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

聚铭综合日志分析系统
(SAS)

聚铭网络
www.juminfo.com

聚铭综合日志分析系统

聚铭综合日志分析系统是聚铭网络以大数据、机器学习技术为核心研发的智能化综合日志分析系统。系统通过三大网络日志分析引擎以及四种流量安全分析策略，为客户打造两大安全分析体系，满足企业对信息安全事件“可发现”、“可处理”、“可审计”、“可度量”的需求。

产品功能示意

1 行业现状

企业网络上部署了多种设备，各设备产生的信息分散，难以全面集中采集并保存

设备产生的原始信息数量庞大，人工处理难以从海量事件中发现潜在问题

分散的设备及系统难以实施集中监控，缺乏统一、可定制的审计告警策略

审计手段落后，自动化程度低，缺乏对多种来源的日志进行关联分析的能力

不能满足最新的法律法规行业要求

2 系统架构

3 核心功能

采集管理　数据识别　过滤归并　实时监控

事件分析　审计管理　告警监控　资产管理

4 产品优势

高实用性

各类日志集中分析挖掘，能实时解析安全日志中IP归属信息，实时监控安全事件并告警安全异常，能支持等保、萨班斯审计合规落地。

高便捷性

系统无需代理程序，资产自动发现，报表自动发送且种类丰富。系统内置多种合规审计策略模板，可定制展示内容，进行可视化地图展示。

高适应性

系统支持IPV6，支持每日上亿条原始日志的分析处理，支持非主流日志的定制化解析，支持多种网络部署方式，系统架构易扩展，满足用户个性化需求。

5 技术优势

全面的采集能力

采集能力全面覆盖各种操作系统、应用系统、网络设备、安全设备，通过 API、协议、文件、SFTP、SNMP Trap、镜像流量等多种方式接入全平台数据，智能地进行数据解析并整合。系统支持 syslog、SNMP Trap 文件、WMI、SMB、文件上传、Netflow、插件接入（定制开发）等多种灵活接入方式。

高效的实时分析

支持基于规则、基于统计、基于情报的分析模型。内置丰富的安全监控场景模板，如堡垒机绕行审计、异常登录时间审计、异常流量审计等。系统采用流式分析模式，实时分析接入的海量日志，每秒可处理百万条以上的日志，实时挖掘潜在威胁。

精准的溯源定位

系统内置全球地理信息库，准确、高效地定位威胁来源，提供用户实时的全球攻击溯源展现。

丰富的合规模板

系统默认提供等级保护三级、SOX 法案的分类，提供对主机、应用、网络安全等多个层面的报表实例。

丰富的策略模型

经过长时间在电信、医疗、高校、政府等行业的应用，积累了丰富有效的安全策略场景模型，包含异常行为分析类、业务攻击分析类、流量统计类等。

强大的检索查询

亿级（TB）原始日志查询耗时低于 1 秒。

6 产品价值

NO.1

满足用户日常信息安全管理的需求，从纷繁复杂的日志中萃取出最具价值的部分，提高安全管理运维效率。

NO.2

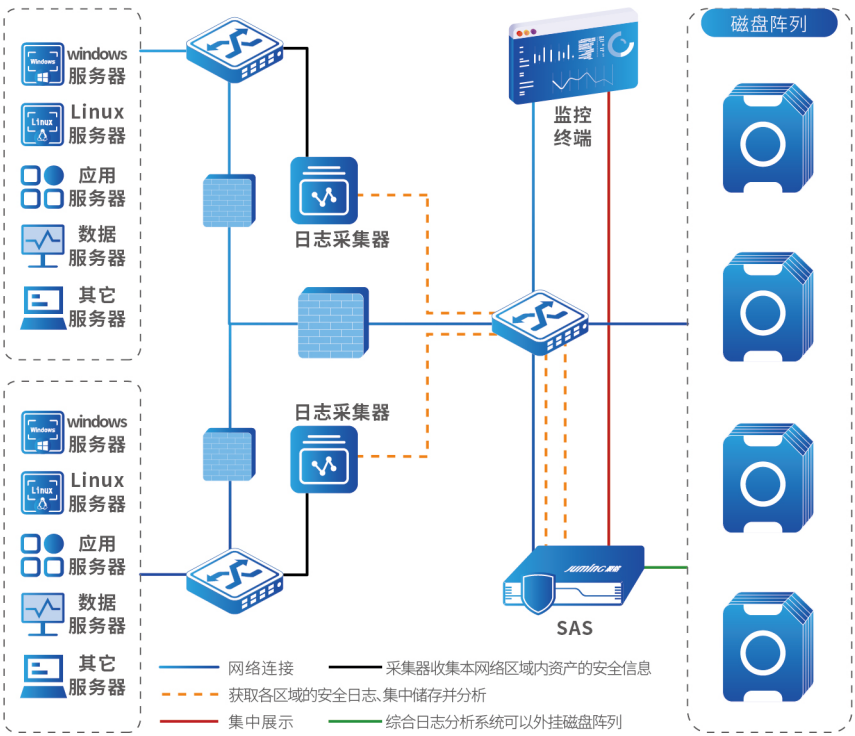
助力建设完整的安全技术保障体系，通过全面分析，及时发现安全隐患并给予告警，避免安全事件的发生。

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。

部署方式

聚铭综合日志分析系统支持单机部署及分布式部署



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