聚铭网络流量智能分析审计系统

产品白皮书

聚铭网络科技有限公司

2024 年 04 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

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。

1 前言

近期，美国网络安全审查委员会发布首份报告称，2021 年年底曝光的 Log4j 漏洞成为难以消除的漏洞，其影响将会持续十年之久。Log4j 事件表明，组织对暴露在外的 IT 资产知之甚少。据统计，大型组织通常拥有数千、数万或更多面向互联网的资产，包括网站、敏感数据、员工凭证、云存储、源代码、SSL 证书等。随着现代数字基础设施加速发展，容器化、Saas 应用以及远程办公混合工作环境相应急速增长，企业面临的攻击面随之扩大。

网络空间中，大部分的安全问题都源自于内网，攻击者普遍会利用漏洞对内网进行渗透，以达到控制整个内网、获取大量有价值信息的目的。据统计 2022 年各大组织内网的安全漏洞数据仍在不断增加，甚至变得越来越复杂。攻击者借助自动化工具在短时间内以更高效、隐蔽的方式进行漏洞扫描和探测，使得组织面临更为严重的安全风险和损失。

除了内外部网络环境的安全风险，近几年，勒索软件攻击态势愈发严重，不仅数量上快速增长，赎金、修复成本等也翻倍增长，勒索软件成为当今社会最普遍的安全威胁之一。可以预见，未来几年勒索软件数量还将显著增长，攻击者数量也将达到空前的程度。同时勒索软件攻击也将迅速蔓延至整个攻击面，威胁将无处不在。

2 客户需求

针对上述问题和挑战，组织的信息安全管理人员不仅对各类安全防护设备**合规**功能有着较高要求，而且对**日常安全问题的发现、潜在问题的萃取、未发生问题的预防等**都有较高期望，特别是对于一些**隐蔽安全问题的追根溯源**（包括各类高级持续威胁等）也有现实需求，包括：

1. 通过互联网暴露端口或者漏洞进行外部攻击；
2. 通过弱口令、邮件钓鱼等途径的社工攻击行为；
3. 访问控制混乱而导致的隐蔽通道或服务端口暴露问题；
4. 内部潜在威胁源或威胁用户的发现；
5. 虚拟货币挖矿行为的发现及阻断；
6. 潜在的数据泄露或外传风险；
7. 其它各类网络异常行为的检测。

以上仅列举了部分内容，但在现实中安全问题远远不止上述部分，例如还有针对各种 0day 漏洞的攻击等等，所以客户对网络流量分析审计的要求包含了对于**未知威胁的检测和防御**，而不仅仅是对于**已知威胁**的发现。

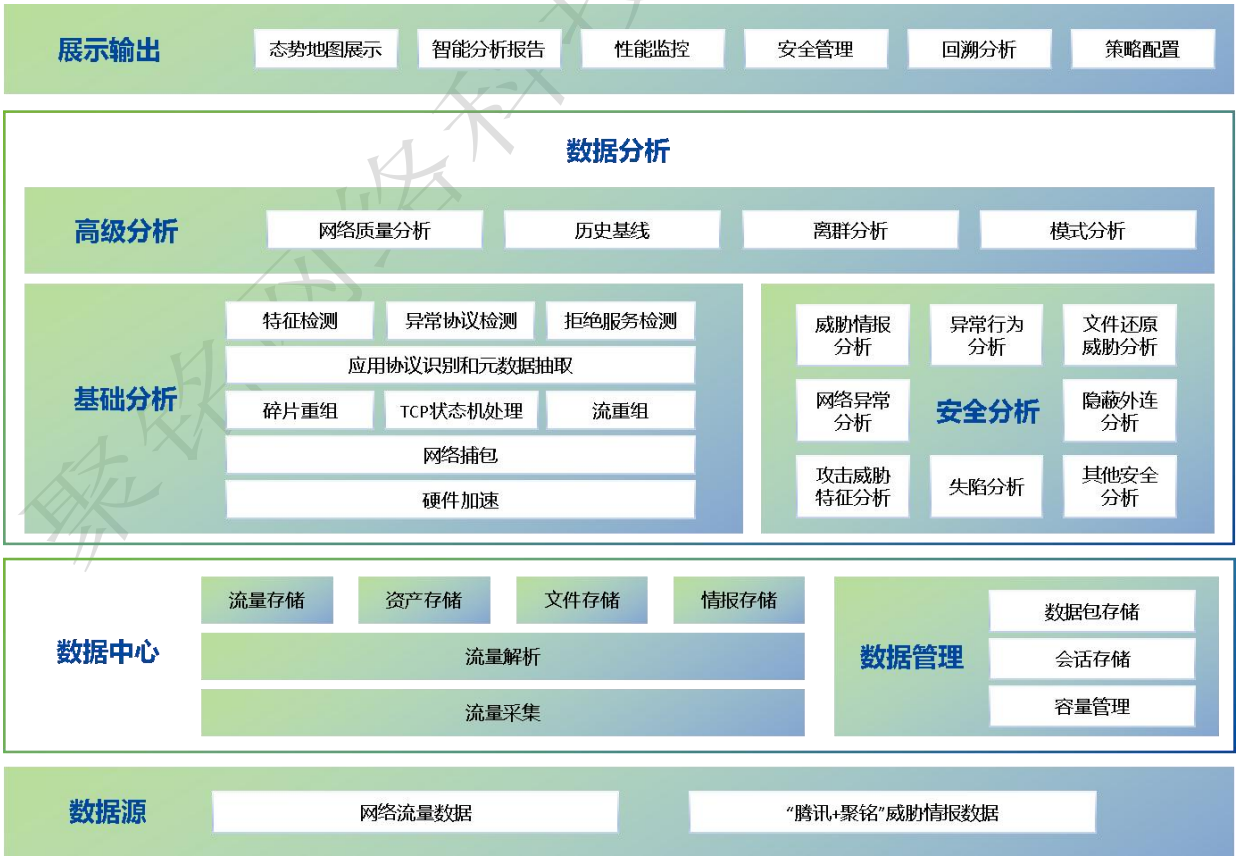
3 解决方案

聚铭网络流量智能分析审计系统（iNFA）是聚铭研发的具有自主知识产权的专业网络流量分析审计系统，它是一款以全流量还原为基础，结合互联网风险暴露面绘制、失陷分析、网络攻击检测、威胁情报分析、隐蔽通道检测、挖矿行为检测、核心数据外泄防御、异常流量行为挖掘、文件检测、网络质量检测、域名异常检测、恶意软件加密流量检测等技术，对全网流量实时进行威胁感知、可疑流量分析，是对传统安全防御系统的完善和补充，能在高级威胁入侵时，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。

3.1. 产品架构

聚铭网络流量智能分析审计系统主要包括如下模块：



◆ 基础分析层

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、异常协议检测等功能。

◆ 安全分析层及高级分析层

结合失陷分析、网络攻击检测、威胁情报分析、异常流量行为挖掘、文件检测、网络质量检测、隐蔽通道检测、域名异常检测等技术，对全网流量实时进行威胁感知、可疑流量分析。

3.2. 主要功能

3.2.1. 资产梳理，收敛风险

风险暴露面，即从攻击者视角出发，发现并持续监控攻击者在针对组织时看到并尝试利用的资产和漏洞。包含了暴露在攻击者视线范围内，可以被利用入侵的系统、设备、信息等。大量的暴露面都潜藏在不容易被发现的暗处，很容易因为资产排查不彻底、人员疏漏等问题被忽略。互联网暴露面资产直接面向外部攻击者的威胁，相对于企业内部资产所面临的安全风险更高。暴露面包含但不限于：操作系统、中间件、应用程序中存在的软件漏洞；系统和软件中的错误配置与安全控制缺失；违反安全制度和合规要求的网络配置；过度宽松的访问控制规则。

一个大型组织自上而下可能有几十或者近百家分支机构，业务范围广泛。每个业务或应用无论部署在云上还是云下都需要有足够的基础设施支撑，业务或应用的上下线清理不及时等情况有可能成为组织或者分支机构的威胁暴露面。

3.2.1.1. 资产自动探测

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 iNFA 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。

3.2.1.2. iNFA 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。风险暴露面梳理

iNFA 通过对互联网边界资产进行探测，比如：应用、系统、IP、端口、服务、域名、中间件等，对自有资产进行全面梳理，及时发现未知资产（如影子资产或孤立的 IT 基础设施）、流氓资产（由恶意人员启动的恶意基础设施，例如冒充的恶意软件、域名、网站、应用程序等）；资产发现完成后可根据类型、业务关键性、合规要求等指标对资产进行重要性分类。

根据探测的结果对暴露资产进行收敛，缩小攻击面。比如可对违规暴露的资产进行下线处理；可关闭违规暴露的端口和服务；对高风险端口进行禁用；可将非必须暴露资产收归内网。

3.2.1.3. 脆弱性动态测绘

iNFA 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。

3.2.1.4. 服务及应用弱口令识别

弱口令是网络安全领域中最常见的安全问题之一，指容易被猜解或破解的密码，由于发现简单、利用容易、危害严重，已成为很多企业和用户信息泄露、威胁扩散的重要入口和途径。

- iNFA 可通过流量镜像还原的方法，利用弱口令扫描引擎识别、还原业务系统访问过程中包含的账号、密码，精准识别其中包含的弱口令。为降低检测误报率、提升弱口令检测识别精准度，在弱密码检测策略的基础上增加了加密解析、提取检测等方式，进一步提高产品的可用性。
- iNFA 支持在 http、ftp、IMAP、pop3、smtp 等协议上进行弱口令检测，从设备、账号、口令等维度展现检测情况，并可呈现命中原因。

3.2.2. 渗透/钓鱼，实时检测

3.2.2.1. 邮件钓鱼社工检测

风险暴露面除了包含互联网边界资产、弱口令等数字攻击媒介外，更易以“人”为突破口，利用人性弱点进行“人性黑客攻击”，也即社会工程攻击面。社会工程会操纵用户分享本不该分享的信息，下载本不该下载的软件，访问本不该访问的网站，向犯罪分子汇款或者犯下其他损害个人或者组织资产或安全的错误。社会工程利用的是人性弱点而非技术或数字系统漏洞。

网络钓鱼是人们最熟悉和最常见的社会工程攻击媒介。在网络钓鱼中，诈骗者发送电子邮件操纵收件人分享敏感信息、下载恶意软件、向错误的人转移金钱或资产，或采取其他破坏性行动。攻击者精心制作网络钓鱼信息使其看起来或听上去像是来自可信或可靠的组织或个人。恶意邮件攻击进攻手段大同小异，一般使用加密或非加密链接/附件诱导用户进行点击、下载以绕过反垃圾、反钓鱼、反病毒检测。

对于钓鱼站点攻击，iNFA 通过将恶意请求信息与聚铭情报进行碰撞，在百亿级恶意文件样本库、数十亿级 IP/域名信誉库、数千万级恶意网址、数十万级漏洞等情报数据加持下，对异常流量进行特征化分析，在不影响正常业务请求前提下实现在线检测并拦截阻断钓鱼站点请求，阻断成功率可达 100%。

对于钓鱼邮件附件攻击，iNFA 通过沙箱模拟执行环境，诱导文件执行，监控并分析其行为特征。通过进程、文件、注册表等综合行为判断文件的威胁情况。在传统签名机制这种已知威胁检测手段基础上，iNFA 结合自研反病毒引擎以及引擎情报库能力，依靠深度沙箱中的动态分析模块、静态分析模块实现自动化、智能化、可定制化的样本分析，对文件进行准确的分析鉴定。通过高覆盖率的恶意样本检测模型精准高效地对网络钓鱼攻击、勒索挖矿病毒进行打击。

3.2.2.2. 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，iNFA 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。

3.2.2.3. 网络攻击检测

iNFA 内置多种网络攻击检测策略，支持对网络攻击进行检测。检测的类型包括端口扫描、拒绝服务攻击、漏洞利用攻击、XSS 跨站注入、SQL 注入攻击、

缓冲区溢出攻击、敏感 SQL 等类型的攻击。

3.2.3. 回连/外泄，坚守防线

3.2.3.1. 隐蔽通道 AI 检测

隐蔽通道是通过将特殊协议封装在常规协议（例如 DNS、HTTP 等）中进行数据传输的手段。由于大部分防火墙和入侵检测设备很少会过滤常规协议，攻击者可以利用它实现诸如远程控制、文件传输等操作。隐蔽通道也经常在僵尸网络和 APT 攻击中扮演着重要角色。

iNFA 通过总结隐蔽通道的构建方法，全面分析隐蔽通道流量的数据分组特征及会话连接的统计特性。在此基础上，通过机器学习算法训练具备了检测新型隐蔽通道的能力。基于机器学习的方法 iNFA 能够准确识别 http 协议、ICMP 等隐蔽通道行为。

3.2.3.2. 加密流量深度检测

聚铭独有的加密恶意软件流量检测核心专利技术，通过以下多种方式搜集/提取以形成恶意加密流量特征：利用 DNS 协议相关特性对相关恶意流量进行预备处理；对 HTTPS 协议握手的若干数据包特征进行检查；整合提取已知恶意软件加密通讯数据流特征相同点。

通过集成智能动态基线、模式信息熵等机器学习算法对恶意加密流量特征建模以达到区分正常通讯流量以及恶意加密流量的目的，精准检测识别出加密恶意软件流量。经过几千万次训练验证，检测总体成功率高达 99.8%，可以检测如 Cobalt Strike、Ursnif、Anubis、Qbot 等典型恶意软件。

3.2.3.3. 挖矿行为实时阻断

对于虚拟货币挖矿行为，在全流量还原基础上，iNFA 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。iNFA 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，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。

3.2.3.4. 违规外联行为审计

外联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、外联恶意服务器、DNS 查询恶意域名、web 访问恶意主机等。此外，违规外联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。

违规外联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，侵入违规外联的计算机，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。

iNFA 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联行为。支持制定各种控制策略，便于进行事后追踪与审计取证。

3.2.3.5. 核心文档外泄检测

近年来，数据泄露屡屡发生。在万物互联的时代，如今的数据量已经比历史上任何时候都要庞大，不光是个人，即使是世界上大型公司也无时无刻不在受到数据泄露的威胁。数据泄露带来的危害和影响随着数据量的指数递增只会愈发深远巨大。

面对此情况，聚铭网络提供了基于网络流量分析的数据泄露解决方案。iNFA 通过旁路方式接入网络环境，将互联网接入口网络流量进行镜像。内置的网络攻击窃密检测模块对恶意攻击行为进行特征识别及匹配；文件解析引擎对协议解析还原出的文件进行内容检测；协议解析模块对传输及收发文件等用户行为进行审计。经过一系列的处理分析手段，将各类告警信息进行关联分析与挖掘，iNFA 可实现及时检测数据泄露并告警、保留证据链实现精准定位溯源。

此外，iNFA 支持对文件内敏感词等内容的检测，用户可通过自定义敏感词，实现对文件中违规违禁敏感词识别并产生告警，以规避法律法规风险。

3.2.4. 抑制扩散，阻断传播

当攻击者获取到内网某台机器的控制权后，会以被攻陷的主机为跳板，通过收集凭证等各种方法访问环境内其他机器，进一步扩大攻击范围。传统的检测与响应手段往往会呈现：防护单一难以全面感知攻击面、横向渗透影响范围难以可视化和量化导致无法快速响应。

iNFA 结合大数据处理、加密流量检测等能力，提供全流量溯源分析与取证，支持多种复杂内网协议的解析识别，既包含已知内网渗透攻击的检测，也能覆盖未知攻击检测，可实时监控来自外部攻击及内部运维人员的数据窃取、高危操作、误操作等行为。

3.2.4.1. 僵木蠕传播抑制

iNFA 基于 kill-chain 攻击模型分析能够宏观感知到攻击过程以及受影响资产，做到有迹可循有证可查。对于在流量引擎侧、威胁情报侧以及沙箱侧检出的告警，通过深度解析网络流量，结合特征匹配、异常行为分析、机器学习等技术，实现迅速、精准识别网络中僵木蠕传播行为且支持在线阻断。例如对于虚拟货币挖矿行为可做到在线动态阻断，在不影响正常业务情况下仅阻断与挖矿相关的请求。

3.2.4.2. 永恒之蓝知名漏洞利用检测

iNFA 采用漏洞特征库匹配攻击手段的方式识别流量中的漏洞扫描和漏洞利用行为。iNFA 在聚铭情报平台数十万级漏洞库数据基础上，同时更新最新出现的漏洞攻击特征，可及时识别和预警已知的漏洞扫描和漏洞利用行为。

以“永恒之蓝”事件为例，“永恒之蓝”事件是黑客利用微软操作系统的 SMB 服务漏洞发动的攻击，通过 445 端口进行。恶意代码会扫描开放 445 文件共享端口的 Windows 机器，在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币矿机等恶意程序。

iNFA 通过主动感知 445 端口的扫描行为和蠕虫传播行为建立行为模型。采用基于行为特征的检测技术，通过对攻击行为分类，并为同类攻击行为建立相应的行为模型，实现威胁检测以应对未知威胁。

3.2.5. 未知威胁，尽在掌控

3.2.5.1. 恶意文件行为动态分析

iNFA 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。

iNFA 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，iNFA 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。

3.2.5.2. 0day 漏洞溯源分析

当 0day 漏洞爆发，并且在相关针对 0day 漏洞的检测规则尚未发布时，安全运营团队需要第一时间对相关资产或特征进行快速排查，对漏洞利用行为进行全局性分析。

即使遭遇 0day 攻击，其后续的攻击手段也会回到基本面上，比如：Webshell 通信行为、恶意文件上传（Webshell）、恶意命令执行、内网端口扫描、内网横向扩散行为、端口转发、C&C 通信等。iNFA 可发现和识别这类异常行为并加以检测分析。

在小流量情况下 iNFA 支持本地数据包全留存，大流量场景下提供配套的全包存储组件，具备灵活的存储能力扩展。支持对网络原始数据进行全流量完整保存，对外秒级提取海量历史流量，并支持在线数据包查看或离线下载分析。通过网络协议实时解码、元数据提取，建立完整的日志、协议、数据包全字段索引，快速提取多维度的网络元数据进行异常行为建模，还原 0day 攻击事件发生时的全部网络通讯内容，实现数据包级的数据取证和责任判定，大幅提升威胁事件溯源的准确性。

3.2.6. 威胁阻断，快速处置

3.2.6.1. 旁路阻断

iNFA 采用旁路部署模式，在聚铭情报平台加持下，当监听检测到威胁的同时，可通过主动构造阻断数据包分别发送至访问端与服务端达到拦截封禁攻击的效果。

为了适应组织不同时期的不同需求、不同场景，可以创建多种阻断策略模板一键切换。

3.2.6.2. DNS 阻断

iNFA 支持 DNS 域名解析+情报判定，如果命中阻断规则，可实现实时阻断。例如，DNS 解析后的 ip 经过与聚铭情报库的碰撞，如被判定为挖矿相关，则可直接封锁挖矿流量。

3.2.6.3. 绿色版恶意程序抓捕

无需安装 agent，使用绿色版抓捕工具，通过 iNFA 深度分析失陷主机的异常流量行为作为抓捕证据输入，即可在失陷主机上对挖矿、木马软件、病毒程序进行精准抓捕。

3.2.7. 安全分析，持续运营

3.2.7.1. Kill Chain 分析

iNFA 汇聚不同层次的攻击事件后，将所有的事件按 Kill Chain 的不同阶段进行归类和统计，并展示到可视化的 Kill Chain 图中，同时提供丰富的筛选条件，以便用户对各个阶段的数据进行深度分析，快速确认攻击是否产生实质影响，判断攻击是否成功。

3.2.7.2. 安全事件降噪分析

随着网络流量数据的不断接入及检测分析，海量告警事件不断产生，分析工作耗时耗力，误报率及漏报率居高不下，且重复性报警居多。iNFA 基于独创的半监督学习聚类算法，以攻击者视角，不断汇总攻击手法、攻击记录、攻击活跃程度、攻击阶段、攻击主机数量、活跃时间等攻击者画像信息，从而达到聚焦分析及处置的目的，实现告警数据降噪的效果。

3.2.7.3. 数据开放与兼容

iNFA 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。

3.3. 产品价值

3.3.1. 数据更全面

iNFA 提供配套的全包存储组件，能提供灵活的存储能力扩展。支持对网络原始数据进行全流量完整保存，对外秒级提取海量历史流量，还原网络事件发生时的全部网络通讯内容，回溯完整攻击链，实现数据包级的数据取证和责任判定，大幅提升威胁事件溯源的准确性。

3.3.2. 分析更精准

基于大数据、AI 技术，精准挖掘可疑流量，结合聚铭情报、八大安全分析引擎，多层次、全方位覆盖安全分析的每一个层面。（八大安全分析引擎：威胁情报分析、异常行为分析、文件还原威胁分析、网络异常分析、隐蔽外连分析、攻击威胁特征分析、失陷分析、其他安全分析）

3.3.3. 处置更智能

iNFA 支持告警收集与指令下发，预置多种处置场景化剧本以应对常见类型的告警事件，对应不同告警事件调用预置的处置流程，通过下发处理动作完成对告警事件的处置，提升业务系统的安全系数。

3.4. 部署方案

聚铭网络流量智能分析审计系统采用旁路 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

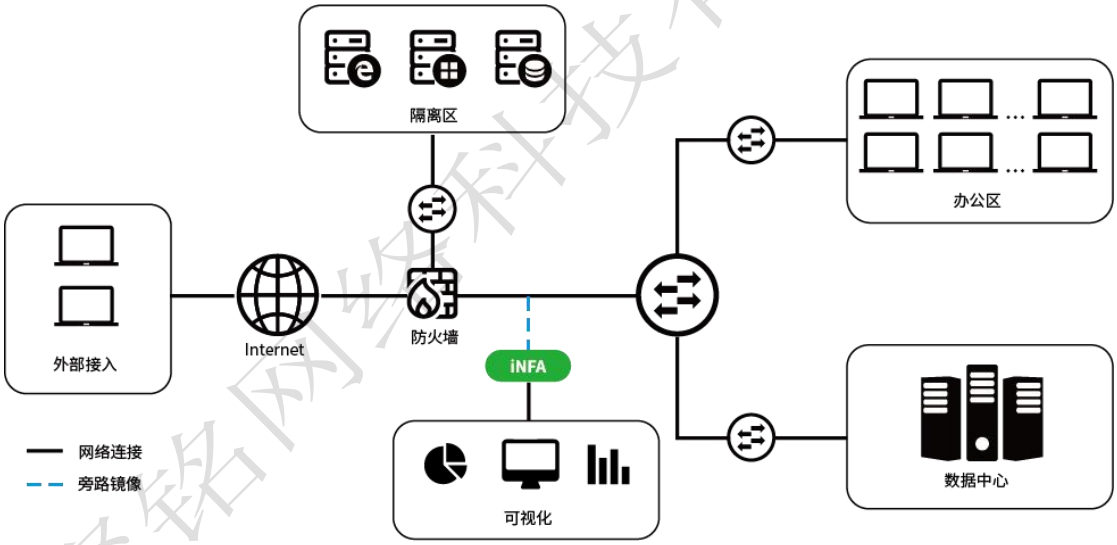
产业务或应用产生任何影响。

3.4.1. 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、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。



3.4.2. 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。

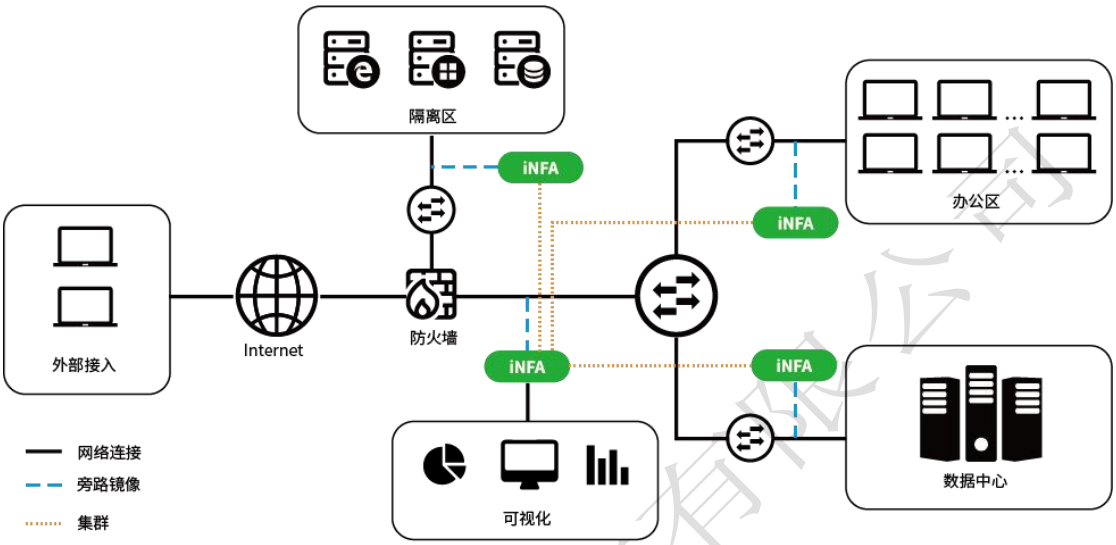
此方案能够解决如下安全问题

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。



3.4.3. 集成 UTA 部署方案

集成 UTA（文件行为检测引擎），是为了发现未知恶意文件，通过在虚拟仿真环境中分析文件的行为，识别文件恶意文件。除此之外，该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。

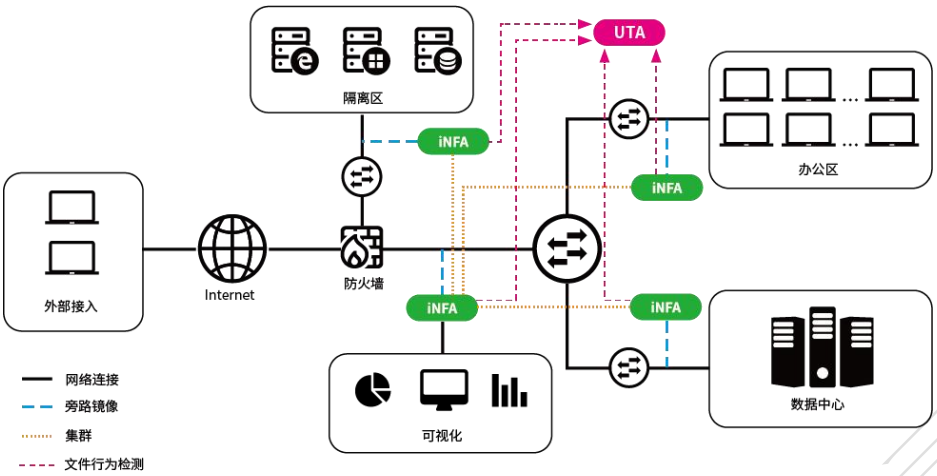
此方案能够解决如下安全问题

1. 全流量采集、分析、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，包含文件行为分析。


UTA
隔离区
iNFA
办公区
iNFA
外部接入
Internet
防火墙
iNFA
iNFA
数据中心
可视化
网络连接
旁路镜像
集群
文件行为检测