聚铭威胁检测系统

产品白皮书

聚铭网络科技有限公司

2023 年 11 月

目录

声明

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

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：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：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

前言

随着企业信息化的不断深入，企业信息化应用及业务种类日益丰富，网络中承载的数据量逐年增大。与此同时，网络攻击成本逐步下降，网络攻击手法更加复杂多变，网络攻击逐渐组织化、专业化。对于企业而言，复杂的网络攻击行为阻碍了企业的健康发展，因此对网络流量的深度分析，从而全面掌控网络中的流量，对于企业来说越来越必要。

目前企业网络安全面临巨大的困境，主要包括：

1. 企业落后的边界隔离理念 VS 攻击者灵活多变的渗透技术

2. 安全设备日益臃肿的攻击特征库 VS 攻击者智能化的攻击工具

3. 一片祥和的监控页面 VS 暗流涌动的隐蔽信道

只重视边界的防护，而忽视内部系统安全问题的传统观念已经无法适应当前日益严峻的安全形势；没有安全事件和告警不等于没有被攻击者盯上和攻击。

企业虽然购置了大量安全设备及产品（防火墙、入侵检测、安全网关、杀毒软件、反垃圾邮件），但这些产品大都是基于已知规则库进行监测，可检测出已知安全威胁，如果数据被加密或者被做了免杀处理，则无能为力；然而新型未知威胁的攻击手段越来越老练，在单个时间点无明显特征，隐蔽能力强，攻击渠道不确定，攻击空间路径不确定，长持续性，传统基于特征的分析手段难以发现和分析。

1.客户需求

随着网络信息技术的飞速发展，安全威胁也日益受到关注，攻击手段千变万化，对于企业来说，面临着巨大的考验，其中包括：攻击手段多样，例如扫描探测、拒绝服务攻击、漏洞利用、暴力破解；内部恶意文件猖獗，例如勒索软件、挖矿软件、间谍软件等；网络资源滥用，包括 P2P 软件、聊天工具、游戏软件、炒股软件、广告软件等；

然而，现实中安全问题远远不止上述部分，新的网络威胁，不断升级。聚铭威胁检测系统，采用全新的检测技术，丰富的分析模型，为用户提供精准的网络威胁检测。

2.解决方案

聚铭威胁检测系统是南京聚铭网络科技有限公司研发的具有自主知识产权的专业网络流量分析审计系统，它是一款以全流量分析为基础，结合失陷分析、网络威胁态势感知、网络攻击检测、威胁情报检测、网络质量检测、内部攻击检测、未知威胁检测等技术，对全网流量实时进行威胁分析，为客户受到网络威胁时，及时察觉，及时止损。

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。

2.1.产品价值

1. 发现网络攻击行为，能够识别扫描探测、拒绝服务攻击、漏洞利用、暴力破解、WEB 攻击、混杂攻击、SQL 注入、ShellCode、钓鱼等。
2. 发现恶意软件流量，能够识别包括勒索软件、挖矿软件、间谍软件、移动恶意软件。
3. 发现企业违规行为，例如使用 P2P 软件、聊天工具、游戏软件、炒股软件、广告软件、远程连接等；发现浏览色情、暴力信息等；发现企业隐私信息泄漏等。
4. 通过失陷分析，帮助用户把安全问题聚焦于设备，减少运维工作量。
5. 流量数据可视化，将威胁流量还原，并呈现应用的关键数据。
6. 可满足如等级保护 2.0、《中华人民共和国网络安全法》等法律、法规对于入侵检测、网络数据审计的要求。

2.2.产品架构

聚铭威胁检测系统主要包括如下模块：

系统采用零拷贝技术，实现高速流量接入。实时进行会话重建、协议识别、网络威胁检测等功能。

2.3. 主要功能

2.3.1. 全流量采集深度包解析

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，也能保证系统整体处理无延时；独有的智能协议识别技术，可高速、准确地识别上千种应用，检测各种协议伪装行为；支持 HTTP、TLS、SMTP、POP3、IMAP、FTP、SMB、RDP、SSH、Telnet 等应用协议的精准解码、元数据提取及存储、搜索、统计功能。

2.3.2. 网络攻击检测

内置多种网络攻击检测策略，支持对一般扫描探测、拒绝服务攻击、漏洞利用、暴力破解、WEB 攻击、混杂攻击、SQL 注入、ShellCode、钓鱼、隐蔽通道等进行检测。

2.3.3. 恶意软件检测

支持发现网络中勒索软件、挖矿软件、间谍软件、移动恶意软件等通讯行

为。

2.3.4. 威胁情报检测

支持僵尸网络、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 的实时检测。

2.3.5. 违规通信检测

支持发现 P2P 软件、聊天工具、游戏软件、炒股软件、广告软件、远程连接等软件通讯。支持发现色情、暴力等信息传播。支持企业隐私数据泄漏检测。

2.3.6. 网络质量检测

支持网络带宽占用异常检测、小包攻击、泛洪攻击、ARP 风暴、ICMP Flood、TCP 建连时延过长、TCP 重传过多、TCP 零窗口过多等常见的网络通讯质量问题检测，同时网络性能监控还能支持用户针对历史网络质量情况进行溯源分析。

2.3.7. 未知威胁联动分析

实现从 HTTP、邮件、SMB、FTP、QQ 等协议中还原文件，并对文件进行黑名单检测、敏感词检测，不仅能够发现恶意软件，还能够检测客户的核心数据外泄。

除此之外还支持未知威胁文件的识别。基于启发式静态文件扫描技术的恶意文件识别；基于虚拟仿真环境动态文件扫描技术的文件威胁行为检测。

2.3.8. 失陷分析

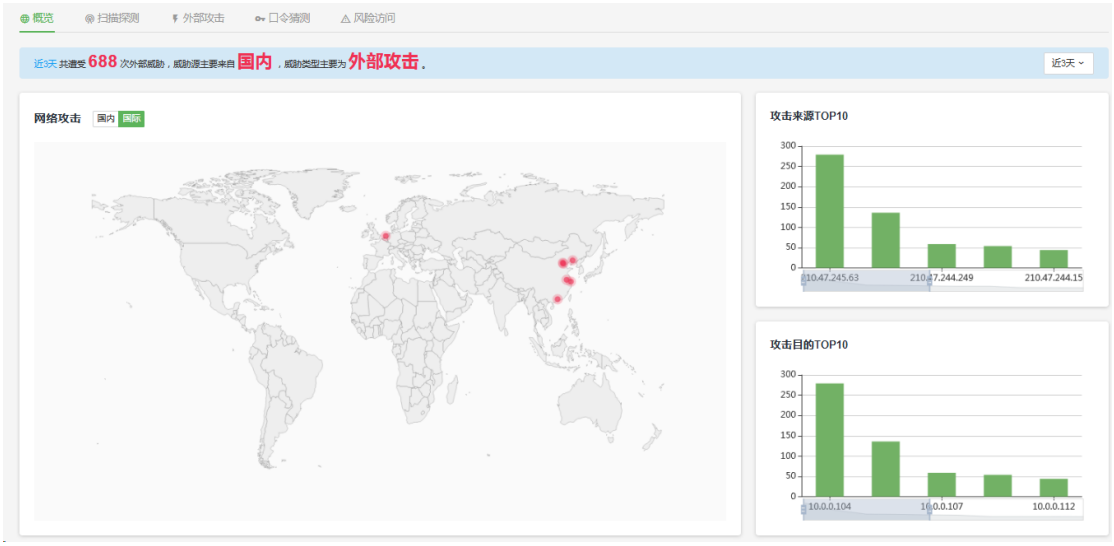
在利用安全情报技术、大数据技术、AI 技术进行安全分析的基础上，结合 Kill-Chain 技术实时发现资产安全失陷情况，并支持分析溯源，详细展示各个失

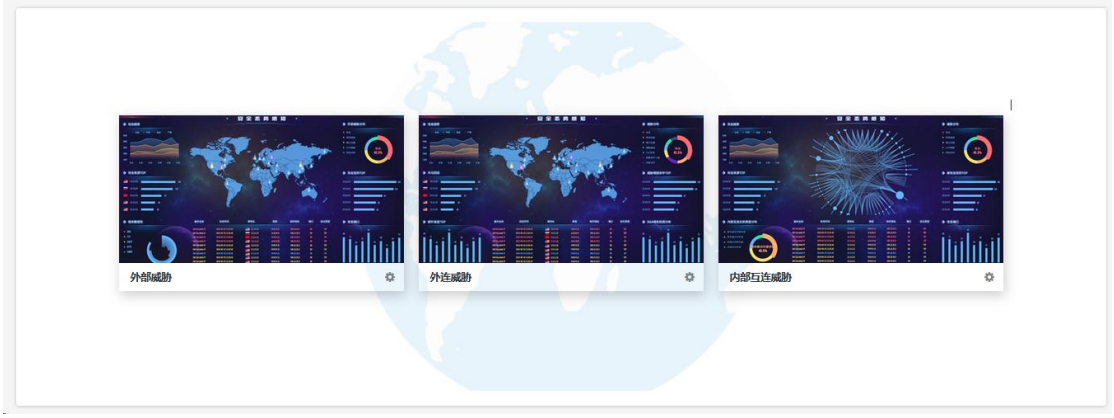
陷阶段的具体安全事件与原因；让运维人员摆脱海量安全事件、告警的困扰，聚焦问题所在，极大提升运维效率。

使用黄金眼功能对失陷主机进行举证分析，支持对失陷主机的外部威胁、外连威胁、内部主动威胁、内部被动威胁以及失陷主机开放端口服务进行全面分析，使客户更容易理解主机失陷的根本原因，以及如何进行威胁处置及安全加固防护。

2.3.9. 网络威胁态势感知分析

综合外部威胁、外连威胁、内部互连威胁三个方向全面监控网络威胁态势感知情况，关注扫描探测、外部攻击、口令猜测、C&C 回连、恶意程序活动等网络威胁行为，并支持大屏投放监控。





2.3.10. 云端威胁情报溯源

支持情报详情追踪溯源，支持恶意 IP、恶意域名、恶意 URL、恶意文件溯源查询，呈现威胁情报详细信息，包含情报历程、恶意标签、相关事件、相关样本等。

2.4. 部署方案

聚铭威胁检测系统采用旁路 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。

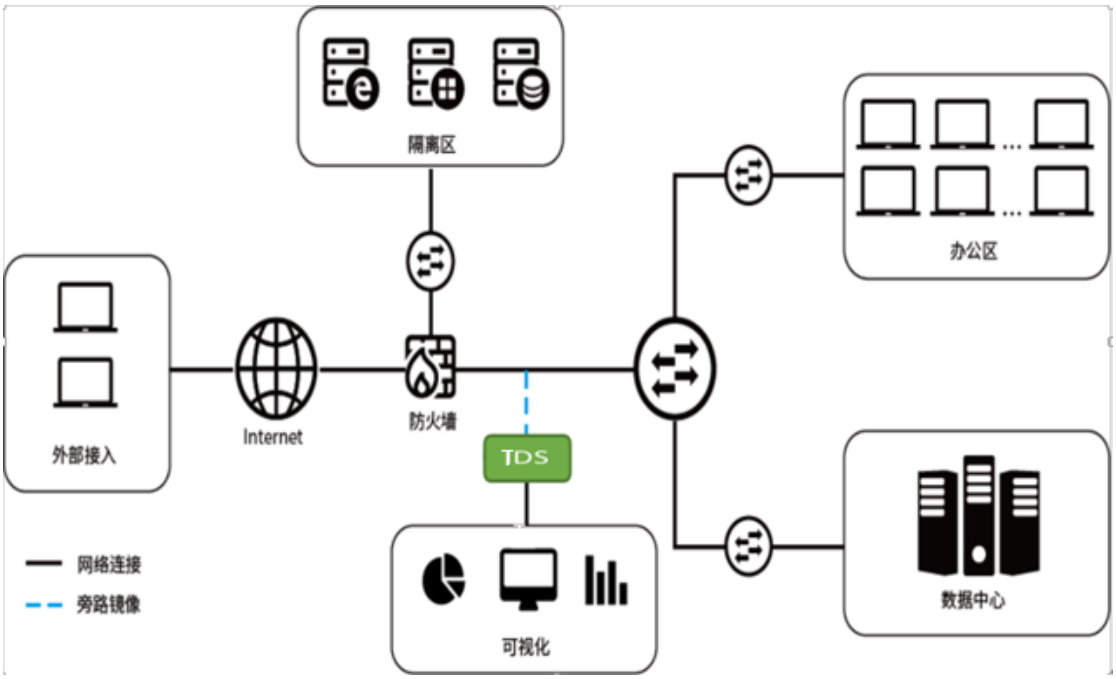
2.4.1. 单机部署方案

单机部署方案可以帮助用户及时有效的发现网络中的异常情况，提升运维人员对安全问题处置效率，为客户在高级威胁入侵时，及时察觉，及时止损。

此方案能够解决如下安全问题

1. 全流量采集、分析、恶意流量会话存储及检索，为安全回溯提供强大的支撑。
2. 发现网络威胁，包含常规网络攻击及未知威胁检测。
3. 发现网络中异常流量、端口。

4. 发现恶意文件及数据泄漏。

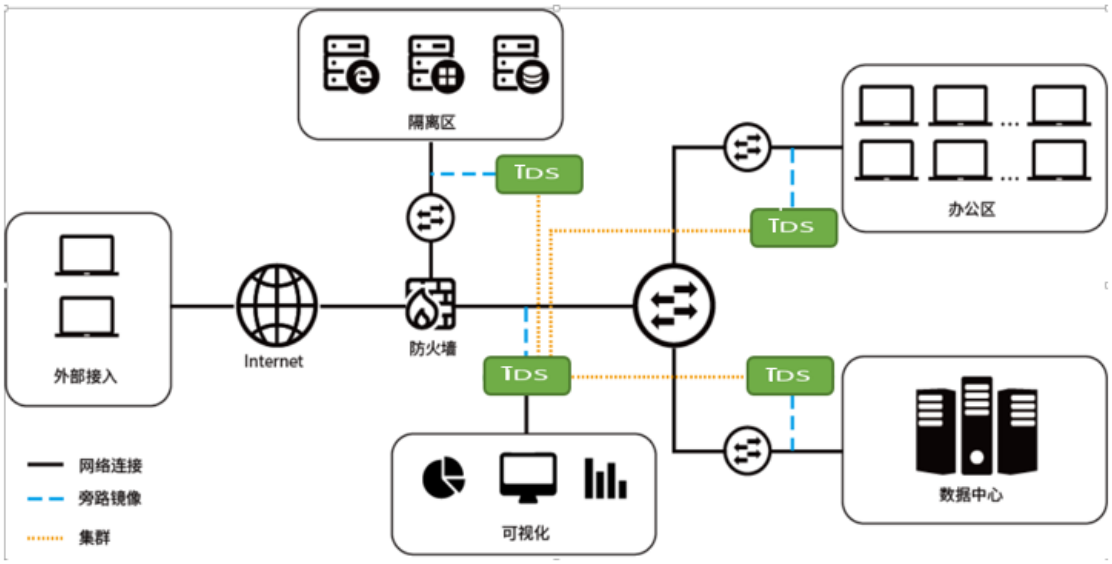


2.4.2. 集群部署方案

集群部署方案，是为了解决流量大、多点部署等问题。该方案可以帮助用户在大流量的情况下及时有效的发现网络中的异常情况，提升运维人员对安全问题处置效率，为客户在高级威胁入侵时，及时察觉，及时止损。

此方案能够解决如下安全问题

1. 全流量采集、分析、会话存储及检索，为安全回溯提供强大的支撑。
2. 发现网络威胁，包含常规网络攻击及未知威胁检测。
3. 发现网络中异常流量、端口。
4. 发现恶意文件及数据泄漏。


隔离区
TDS
办公区
TDS
外部接入
Internet
防火墙
TDS
TDS
网络连接
旁路镜像
集群
可视化
数据中心