聚铭铭溯全流量回溯取证

产品白皮书

聚铭网络科技有限公司

2026 年 07 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

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。

1. 建设背景

随着网络技术的快速发展，高级威胁层出不穷。黑客攻击、恶意软件、数据泄露等事件频繁发生，对组织机构的正常运营和个人隐私的保护带来了巨大挑战。面对日益复杂的网络安全形势，如各种高级持续性威胁（APT）、0day 攻击以及其他形式的网络犯罪活动。许多国家和地区都出台了相关的法规政策，要求组织机构加强网络安全管理，采取必要的技术手段来保护网络数据和信息安全，如《中华人民共和国网络安全法》等，这些法规要求企业必须对网络活动进行记录和审计。

- **网络安全威胁的增长**

多样化的攻击手段：网络攻击手段日益多样化，包括木马通讯、隐蔽信道、异常 DNS 解析等，这些手段往往难以被传统安全设备检测出来。

复杂性增加：网络攻击的复杂性不断增加，攻击者采用加密、混淆等技术手段，使得安全事件的识别和追踪更加困难。

- **大数据环境下的安全挑战**

海量数据处理：随着大数据技术的应用，网络流量和数据量激增，对安全事件的分析和处理提出了更高的要求。

高速网络环境：在高速网络环境下，传统的安全设备难以实时处理大规模的网络流量，需要更高效的解决方案。

- **法律法规的要求**

合规性需求：随着信息安全相关法律法规的出台，企业需要遵守严格的数据保护和隐私保护规定，对安全事件进行有效的记录和取证成为法律合规的必要条件。

责任界定：在网络安全事件发生时，能够准确溯源和取证是界定责任和止损的关键。

- **企业对网络安全意识的提高**

风险管理：企业对网络安全的重视程度不断提高，对于潜在的网络威胁需要进行有效的管理和风险控制。

安全投资增加：企业愿意投入更多资源用于网络安全建设，以提高信息系统的安全性和可靠性。

2. 建设需求

安全建设不仅要对网络中全部流量的采集和分析，来追踪和识别潜在的安全威胁和攻击行为，同时要满足合规要求。对网络流量数据全量接入、解析、检测、存储，具备对历史数据进行回溯取证能力，使网络分析突破时间的限制，当发生网络质量、业务性能、网络安全等各类故障后，能够及时对故障发生时的网络链路指标、应用性能指标、网络安全事件上下文进行完整还原，从而定位问题根因，帮助用户解决网络中的各类问题。

2.1. 等保建设需求

- 网络行为分析：网络行为分析需要能够完整记录网络中的所有行为， 再基于网络行为进行分析，发现网络中异常流量、异常访问、异常连接等行为。
- 网络流量回溯：针对网络中出现 APT 攻击，需要通过全流量威胁取证分析，因此也离不开全流量产品做数据支撑。
- 未知新型网络攻击：针对未知的新型攻击的分析，传统安全设备难以发现，需要通过全流量存储，按需进行回放挖掘潜在未知威胁。

2.2. HW 及监管通报需求

- 资产不清晰：家底不清、资产间的访问关系不清晰，存在影子资产被威胁利用，导致用户单位被通报。
- 未知威胁防守难：在网络安全的攻防对抗中，红队在利用 0day 漏洞攻击时，防守方纵使有千般武艺，也难免在疲于奔命中偶尔被“打穿”。
- 攻击过程溯源难：即便再高级的攻击，也需要通过流量来掌握其漏洞利用和攻击过程，传统安全设备无法溯源整个攻击链路过程。

2.3. 当前安全检测类产品的不足

- 现有安全设备误报多：每天成千上万条安全事件，缺乏价值数据，无法分析研判。

- 安全检测规则滞后：安全设备检测规则的滞后性，大量威胁难以及时发现。
- 东西向流量采集方式重：内部东西向数据监测需要部署大量探针，导致整体建设方案投入较大，且维护成本高。
- 历史流量回溯分析有挑战：针对历史已发生的 APT，由于安全设备未能检出，无法回溯分析。

2.4. 网络及业务故障难排查

- 网络卡顿难定位：用户内部网络链路访问卡顿，网络故障难定位。
- 业务系统难诊断：业务系统访问无响应或响应慢，业务异常节点难诊断。

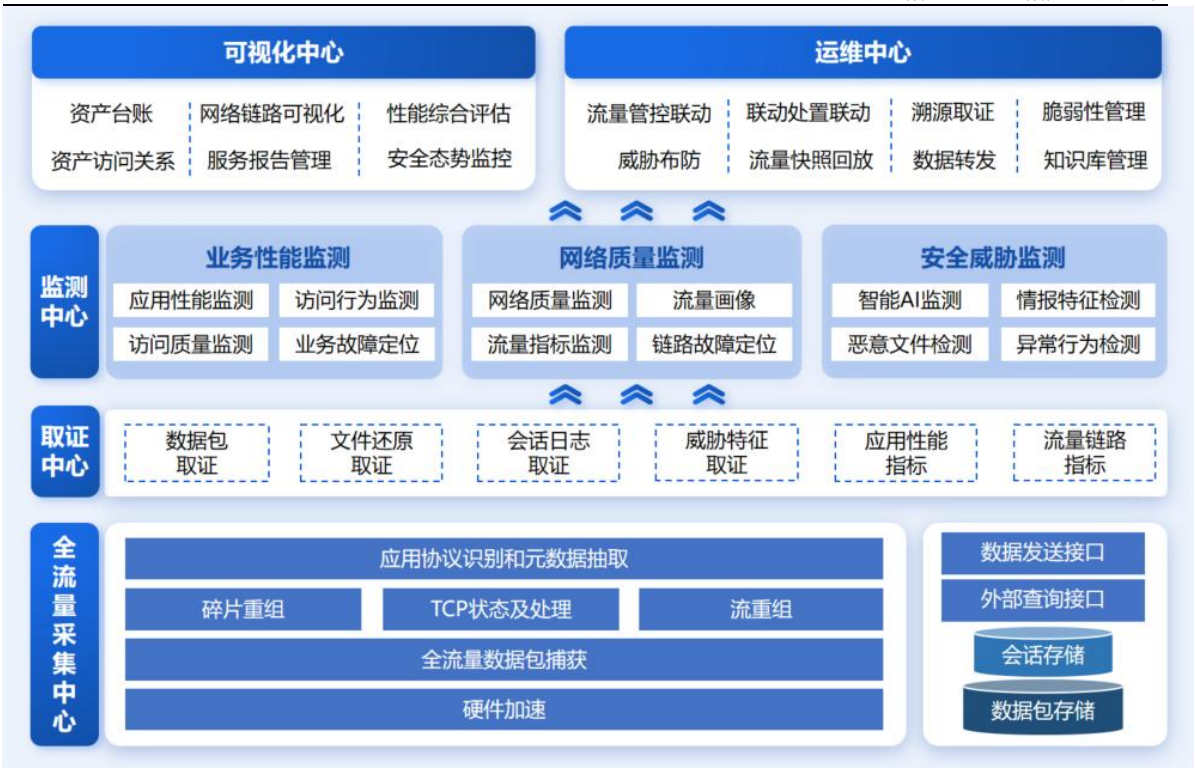
3. 解决方案

3.1. 产品简介

聚铭铭溯全流量回溯取证系统（iNTF），以旁路方式接入网络，对网络流量数据全量接入、解析、检测、存储，具备对历史数据进行回溯取证能力，使网络分析突破时间的限制。采用高可靠性和高性能的数据包捕获技术，确保即使在网络高峰时段也能无遗漏地记录数据，并将其解析为元数据和 PCAP 文件形式存储。内置多个检测引擎，运用人工智能和规则特征，对流量数据进行深度分析,当发生网络质量、业务性能、网络安全等各类故障后，能够及时对故障发生时的网络链路指标、应用性能指标、网络安全事件上下文进行完整还原，从而定位问题根因，帮助用户解决网络中的各类问题。

3.2. 产品架构

聚铭全流量回溯取证系统主要包括如下模块：



3.3. 主要功能

3.3.1. 采集与解析

对网络中传输的所有数据包进行捕获、存储和分析的过程，系统能够不间断地捕获网络中的所有流量数据，包括进出的数据包，并将其解析为易于分析的格式，通常以元数据和 PCAP（Packet Capture）文件形式存储，为后续的分析提供了详实的数据基础。

3.3.1.1. 全流量数据采集

1) 南北向流量采集

在网络关键节点如核心交换机、边界网关等上通过网络镜像旁库部署方式，对南北向网络的数据包进行全面捕获，以确保不影响原有网络数据的正常传输。

2) 东西向流量采集

与传统的南北向流量相比，东西向流量发生在系统内部组件或服务之间，其特点是流量大、交互频繁且不易监控，因此对在同一网络平面内（例如，云平台内部或数据中心内部不同服务器之间）流动的数据流量进行远程监测和分析的技术，使用专业流量数据遥测技术，自动采集东西向流量的数据包，采用轻量化部署方式，再确保不影响生产环境的前提下进行东西流量采集。

3.3.1.2. 全流量数据解析

1) 元数据解析

独有的智能协议识别技术，可高速、准确地识别上千种应用，支持对 IPv4/IPv6 协议中 2-7 层流量数据进行识别和元数据提取，可解析还原 DNS、FTP、HTTP、IMAP、POP3、SMB、SMTP、ICMP 等协议并以元数据形式存储。

2) 工控协议解析

支持 EthernetIP CIP、IEC、MMS/S7Common、Mobus、OPC、OPCUA 等工控协议解析，满足工控审计的需求。

3.3.2. 全流量数据筛选及留存

3.3.2.1. 灵活的筛选策略

支持根据五元组（源 IP、目的 IP、源端口、目的端口、协议）、域名等策略进行筛选，进行流量的智能过滤与定向捕获留存，以适应不同的网络环境和安全需求。

3.3.2.2. 高性能数据留存

采用高可靠性和高性能的数据包捕获技术，确保即使在网络高峰时段也能无遗漏地记录数据。同时，通过高效的磁盘压缩技术，降低了存储成本且不影响数据的完整性。

3.3.3. 全流量回溯及取证

3.3.3.1. 网络会话回溯取证

秒级数据精度下 IP 会话回溯分析，指标包括但不限于以下类型：源地址、源地理位置、目的地址、目的地理位置，便于追踪攻击路径、确认数据泄露细节或验证合规性要求至关重要。

1) 会话识别与关联

通过分析数据包的五元组（源 IP、目的 IP、源端口、目的端口、协议）及时间顺序，将散乱的数据包聚合成逻辑上的网络会话。

2) 精确数据包检索

建立完整的日志、协议、数据包全字段索引库，以便于快速提取多维度的网络元数据进行检测与分析，为后续异常数据挖掘、分析、取证建立牢靠的基础。

3) 会话结果呈现

检索结果清晰展示会话的起始时间、结束时间、源目 IP、协议详情、数据传输量等关键信息，便于安全人员快速理解和分析。

3.3.3.2. 数据包级回溯取证

数据包回溯取证是一种高级的网络安全调查方法，专注于利用捕获并存储的全网流量数据进行详细的事件分析和证据收集。

1) 数据包存储与管理

iNTF 通过捕获的全流量 PCAP 包并留存，PCAP 存储可根据实际需求减少或扩容存储周期。通过数据压缩、索引构建以及长期归档，以确保在需要时能快速访问到相关数据包。

2) 数据包级回溯

当安全事件发生时，所有与事件相关的数据包及其上下文信息会被详细记录和保存，作为法律或内部审查的证据，这包括但不限于 IP 地址、端口信息、时间戳、数据内容等。

3) 数据包内容标记

在发生安全威胁情况下，秒级检索回溯原始流量数据包，发现可疑活动即自动标记相关数据包内信息，便于后续快速定位和分析。

4) 数据包导出/导入取证

依据用户需求对于留存 PACP 包导出，或将 PACP 包从原始捕获设备或环境导入到 iNTF 系统中进行留存分析，这种分析方式适用于多种场景，包括但不限于故障排查、安全审计、性能优化等。

5) 数据包离线分析

为满足对离线流量数据进行事后检测查询的需求，对于离线数据包进行定期检索分析，尤其在安全威胁规则库、情报等更新以后，针对与历史数据包进行二次分析，呈现历史流量数据相关风险，帮助安全分析人员从历史流量中发现资产所存在 web 相关风险信息、攻击事件、异常行为和威胁情报。

3.3.3.3. 文件回溯取证

1) 文件还原解析

产品支持识别网络流量中的 HTTP、SMTP、IMAP、POP3、FTP、SMB 等多种协议识别，可提取流量中 200+种类型的原始文件，如 DOC、DOCX、PPT、PPTX、XLS、PDF 等文件，同时可识别还原加密文件、多层压缩文件。

2) 文件回溯取证

iNTF 具有还原文件并存储能力，同时数据包重组提取网络中传输的文件和对应的还原信息，建立完整的文件字段索引，帮助安全运维人员快速检索文件信息。

3.3.3.4. 网络链路指标

网络流量链路指标回溯是对网络流量数据进行追溯分析的过程，不仅有助于应对即时的安全威胁，还能为网络规划、资源调配和长期性能优化提供宝贵的数据支持，网络链路指标主要收集关键信息包括：源地址、目的地址、TCP 会话、UDP 会话、平均包长、总连接数、并发流、新增流/老化流、标准差、总请求数、平均时延、响应时间、应用吞吐量、错误率、并发连接数、会话持续时间、重定向次数等。

网络链路指标对于网络管理员和工程师来说非常重要，它们可以帮助他们优化网络性能，解决网络问题，并确保网络服务的质量和可靠性。

3.3.3.5. 秒级回溯检索

iNTF 具备对海量数据的超快检索能力，能够查询任意时间范围内，PB 级别的原始流量，可做到 PB 级数据秒级检索。

可对源/目的 IP、源/目的端口、源/目的 MAC 的字段进行检索，可设定单一检索条件和检索条件的逻辑与或非组合。

3.3.4. 网络及应用监测

3.3.4.1. 应用性能监测

应用性能监控通过 WEB、流媒体、数据库、邮件、远程登录、文件传输、DNS、ICMP 等维度进行监控，收集关于应用程序性能的数据和信息。这些数据可以帮助诊断诸如导致应用程序延迟的代码部分、引发性能下降的网络请求或数据库查询，以及成为性能瓶颈的服务器或资源等问题。使用应用性能监控还可以实时监测应用程序的健康状况，并在检测到故障时发出警报，从而尽早识别并解决问题。

3.3.4.2. 网络质量监测

网络质量监测关注的指标包括响应时间、网络抖动、丢包率等。响应时间衡量数据从源头传到目的地所需的时间。以下为网络质量监测的几个关键指标

1) 网流量实时统计

通过 iNTF 系统收集网络流量数据，包括出入网流量、带宽使用率、丢包率、延迟等关键指标，实时采集存储，按需提取分析。

2) 流量智能关联分析

在回溯过程中，将流量数据与其他网络组件（如服务器、应用程序、用户行为）的数据关联起来，可以从不同维度分析问题根源。例如，将流量突增与特定服务或用户活动对应起来。

3) 可视化链路质量分析

通过图表等形式直观展示流量变化趋势，支持流量趋势图、连接趋势图、时延趋势图展示等趋势图，使得用户能够快速定位问题时间点和受影响的链路。

4) 时间段内 TOP 分析

包括流量大小、连接数、时延 TOP 统计及趋势分析，支持 top 资产、top 应用、top 外部地址、top 区域、top 虚链路、topVLAN、top 端口等维度，分析指标包括总字节数、占比、流入、流出、连接数、并发流、新增流、老化流、总请求数、时延分布占比，有助于理解企业内网络使用习惯和异常流量行为。

5) 主机网络性能实时分析

以图表的形式监控主机的带宽占用情况、端口/应用的流量吞吐、TCP 建连成功率、TCP 三次握手时延、TCP 重传以及 TCP 零窗口等，并且支持查询模式回溯历史时间的网络质量情况。

3.3.5. 安全威胁监测及分析

3.3.5.1. 威胁监测

1) 资产识别监测

网络空间资产是指组织所拥有的一切可能被潜在攻击者利用的设备、信息、应用等数字资产，具体包括但不限于硬件设备、云主机、操作系统、IP 地址、端口、证书、域名、Web 应用、业务应用、中间件、框架、小程序、App、API、源代码等。

通过对网络流量中的 IP 地址、端口及服务等进行分析和监测，自动快速识别出网络中各种资产。基于 iNTF 对各种资产属性的识别，记录设备类型、操作系统、组件、活跃状态、应用类型等详细信息，实现准确分类资产、精细化管理，有助于后续对不同类型资产制定不同的安全策略。

iNTF 支持对特定资产进行标记分类以强化资产管理，当检测到关注资产相关流量出现异常或威胁时，可以更快采取相应安全措施。此外，产品采集并分析网络资产基础信息后支持外送给第三方安全设备，可以进一步提高威胁检测的准确性与可靠性。

2) 脆弱性动态监测

iNTF 通过对组织互联网边界资产进行探测梳理，建立资产基线，对违规暴露资产及资产变化情况进行动态监测，可对暴露面攻击情况及时预警，动态防护网络边界安全。

通过全流量采集分析，可实时探测到：新增的违法暴露资产、新增的违规暴露端口和服务以及反复暴露的资产。可对资产脆弱性实时检测，如漏洞、弱口令、高危端口等，也支持对篡改、暗链等安全事件进行实时检测。

3) 威胁情报监测

通过海量情报数据的采集、分析、验证及生命周期管理后生成威胁情报并内嵌于系统中形成情报中心，并将从流量中提取出的域名、IP、URL 等与系统内置情报进行关联比对，进一步确认网络威胁，并支持恶意加密流量检测，辅助各行业安全运营人员进行运营决策。

4) 异常流量检测

平台提供网络异常分析，主要支持对一般的网络带宽占用进行检测，包括支持 IP 分片、小包攻击、ARP 泛洪、ICMP 泛洪、UDP 泛洪、TCP 比例异常等网络异常检测。

另外，对于 TCP 协议连接，平台提供对相关指标进行检查及查询机制，这些 TCP 指标包含如 TCP 建立连接成功率、TCP 零窗口率（分为客户端和服务器端）、TCP 重连率（分为客户端和服务器端）等重要内容，为网络的异常分析提供重要依据。

5) Webshell 上传 AI 检测

Webshell 是黑客经常使用的一种恶意脚本，即 asp 或 php 木马后门，黑客在入侵网站后，在网站服务器 web 目录中将 asp 或 php 木马后门文件与正常网页文件混合，通过 asp 或 php 木马后门控制网站服务器。比如执行系统命令、窃取用户数据、删除 web 页面、修改主页等，其危害不言而喻。黑客通常利用常见漏洞，如 SQL 注入、远程文件包含（RFI）、FTP，甚至使用跨站点脚本攻击（XSS）等方式作为社会工程攻击的一部分，最终达到控制网站服务器的目的。

对于 Webshell 上传，iNTF 主要的检测手段除了针对敏感指令进行判断，例如执行、网络连接、数据库连接、文件操作等，而且还会针对脚本语义混淆编排、拆分以及语言统计特征（例如长度、最长单词、文本熵等）等进行总结归纳，以此形成高维特征向量，利用 SVM（支持向量机）、回归等算法对相关脚本内容进行判定。

6) 智能 AI 模型监测

iNTF 内置多个智能 AI 检测模型，支持对恶意加密流量、DNS 隐蔽隧道、ICMP 隐蔽隧道、DGA 域名、钓鱼欺诈邮件、Webshell、SQL 注入攻击、XSS 跨站脚本攻击进行检测、目标遍历攻击。

通过检测模型检测的方式可大幅度降低对特征规则数量的要求，具备更新频率

低、数据量小、准确率高、误报率低、自动判断、人工干预少等优势。从告警、威胁事件、元数据到原始流量 PCAP，真实还原攻击者入侵的全过程，从而对高级威胁等网络安全事件进行精准的分析，进而迅速定位 APT 攻击。

7) 联动沙箱文件监测

1．静态文件监测

静态文件检测指在不运行程序的情况下，对样本文件进行静态特征检测。产品内置多个反病毒引擎，支持多个反病毒引擎交叉检测，可检测包括 Shellcode、Webshell、后门程序、挖矿木马、间谍软件、蠕虫病毒、恶意软件、远程木马等，对已知威胁进行基于特征的静态检测和多检测模块交叉验证，最终给出检测结果。

2．动态文件监测

iNTF 还原未知威胁文件，将文件传递到沙箱动态执行行为来识别恶意文件，其利用虚拟化技术仿真出组织常用的操作系统和应用环境，然后利用虚拟执行手段使文件运行并捕获其对系统产生的影响，如释放文件、加密文档、增加启动项、API 调用等，并对这些影响进行评估，识别对系统产生破坏的恶意文件；动态沙箱支持行为签名检测，根据主机或网络行为判断其是否为恶意文件，支持多种沙箱运行模式，包括 Windows、Android 和 Linux 等类型沙箱，单设备支持至少 10 个沙箱，支持对沙箱内样本的流量进行检测、支持反虚拟机和反调试行为检测、支持恶意代码及变种检测，最大限度发现 APT 等未知网络攻击。

图 3.1 联动沙箱动态监测的内容

3.3.5.2.威胁分析

1) 失陷综合分析

平台提供基于 Kill-Chain 理论的主机失陷分析，精准定位失陷主机，还原完整攻击路径；网络态势感知从外部威胁态势、外连威胁态势、内部互连威胁态势，全方位的呈现全网安全状况，不仅能够聚焦隐藏的 C&C 回连、隐蔽通道、恶意软件活动，还能监控内部设备间的横向威胁传播，如蠕虫、木马等。具体如下：失陷分析将获取行为监测引擎分析、特征匹配分析、情报线索智能关联、涉密信息外泄分析、可视化关联分析、沙箱行为分析、连接流量分析等分析引擎的分析结果，将分析结果映射到失陷分析的各个阶段，并结合攻击利用漏洞与主机漏洞存在真实性进行可信度计算，将误报率将至最低。

平台将提供综合的安全态势感知分析，包含如下内容：

(1) 外网攻击威胁分析：包含扫描探测、外部攻击、恶意软件下载等内容。

(2) 内部外连攻击威胁分析：包含扫描探测、外连攻击、C&C 回连、隐蔽通道等内容。

(3) 内部互连攻击威胁分析：包含扫描探测、外部攻击、恶意软件下载等内容。

2) 挖矿专项分析

对于虚拟货币挖矿行为，在全流量还原基础上，iNTF 可对异常流量进行特征提取，实时监控并检测攻击特征；也支持自动学习历史流量访问信息，建立异常流量检测模型。

异常流量经过与聚铭情报平台进行碰撞，可实时动态识别攻击行为以及挖掘潜在未知挖矿信息。iNTF 内置的动态阻断策略支持对挖矿行为的在线拦截，在不影响正常业务请求前提下阻断挖矿行为，联动阻断能力上能达到 100%成功率，且将阻断动作在客户内网实现，真正做到挖矿流量不出网。

3) 违规外连分析

外连威胁是指主机对外部机器发起的异常行为，如恶意服务器扫描、外连恶意服务器、DNS 查询恶意域名、web 访问恶意主机等。此外，违规外连还包括由于用户或者运维人员的不当操作将内网计算机直接连接互联网、通过其他网络访问互联网、专网设备未经安全防护及策略设置直接连通其他网络等行为。比如，办公电脑连接手机热点、将涉密网电脑连入普通办公内网使用、将业务专网计算机网线误接入互

联网、因业务测试或紧急业务需要临时连通违规互联网出口等。

违规外连相当于在网络安全区域之间、内网与外网之间建立新的通道，使外部黑客、病毒能够绕过防火墙、网关等防护屏障，侵入违规外连的计算机，非法篡改或窃取敏感数据，甚至利用该设备作为跳板，进一步渗透内网的重要服务器，使整个内部网络面临巨大的安全风险。

iNTF 通过收集内网流量，分析学习用户流量网络行为，经过与聚铭情报平台海量情报数据的碰撞，结合 TCP 和 UDP 探测技术，全面准确发现异常外连行为。支持制定各种控制策略，便于进行事后追踪与审计取证。

4) 攻击威胁分析

攻击威胁检测模块主要针对常见的网络攻击进行检测，包括但不限于：病毒、蠕虫、木马、DDoS、扫描、缓冲区溢出、欺骗劫持等威胁的检测能力，同时实现对常见 Web 应用类攻击包括跨站、跨站请求伪造、文件上传、SQL 注入、命令执行、文件包含等，还有其它的多种攻击方法，监控这些攻击的特定动作或者关键字，判别是否存在 Web 类应用攻击。

5) 恶意文件分析

iNTF 从 SMB、FTP 等协议中对文件进行还原，并对还原后的文件进行深度检测，包括静态检测、动态沙箱检测、机器学习检测和威胁情报检测等多种检测引擎，识别恶意文件的传播。

iNTF 除了具备与 IDS、IPS、杀毒软件等安全产品类似的特征方式检测引擎外，还实现了沙箱检测、机器学习、隐蔽通道、异常通信检测等未知威胁的检测引擎。这些引擎区别于特征检测，采用了行为分析、机器学习算法等新兴技术，即使病毒变种、出现新型木马，也可以通过其恶意行为和算法进行识别。

因此，iNTF 既可识别已知的攻击，也可检测未知的恶意文件和恶意流量的攻击行为，最大限度发现 APT 新型网络攻击行为。

3.3.6. 多维联动及阻断方式

3.3.6.1.多维联动方式

iNTF 内置众多异构设备联动技术，除接口联动方式以外，独具模块化万能联动

技术无需代理工具，仅需提供联动设备用户名、密码即可，基于模拟用户行为联动技术，联动设备不限与防火墙、IPS、WAF、交换机等异构品类，实现异构设备联动快速处置能力，进一步降低安全运维人员的工作负担。

异构设备多维联动可实现一次配置长期稳定使用，结合场景策略，实现智能布防，提升安全运维人员工作效率。

3.3.6.2.旁路阻断

iNTF 采用旁路威胁阻断防御，用户可以根据已命中的安全事件精准对已知和未知攻击进行实时阻断，系统提供多种特征组合的阻断方式，并支持用户查询执行阻断策略的网络会话。

3.3.6.3.DNS 阻断

可基于 DNS 域名解析在线阻断，防通报问题的处理场景，包括但不限于恶意外联，恶意行为等安全通报问题，如矿池连接，垃圾邮件，远控主机外连，恶意外部扫描，木马连接等安全问题。支持配置 DNS 阻断策略，结合威胁情报检测发现安全事件，动态实时阻断。

3.4.数据输出与外发

iNTF 提供标准化的资产数据，具备高度的数据扩展能力。可与 SOC、XDR、态势感知等平台无缝打通，满足多维度的联动分析需求。

3.4.1. 网络元数据输出

对网络元数据（网络日志）进行标准化输出，协议覆盖常见：HTTP、DNS、SMTP、POP3、IMAP、SSL、FTP、Telnet、MySQL、MongoDB、SMB、Socks、Kerberos 等进行实时输出。

3.4.2. 多方式数据外发

课题通过 Syslog、Kafka 等多种方式进行数据外发，同时提供 API 接口方式，外发系统日志（告警日志、网络日志、运行日志等）。

4. 产品价值

4.1. 轻量化采集东西向流量，最小成本投入

全量采集东西向网络流量，无需部署大量探针或代理，包括收集和分析数据中心内部或云环境中虚拟机之间的东西向流量，不仅投入及运维成本低，而且具有灵活、可扩展性，对现有系统性能影响较小。

4.2. 弹性扩容，无带宽负担

通过分布式部署，对于新建分支机构、网络扩容等场景，增加分布式节点，节点自带独立分析能力，无需网络流量回传，对已有专网带宽零负担。

4.3. 多维流量快照，快速回溯检索

系统针对流量数据进行分层快照，留存流量链路指标、性能指标、威胁上下文、网络会话日志、还原文件、原始数据包多种维度数据，便于遇到故障时，多维度数据纵向关联分析，快速定位问题原因。

4.4. 万能异构联动，智能布防

不受第三方设备 API 限制，可智能化完成第三方设备的对接，实现阻断设备、流控设备联动，结合业务场景策略，智能完成网络维威胁、拥塞等故障治理。