RELIABLE NETWORK
SAFE WORLD
TOPSEC

天融信 APT 安全监测系统
技术白皮书

天融信 TOPSEC

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

互联网和移动互联网的高速发展，推动传统行业的转型，促进生产力增长，同时也带动许多新兴行业的衍生，大力提升我国经济发展。网络和信息化产业在我国的重要性，也将网络安全推向了不容忽视的高度。“没有网络安全，就没有国家安全。”习近平总书记在中央网络安全和信息化领导小组第一次会议上，就将网络安全提升至国家主权的高度。

虽然近年来，政府、学校、能源、金融、医疗等各行各业都加大对网络安全的建设投入和教育普及，但是总体来说，我国网络安全的保障无法应对当前网络空间的快速发展。我国作为经济大国和网络大国，一直被各黑客组织视为重要的“猎物”。当前的网络安全依然面临以下现状：

（1）恶意程序是主要的网络威胁之一

国家计算机网络应急技术处理协调中心发布《我国互联网网络安全态势》中提到 CNCERT 新增捕获计算机恶意程序样本数量约 4,298+万个，计算机恶意程序传播次数日均达约 998 万次，虽然数量同比无增长，但是恶意程序当前在我国的安全威胁占主要分布。

（2）僵尸网络密布

恶意程序的频繁传播使感染恶意程序的计算机数量居高不下，据 CNCERT 抽样监测，我国境内感染计算机恶意程序的主机数量约 240 万台，境外的约 3.9 万个恶意程序控制服务器控制了我国境内约 210 万台主机。在抽样检测数据中，由感染恶意程序的计算机造成僵尸网络，规模在 10 万台以上的僵尸网络数量达 21 个。

（3）新型威胁层出不穷

从勒索病毒、恶意代码程序、APT 攻击、未知攻击的快速增长，可以看出当前网络安全的现状是入侵攻击不断进化，新型威胁层出不穷。从安全事件应对方式上来分析，传统流量监测安全产品，采用特征匹配、行为分析等方式，只有监测到已发生攻击的特征和行为，才采取响应手段，这种被动防御的方式已经无法应对当前新型的网络威胁。

（4）国产化需求增多

各级党政军机关、企事业单位系统环境中承载了越来越多的重要业务与数据，这些内容有的关乎社会经济稳定发展、有的甚至专门用于传输和处理国家机密信息，如果关键基础设施设备受制于人、网络安全与信息保密防范不力，稍有疏忽，就会危及国家的安全、稳定和利益等多个方面。国产化安全任重而道远，要从根本上保障国家信息安全，实现真正的自主可控，加快国产化自主可控的体系建设，在面对日益增多的安全事件与威胁时，通过具备完全自主可控的网络安全产品和技术，保障国家关键基础设施、网络和信息系统安全，是我们当前需要重点关注和执行的工作之一，亦是我们维护国家信息安全工作的重要意义。

国产化的探针设备做为网络边界安全的基础设施，应对当前的网络状态，威胁检测设备上必须做到全面检测、精准检测，满足已知和未知威胁检测能力，在被动防御攻击的同时也应当主动感知网络中存在的威胁，提早防御。

很多企业单位在网络安全建设中，为应对网络中的多种威胁检测，会在网络边界处部署多款威胁检测设备。很多威胁检测类设备在功能上会存在部分重叠，这种建设方案会增加采购成本，同时增加设备管理工作。所以当前的网络边界安全产品应当朝着高效、集合多功能、管理方便的方向发展。

2 产品概述

2.1产品简介

天融信 APT 安全监测系统（以下简称 TopAPT ）是一款由天融信自主研发的全流量威胁检测产品，该产品集合了攻击检测、僵木蠕检测、DDoS 检测、恶意程序检测、APT 检测、WEB 安全检测、虚拟沙箱、元数据提取、流量分析九大功能，该产品通过深度解析网络流量，结合特征匹配、异常行为分析、威胁情报、机器学习、虚拟沙箱等技术，实现迅速、精准识别网络中各种已知和未知威胁。TopAPT 全面的威胁监测能力，让网络安全状态一目了然，提升风险应对。

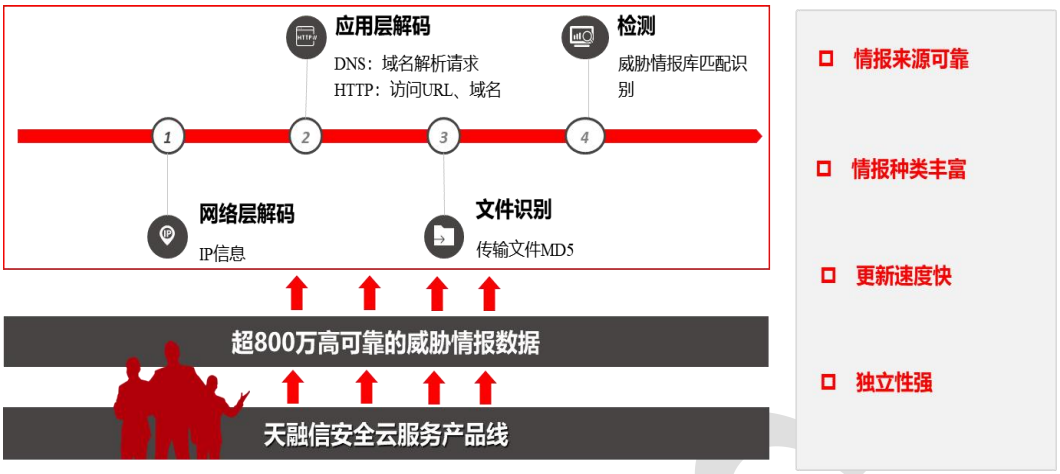
TopAPT 可采用设备-管理一体化模式，直接在检测设备上集成管理系统，亦可分布式部署，通过集中管理平台进行统一管理，探针分布式部署。

2.2流量安全检测

TopAPT 是集攻击检测、僵木蠕检测、DDoS 检测、恶意程序检测、APT 检测、WEB 安全检测、虚拟沙箱、元数据提取、流量分析九大功能于一体，实现对网络威胁全面检测的效果。在多需求的探针应用场景，无需部署其他设备，TopAPT 单款设备即可做到多种检测效果，即节省安全建设成本，又减少运维管理工作量。

2.3嵌入式威胁情报

TopAPT 采用本地嵌入威胁情报库的方式，无需和第三方威胁情报平台联动即可独立实现威胁情报能力。TopAPT 的威胁情报库是由天融信安全云服务产品线分析生产的，具备恶意 IP、恶意 URL、恶意域名、恶意文件等多种情报类型，包含 800 多万高可靠的威胁情报数据。嵌入式威胁情报库情报来源可靠、情报种类丰富、更新速度快、独立性强。



2.4未知恶意程序检测

TopAPT 首创应用智慧引擎，结合虚拟沙箱的检测技术，在不依赖任何规则库情况下，达到高效、精准的恶意程序检测能力。智慧引擎通过海量样本训练的机器学习模型识别恶意程序。虚拟沙箱检测采用仿真技术，模拟操作系统环境，构建执行引擎，动态化分析发现恶意程序。智慧引擎+虚拟沙箱的方式，打破了传统特征匹配技术的束缚，既能检测已知恶意程序，更能够检测未知恶意程序，是发现未知威胁特别是 APT 攻击的有力工具。

2.5多维知识库支撑

TopAPT 拥有攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL 分类库六大知识库。其中攻击规则库数量 13000+，威胁情报库数量 800 万+，URL 分类库数量 1000 万+，多维、丰富的知识库，使产品在威胁检测、攻击定位、上网行为分析等方面更加精确、迅速。知识库由天融信专业团队支持，保证高频更新。

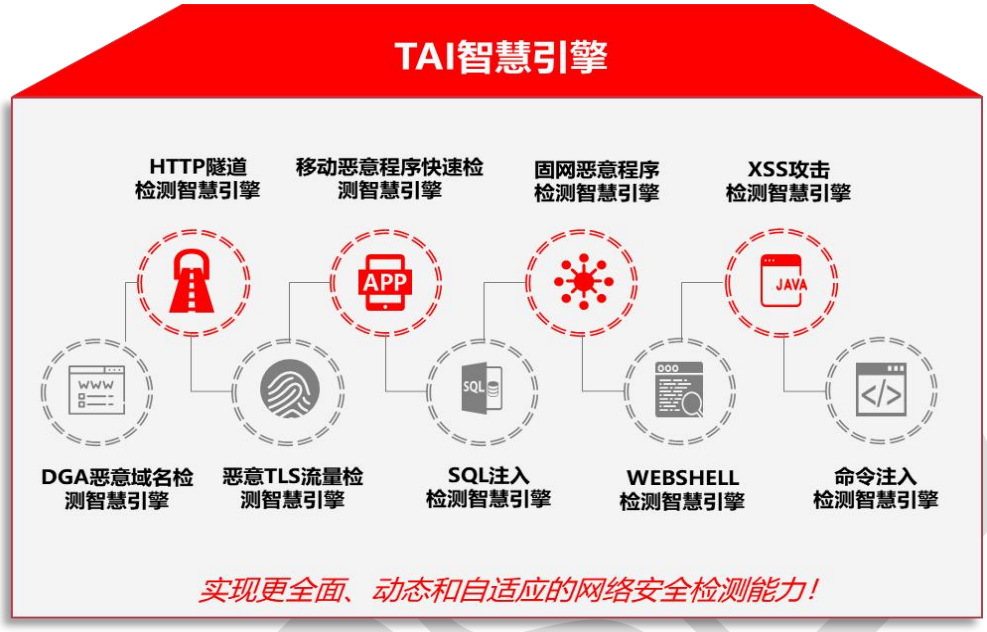
2.6全流量元数据挖掘

TopAPT 具有全流量元数据深度挖掘能力，以流量元数据为基础，实现能够对攻击事件信息、僵尸主机行为信息、恶意软件信息、恶意域名/URL 访问信息、DDoS 攻击等多种安全事件信息记录，对安全事件进行攻击报文、恶意样本文件取证，并且能够详细记录多种网络通信的元数据信息。TopAPT 可对所有的安全事件信息、取证信息、元数据信息加密输出，为态势感知等第三方平台提供丰富的数据。

2.7AI 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，利用多年持续积累上亿级别的海量文件和流量样本，将数据构建成特征矩阵并训练 AI 模型，而研发了 TAI 系列智慧引擎，广

泛应用于天融信多款检测和防护产品中，通过智慧引擎整体提升检测效果，既能检测各种传统攻击行为，也能够检测知威胁，提高整体的安全检测能力，大幅提高安全检测的效率和准确性。

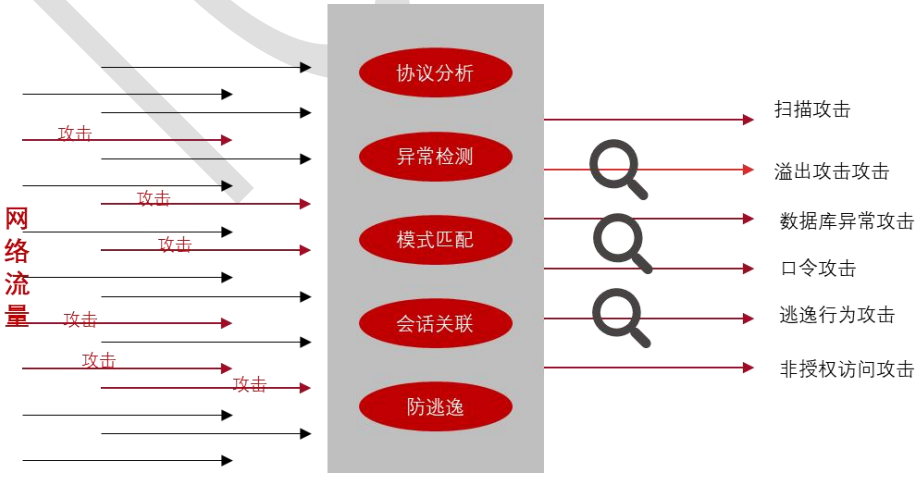


3 产品核心功能

3.1攻击检测

TopAPT 攻击检测是集成天融信 IPS 产品的专业检测引擎，采用协议分析，融合模式匹配、统计阀值和流量异常监视等综合技术手段，深入分析 L2~L7 层网络，精确检测网络中的入侵行为。能够检测出以下多种攻击行为：

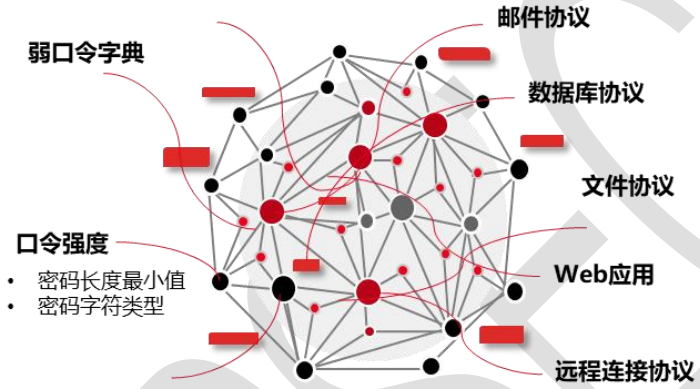
- **常见攻击行为：**支持对扫描攻击、缓冲区溢出攻击、拒绝服务攻击、漏洞扫描攻击、蠕虫病毒攻击、非授权访问攻击、后门木马攻击、文件漏洞攻击等常见攻击行为检测。
- **攻击逃逸的检测：**具有防逃逸检测能力，做到从根源上检测逃逸行为攻击。支持对 IP 分片逃逸行为、TCP 流重组逃逸行为、协议端口重定向逃逸行为、URL 变形逃逸行为等多种逃逸行为攻击识别。
- **DNS 投毒检测：**具备 DNS 投毒检测能力。
- **ARP 攻击检测：**支持从源目 IP、MAC 等维度分析 ARP 请求、响应的合法性。



3.2账号安全检测

3.2.1 弱口令

近两年，随着企业数字化转型的推进，业务应用与互联网交互不断深入，大量重要数据与信息存储、流转于业务系统内，成为被黑客觊觎的焦点之一。目前，因弱口令问题造成的信息泄露、内网渗透等安全问题仍层出不穷。

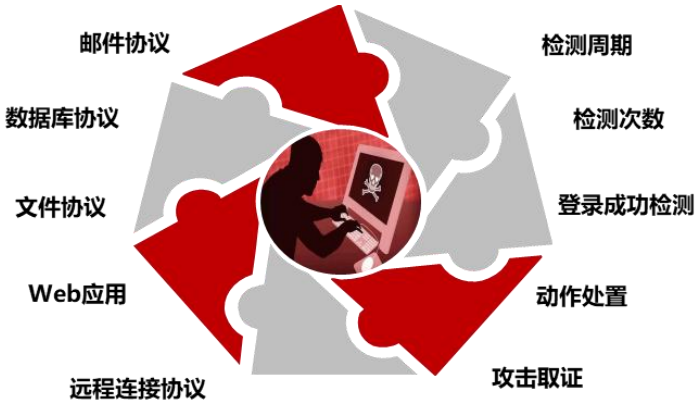


TopAPT 的弱口令检测是根据密码字典和口令强度双重模式实现对弱口令的攻击检测，设备检测到密码符合弱口令字典或者密码符合配置的密码强度，则会判断为弱口令。可支持对邮件协议、文件协议、远程连接协议、数据库协议、web 应用多种协议识别检测，有效应对弱口令攻击行为。

3.2.2 暴力破解

暴力破解主要指攻击者使用暴力破解工具，通过无限次的尝试登陆，最终获取到正确的登录口令，暴力破解成功后攻击者通过非授权访问的途径获取合法用户的授权，窃取用户资源信息，造成严重损失。

TopAPT 会判断在配置的周期时间内登录失败的次数超过了配置的检测次数，需要超过检测次数，登录成功检测次数等多种检测方式。如配置了 9 次，需要登录失败 10 次则会判定为暴力破解攻击行为。系统支持对邮件协议、文件协议、远程连接协议、数据库协议、web 应用多种协议识别检测，有效应对暴力破解攻击行为。



3.3僵木蠕检测

被感染木马、蠕虫病毒的计算机，会与外部黑客控制端进行 C&C 通信，接受黑客命令与控制，从而成为僵尸主机。TopAPT 根据木马、蠕虫病毒的活跃周期，采用行为特征匹配、智慧引擎技术、异常行为分析等多种检测方式，有效帮助客户排查网络中的木马扩散、肉鸡、挖矿、勒索、被恶意监视等威胁。

TopAPT 通过对网络中协议异常、访问异常、连接异常的主机提取通信行为特征，采用木马特征库匹配的方式检测网络中木马、蠕虫的活动行为，从而识别定位网络中的僵尸主机。支持对僵尸网络行为、木马控制行为、蠕虫活动行为、勒索病毒行为、移动端木马控制行为等多种僵尸主机行为检测。对被检测到的僵尸主机异常行为，TopAPT 支持对异常行为报文取证、事件记录，事件记录包括攻击源信息、事件应用协议、事件描述等信息。

特征提取

僵尸主机与C&C通信过程中提取行为特征，支持11000+种行为特征

失陷主机研判

判断是否已经成为僵尸主机

3.4DDoS 检测

TopAPT 的 DDoS 攻击检测，是集成天融信专业抗 DDoS 产品的检测引擎。支持对 IP 扫描攻击、端口扫描攻击等多种扫描类的 DDoS 攻击检测。支持对 ICMP FLOOD、TCP FLOOD、UDP FLOOD、SYN ACK FLOOD、FIN FLOOD、RST FLOOD、DNS FLOOD、HTTP FLOOD、HTTPS FLOOD 等多种 FLOOD 攻击行为检测。

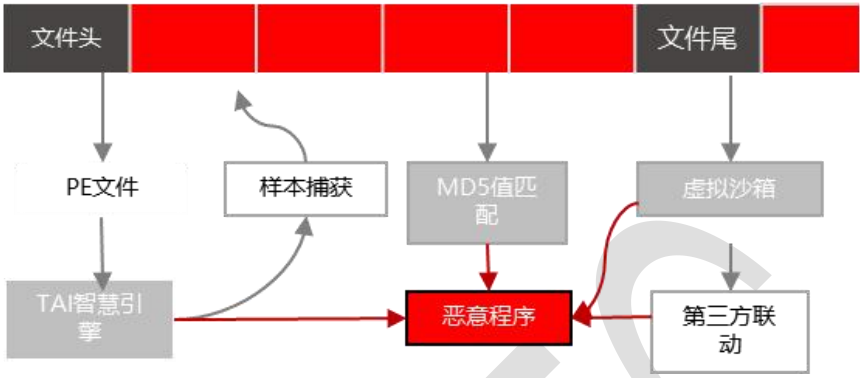
TopAPT 具有流量阈值自学习的能力，能够根据某一时间段内的流量状态，自动学习设置流量阈值，当流量状态异常时，触发阈值，系统自动进行告警。

3.5恶意程序检测

TopAPT 对网络中使用 HTTP、FTP、SMTP、POP3、SMB、DNS、NFS、IMAP 等非加密协议以及 HTTPS、FTPS、SMTPS、IMAPS 等加密协议传输的文件，采用特征检测、TAI 智慧引擎、虚拟沙箱、第三方联动等多种技术手段检测是否存在恶意程序。

TAI 智慧引擎采用机器学习技术，以文件数据流中提取 PE 头的二进制信息为源数据，通过海量样本训练的机器学习模型识别恶意程序。虚拟沙箱是模拟高仿真系统环境，对文件进行一系列的仿真执行指令，发现文件的异常行为，从而验证恶意程序。特征检测是提出文件 MD5 值，通过与恶意文件库的匹配精准验证已知恶意程序。

TopAPT 支持对压缩类型、Windows 可执行类、Linux 可执行类型、移动端类、图片类、文档类病毒文件检测。同时，对被检测文件，可对样本还原和留存，对留存样本文件支持用户本地下载和加密外发。



3.6APT 检测

APT 攻击是黑客组织对特定对象展开的持续有效的攻击活动，这种攻击活动具有极强的隐蔽性、针对性、持久性。TopAPT 在 APT 的检测上具有三种方式：

- 依靠威胁情报检测已知 APT 攻击行为

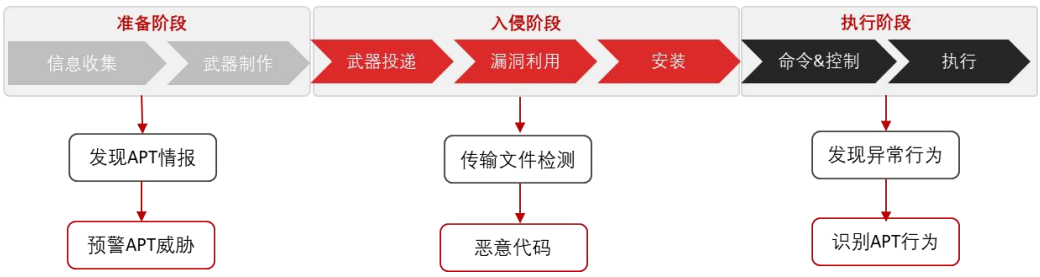
TopAPT 的威胁情报库中具有多种 APT 威胁情报信息，包含 APT 攻击涉及的恶意 IP、恶意域名、恶意 URL、恶意文件等情报。通过对 APT 威胁情报的感知，可在 APT 攻击的早期阶段，提前防控 APT 风险。

- 依靠智慧引擎检测未知威胁

在 APT 攻击中，黑客组织通常是将特意制作的恶意程序植入到目标网络中，利用植入的恶意程序命令、控制目标网络从而发动攻击行为。设备具有精准的恶意程序检测能力，可以对网络中传输的隐蔽性高的 APT 恶意文件有效识别。在对恶意程序检测上，TopAPT 特有的 TAI 智慧引擎+虚拟沙箱检测方式，可对未知恶意代码检测，从而检测出未知 APT 事件。

- 依靠僵尸主机检测已知 APT 组织

通常 APT 组织在活动过程中，都具有属于自己的行为，TopAPT 采用通过僵尸主机行为库检测异常主机行为的方式，识别网络中活跃的 APT 组织，对 APT 攻击组织的异常行为监测。



3.7WEB 安全检测

WEB 攻击主要是针对用户上网行为或网站服务器等设备进行攻击，对存在安全漏洞的 WEB 应用植入恶意代码，修改网站权限，获取网站用户隐私信息等攻击行为，这会导致系统网页被篡改、恶意弹窗、域名劫持等危害导致隐私信息被泄露，因此确保 WEB 安全十分重要。

设备采用攻击特征匹配+智慧引擎的方式，实现对 WEB 安全检测。支持对 SQL 注入攻击、跨站攻击、浏览器劫持攻击、URL 跳转攻击、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、Webshell 上传攻击、文件上传、爬虫等多种类型的 WEB 攻击检测。

3.8虚拟沙箱

虚拟沙箱是采用仿真技术，模拟操作系统环境，构建执行引擎，实现对恶意代码的检测。虚拟沙盒的三个基本要求：虚拟化执行效率要足够高，具有完备的操作系统环境仿真，能够捕获记录程序虚拟执行时的行为。

TopAPT 虚拟沙箱中的系统环境中具有文件系统、注册表系统、窗口系统等多种操作系统核心机制，达到高度仿真效果，具有跨平台特性。执行引擎具有虚拟化执行引擎和动态翻

译执行引擎两种，两种执行引擎的结合既能保证对文件的执行效率达到与真实机相当，又能实现对目标代码的细粒度控制。

TopAPT 的虚拟沙箱可实现对恶意代码进行通用脱壳、深度扫描、动态行为分析等深度检测。

- **通用脱壳**：在不需要识别样本是否加壳的情况下，通过将样本放入虚拟沙箱深度执行并通过启发式逻辑分析样本数据是否已被还原。
- **深度扫描**：跟踪其中进程释放的文件、创建的进程等，沙箱在扫描过程中会对这些衍生物进行扫描，以此来实现对样本的深度扫描。
- **动态行为分析**：支持跟踪和记录运行在沙箱中的程序行为，通过一系列分析算法对程序行为分析。

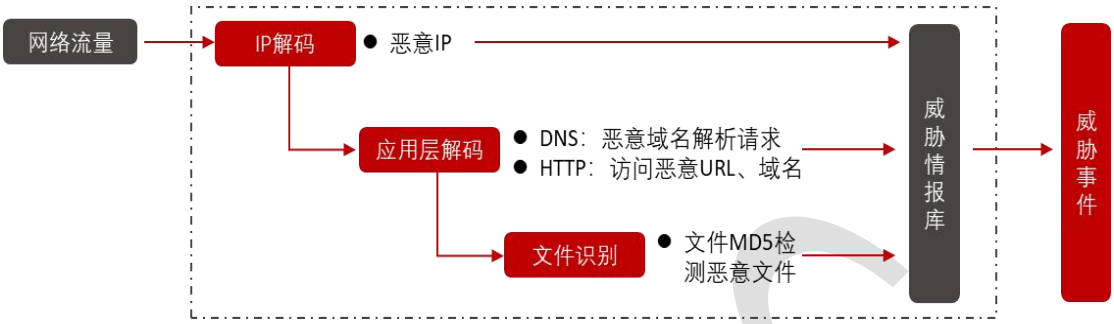
TopAPT 通过虚拟沙箱，实现对恶意代码威胁的动态检测，打破静态检测的壁垒。

3.9 威胁情报

威胁情报是将收集来的原始数据和信息经过分析处理，提炼出与目标网络威胁相关的指标，用于发现当前网络所面临的现有或潜在威胁及风险。不同于传统安全手段，当安全事件发生时才采取防御响应，威胁情报的基本目标为早发现、早预防。

TopAPT 的威胁情报功能通过对网络数据流深入解析，解析出 IP、URL、域名、文件 MD5 值等多种信息放入威胁情报库匹配，并且能够对恶意威胁样本还原捕获。相比传统的特征检测方式，威胁情报检测范围更大。

威胁情报库是从海量的威胁情报中提取出 800 万+高可信威胁，检测威胁类型多维，检测速度快。产品的威胁情报功能在满足精准、高效的同时，也保持高频率更新，及时更新热点威胁情报信息。



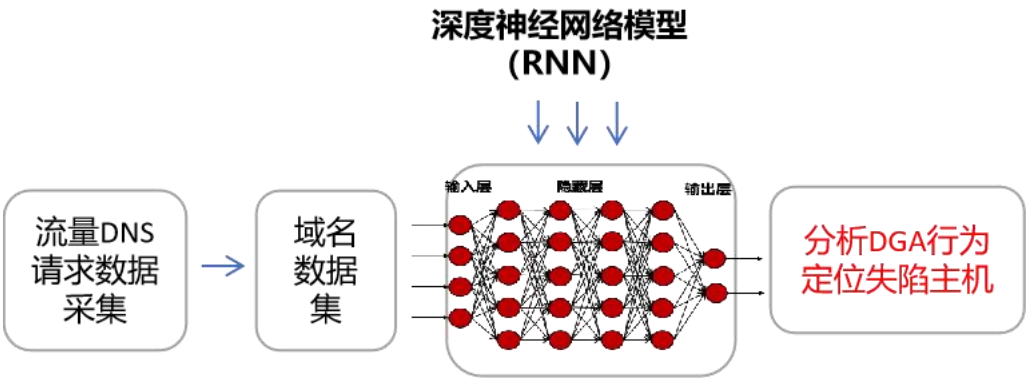
3.10异常流量检测

3.10.1 非法外联检测

该部分主要对服务器进行保护，根据管理员配置的合规行为，对服务器外联行为进行监控，检测服务器是否会主动和外部进行通信（可能中毒），针对异常的通信行为会进行告警并上报管理员进行进一步的处理，系统支持服务器非法外面检测并支持外联自学习。

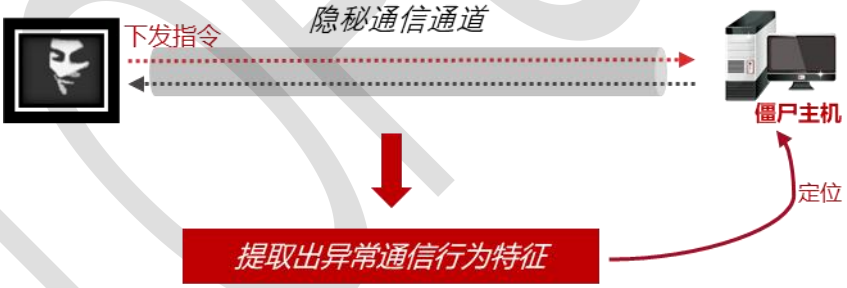
3.10.2 DGA 域名检测

TopAPT 可通过 AI 深度学习技术中的循环神经网络（Recurrent Neural Network, RNN），对海量恶意域名样本充分训练生成检测模型来识别网络中伪随机域名，解决 DGA 域名算法逆向破解难题，实现对隐秘性高的 DGA 恶意域名进行深入检测。RNN 具有自动提取样本特征的能力，可挖掘其内在的字符分布统计特征，将传统方法的分类精度大幅度提升，实现检测率高，误报率，漏报率低。



3.10.3 隐蔽隧道检测

TopAPT 支持针对失陷主机异常外联通信行为进行非法外联监测，做到从内到外的威胁监测能力。对通信协议采用智能分析的手段，能够有效识别僵尸主机使用“私有”协议建立的隐秘通信通道。采用异常行为检测+智慧引擎检测多种手段，对 DNS 隧道、ICMP 隧道、HTTP 隧道的异常通信监测，排查失陷主机异常请求，通过发现主机异常通信行为来深入检测隐蔽隧道。

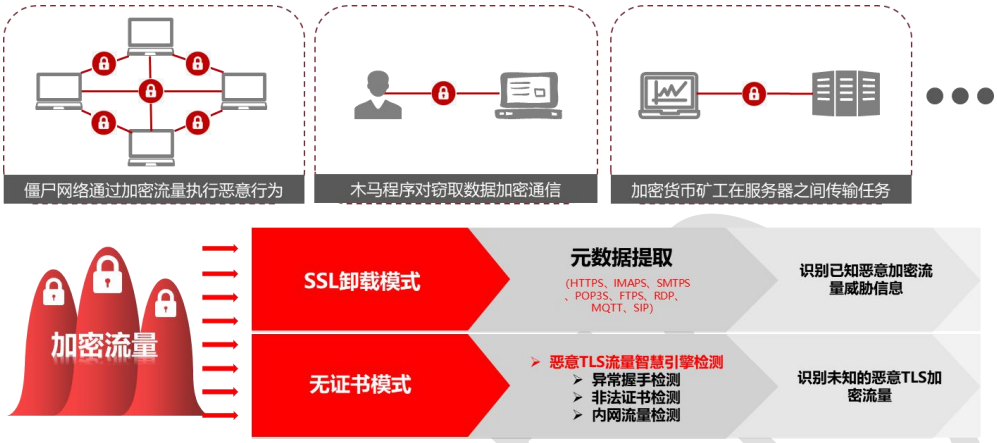


3.11加密流量检测

在网络通信中，为了保证传输内容的安全，不被篡改或利用，通常的做法是将通信流量加密处理，但流量加密也让恶意流量有了隐藏、躲过检测的机会。

TopAPT 可通过导入证书+无证书检测相结合的方式，直接对加密流量进行解密处理，实现对加密流量元数据的深度提取，检测恶意威胁信息。设备通过智慧引擎检测、异常握手检测、非法证书检测、内网流量检测等多种方式发现恶意程序的加密通信，实现无证书检测加密通信的效果。由天融信安全研究团队通过对恶意程序行为进行深入分析，提取出恶意程序

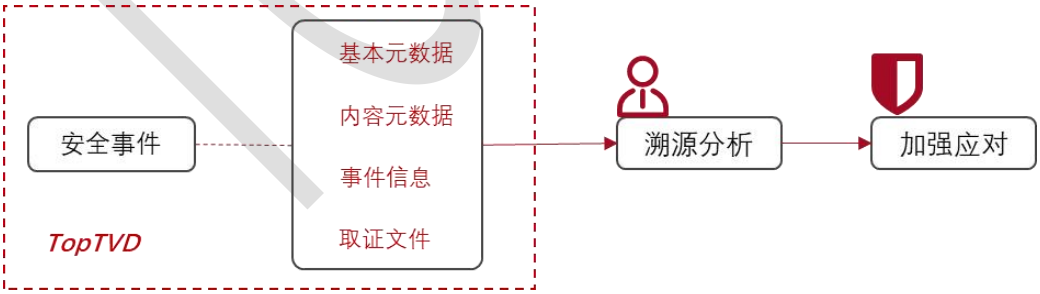
加密通信的指纹特征，从而生成指纹特征库。TopAPT 的加密检测引擎对加密流量的报文深度解析，从中筛选出潜在的恶意加密流量，提取报文中的摘要信息，通过将摘要与指纹特征库匹配的方式，确认恶意程序的通信行为，从而让恶意程序加密通信无处遁形。



3.12溯源取证

TopAPT 支持对入侵攻击、僵尸网络、恶意程序等威胁事件进行取证记录，支持流量报文取证和样本文件取证。具备全流量取证能力，能将恶意事件的事前、事中、事后流量全部抓取存留。系统将安全事件元数据信息和取证文件关联，用户通过对威胁基本元数据检索的方式即可获取全面的威胁信息，友好支撑用户对威胁的深入溯源分析。

此外，设备还具有攻击有效性研判能力，通过会话关联分析的方式判断攻击的有效性，节省用户威胁溯源排查时间。



3.13URL 检测

在重视外部对内部网络发起的攻击威胁时，也应当注意从内到外的威胁主动访问。内网用户对钓鱼网站、挂马网站等恶意网站的访问，也是网络威胁的一种来源，具有极大的网络安全隐患。

TopAPT 拥有上千万条 URL 分类库，地址库种类全面、详细，包括搜索引擎、社交网络、网上购物、求职招聘、休闲娱乐、财经、恶意网站、非法及不良、成人内容、网络安全、下载网站等地址，通过对网络中 URL 的识别，精准有效发现用户对非法网站的访问动作，有利于对威胁、恶意风险的控制。

同时， 通过对网络中的 URL 实时监测，详细记录各主机对网站的访问行为，可以按网站、主机等维度进行统计，有效的帮助管理员分析用户上网行为。

3.14威胁处置

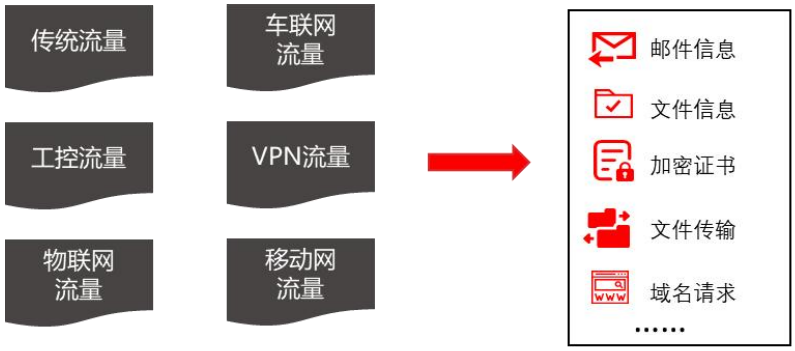
TopAPT 在威胁检测的同时也具有威胁处置能力，支持对入侵攻击、僵木蠕行为、恶意程序传播、APT 攻击、WEB 攻击、访问非法 URL/域名、恶意 IP 通信等安全事件进行阻断处置，支持旁路阻断处置、防火墙联动阻断处置、EDR 联动阻断处置三种方式。通过阻断处置，使产品在威胁检测的同时，也具备威胁防御能力，更好保证网络安全。

3.15元数据提取

TopAPT 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。

支持对 TCP/UDP 流量、ICMP 流量、HTTP 流量、邮件流量、FTP 流量、DNS 流量、NFS 流量、SMB 流量、SSL 流量、LDAP 流量、RDP 流量等多种非加密流量以及 HTTPS 流量、加密邮件流量、FTPS 流量等多种加密流量深度提取元数据信息。提取的元数据，除基本的五元组信息外，还具有多种类型的内容层信息，如邮件元数据、文件元数据、URL 访问元数据等。

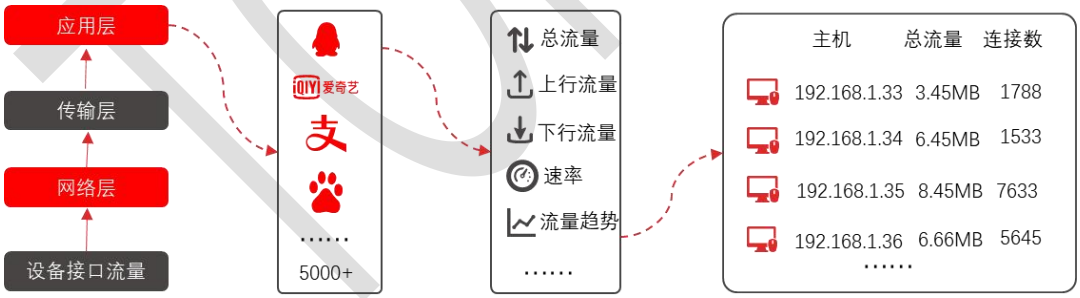
支持对 NDP3、MODBUS 工控物联网协议提取元数据信息。



3.16流量分析

TopAPT 对所有网络数据流通过流量解析、协议还原、会话关联等方式实现全面的流量分析。支持按接口对报文流入流出速率实时监控，每分钟对接收的报文按传输层协议、网络层协议、报文字节大小等多维度进行统计分析。对各接口的流量趋势按天、周、月图形化记录。

TopAPT 支持对所有网络流量从应用维度详细分析，支持记录统计各应用的总流量、上下行流量、当前上下行速率、连接数等。同时，记录应用天、周、月的流量趋势图。并且分析记录应用的主机访问详情，包括主机 IP、总流量、连接数等信息。TopAPT 支持对文件传输、P2P、即时通讯、工控物联网、加密隧道、数据库、移动应用等 24 大类超过 5000 种应用识别分析。



3.17资产识别

TopAPT 支持识别网络中的资产信息，具备资产识别能力，帮助用户全面掌握当前网络资产情况。主动识别是从镜像采集的网络流量中主动解析存在的资产信息，识别效率高。被动扫描是对指定网络中存在的活跃资产信息全面深度扫描，扫描结果更全面。

资产信息记录资产 IP、MAC、操作系统、资产类型、分组、具有的应用服务列表等详细信息。

3.18 日志报表

TopAPT 能够详实且细粒度记录安全事件日志、系统日志、元数据提取日志等多种类型日志。不同日志类型按不同的维度记录，用户可按日志类型配置存储空间、日志级别，并且支持对日志合并以及加密外发。

此外，TopAPT 还具有强大的报表能力，能够按事件类型、主机、业务等多维对指定时间段的检测结果进行汇总统计，支持自定义模板内容，可以选择不同种类事件，定时发送报表，帮助管理员迅速了解当前的网络安全状态。

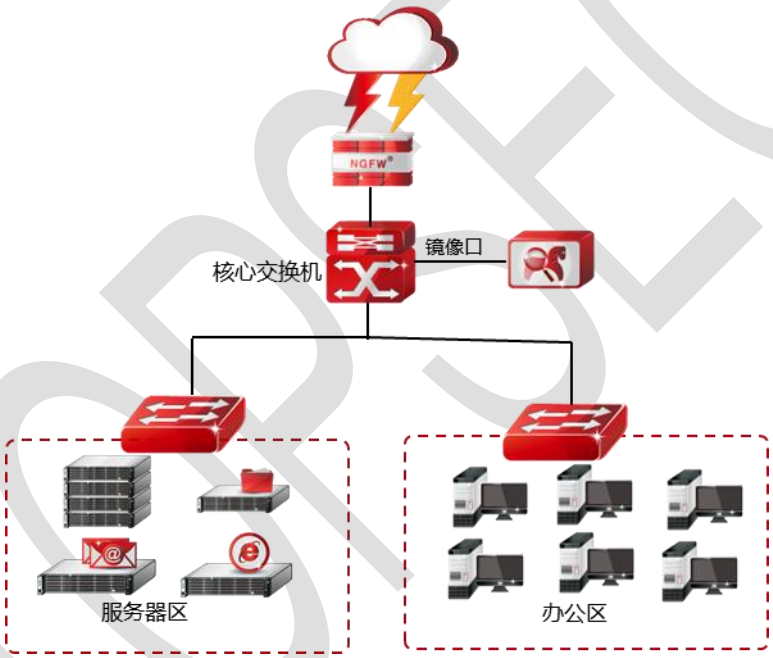
3.19 可视化管理

秉承着对安全检测高效管理的设计理念，在集成多种功能的同时，也拥有良好的可视化管理。产品在威胁检测、分析、处理、审查等管理上实现可视化、透明化，用户能够迅速了解安全事件的攻击源、受害主机、触发规则、响应动作、事件说明等信息。同时通过大量的事件数据关联，能够从被攻击主机、攻击源主机、时间等多种维度统计展示，帮助用户从宏观的角度了解全网的安全态势。

4 部署方案

4.1 单机部署

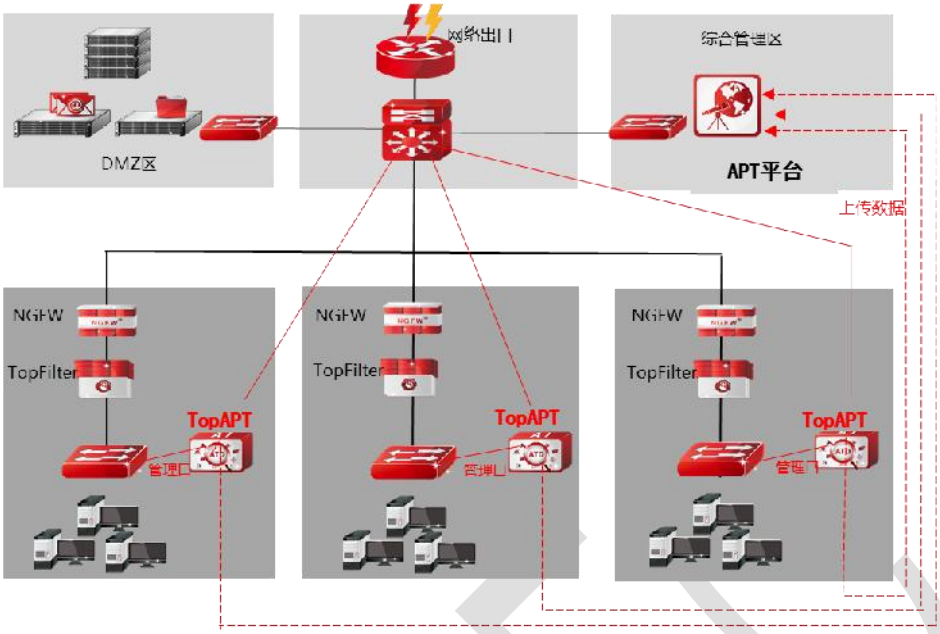
TopAPT 采用旁路镜像部署模式，设备部署在用户环境的网络出口或者核心交换机等位置，在实现网络流量威胁检测的同时，完全不需要改变用户的网络环境，避免设备影响用户网络架构。部署方式见下图：



4.2 平台部署

根据用户的网络情况以及项目需求，采用 TopAPT 探针、TopAPT 管理平台产品组合建设

探针设备部署在客户分支机构或者下级单位等多个网络出口处，完全不需要改变用户的网络环境，避免设备影响用户网络，探针设备将监测到的流量数据、分析信息等上报给管理平台进行分析。部署方式见下图：


DMZ区
APT平台
上传数据
NGFW
TopFilter
TopAPT
NGFW
TopFilter
TopAPT
NGFW
TopFilter
TopAPT

5 产品规格

型号	APT 平台	APT 探针
CPU	海光 7360*2	海光 3250
操作系统	银河麒麟 V10	统信 V20
固定接口	2GE&4SFP+	6GE&4SFP&2SFP+
USB 接口	2 个	2 个
产品形态	硬件	硬件
内存	128G	32G
硬盘	960G SSD+32TB 企业级硬盘	4TB 企业级硬盘
冗余电源	是	是

声明

1. 本文档所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。

2. 本文档中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此种情况产生的差异为正常现象，产品功能或性能请以产品用户手册等资料为准。

3. 本文档中提到的信息为正常公开的信息，若因本文档或其所提到的任何信息造成或可能造成他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。