方式

系统采用旁路 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。



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