聚铭恶意外连智能检测及治理系统产品白皮书

聚铭网络科技有限公司

2026 年 7 月

目录

声明

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

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

比特币是一种 P2P 形式的数字的加密虚拟货币。点对点的传输意味着一个去中心化的支付系统。与所有的货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个 P2P 网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。由于比特币不是法定货币，且交易存在较大风险，自 2013 年以来，国家有关部门对比特币进行了有效的管控，并出台了相应的政策和法规。

基于目前比特币等虚拟货币存在着大量的商业价值，市场上许多黑客和不法分子通过植入后门等途径，非法利用第三方计算机资源进行挖矿行为。目前国内很多数据中心、办公电脑成为了很多不法分子挖矿的资源。为更好净化网络环境和节能减排，需对数据中心出口、网络边界出口进行流量监控和分析，发现非法挖矿应用，并对相关应用进行有效的阻断，从而保障服务器、办公电脑等资产不被侵占。

1.客户需求

随着网络信息技术的飞速发展，虚拟货币挖矿也日益受到社会大众各方面的关注，对于政府和企业来说，主要有以下三点危害：

1、 挖矿活动需要通过专用矿机计算，产生的能源消耗和碳排放量大，对产业发展、科技进步不具有积极的带动作用，导致电力资源的大量耗费，还可能被增加惩罚性电价；

2、 以挖矿产生的虚拟货币促使了网络黑产快速升级，变相滋生了各种网络犯罪，如勒索病毒往往都和虚拟货币关联在一起，时刻威胁着网络环境；

3、 参与挖矿的设备，因其设备资源，如 CPU、GPU、存储等长期处于高负荷运转状态，会加速其老化，减少其使用年限，带来严重的经济损失和安全威胁。

然后，现实中安全问题远远不止上述部分，挖矿手段不断的更新迭代会对网络环境带来更多威胁。聚铭恶意外连智能检测及治理系统，基于全流量还原及威胁情报碰撞能精准定位挖矿行为，内置丰富的阻断策略，为用户提供精准的挖矿行为检测及阻断。

2.解决方案

聚铭恶意外连智能检测及治理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挖矿阻断智能防护系统，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、内部攻击检测等技术，对全网流量实时进行威胁分析，为客户受到挖矿行为等网络威胁时，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. 通过针对流量特征检测基础上快速识别矿池登录行为，定位挖矿主机；通过威胁情报的碰撞可在挖矿早期识别矿池连接行为，精准定位挖矿；
2. 挖矿在线动态阻断策略，在不影响正常业务的前提下，仅阻断与挖矿相关请求，对挖矿流量实现动态阻断；
3. 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。
4. 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。
5. 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。
6. 流量数据可视化，将威胁流量还原，并呈现应用的关键数据。
7. 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

聚铭恶意外连智能检测及治理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. 挖矿检测及在线阻断

通过在全流量还原基础上通过对异常流量特征化，落地形成检测特征，实时监控不断提取攻击特征，确保及时检测到攻击行为；通过自动学习历史流量访问信息，建立异常流量检测模型，挖掘潜在的未知挖矿信息；等一系列手段实现对挖矿行为的在线拦截，且从阻断方式上是采用在线动态阻断进行拦截，能做到在不影响正常业务请求前提下完成挖矿行为；挖矿阻断能力上能做到 100%阻断成功率，并且将阻断动作在客户内网实现，真正做到挖矿流量不出网。

且支持与多品牌设备联动，对挖矿流量进行阻断，避免威胁进一步扩散。

2.3.2. 互联网风险暴露测绘

基于实时流量动态测绘客户网络环境中对互联网暴露的服务器 IP、端口、应用服务、版本以及存在的漏洞，用户可以指定风险暴露测绘的地址范围，并通过主机视角和漏洞视角查看风险测绘结果，相比漏扫设备，流量产品基于实时的流量进行测绘，实时性更高，针对性更强。

2.3.3. 僵木蠕、勒索、钓鱼等多威胁阻断

在聚铭混合高精准情报引擎的加持下，基于请求域名与情报库实时进行威胁情报碰撞，安全域名稳定高效解析，如若检测到恶意域名直接拦截实现安全防护。在挖矿阻断基础上，可更全面、更精准实时检测并阻断诸如僵尸网络、木马软件、勒索软件、钓鱼站点等恶意请求。在全面防护基础上实现检测、拦截、定位、取证全流程闭环。

2.3.4. 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。

2.3.5. 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。

2.3.6. 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。

2.3.7. 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。

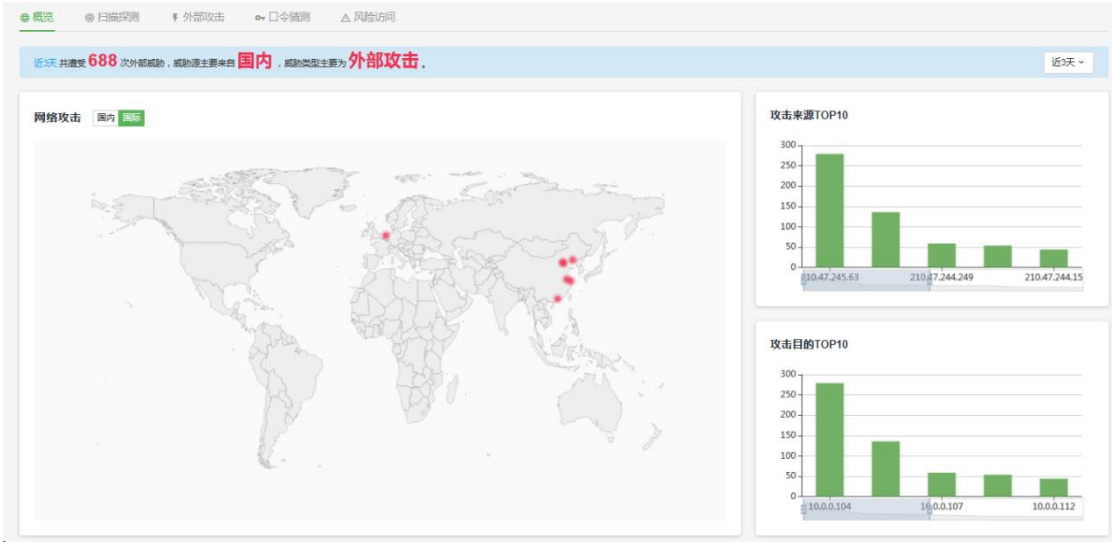
2.3.8. 失陷分析

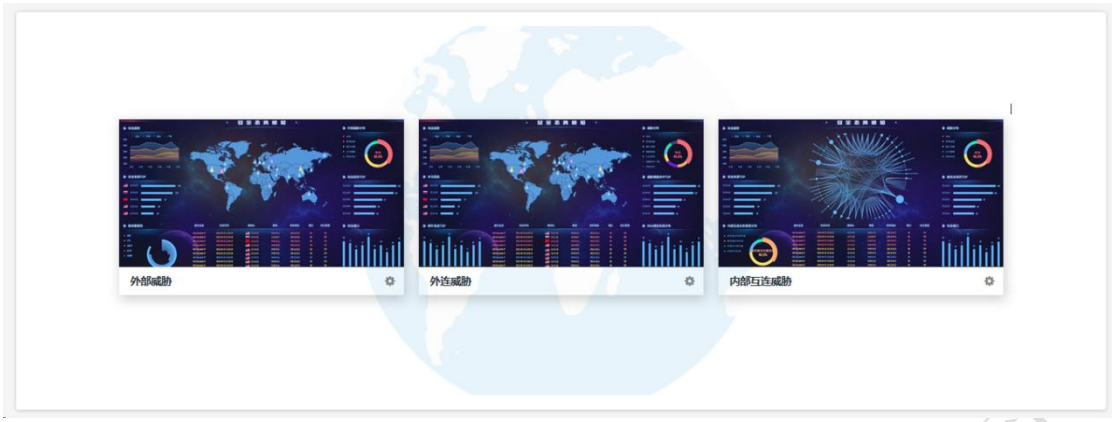
在利用安全情报技术、大数据技术、AI 技术进行安全分析的基础上，结合 Kill-Chain 技术实时发现资产安全失陷情况，并支持分析溯源，详细展示各个失陷阶段的具体安全事件与原因；让运维人员摆脱海量安全事件、告警的困扰，聚焦问题所在，极大提升运维效率。

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. DNS 穿透精准溯源

利用独有的 DNS 代理穿透技术，从 DNS 解码错误、解析失败、解析超时、威胁情报、DGA 域名、隐蔽通道等维度对 DNS 协议进行全面系统的检测和展现，并在全流量还原分析基础上通过对流量特征进行检测，以及 AI 加密流量分析引擎等技术，发现主机横向渗透与失陷破坏行为，精准定位真实失陷主机，完整还原攻击链条，彻底解决 DNS 代理误报导致的用户溯源定位难问题，提升取证溯源效率，协助用户缩短 MTTD（平均检测时间）与 MTTR（平均响应时间），极大提升企业整体的安全运营能力与运维效率。

2.3.11. 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

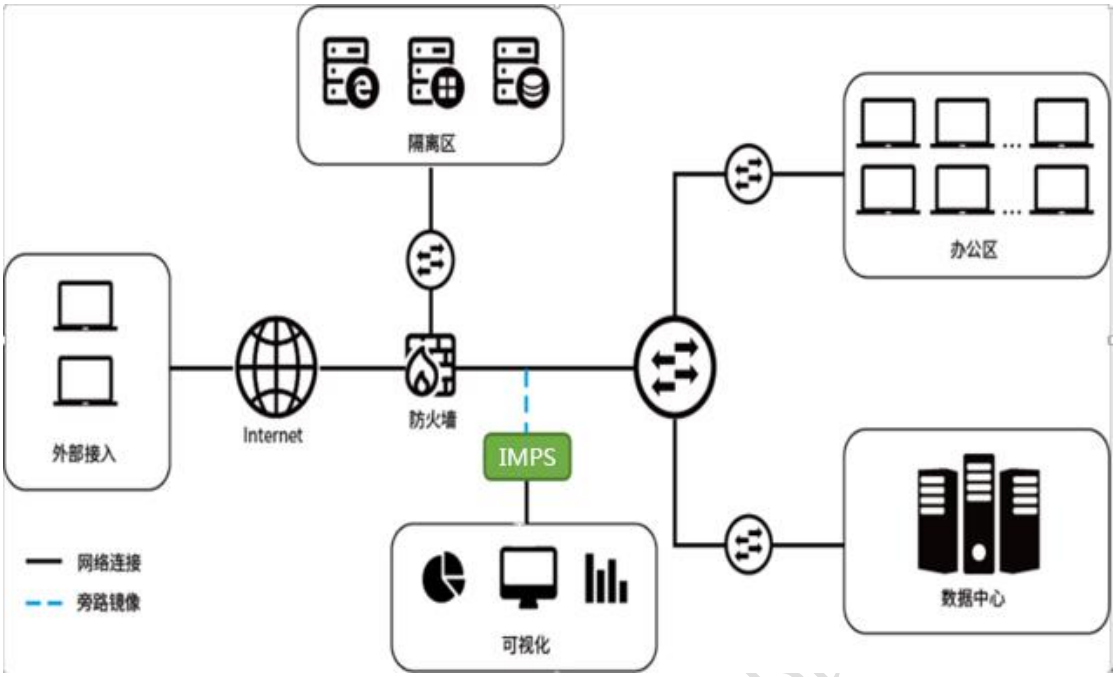
聚铭恶意外连智能检测及治理系统采用旁路 SPAN 部署方式和 TAP 部署方式，两种部署方式均不会改变用户现有网络架构和网络配置，且不会对用户现有的生产业务或应用产生任何影响。

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。

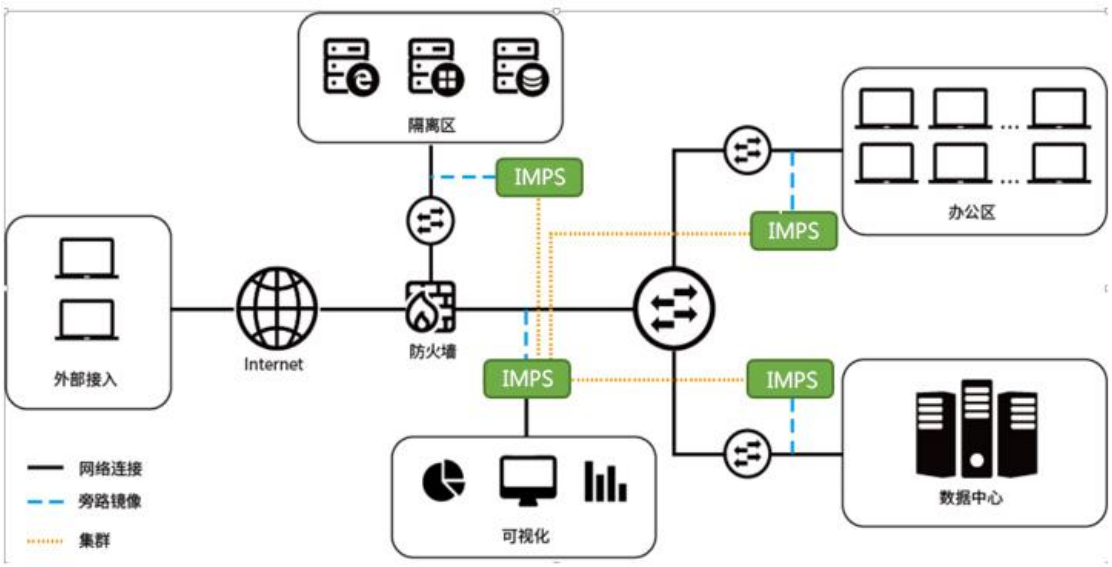


2.4.2. 集群部署方案

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