天融信全流量监测设备
产品白皮书

产品版本：V3.1.01

文档版本：V25.1.8

发布日期：2025.7.18

北京市海淀区西北旺东路 10 号院西区 11 号楼 1 层 101 天融信科技集团 100193

电话：010-82776666

传真：010-82776677

服务热线： 4007770777

http://www.topsec.com.cn

版权声明

商标声明

信息反馈

http://www.topsec.com.cn

目录

1 前言

全球企业数字化转型浪潮下，伴随着网络的复杂化、应用业务的多样化、各类安全风险问题层出不穷，安全威胁也在不断升级，网络空间中的攻击持续频发，攻击手段也呈现广泛化、多样化和隐蔽化的特征，网络攻击“AI”化趋势明显。因此针对网络的攻击行为能够的防范难度也日益剧增。当前世界格局深刻调整，网络空间加速变革，在以经济利益为目标的攻击基础上，高级持续威胁攻击越来越多地被曝光。对企业而言，仅以单一防护手段已无法有效抵御高级持续威胁攻击，需要建立高级威胁防护运营体系并持续运营，才能及时有效地发现、阻断风险，避免企业损失。

高级持续威胁通常是一套完整的攻击体系，具备攻击能力高、隐蔽性强等特点。企业需通过构建协同联动体系，实现高级威胁防御的持续运营改进、全面监管联动、产业情报共享，以此努力扩大守方优势、逆转攻防态势，共同应对高级威胁挑战。然而，发现高级持续威胁是一个复杂的过程，不仅需要关注某个攻击点所采用的攻击手段，更需要关注整个攻击的全作业流程。企业只有通过对攻击流程中扫描探测、能力获取、渗透作业、远程控制、横向渗透、行动收割的每一个阶段进行技术防护、管理细化，并基于业务的持续安全运营，才能及时有效发现、阻断风险，避免企业损失。

人工智能作为新质生产力的重要驱动力，通过智能化手段提升了网络安全水平，在检测防护、交付能力、安全运营等安全能力上实现“提质增效”。在网络攻击"AI"化趋势明显的大背景下，天融信等安全企业多年来积极探索"AI+安全"的深度融合，基于在智慧引擎、机器学习等技术的研究基础，以及长期积累的海量安全知识数据，依托安全实验室的支撑，推动安全能力建设从单点增强防护向智能聚合分析、全面智能协同能力进化，实现 AI 融入安全的真正结合。

在大背景环境下，国家也相继颁布了一系列重要指示和法律规范，本产品主要为**行业监管与企业自监管相关政策重要的技术支撑手段。**

- 《关键信息基础设施安全保护条例》

国务院发布涉及公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域要求运营者设置专门安全管理机构，开展网络安全监测、检测和风险评估发现安全问题要求整改，并向保护工作部门、公安机关报告。

- 《公共互联网网络安全威胁监测与处置办法》

工业和信息化部发布要求相关专业机构、基础电信企业、网络安全企业、互联网企业、域名注册管理和服务机构加强和规范公共互联网网络安全威胁监测与处置工作发现网络安全威胁后，本单位问题应当立即进行处置涉及其他主体，上报工信部与通管局。

- 《互联网政务应用安全管理规定》

网信办、中央编制委员会、工信部、公安部联合发布党政机关要实时监测互联网政务应用运行状态和网络安全事件情况《规定》划定了监督职责，违反及未能正确履行本规定，依法追责。

- 《通信网络安全防护管理办法》

工业和信息化部发布要求“通信网络运行单位”应当建设和运行通信网络安全监测系统，对本单位通信网络的安全状况进行监测。电信管理机构开展通信网络安全防护工作的情况进行检查，违反本规定，由电信管理机构依据职权责令改正。

- 《工业控制系统网络安全防护指南》

工业和信息化部发布要求工业和信息化主管部门，有关企事业单位在工业控制网络部署监测审计相关设备或平台，在不影响系统稳定运行的前提下，及时发现和预警系统漏洞、恶意软件、网络攻击、网络侵入等安全风险。

- 工信行业监管考核要求

工信部《关于印发 2022 年省级基础电信企业网络与信息安全工作考核相关网络安全标准规范的通知》（工网安函〔2022〕303 号）、《2023 年基础电信企业省级公司网络与信息安全工作考核要点与评分标准》（工信厅网安函〔2023〕83 号）、《2023 年省级基础电信企业专业公司网络与信息安全工作考核要点与评分标准》，明确提出要求基础电信企业开展木马和僵尸网络监测与处置系统建设，对系统的能力和数据质量进行检测评估，对建设运维情况进行书面通报，并按通报次数扣分。

- BM 行业政策要求

《“十四五”时期全国 BM 事业发展规划》、《“十四五”时期全国 BM 科技工作实施意见》、《全国 BM 技术检查监管平台总体建设方案》、《BM 技术监管产品规划》《全国 BM 技术检查监管业务体系框架》等政策颁布实施，统筹推进全国 BM 技术检查监管平台建设工作。根据建设任务要求，到 2025 年，全面完成 BM 技术检查 JG 平台的建设任务，形成覆盖全市党政机关、BM 资质单位（以下简称“机关单位”）的 BM 管理全要素、全流程综合 JG 格局。充分发挥技术检查 JG 平台在建立机关单位 BM 态势基础业务数据、发现机关单位 BM 态势隐患、促进机关单位安全 BM 防护方面的重要作用，提升 BM 行政管理部门态势感知能力、业务协同能力、风险预警能力和应急处置突发能力。

- 《关于落实网络安全保护重点措施 深入实施网络安全等级保护制度的指导意见》（公网安〔2022〕1058 号）

《指导意见》要求全面落实“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施。深化网络安全等级保护建设整改、检查检测、监测预警、应急处置等各项重点工作。工作目标涵盖网络安全整体防护能力和水平显著提升。加强安全监测、通报预警、检测评估、演习演练、应急处置和技术对抗，显著提升网络安全整体防护能力、技术对抗能力和抵御大规模网络攻击能力。

- 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》公安部 1960 号文

《指导意见》是落实等级保护 2.0 制度的重要标志，系统、明确地对关键性基础设施的保护提出了要求，由公安部制定出台。于 2020 年 7 月 22 日，公安部下发 1960 号文。进一步健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置重大网络安全事件，切实保障关键信息基础设施、重要网络和数据安全。

- 《检察工作网安全保障系统建设指导意见》

由中华人民共和国最高人民检察院发布，《指导意见》提出“依据国家网络安全等级保护三级标准要求，建立和完善检察工作网网络安全保障系统，增强精确感知的安全预警能力和及时有效的安全防御能力。”涉及高检院和省级院态势感知平台、地市级检察院网络威胁探针设备建设，需要安全风险评估和威胁感知，实现检察工作网安全事件的辅助决策和应急处置。

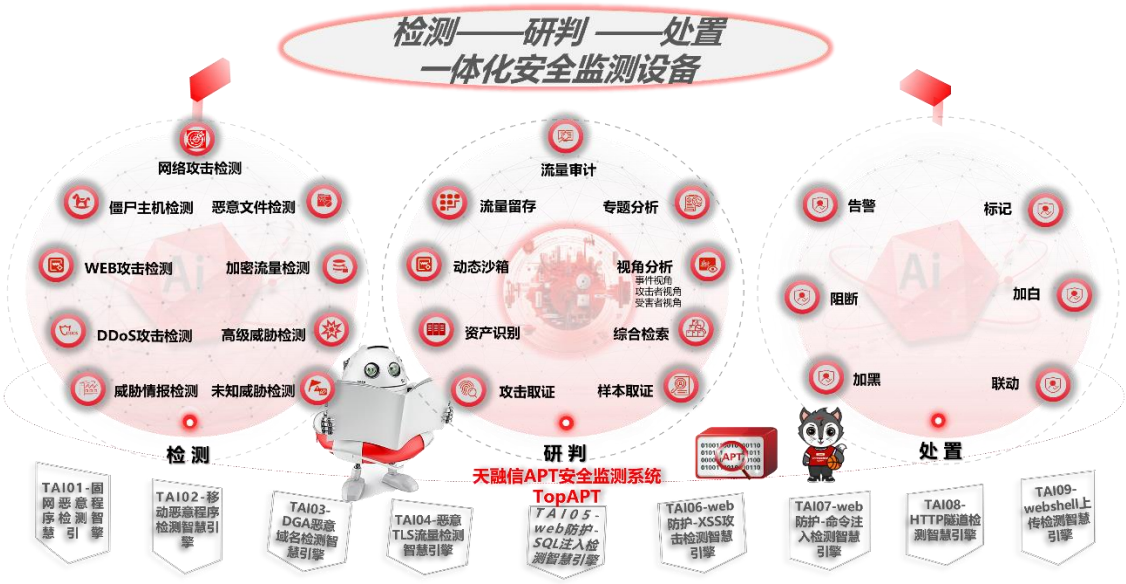
- 《人民法院信息化建设五年发展规划（2021-2025）》

由中华人民共和国最高人民法院发布，要求构建人民法院主动安全防御体系，建立常态化全行业渗透测试机制，及时发现和修复安全漏洞；建设实网攻防演练平台，最高人民法院组织各级人民法院建立常态化实网攻防演练机制；完善安全风险分级分类，优化安全事件应急预案，定期开展安全培训，补强安全防御薄弱环节，提升基于安全态势的全方位主动安全防御能力。

2 产品概述

2.1 产品简介

天融信全流量监测产品是天融信公司自主研发的集检测、研判、处置为一体的一体化安全监测设备。产品内置九合一检测引擎，具备网络攻击检测、僵尸主机检测、WEB 攻击检测、DDoS 攻击检测、威胁情报检测、恶意文件检测、加密流量检测、高级威胁检测、未知威胁检测九大检测功能，同时运用 TAI 系列智慧引擎核心技术，能够检测各种已知和未知威胁。产品结合流量审计、流量留存、动态沙箱、资产识别、攻击取证、样本取证等功能，支持从事件、攻击者、受害者等不同角度分析研判，能够从海量告警中发现高价值威胁事件，并通过设备本身或联动其它安全产品实时响应处置。产品既可以作为探针设备与天融信态势感知系统协同，构建前后端系统，满足行业监管场景需求，也可以作为一体化安全监测设备满足中小企业自监管场景的一体化部署需求，可广泛适用于运营商、金融、能源、政府、中小企业等行业或领域。



2.2 产品架构

产品采用独特的 SmartAMP 技术架构，支持同构和异构处理器计算资源工作分配，并能够在两种模式之间灵活转换，结合基于字节流的动态平衡算法，既可以适应各种复杂

网络流量处理，也可以针对分组结构的国产化处理器优化，从而最大化发挥处理器计算能力，保障产品运行的高性能和高可靠性。产品可以接收线路分光或交换机镜像的流量数据，也可以从 pcap 文件中直接读取流量数据，从架构上同时支持在线和离线两种检测方式，并广泛支持互联网、工业网、移动网、物联网，车联网等不同场景网络协议，是全流量全场景集检测、研判、处置为一体的闭环处理技术结构。

- **协议解码：**产品利用网卡的 RSS 和 DDP 特性，最大限度发挥多核计算性能，并实现从以太网（VLAN、QINQ），到广域网（MPLS），到云环境（VXLAN、SRv6）的高性能流量接入。
- **会话管理：**在硬件分流的基础上，增加了软件会话调度功能，实现了多个 CPU 核心之间的会话负载均衡。同时，它还优化了网络协议栈，以适应检测设备的需求，能够轻松处理半连接、不完整连接以及包乱序连接的情况。
- **应用识别：**支持基于特征、端口、统计和父子连接关联等多种识别方法，能够精确识别流量中的协议和上层应用。它内置了算法识别引擎，有效解决了弱特征应用识别不准确的问题。此外，产品还支持自定义扩展，以实现更精确、全面的应用程序识别，为后续协议的解析和还原提供了坚实的基础。
- **流重组：**产品采用目标操作系统流重组技术，有效优化了对重叠及不规则 TCP 报文的处理能力。此外，该产品通过应用层协议状态清洗机制，显著减少了处理延迟，从而提升了整体性能。
- **协议解析：**产品通过全面而细粒度的流式解析应用层事务，深入感知内容层，能够完整还原整个交互过程。同时，它对协议字段进行规范化处理，使得任何企图绕过的攻击行为都无处隐藏。
- **文件还原：**产品根据应用层状态和文件内容智能识别文件类型，并增加人工智能的筛选方式，从海量文件中高效、精准筛选出需要检测的样本。在管理面将数据流中提取的文件块，恢复成原始文件，以便进行后续的分析及检测。

产品以威胁检测能力为核心，基于自研九合一检测引擎，形成了一个综合的威胁检测系统，能够从多个维度监控和分析网络活动，及时发现并响应各种安全威胁。九合一检测引擎包含：网络攻击检测、僵尸主机检测、WEB 攻击检测、DDoS 攻击检测、威胁情报检测、恶意文件检测、加密流量检测、高级威胁检测和未知威胁检测。

产品威胁检测能力依托五大知识库和九大 TAI 检测智慧引擎，五大知识库和九大 TAI 检测智慧引擎为威胁检测提供强大的数据支撑和深度智能分析能力，确保能够精确识别和响应各种网络威胁。

- **TAI01-固网恶意程序检测智慧引擎。**基于混合非加密哈希方法，对样本元数据，字节分布，函数调用进行处理，高效提取非冗余关键信息，建立机器学习检测模型，是发现未知威胁特别是 APT 攻击的有力工具。
- **TAI02-移动恶意程序检测智慧引擎**。通过先进的结构分层信息萃取技术，结合多维度融合比对，快慢因子分离，多阈值机制，实现对移动恶意程序的快速精准识别。
- **TAI03-DGA 恶意域名检测智慧引擎**。通过深度循环神经网络模型(Deep-RNN)和多层感知机技术建立检测模型，高效识别定位超过 50 余种 DGA 恶意域名家族，具备高准确率和低误报率。
- **TAI04-恶意 TLS 流量检测智慧引擎**。通过深度包解析技术提取加密流量握手协议字段和流量传输统计数据，建立 AI 检测模型，无需解密即可精准辨识 TLS 加密流量中的异常模式，有效应对加密通信中的恶意行为风险。
- **TAI05-web 防护-SQL 注入检测智慧引擎**。采用双向门控循环神经网络(Bi-Gated Recurrent Unit)架构，利用词嵌入技术实现 SQL 语句的深度语义表征，支持多种编码，多注入点的检测，能够应对传统规则难以识别的复杂 SQL 注入攻击。
- **TAI06-web 防护-XSS 攻击检测智慧引擎**。采用模型堆叠策略，建立多层模型架构，使每一层模型都能专注于特定模式的跨站脚本(XSS)攻击，显著提升对 XSS 攻击的检测精度和模型鲁棒性。
- **TAI07-web 防护-命令注入检测智慧引擎**。基于 Windows 和 Linux 系统命令建立全面覆盖的训练数据集，采用高性能 GBDT 算法优化模型训练过程，实现快速，低内存消耗的高准确率检测，能够有力阻止利用 WEB 漏洞执行有害命令。
- **TAI08-HTTP 隧道检测智慧引擎**。基于海量流量数据并结合随机森林（Random Forest）算法进行模型训练，通过分布式训练和并行执行提升处理海量数据的能力，自动化进行模型评估验证和持续优化，同时加入辅助评分机制，高效识别 HTTP 隧道工具流量。
- **TAI09-webshell 上传检测智慧引擎**。采用卷积神经网络(CNN)和循环神经网络(RNN)融合架构，结合自然语言处理(NLP)技术， 提取 webshell 脚本程序空间层次结构和文本之间的依赖关系，基于全面的 token 信息增强表达进行检测，可以有效的对抗代码混淆和逃逸技术。

此外，产品集成了沙箱技术，采用了动静结合的鉴定方式和先进的机器学习引擎，能够深度分析文档、可执行文件、压缩文件和脚本等各类文件的安全威胁。产品运用基

于沙箱的恶意代码检测技术、机器学习检测技术以及反逃逸行为检测技术等多种高级检测手段，精准识别病毒、木马、蠕虫、勒索软件等已知和未知威胁。产品能够提供内容详实的分析报告，展示威胁鉴定结果，从而增强用户对高级持续性威胁（APT）的防御能力。

产品具备流量审计、流量留存、动态沙箱、资产识别、攻击取证、样本取证、综合检索、视角分析、专题分析九大研判引擎。这些研判分析手段，能够帮助用户快速感知潜在威胁的入侵路径，构建攻击事件的完整视图，绘制攻击者的详细轮廓，也为深度挖掘潜在的未知威胁提供了重要线索。同时产品支持告警、标记、阻断、加白、加黑、联动等处置方式，为用户提供了从预警到响应的闭环安全解决方案，确保在面对复杂多变的网络威胁时，能够迅速采取行动，有效降低安全风险。

3 优势特点

3.1 全检测

产品内置九合一检测引擎，具备网络攻击检测、僵尸主机检测、WEB 攻击检测、DDoS 攻击检测、威胁情报检测、恶意文件检测、加密流量检测、高级威胁检测、未知威胁检测九大检测功能。实现对扫描探测、拒绝服务攻击、跨站攻击、注入攻击、暴力猜解、弱口令、溢出攻击、木马、蠕虫、挖矿、勒索、隐蔽隧道、DGA 恶意域名、爬虫、钓鱼邮件、敏感信息泄露、恶意加密流量、APT 活动等威胁的全面检测，对网络节点中的流量可检尽检、应检尽检。

3.2 全留存

全流量监测产品可对业务流量、加密流量、攻击流量、恶意程序传播流量、异常流量实现 7×24 小时实时无遗漏的留存，确保网络活动的每一个细节都被精准记录与检测。通过完整流量留存为攻击溯源提供关键证据链，支持快速回溯攻击路径、精准定位威胁源头，大幅提高安全事件定位效率，提升应急响应速度，满足从日常运维到高级威胁应对的全场景溯源需求。

3.3 全场景

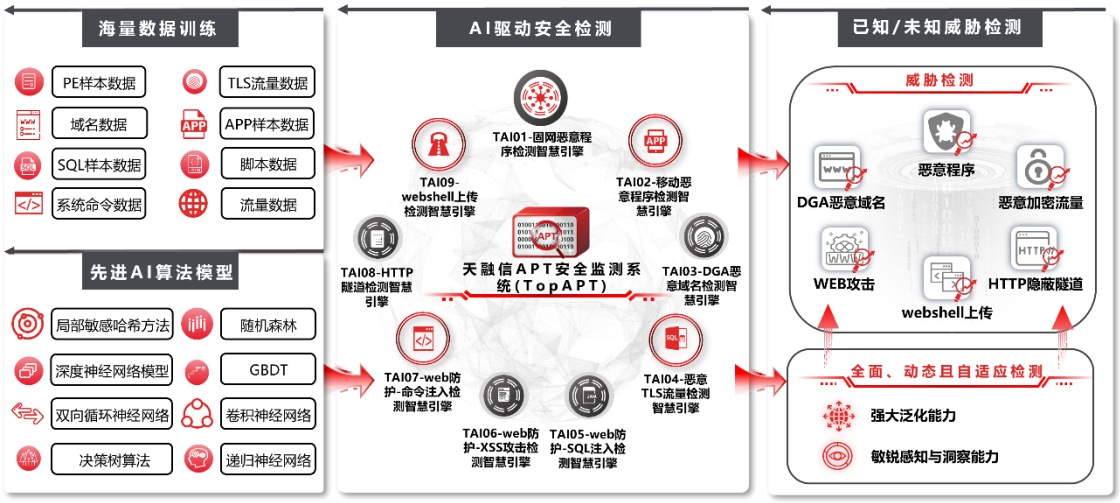
产品依托深度协议解析引擎，可以在固网、移动网、工业互联网、物联网、车联网及云环境等所有场景中使用，全面监测各场景通信交互与数据传输，深度解析各场景流量的应用协议，实时预警潜在威胁，为能源、运营商、交通、金融、企业等全行业用户提供安全监测保障。

3.4 全闭环

产品是集检测、研判、处置为一体的一体化安全监测设备。当产品监测到攻击事件、恶意程序传输、异常流量或数据泄露等情况时，会实时触发告警，并自动从事件、攻击者、受害者等视角分析研判，在海量告警中发现高价值威胁事件，可直接或联动其它产品进行处置。形成从预警到处置的高效全闭环流程，有效提高用户网络安全运营效率。

3.5 AI 融入安全

天融信专注于 AI 技术在安全检测中的实践和应用，凭借多年持续积累的海量恶意程序和流量数据，结合深度神经网络等先进 AI 算法，精心打造出 TAI 系列检测智慧引擎，并将其应用于全流量监测产品中。TAI 系列智慧引擎采用统计机器学习，深度神经网络等技术，不依赖于任何规则库，识别隐藏在复杂流量数据中的攻击，智能应对未知威胁，精准检测加了混淆的恶意程序攻击、“人工(自动化)绕过”的 web 注入攻击、复杂加密流量攻击和隐蔽隧道传输等隐匿性强且危害性高的威胁行为，同时利用模型集成门控单元神经网络等技术大幅减少检测误报。TAI 智慧引擎在全流量监测产品中的集成，显著提升了产品整体安全检测能力，成为发现未知威胁，特别是 APT 攻击的有力工具，更为用户提供了前所未有的安全保障。



4 产品核心功能

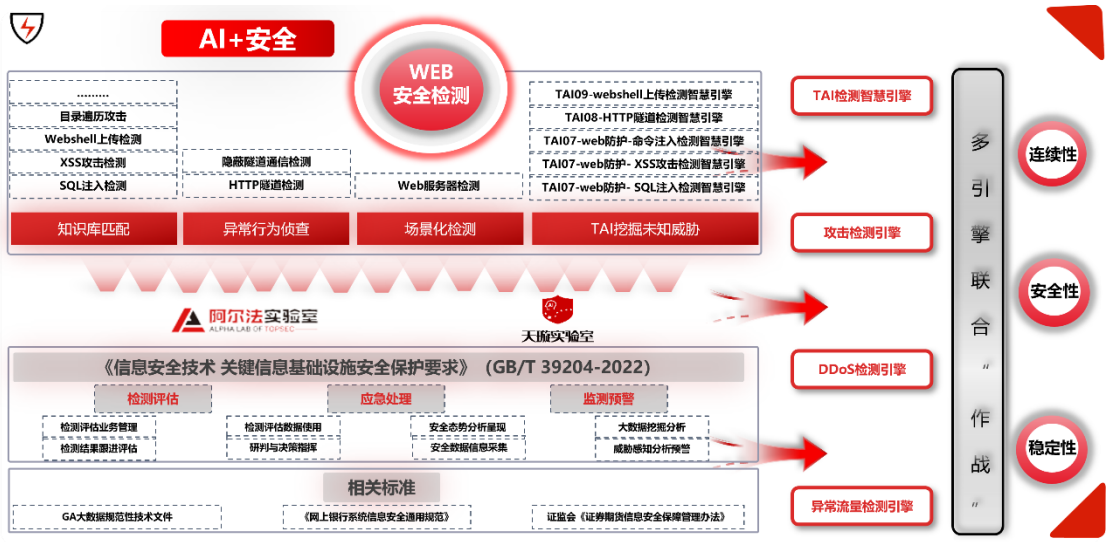
4.1 网络攻击检测

全流量监测产品依托于天融信公司专业的攻防研究实验室，通过与国际领先厂商及国家权威安全机构的紧密合作，持续监控并深入分析全球范围内的最新安全威胁与漏洞。帮助企业应对当前的安全挑战，确保企业的信息化资产安全无虞。

全流量监测产品提供网络攻击检测功能，全面检测发现包括扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、webshell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、车联网漏洞攻击、物联网漏洞攻击、凭据异常等在内的 17 大类网络攻击行为。产品攻击检测规则库以周为单位定期更新，如遇紧急事件则实时更新，从而确保及时有效的检测各种已知网络攻击行为。

4.2 WEB 攻击检测

天融信公司积极响应《关键信息基础设施安全保护要求》，在 WEB 安全检测领域，专注于监测预警、应急处理、检测评估三大核心业务场景。为了满足特定场景下的流量检测需求，全流量监测产品提供全面的 WEB 安全检测功能，包括异常行为侦查、知识库匹配、场景化检测以及利用 AI 技术挖掘未知威胁等。在 WEB 攻击行为检测方面，全流量监测产品通过融合 AI 技术与多种检测引擎，实现从点到面的全方位 WEB 攻击行为挖掘，多重引擎联合作战不仅提高了检测的准确性，还增强了对新型攻击和复杂攻击的识别能力，确保 WEB 业务的安全性、连续性、稳定性。



产品具备全面的 WEB 攻击检测能力，检测发现包括 SQL 注入、XSS 攻击、HTTP 隧道、webshell 上传、目录遍历攻击、WEB 缓冲区溢出攻击、WEB 漏洞攻击、WEB 越权攻击、WEB 远程代码执行攻击、WEB 扫描攻击、WEB 口令暴力破解等 WEB 攻击行为，显著提高用户 WEB 应用的安全性，有效应对各种 WEB 安全检测场景。

4.3 僵尸主机检测

全流量监测产品依据木马及蠕虫病毒的行为活跃周期和入侵控制手段，挖掘分析结果。采用行为特征匹配、智慧引擎分析、异常行为监测等多种手段，全面识别发现网络中的木马传播、被控制的“肉鸡”、挖矿、勒索软件攻击等安全威胁，实时监控全球范围内的控制主机、境内控制主机、僵尸主机以及木马文件的传播行为。依托监控内容形成僵木蠕攻击大屏，为用户提供全面的网络安全视图。

全流量监测产品具备精准识别并捕捉网络异常行为能力，包括僵尸网络活动、木马控制、蠕虫传播、勒索病毒以及移动端木马控制等。产品不仅能够提取和分析通信行为特征，还结合了木马特征库匹配和威胁情报匹配等多种检测技术，从而有效地识别和定位网络中的僵木蠕威胁。此外，全流量监测产品提供异常行为报文取证功能，详细记录僵木蠕事件信息，包括攻击源的详细数据、事件涉及的应用协议以及事件的具体描述等，为后续的安全分析和响应措施提供了坚实的数据基础。

全流量监测产品还具备对威胁事件进行综合研判能力，不仅能够检测和记录威胁，还能对发现威胁进行深入分析，从而为用户提供更加精确的安全建议和响应策略。这种综合研判能力，使得全流量监测产品成为了一个强大的网络安全工具，有效帮助用户在面对复杂多变的网络威胁时，做出更加明智和迅速的决策。

4.4 DDoS 攻击检测

全流量监测产品具备独立的 DDoS 检测引擎，专门设计用于识别和检测分布式拒绝服务攻击以及 DoS 攻击行为。该引擎基于行为分析，并结合阈值设置、协议分析和端口监控等多种技术，通过构建统计型攻击模型和异常数据包攻击模型，全面检测包括 IP FLOOD、IP FRAG FLOOD、端口扫描、IP 地址扫描、ICMP FLOOD、TCP FLOOD、SYN

FLOOD、ACK FLOOD、SYNACK FLOOD、FIN FLOOD、RST FLOOD、UDP FLOOD、HTTP FLOOD 等在内的多种 DoS/DDoS 攻击行为，产品多维度的 DoS/DDoS 攻击检测能力，确保企业网络链路和业务操作的安全性与稳定性。

全流量监测产品利用先进的基线自学习技术，能够智能地学习和理解网络的正常流量模式，并据此识别出偏离正常模式的异常行为。此外，全流量监测产品融合数据转发、内核检测、数据挖掘等多种独立检测算法，对网络流量进行深入分析，提取关键特征，对数据进行预处理，并将其输入到模型训练模块中，最终输出高准确性的识别结果， 使全流量监测产品能够自动适应网络流量的动态变化，有效检测未知的 DDoS 攻击，让用户免受因链路拥塞、服务器资源耗尽而导致的业务无法正常运行访问情况。

4.5 恶意文件检测

全流量监测产品提供恶意文件检测功能，采用多检测引擎协同工作机制，深度检测和分析恶意文件。其功能主要包括以下关键组件：

文件类威胁情报：利用威胁情报数据，帮助产品识别已知恶意文件和潜在威胁。

TAI01-固网恶意程序检测智慧引擎：引擎分段提取样本元数据、字节分布、函数调用等信息，剔除冗余、无效数据，训练高效 AI 模型。该智慧引擎无规则库依赖，确保检测恶意文件的准确性与效率，是发现未知威胁特别是 APT 攻击线索的有力工具。

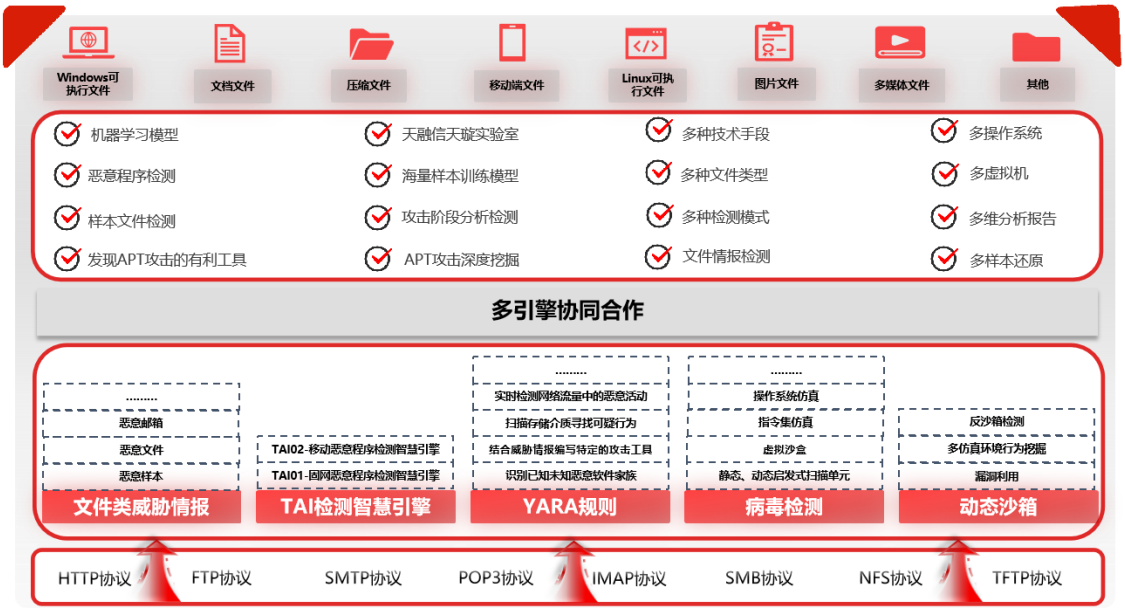
TAI02-移动恶意程序检测智慧引擎：引擎提取移动恶意程序结构信息形成表征向量，通过多维度比对、快慢检测因子分离、多阈值机制等，辨识恶意文件。该智慧引擎可自动归类样本家族，抗混淆能力强，为移动网络安全提供有效支撑。

YARA 规则：使用 YARA 规则识别基于文本或二进制模式的恶意文件，YARA 规则匹配机制具备快速、灵活等特点。

病毒检测：采用病毒检测引擎，并依托指令集仿真、启发式扫描等技术，检测已知恶意文件。

动态沙箱检测：通过创建一个隔离的虚拟操作系统环境来执行可疑文件，实时监控恶意文件行为并记录行为特征。动态沙箱检测能够揭示恶意文件在实际运行中可能展现的潜在风险行为，结合可视化技术，不仅能够捕捉到恶意文件的行为轨迹，还能够使这些行为轨迹的分析变得更加直观和易于理解 。

在沙箱动态分析中，产品具备捕捉和记录恶意文件关键风险行为的能力，包括但不限于对文件系统的修改（例如安装设备驱动程序、调整系统配置文件）、对注册表的更改（例如更新注册表键值、调整防火墙配置）以及网络活动（例如域名解析、发起 HTTP 请求）等。通过细致记录这些行为，产品为安全专家提供了深入洞察恶意文件操作机制和潜在威胁的途径。这种深入的分析不仅揭示了恶意文件的行为模式，还帮助专家理解其目的和攻击策略。这些信息对于制定针对性的防御措施至关重要，使安全团队能够更有效地预防和应对复杂的网络威胁，保护企业关键资产安全。



此外，产品还采用了文件哈希值计算、查找字符串、病毒查壳、PE 文件头分析等一系列技术手段来识别和分析潜在的恶意文件，这些综合的检测方法使得全流量监测产品具备全面而深入的恶意文件分析能力。以多层面、多技术的检测策略为支撑，不仅提高了恶意文件检测的准确性，还增强了对未知和变种恶意文件的检测能力，确保用户网络环境的安全性和业务的连续性，保护用户免受复杂网络威胁的侵害。

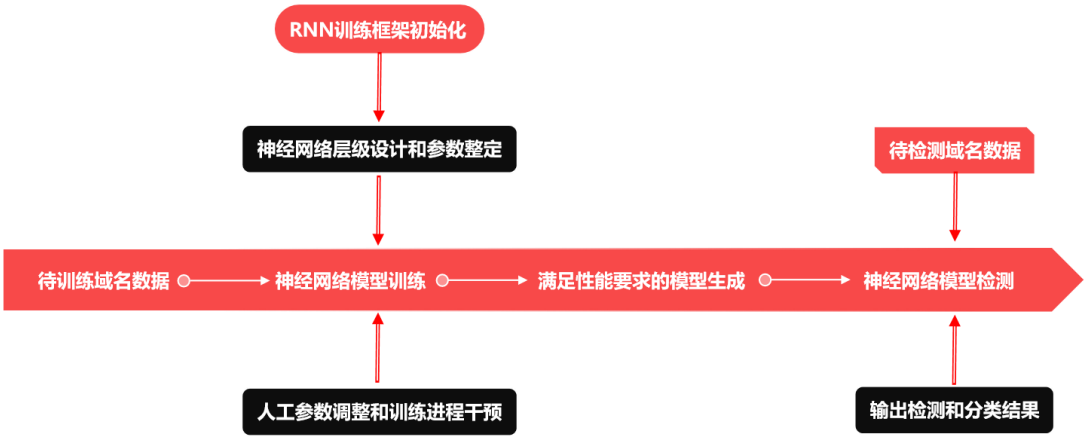
4.6 未知威胁检测

在数字化时代，网络攻击手段不断演变，尤其是那些尚未被广泛识别的未知威胁，它们常常能够无声无息地避开传统安全措施。传统网络安全检测依赖于不断更新的已知特征规则库，这种方法缺乏时效性和主动性，难以有效识别和预防未知威胁。

为了提升网络安全检测能力，全流量监测产品通过 TAI 系列检测智慧引擎，在不依赖任何规则库情况下，达到高效、精准的威胁检测能力，突破了传统检测技术的局限性，它不仅能检测各种传统攻击行为，还能够检测未知威胁，从而显著提升了整体安全检测能力，成为发现未知威胁，特别是 APT 攻击的有力工具，更为用户提供了前所未有的安全保障。

- **DGA 恶意域名**

攻击者常常利用 DGA 域名算法随机生成恶意域名，这些域名使用传统黑名单和 URL/域名过滤无法检测发现。为了解决 DGA 恶意域名随机生成难以检测问题， TAI03-DGA 恶意域名检测智慧引擎的深度循环神经网络模型可深入挖掘分析域名特征，具有自动提取特征的能力，能够有效提取域名的字母组合特征，并捕捉到域名中字母的位置信息，如域名中的首部和尾部字符、字母间的位置关系等特征，通过特征学习域名之间的隐藏共性可对 DGA 恶意域名高效检测发现。在此基础上，TAI03-DGA 引擎的设计注重于高准确率和低误报率与漏报率，利用深度神经网络模型对同类域名之间隐藏共性的提取，识别并定位 50 余种当前流行的 DGA 恶意家族，涉及木马、后门、挖矿、勒索等多种攻击形式，同时采用先进自动化的研判机制，显著提升对恶意域名的检测能力和准确性。



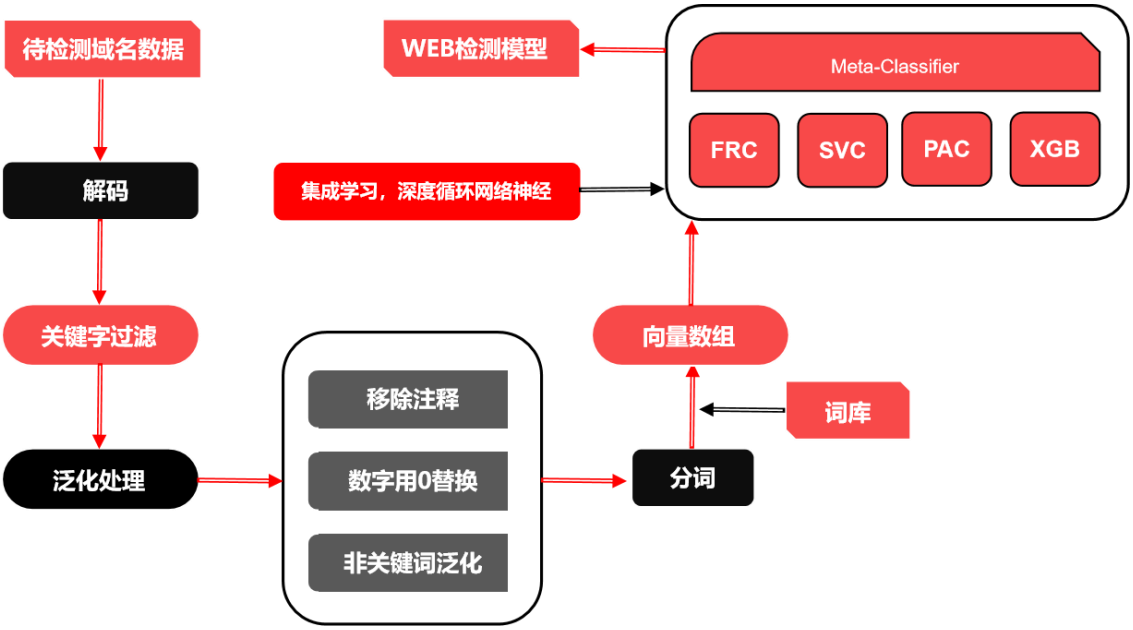
- **恶意 TLS 流量**

加密流量因难以解密常被忽略检测，或检测中仅对 IP、域名及证书进行威胁情报匹配，易被攻击者采用信息伪装正常加密会话方式绕过检测。解密检测需要对应密钥，且性能消耗过高，难以实现精准检测。为了解决恶意 TLS 流量加密难检测，易绕过的检测难点。全流量监测产品中的 TAI04-恶意 TLS 流量检测智慧引擎支持机器学习算法优选，

迭代和交叉验证训练模型，旨在深入分析和识别 TLS 流量中的异常模式和行为。该引擎能够在不解密的情况下，深度挖掘流量内在模式，结合天融信完善的数据支持，在海量训练数据之间学习到隐藏共性。机器学习的方法进行数据增强与标准化，增加模型的泛化能力，优化分类准确度，显著降低误报和漏报率，实现对恶意 TLS 流量进行准确分类，为加密流量的检测提供有力的支撑。

- **WEB 类攻击**

针对 WEB 业务系统的入侵成为近些年最主要入侵方式，攻击者利用 SQL 注入、XSS 攻击、命令注入、webshell 等 WEB 类攻击，使用变形或混淆等方式绕过规则检测，实现 WEB 业务层面入侵。传统检测方式一般采用增加规则或扩大缓存队列等检测手段，势必会影响设备性能，且无法满足检测时效性要求。为了解决 WEB 类入侵攻击绕过问题，全流量监测产品为每类攻击设计 AI 模型，实现 WEB 类攻击的动态化威胁感知，摆脱传统特征匹配检测技术的束缚，更加智能、高效和精准的应对 WEB 类未知威胁攻击，有效保障用户 WEB 业务的安全性。

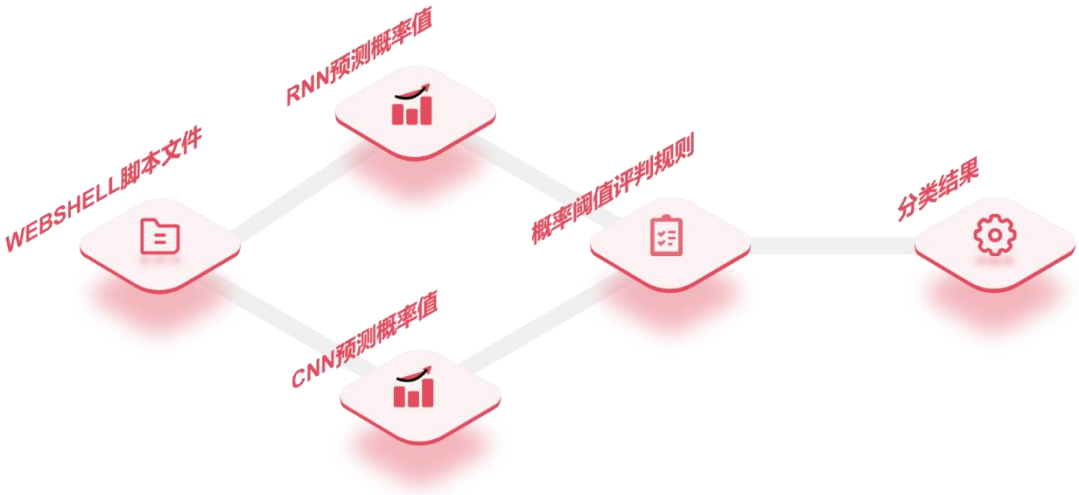


TAI05-web 防护-SQL 注入检测智慧引擎具备双向门控单元循环神经网络技术，针对黑/白 SQL 语句样本进行训练，深度解析 SQL 语句语义，并内置防误报机制，可有效应对规则无法检测的攻击；

TAI06-web 防护-XSS 攻击检测智慧引擎采用堆叠法，运用多层模型训练能力，以提升对 XSS 攻击的检测精度和模型稳定性。该引擎通过深度学习对差异性数据优化，有效提升预测精准度与稳定性，避免机器学习过程中常见的误报问题。通过持续的算法优化，该引擎可精准识别复杂的攻击行为，超越传统的特征匹配方法，为 WEB 业务提供全面的安全防护，确保网络环境的安全性。

TAI07-web 防护-命令注入检测智慧引擎基于 Windows 和 Linux 系统命令，具备相互组合构建全面的覆盖性训练数据集能力。该引擎采用高性能 GBDT 算法，优化训练过程并提高模型性能。GBDT 算法快速的训练速度、低内存消耗和高准确率的特性使得该引擎在处理大规模数据时更为高效和精确。通过并行处理和分布式训练，进一步提升了模型处理海量数据的能力。通过覆盖 HTTP 协议全字段的检测，该引擎能够有效地检测并阻止利用 WEB 漏洞执行有害命令，从而保护系统免受命令注入攻击的影响，为 Web 业务提供了强有力的安全保障。

TAI09-webshell 上传检测智慧引擎具备深度学习技术，结合自然语言处理理念，通过特征提取技术整合词频特征和词嵌入特征，并基于完整特征库获取信息增强特征表达，构建全面的 AI 检测模型。该模型可深入分析 webshell 脚本的行为模式和代码结构，相较于传统基于规则和机器学习的检测方法，支持深度神经网络的多层抽象能力，引擎能够有效识别并抵御恶意脚本的混淆和绕过行为，从而显著提升了检测的准确性和效率。



- **隐蔽隧道类攻击**

攻击者在入侵成功后的控制阶段，为了更加隐蔽的与目标进行通讯交互，会利用协议请求头部的某些字段传输恶意内容，实现隐蔽隧道通信。因会话采用正常会话机制，使用传统特征匹配很难检测，容易被绕过。为了有效遏制隐蔽隧道通信行为，全流量监测产品中的 TAI08-HTTP 隧道检测智慧引擎，采用随机森林（Random Forest）算法进行模型训练能力，实现了自动化的模型评估验证和持续优化。该引擎通过分层检测机制，不仅能够识别 HTTP 隧道的存在，通过深度分析网络流量和行为模式，还能进一步高效识别各种隧道工具名称。为提高检测结果的可解释性和可信度，设计了辅助评分系统，该系统在解决机器学习检出结果可解释性差的同时进一步提高模型的准确率。在模型训练过程中，融合机器学习算法与专家知识进行误报研判和精准识别，使引擎在处理复杂和混淆的隐蔽隧道通信时更为精准。该引擎有效解决攻击者利用 HTTP 隧道隐蔽通信提升攻击隐蔽性的问题，发现并增强隐蔽通信行为的安全检测能力。

- **文件未知威胁检测**

传统的恶意文件检测方法，例如病毒库哈希（hash）特征匹配，存在明显缺陷：一旦恶意文件特征部分的二进制代码发生微小变化，其哈希特征值也会改变，但是恶意样本仍具有危险性，导致传统检测失效，且无法识别未知的恶意文件。为了有效应对恶意文件的检测难点，全流量监测产品中的 TAI01-固网恶意程序检测智慧引擎、TAI02-移动恶意程序检测智慧引擎，运用机器学习统计特征提取技术，通过多维度的特征提取和对比分析，为不同类型的恶意样本设计了专门的训练模型，确保能够在不依赖任何规则库，病毒特征库的情况下，全面检测网络环境中未知恶意程序，有效解决了特征库覆盖面不足和恶意程序变种逃避检测的问题。在实际应用中依靠快速检测病毒、低性能消耗和强抗混淆等多重检测优势，全面提升了用户对文件未知威胁的检测能力，成为发现未知威胁，尤其是 APT 攻击线索的有力工具。

4.7 异常流量检测

全流量监测产品异常流量检测包含： 非标端口通信检测、违规应用检测、钓鱼邮件检测。

非标端口通信检测引擎允许用户根据自身业务情况绑定业务相关端口，生成业务端口通信基线，有效应对非标端口通信行为，包括检测 UDP 承载 IPSEC 隧道协议下 500、4500 端口流量。

在违规应用检测方面，全流量监测产品提供了一个集成的解决方案，覆盖了远程控制、挖矿、隧道、HTTP 代理和自定义等多种潜在威胁。这些威胁可能导致敏感数据泄露、系统资源滥用和非法远程访问，从而严重威胁组织的网络安全和业务连续性。产品具备行为分析和异常流量检测技术，能够及时发现远程控制和挖矿等恶意行为。支持异常流量非法外联自学习，并自动记录外联信息（IP、协议、端口、连接数等）。深度包检测和协议分析技术使得隧道和 HTTP 代理等隐藏通信行为得到有效监控。自定义规则的灵活性使用户能够根据安全策略和风险偏好，定义和监测特定的违规应用行为。

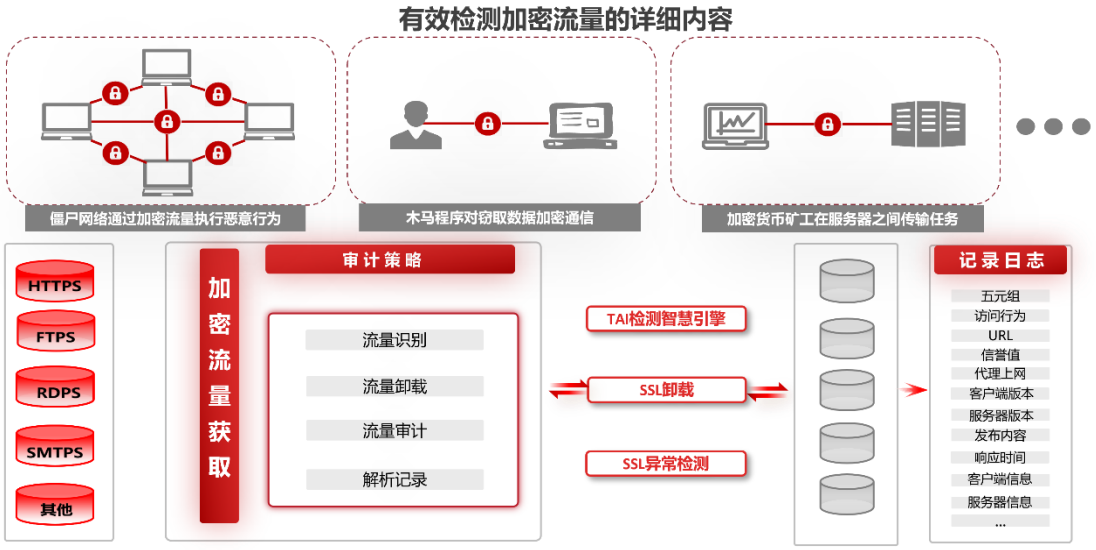
在钓鱼邮件检测领域，全流量监测产品具备超越传统杀毒软件特征检测的先进技术手段，能够实现对钓鱼邮件的及时和有效识别。通过综合运用行为分析、威胁情报和机器学习等技术，显著提升了对钓鱼邮件的检测能力，从而有效保护用户账户安全，防止敏感信息的泄露。

4.8 加密流量检测

在网络通信中，确保传输内容的安全，防止数据被篡改或滥用，通常采用加密技术来保护通信流量，然而这种加密信息的传输也给恶意流量提供了隐藏和逃避检测的机

会。为揭露恶意程序的加密通信行为，天融信安全研究团队通过对恶意程序行为的深入分析，提取出恶意程序加密通信的指纹特征，并建立指纹特征库，使得恶意程序的加密通信无处隐藏。

针对加密流量检测，全流量监测产品具备 TAI04-恶意 TLS 流量检测智慧引擎结合 SSL 卸载和 SSL 异常检测等多种手段结合的方法，可支持恶意 TLS 流量、异常握手、非法证书检测（非导入证书方式）实现对 HTTPS 等加密流量解析。给用户提供了一个全面而坚固的网络安全检测分析架构，匹配机器学习算法和行为分析技术不断提高检测的准确性和效率，确保网络环境的安全与稳定，对加密流量元数据的深度提取实现对加密流量进行解密处理和无证书检测加密通信检测的效果，检测出隐藏其中的恶意威胁信息，从而适应不断演变的网络威胁能力，为用户的关键业务提供了持续的保护。



4.9 威胁情报检测

全流量监测产品提供威胁情报检测功能，该功能所依赖的威胁情报库得到了天融信安全云服务团队的专业维护和支持。具备运用网络流量深度分析、恶意软件样本分析能力，以及广泛整合公开和私有情报源数据等多元化手段，天融信安全云服务团队能够全面、多角度地收集和整合全球最新的威胁情报。对于收集到的原始数据和信息，天融信实施了一套严格的数据处理流程。这些数据会根据威胁的严重性和潜在影响进行深入的评估和细致的分类。通过此流程能够提炼出与目标网络环境高度相关的威胁指标，从而显著提升信息系统对当前和潜在网络风险的识别和洞察能力。

全流量监测产品具备嵌入式威胁情报库，该库从海量的威胁情报数据中精选出超过800万条高可信度的威胁记录，确保了检测的高精准度和高效率。这一设计支持对多维度威胁类型的检测，威胁情报检测响应速度快，能够在网络环境的快速变化中迅速定位威胁源头。

威胁情报检测功能通过对网络数据流的深度解析，能够精准识别并提取 IP 地址、URL、域名、邮件地址等关键信息，并与内置的威胁情报库进行高效匹配。此外，全流量监测产品还具备还原和捕获恶意威胁样本的能力，这进一步增强了威胁检测的全面性。

产品具备高频率的情报更新，确保用户能够及时掌握最新的热点威胁情报信息，有效应对不断演变的网络安全挑战。与传统的基于特征的检测方法相比，全流量监测产品的威胁情报检测功能在检测范围、检测精度和响应速度上都有显著提升。有效实现对威胁的早期发现和预防，为用户在复杂多变的网络环境中提供强有力的安全保障。

4.10 综合溯源

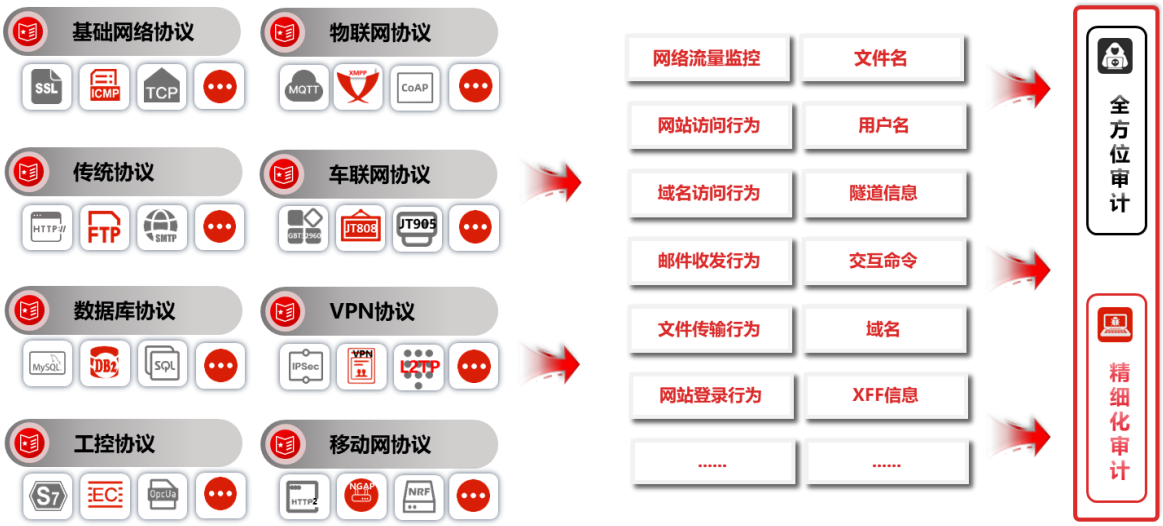
全流量监测产品通过提供丰富的协议解析和全要素数据留存，结合先进的全流量PCAP（Packet Capture）留存技术，以及秒级的数据检索能力，为用户展示完整的攻击过程。它不仅支持广泛的网络协议深度解析，确保每个会话的详细信息都被记录，还能高效保存和迅速检索所有关键数据元素，极大提升了威胁研判的精准度和日常运营效率。无论是识别潜在威胁还是追踪复杂的攻击路径，全流量监测设备都能提供强有力的支持，确保数字资产得到最佳保护。


提供全流量采集、解析、存储、检测、检索、分析、溯源整体解决方案
全包存储 全流量溯源
安全事件回溯分析及取证
全量存储
威胁检测与响应
全量采集
协议解析
威胁检测
全量存储
全流量溯源取证
威胁检测
高速数据挖掘能力
实时检测
APT挖掘
秒级检索
TopAPT
索引构建
算法模型
会话存储
全面支撑
支撑多种检测能力
攻击检测
僵尸主机
暴力破解
SQL注入
SSL卸载
非标端口
DDoS检测
威胁情报
恶意文件
加密流量
海量数据提取关键信息
强大的数据支撑
全包存储 全量回溯
溯源取证
原始流量留存
发现APT等高级威胁攻击线索
回溯分析
多维回溯分析技术
溯源威胁统计
告警关联取证
会话元数据解析
文件还原追溯
超快检索数据
在线报文预览
管理面
全流量采集
策略添加
策略匹配
过滤开关
全流量采集
取证配置下发
取证策略下发
动态缓存删减
双环链表TAJQ
发送消息处理
数据包缓存
定时任务
文件线程
缓存更新
缓存容量
数据面
数据包处理
策略采集
会话管理
数据缓存
缓存通知

4.11 流量审计

在企业复杂网络环境中，除了面对已知的网络安全威胁与不断演变的未知风险外，还面临着因网络访问与使用不当而引发的严峻挑战，包括敏感信息泄露、违规访问数据库、以及通过邮件等渠道非法传播数据等问题。这些行为不仅威胁到企业的数据安全与业务连续性，还可能引发合规性危机。因此，构建一个全面的网络行为审计系统，以有效监控并防范违规用户行为所带来的潜在威胁，显得尤为重要。

产品提供了一套综合性的网络流量审计解决方案，具备对多种常见协议深入内容层解析，实现对流量元数据的细粒度提取，帮助安全分析人员快速了解网络内容。流量审计覆盖传统协议、数据库协议、工控协议、物联网协议、车联网协议、VPN 协议、移动网协议等。



全面的网络协议支撑能力，使流量审计功能不仅限于简单的网络流量监控，而是深入到具体的网络行为层面，包括但不限于网站访问、域名访问、邮件收发、文件传输等行为，具备对网络行为的全方位、精细化审计。实时捕捉用户网络行为及通信内容，及时发现违规行为，并提取日志，帮助企业能够积极响应政策与法规的合规性要求，确保网络活动的透明度与可追溯性，更为后续全面的安全分析提供多维有力依据。

4.12 账户安全

随着企业数字化转型的加速和互联网交互的不断深化，业务系统中存储和流转的大量重要数据与信息，日益成为黑客攻击的主要目标。账户安全，作为保护这些敏感信息的第一道防线，其重要性不言而喻。如果企业未能及时采取有效措施应对暴力破解和弱

口令攻击等威胁，可能会面临信息泄露、内网安全受损、系统被非法入侵、身份被冒用以及巨大的经济损失等严重后果。

产品拥有全面的账户安全检测能力，具备弱口令检测功能，利用协议认证信息提取技术，结合预定义的弱口令字典、用户自定义字典、口令强度评估规则以及白名单机制，对各类账户密码进行全面筛查。一旦密码被判定为弱口令，即符合弱口令字典中的条目或未达到预设的强度标准，将立即发出告警，有效识别弱口令风险。该功能广泛适用于邮件、文件、远程连接、数据库及 Web 应用等多种协议。

此外，产品还具备暴力破解检测功能，旨在及时发现针对系统账户的暴力破解尝试。该功能通过分析各协议下的认证信息，统计登录失败次数，并与预设的安全阈值进行比较。如果在特定时间窗口内检测到大量失败的登录尝试，以及在认证成功前的失败次数异常，将视为暴力破解攻击行为，并立即触发告警。此功能同样覆盖邮件、文件、远程连接、数据库及 Web 应用等多种协议。

通过全面的弱口令检测与暴力破解检测功能，确保各类业务系统的账户安全，为企业的网络安全保驾护航。

4.13 研判分析

产品具备海量事件研判分析能力，通过多种尖端技术的综合应用，构建了一个全面而强大的研判分析框架。该框架的关键功能包括流量审计、流量留存、沙箱分析、资产识别、攻击取证、样本取证、综合检索、视角分析（事件视角、攻击者视角、受害者视角）、专题分析（APT 事件、挖矿事件）等，具备威胁事件日志和取证文件关联获取威胁详情能力。产品致力于提供一个综合而高效的研判分析解决方案，旨在显著提升分析效率，并确保结果的精准与可信度。其创新设计使其成为网络安全专家在应对复杂网络攻击时不可或缺的研判利器。

产品通过实时监测和记录网络全流量数据，为研判分析和事后追踪提供了坚实的基础。该产品能够进行细粒度的流量审计与留存，助力安全团队追踪攻击路径，识别攻击源，并分析攻击手法。同时，通过资产识别功能智能扫描网络，识别并分类网络中的所有资产，包括硬件、软件和数据，为资产管理和保护提供精确视图。此外，全流量监测具备攻击取证和样本取证能力，能够捕获恶意文件样本，识别攻击特征，并通过关联分析、事件追踪和回溯，揭露攻击者身份和手段。它还能识别异常网络行为，如 APT 攻击或其他恶意活动的信号，并通过异常行为分析、TAI 检测智慧引擎、嵌入式威胁情报和沙箱分析等手段，精准识别和解析网络应用协议中的潜在安全威胁。全流量监测产品还提供了原始数据包全量存储功能，为回溯分析提供完整依据，尤其对于隐蔽且持续时间长的 APT 攻击至关重要。凭借这些核心能力，全流量监测产品在数据综合检索方面表现卓越，提供了详尽的字段信息，从而为研判分析工作提供了坚实的支撑。

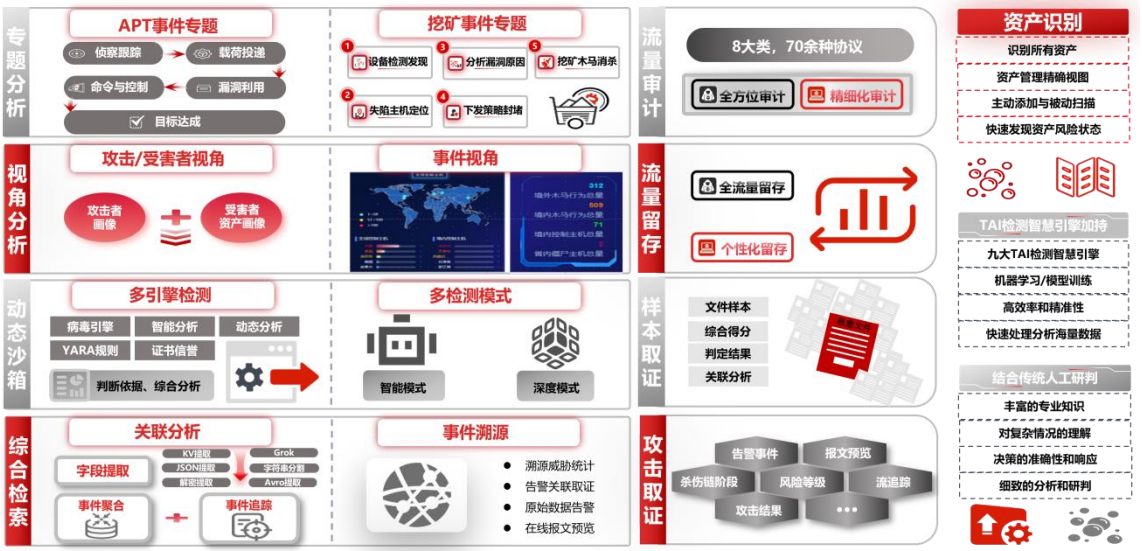
沙箱分析：全流量监测产品集成了先进的沙箱分析技术，能够在一个安全隔离的环境中运行可疑样本文件，以揭露潜在威胁的真实性质。在此过程中，系统会精确追踪并深入分析可疑样本文件的每一个执行动作，包括文件操作、网络活动和系统调用等细微行为。这些详尽的行为记录对于揭示恶意软件的行为模式和攻击者的战术意图极为关键，为安全专家提供了准确的鉴定结果数据，以便精准研判攻击行为并制定有效的防御措施。极大地提升了对网络威胁的识别精度和对复杂攻击场景的应对效率。

视角分析：全流量监测产品提供多角度的分析视角，包括事件视角、攻击者视角、受害者视角，可全面了解安全事件的复杂性和多维度影响。凭借攻击画像综合分析方法，可全面描绘攻击者的行为和目标，从而发现潜在威胁、优化安全策略、提前预测未知威胁、优化资源分配等。攻击者画像，深入描绘了攻击者的特征，包括攻击者的技术水平、攻击偏好和历史行为，从而预测攻击者可能的下一步行动；横向攻击，攻击者在成功入侵内网的某一系统后，不直接进行破坏性行为，而是通过进一步的信息收集、凭证窃取、漏洞利用等手段，逐步渗透并控制更多主机和资源的过程，结合境外攻击和境内攻击识别攻击的来源和背后的意图，全流量监测产品支持追踪横向攻击行为的挖掘能力，从而缩小攻击范围的扩散；受害资产画像则关注于受攻击影响的资产，包括类型、分布和安全状况等，具备攻击路径推演、预测和防范可能的攻击，从而提升整体的防御能力。通过构建这样一个多维度的攻击画像，不仅能够更准确地识别威胁，还能够更有效地制定防御策略，保护用户的网络环境免受侵害。

专题分析：全流量监测产品凭借其专题分析能力，为安全团队提供了识别、分析和应对 APT 事件及挖矿事件的深度洞察能力，从而确保关键资产和业务运营的安全。该产品能够全面揭示 APT 事件和挖矿事件的全貌，对预防此类攻击至关重要。产品能够精准地揭露 APT 攻击链的每个环节，包括侦察跟踪、载荷投递、漏洞利用、命令与控制直至

目标达成， 另外，挖矿专题分析能够识别挖矿软件的异常网络行为，它提供关于挖矿软件传播途径、受影响系统等详尽信息，帮助安全团队进行准确研判，并制定和实施有效的安全措施。通过这些功能，全流量监测产品为安全团队提供了对抗高级网络威胁的有力工具。

综上所述，产品综合运用了多种前沿技术来评估和研判攻击风险，再结合传统的人工分析、新兴的攻击面管理技术，以及 TAI 检测智能引擎的加持。有效提升网络安全防护的效率和精准度，有效降低误报和漏报率。通过这些综合能力，全流量监测设备能够更有效地保护企业和组织的网络安全，确保关键信息资产的安全。

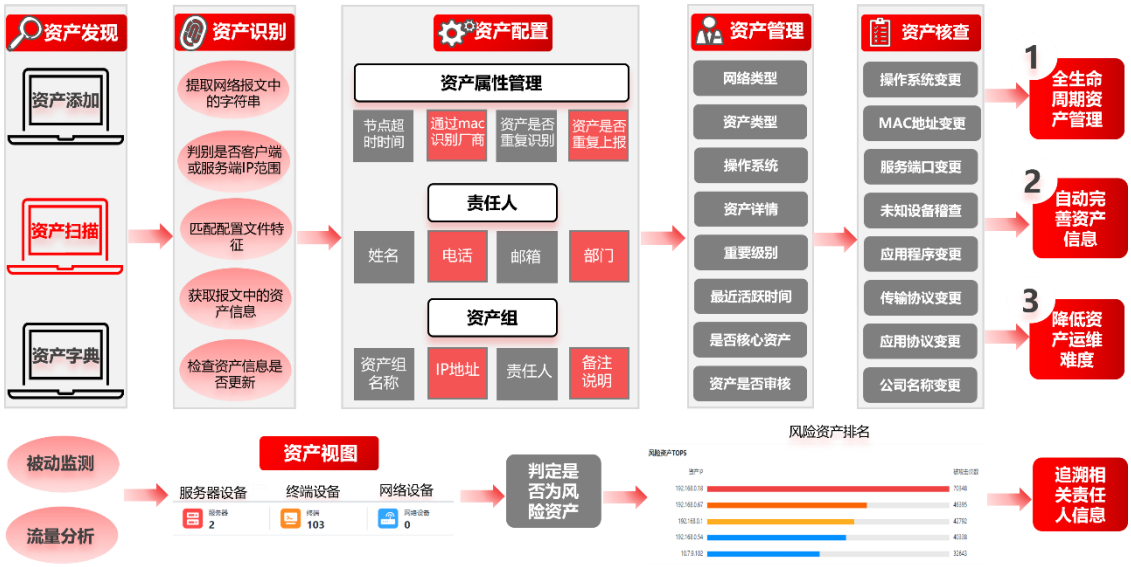


4.14 资产识别

全流量监测产品具备资产识别功能，包括主动添加与被动扫描两种识别方式，该功能由资产解析和资产管理两个部分组成。资产解析根据资产识别范围，以资产 IP 为资产标识对原始资产日志进行归并处理，生成资产数据。资产管理部分则根据功能划分为资产列表、资产组管理和责任人管理，其中资产列表模块用于资产的分类统计、展示、查询和添加等功能， 资产组管理模块负责管理资产组的相关信息，包括资产组的范围和责任人等。责任人管理模块则用于添加、更新和删除资产责任人信息。

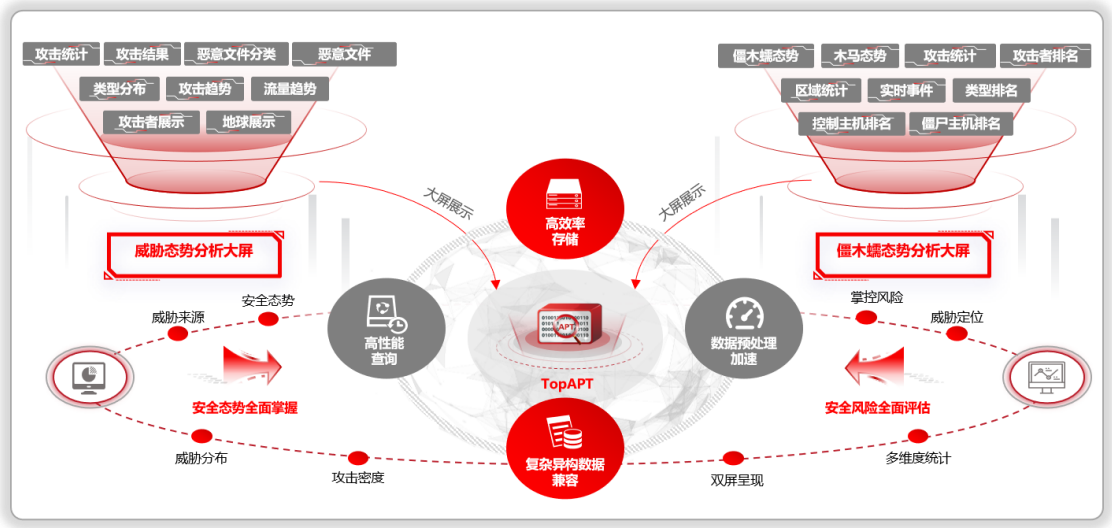
资产识别功能具备多维度的资产信息管理能力，包括资产 IP、资产 MAC、地理信息、资产类型、操作系统、应用程序、硬件厂商、资产组、责任人、资产来源、首次发现时间以及最近活跃时间等关键信息，并提供不同资产类型统计和管理功能。全面且细粒度的资产识别功能，实现了企业资产的精细化管理，使企业能够直观掌握现有信息系统资产的详细情况， 通过快速发现资产风险状态，企业可以进一步实施安全策略，从而

有效提升安全运营效率。



4.15 大屏展示

全流量监测产品具备强大的综合安全大屏分析和僵尸网络大屏分析功能，并提供丰富而多维的大屏展示能力。采用列式数据库技术结合先进的数据压缩技术，显著提升了存储效率并降低了存储成本，还加快了数据传输速度。得益于这些技术的应用，使得大屏展示在数据查询性能上更加灵活高效，能够兼容处理复杂的异构数据，并且支持的数据展示容量达到亿级规模。大屏内容的呈现基于实时数据计算，利用数据预处理等加速技术实现了页面内容在毫秒级别的快速刷新。此外，产品还整合了地理信息库，将网络攻击数据与全球地理信息紧密结合，为用户提供了直观的网络安全展示图。这种创新的展示方式，不仅增强了数据的可视化效果，还帮助用户更快速、更准确地理解和响应网络安全威胁。



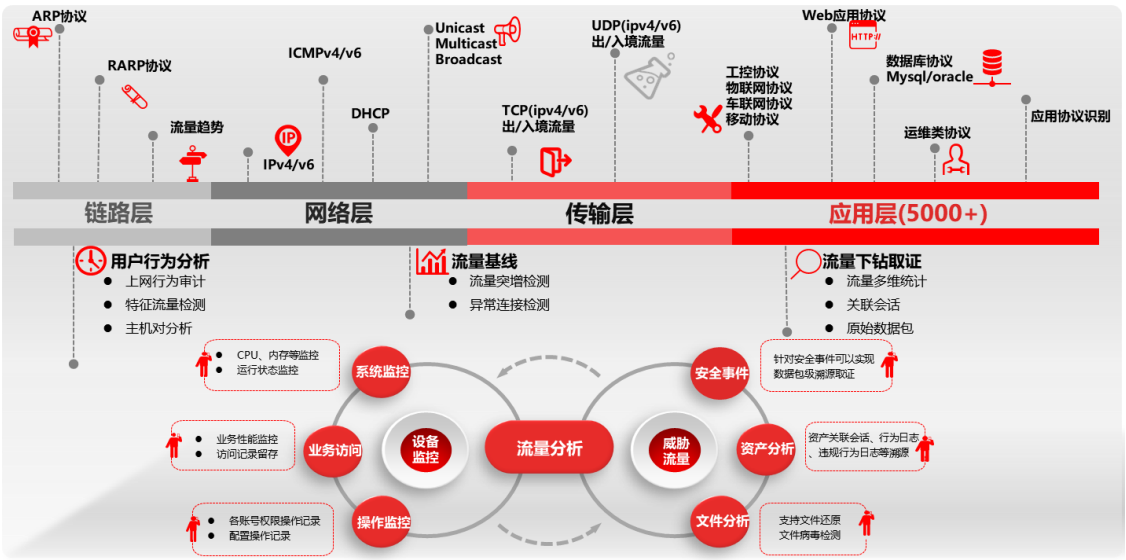
全流量监测产品综合安全分析大屏划分为九大展示区，包括攻击统计、攻击结果、恶意文件分类、恶意文件排行、攻击事件类型分布、攻击趋势、流量趋势、攻击者展示和地球展示。这些区域提供图形化的展示方式，旨在帮助用户全面掌握业务系统的安全状态，并深入了解网络攻击、恶意文件等威胁的主要来源和分布情况。结合业务流量和攻击趋势图，用户能够对攻击密度进行有效评估，从而做出更加精准的安全决策。

全流量监测产品僵尸网络大屏分析则涵盖了全球/境内控制主机分布、全球/境内控制主机排名、木马行为统计、控制主机统计、僵尸主机统计、木马行为排名、木马文件传播情况以及省内僵尸主机/控制主机统计等多个方面内容。通过图形化的方式展示多维度信息，使用户可以全面了解当前网络中的僵尸网络威胁情况，快速定位僵尸主机，有效提升对僵木蠕风险的掌握和应对能力。僵尸网络大屏分析展示方式不仅增强了相关数据的可读性，还提高了用户对僵木蠕威胁的感知和响应速度。

4.16 流量分析

全流量监测产品的流量分析功能通过深入解析网络数据流、协议还原和会话关联等技术，为用户提供了全面的流量分析能力，以图形化的形式实时监控接口的流入流出流量、并发连接数以及新建连接数量，并且支持按天、周、月或自定义时间周期对流量和连接趋势进行统计分析。

此外，流量分析功能还能从应用维度对网络流量进行详尽的分析，统计传输层和应用层协议的总流量及其分布占比，并记录网络连接的详细信息。识别和分析内容包括：HTTP 应用、IM 文件传输、P2P 下载、P2P 音频、P2P 视频、标准协议、财经软件、电子商务、工控物联网、即时通讯、加密隧道、软件更新、社交网络、数据库、网上银行、网络游戏、网页视频、网页音频、网络硬盘、网页邮箱、语音电话、远程控制、移动应用等在内的 24 大类超过 5000 种应用。



全流量监测产品具备强大的应用识别能力，这极大地扩展了系统流量分析的深度和广度。能够帮助用户全面评估应用性能，优化用户体验，并有效提升业务转化率。通过细致的分析，使用户能够更精准地理解和管理网络流量。这样，不仅保障了网络安全，还提高了网络资源的利用效率。

4.17 日志报表

全流量监测产品的日志审计功能以其详实和细粒度的记录能力，为用户提供了全面的日志记录，包括安全事件、系统管理和流量审计等多种类型的日志。产品通过综合检索、告警列表、攻击者视角和受害者视角等多角度展示方式，将日志信息以统计、关联和聚合的形式呈现，覆盖了 70 余种字段信息。此外，系统还提供了丰富的检索条件查询功能，帮助用户快速、直观地掌握现有信息系统的安全状况。

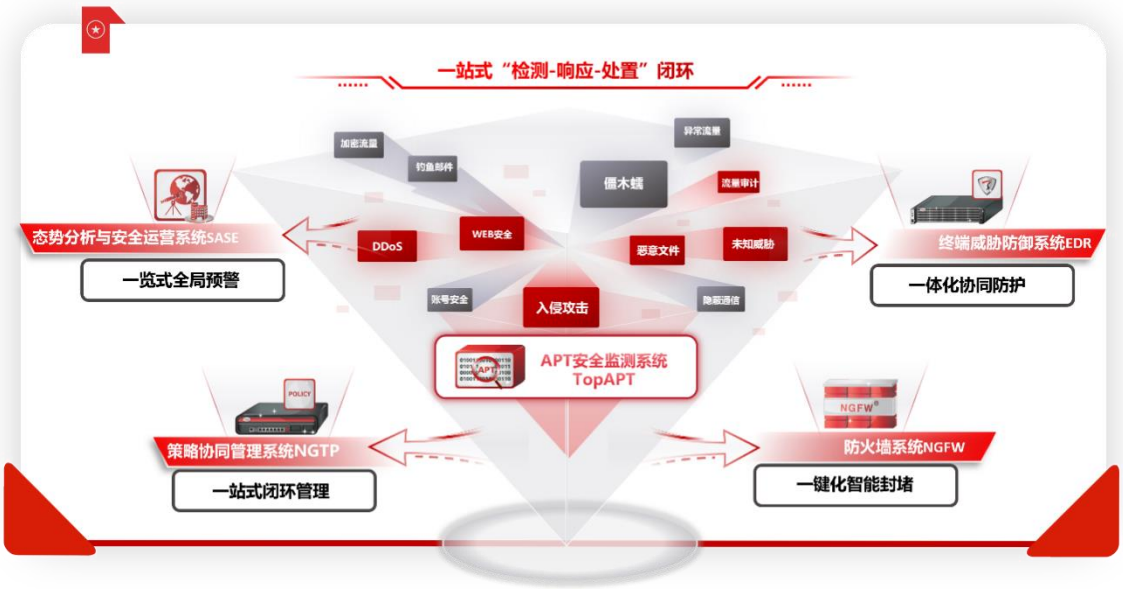
产品的报表管理功能支持两种报表形式：实时报表和周期报表。实时报表在任务创建后即刻执行，而周期报表则根据时间维度分为日报、周报、月报、季报和年报。用户可以根据不同时间范围查询和统计安全日志数据，并定时生成报表以供查看。报表管理功能不仅提供预定义模板，还允许用户根据主机地址、风险等级、TopN、总览、攻击成功事件、失陷主机、恶意文件事件、威胁事件等多个维度自定义报表模板。此外，报表功能支持多种文件格式，并具有高内容可读性，从而全面提升用户对信息系统安全风险的查询和分析能力。

4.18 联动处置

全流量监测产品具备高精准的网络流量攻击检测和溯源能力，全面评估网络信息系统的脆弱性，并深入监测潜在威胁。它还能与现有的安全检测产品协同工作，减少信息

孤岛，增强威胁检测能力，实现一站式的“检测——响应——处置”闭环管理。产品通过多元化的分析手段，对海量安全数据进行深度分析，实现以下效果：

- 策略协同管理系统（NGTP）：实现一站式闭环管理。对多台全流量监测产品进行集中管理，最大限度整合现有的安全资源，提升整体安全管理水平。
- 防火墙系统（NGFW）：提供一键化智能封堵功能。为用户建立纵深防御体系，大幅加强用户对精细化、高级化威胁的感知防御能力，提升用户整体安全运营水平。
- 终端威胁防御系统（EDR）：实现一体化协同防护。实现自动化的响应和处置机制，一旦检测到威胁可以自动执行预定义的安全策略，从而减少对人工干预的依赖。
- 态势分析与安全运营系统（SASE）：提供一览式全局预警。态势感知系统负责对全流量监测产品数据进行深入分析，识别潜在的安全威胁。提供从网络层面到内容层面的全面监控，实现对潜在威胁的全面识别。



4.19 自主可控

全流量监测产品获得中国信息安全测评中心颁发的国家信息安全测评自主原创产品测评证书，CPU、Flash 颗粒、操作系统、应用软件及管理软件产品组件均自主可控。天融信公司为国产化组件供应商（海光、麒麟软件）重要的生态合作伙伴。

5 部署方案

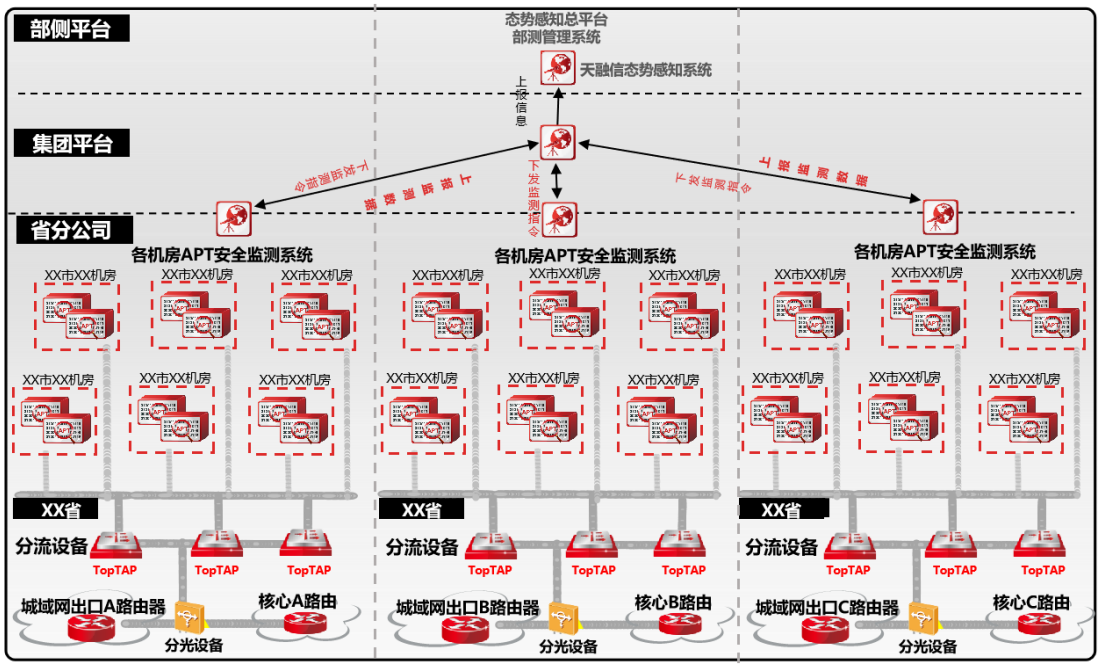
5.1 行业监管场景

5.1.1 场景一

场景需求：

- 需流量检测探针设备输出威胁信息
- 已有自建的分析平台
- 满足持续安全运营的需要
- 针对行业监管场景使用

推荐方案：



方案价值：

✓ 围绕检测-研判-处置为一体的安全监测系统，实现运营闭环

✓ 威胁信息统一外发第三方进行综合展示

✓ 多种监测信息上报

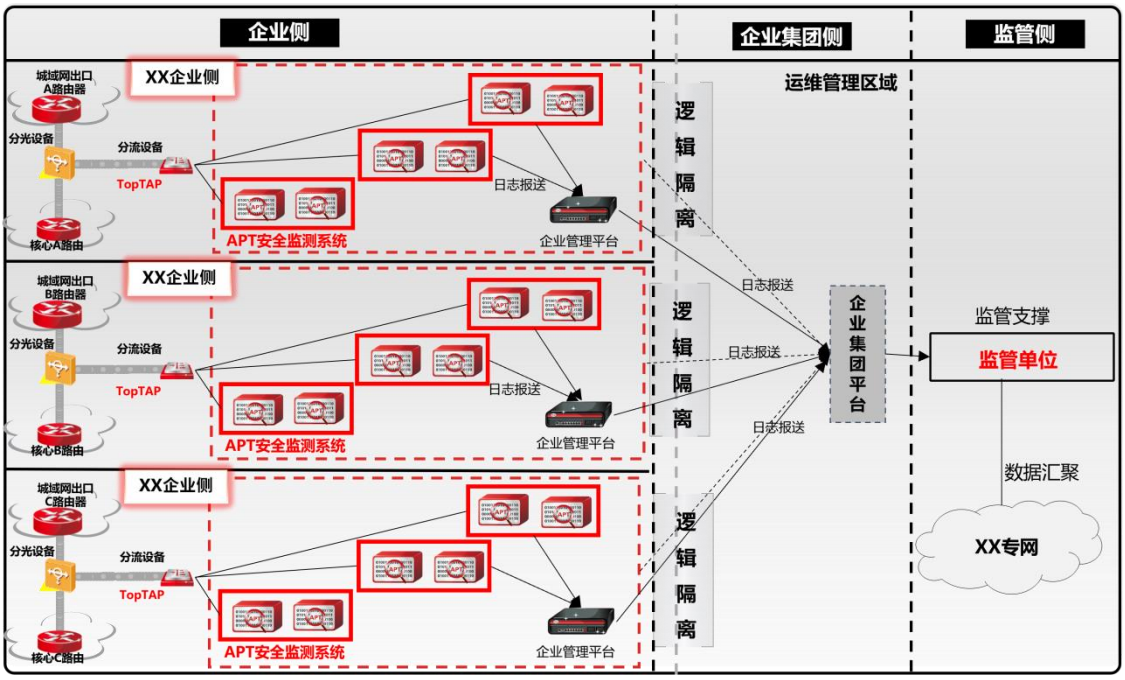
✓ 构建前后端系统，满足行业监管场景需求。

5.1.2 场景二

场景需求：

- 了解整体网络安全情况
- 满足行业监管的需求
- 前后端配合使用
- 构建数据可视，满足不同角色对平台的应用需求

推荐方案：



方案价值：

✓ 构建数据可视，通过流量、各类日志关联资产了解整体网络安全情况

✓ 了解网络安全态势情况、安全管理情况、安全事件处置情况、内部人员异常违规事件情况

✓ 多种监测信息上报

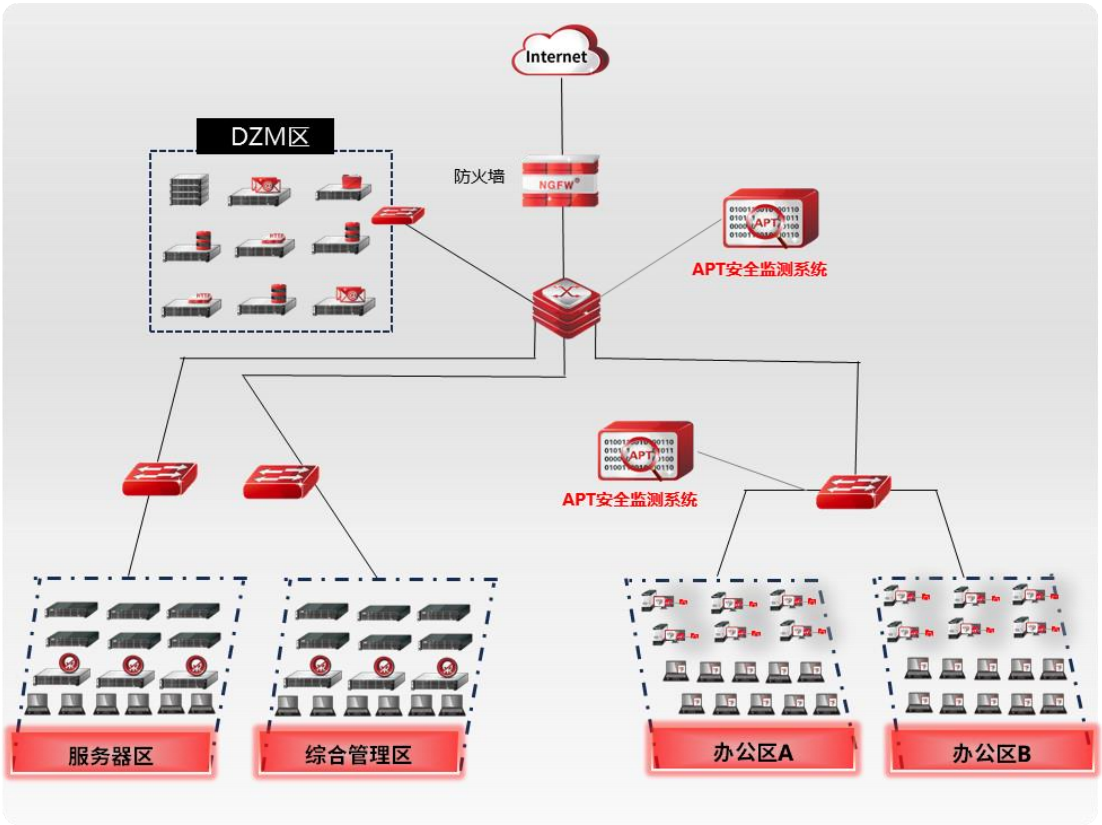
✓ 构建前后端系统，满足行业监管场景需求。

5.2 中小企业自监管场景

场景需求：

- 小型网络环境
- 满足自监管需求
- 功能丰富多样
- 减少设备冗余搭建

推荐方案：



方案价值：

✓ 基于业务环境构建威胁检测和响应模型，及时发现用户内部的安全事件及安全风险

✓ 帮助用户辅助决策、管理落地、运营支撑

✓ 作为一体化安全监测设备满足中小企业自监管场景的一体化部署需求

6 产品规格

PN 码型号	APT-82106-H-YNYD	IDP-82106-H-YNYD	APT-81208-H-YNYD
固定接口	4 个千兆电口(包含 1 个管理口)，4 个万兆光口插槽	4 个千兆电口(支持一组 bypass)，4 个万兆光口插槽	4 个千兆电口(包含 1 个管理口)，4 个万兆光口插槽
扩展槽	4 个，可扩展至 20 个万兆光口	4 个，可扩展至 20 个万兆光口	4 个，可扩展至 20 个万兆光口
USB 接口	≥2 个	≥2 个	≥2 个
产品形态	2U	2U	2U
性能	网络流量处理性能：20Gbps	网络流量处理性能：20Gbps	网络流量处理性能：40Gbps