RELIABLE NETWORK
SAFE WORLD
TOPSEC

天融信入侵检测系统
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 1

2 系统概述 4

3 系统组成与架构 5

3.1 产品构成 5
3.2 系统架构 6

4 特点与优势 8

4.1 攻击检测 全面精准 8
4.2 僵尸主机 精准定位 8
4.3 威胁情报 独立可靠 9
4.4 全能沙箱 10
4.5 平滑升级 无缝满检 10
4.6 未知威胁 多维挖掘 11
4.7 AI 融入安全 11

5 系统功能 13

5.1 攻击检测 13
5.1.1 弱口令 15
5.1.2 暴力破解 15
5.2 僵尸主机行为检测 16
5.3 DDoS 检测 17
5.4 WEB 安全检测 17
5.5 异常流量检测 18
5.5.1 非法外联检测 18
5.5.2 DGA 域名检测 18
5.5.3 隐蔽隧道检测 18
5.6 应用识别 19
5.7 威胁情报 20
5.8 病毒检测 20
5.9 URL 访问 21
5.10 流量审计 22
5.11 黑白名单 23
5.12 加密流量 23
5.13 溯源取证 24
5.14 日志报表 24
5.15 威胁分析 24
5.16 多维联动 25
5.17 日志告警 25

6 部署方案 26

7 产品规格 27

8 产品资质 28

1 前言

在高科技发展为代表的 21 世纪，随着网络信息化的高度应用，网络已深入到每一个空隙成为人们生活中必不可或缺的工具，小至人与人之间沟通，大至世界交互，越来越多的企业、政府构建了自己的互联网络信息化系统，因其不可或缺的重要性，网络空间已发展为继海、陆、空、天之后的第五空间，成为影响人们生活、企业运营、及至国家安全的重要因素之一。

随着信息网络承载并连接了全国各地的各个业务，如企业、政府构建了自己的互联网络信息化系统，如政府、学校网站，便捷人们在网上办理报名、申请、查询等工作；企业 CRM 系统，汇集了大量的客户项目资料信息，便于项目机会的统计、跟踪；人力资源系统，涵盖了整体的员工个人资料信息等。信息网络在带来高效和便捷的同时，因其承载了大部分的重要业务，以及关键信息，被破坏时产生的巨大影响力也成为了黑客攻击目标的一块更大的市场。

1）勒索软件“日屠一龙”，安全事件响应面临严峻挑战

从本田、佳明、佳能到富士康、研华.....“日屠一龙”的勒索软件无疑是 2020 年最危险，也是最受关注的网络犯罪活动。2020 年勒索软件攻击持续快速增长，攻击规模、赎金金额都屡次创下新高。根据 SonicWall 的最新报告，2020 年前三季度全球勒索软件攻击同比激增 40%（1.997 亿）。2020 年前三季度，美国遭遇的勒索软件攻击达到了惊人的 1.452 亿，同比增长了 139%。在勒索软件“每天屠掉一条大龙”，远程办公导致全球网络犯罪激增 400%的大变数驱使下，全球网络安全市场正在趋向两大热点，那就是：深度防御、快速检测/响应。

2）疫情期间多个 APT 组织对我国发起网络攻击

2020 年 2 月，在中国境内疫情期间，境外多个国家和地区对中国发动网络攻击，越南“海莲花”黑客组织利用疫情话题攻击我国政府机构，印度“白象”黑客组织借新型肺炎对我国发起攻击，台湾“绿斑”黑客团伙的利用虚假“疫情统计表格”和“药方”窃取情报。

3）微软 Win10 爆出史诗级漏洞，堪比永恒之蓝

2020 年 3 月，Win10 爆出了一个史诗级漏洞，危险程度堪比前几年肆虐全球的永恒之蓝。这个漏洞编号 CVE-2020-0796，与微软 Server Message Block 3.1.1 (SMBv3)协议有关，在处理压缩消息时，如果其中的数据没有经过安全检查，直接使用会引发内存破坏漏洞，可能被

攻击者利用远程执行任意代码。这个漏洞被评为“ Critical”高危级别，攻击者利用该漏洞无须权限即可实现远程代码执行，受黑客攻击的目标系统只需开机在线即可能被入侵。

4）FireEye、美国财政部和商务部被 APT 29 攻击，18000 名客户面临“窃听”威胁

2020 年 12 月，黑客利用 SolarWinds 在今年 3 月至 6 月间发布的网络管理产品 Orion 更新中，植入恶意代码，从而入侵了美国财政部、商务部下属的国家电信和信息管理局(NTIA)、FireEye 的网络，此外，多达 1.8 万的 Orion 客户也正面临着这次供应链攻击带来的巨大威胁。这意味着，在长达 9 个月时间里，黑客可以持续监视这些企业和机构，窥探内部电子邮件流量。不得不提及的是，SolarWinds 的全球用户中包括了白宫、国防部门、美英信号情报机构等敏感机构。

5） 安全漏洞持续增高

2020 年，Web 应用程序依然是漏洞的“主力军”，但是来自 Bugcrowd 数据显示，随着黑客技能的多样化，其他类别应用的漏洞数量也在赶上。到 2020 年，所有类别的漏洞提交量都增加了。今年以来，API 漏洞翻了一番，Android 漏洞翻了三倍还多。根据 HackerOne 10 月底发布的十大漏洞列表，跨站点脚本（XSS）仍然是影响力最大的漏洞，2020 年为黑客赢得了 420 万美元的漏洞赏金，比 2019 年增长了 26%。

从近几年攻击事件可见，攻击规模变的越来越广，危害越来越深，影响也越来越大，甚至是毁灭性的。范围上，网络安全形势从早期的随意性攻击，逐步走向了以政治或经济利益为主的攻击；技术上，攻击手段越来越专业，攻击的层面也从网络层，传输层转换到高级别的网络应用层面；类型上，攻击的类型越来越多，如 DDoS 攻击、僵尸主机攻击、病毒传播等。

为应对如此复杂、猛烈的网络攻击趋势，网络安全防护设备形态也相应不断增多、检测越发专业，从基础的防火墙、入侵检测、病毒网关、VPN 到数据防泄漏系统、WAF、僵木蠕监测系统、邮件网关等。

国家、行业也意识到攻击的频繁及危害，不断增强法律法规建设，《中华人民共和国网络安全法》、《互联网安全保护技术措施规定》、《信息安全二级等保要求》、《信息安全三级等保要求》等相继发布，成为各行业、单位的网络建设标准依据。

无论攻击如何衍生，黑客以漏洞方式的攻击母体方式一直是攻击的主导模式以及攻击的主要手段，因此，网络入侵检测一直做为网络安全法律法规的网络安全基础设备建设的基础与重点，各安全届也一直将入侵检测做为网络安全解决方案的基本配备系统。

IDS 做为网络边界安全的基础设施，攻击检测的主力，再加客户网络环境日趋重要和复杂的特点，IDS 的高性能、实用性以及准确性成为了产品要求的重点。

✧ 高性能

IDS 面对现在不断扩充的高网络流量，如何能在大部分策略均开启防护的前提下，依然保证其应用层面的检测能力，不丢包，不漏检，是 IDS 的关键。

✧ 准确性

黑客攻击层层深入，IDS 能够深入网络检查，准确发现攻击，避免黑客攻击躲过检测，同时，具有精确的检测规则，具有趋于零的误报率、漏报率，保证检测的有效性，是 IDS 的重点。

✧ 实用性

除黑客的漏洞入侵攻击外，病毒木马传播、DDoS 攻击，以及内部的恶意网站访问风险、网络资源滥用占用带宽等问题也是客户网络安全的常见问题，通过扩展进行多方面立体监控，是 IDS 的责任。

2 系统概述

天融信入侵检测系统（简称：TopSentry）是天融信公司自主设计并开发的入侵检测系列产品。TopSentry 软件系统采用天融信自主知识产权的下一代安全操作系统（即 NGTOS），该系统基于国产 CPU 硬件架构+国产操作系统 OS，运用多个数据平面的独立协议栈以及安全引擎进行工作。入侵检测系统具有完整的 IPv4/IPv6 协议栈、多路检测能力，通过检测流经的网络流量，精准发现网络中漏洞利用攻击、DDoS 攻击、恶意程序、恶意 URL 访问等威胁，同时对应用访问监控、对网络流量深入内容层审计，具备精确威胁检测、全面应用安全监控、丰富日志展示及大容量日志存储等多个特点，进一步提升信息系统安全性，全面监控、保护用户网络安全。

TopSentry 集合攻击检测、WEB 安全检测、DDoS 检测、弱口令检测、暴力破解检测、僵尸主机检测、非法外联检测、恶意程序检测、APT 检测、威胁情报十大功能于一体，实现对网络威胁全方位深层次检测的效果。TopSentry 具备攻击检测规则库、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，专业、权威、丰富、多维的知识库，使得产品在威胁检测方面更加精准、迅速。面对当前复杂的网络攻击环境，TopSentry 全方位深层次的威胁检测能力，可持续对抗不断出现的各类安全威胁。

3 系统组成与架构

3.1 产品构成

天融信入侵检测系统（以下简称：TopSentry），采取软硬件集成的模式，无需单独管理控制台以及其他组件，即可实现一体化方式应用，增加系统部署的灵活性。TopSentry 通过 B/S 管理中心进行系统的配置、维护与管理，系统功能均通过一体化设备实现，在威胁检测、日志信息存储等方面，一体化模式可有效降低信息传输窃取风险，并减少系统应用故障点，使 TopSentry 更灵活，更安全。

3.2 系统架构

在系统内核基础之上，TopSentry 系列产品采用天融信自主知识产权的下一代安全操作系统（即 NGTOS）（国产化型号则采用国产化操作系统，如银河麒麟/统信/欧拉等），系统基于多核硬件架构，为了实现高性能的应用层安全检测需求，NGTOS 采用了先进的用户态协议栈，该协议栈不但兼容最新 TCP/IP 特性，同时避免了由传统内核态协议栈所带来的从内核态到用户态的中断调度和数据复制问题。

在此基础上，系统存在多个数据平面，每个数据平面占用一个 CPU 核心，每个数据平面都具有自己独立的（NGTOS）协议栈，数据平面之间的协议栈基本互不影响，保证了随着 CPU 核心数量的增加，业务性能的线性增长。另外，每个数据平面包含了多个安全引擎：攻击检测、应用识别、恶意程序检测、URL 分类检测、僵尸主机监控、网络审计等等，使 TopSentry 的高效并行处理与全面安全检测能力有机结合，从而胜任高速网络的安全检测要求。

架构中的安全操作系统用于网络层处理、报文收发、会话处理以及 DDoS 检测等工作，通过应用识别库进行应用协议识别与解析，并以天融信庞大的知识库作为依托，运用攻击检测、僵尸主机、恶意程序等检测引擎检测漏洞利用攻击、恶意软件等已知威胁。运用审计功能模块审计用户网站访问、域名访问、邮件收发、文件传输等网络行为。针对疑似恶意程序，TopSentry 可联动高级威胁检测系统，实施深度检测，从而拓展本系统对于未知威胁的检测能力。

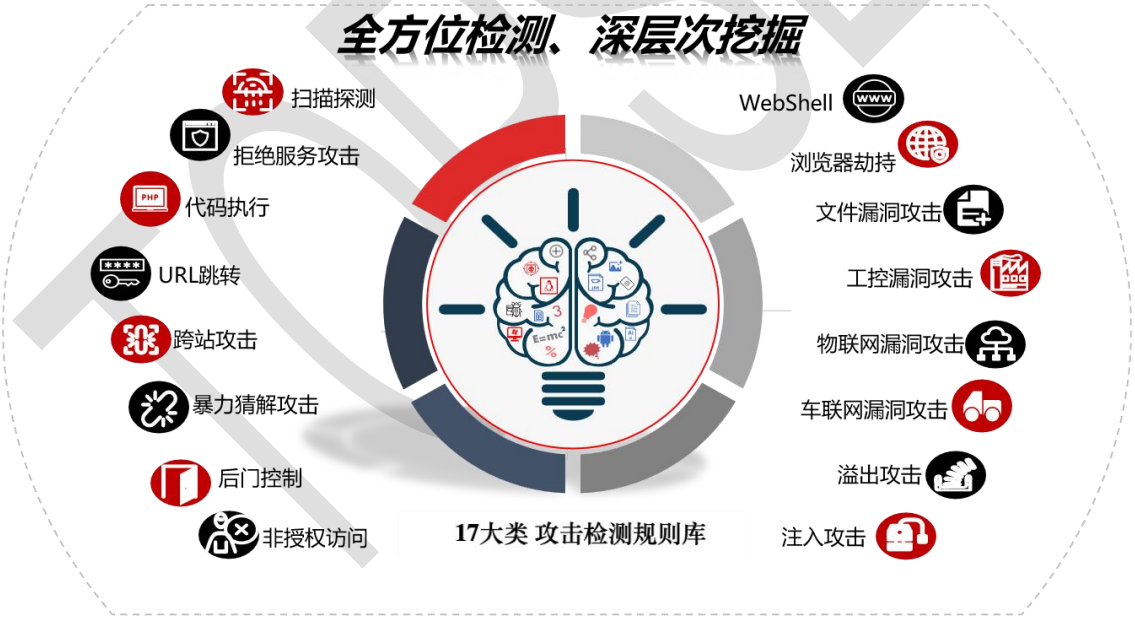
TopSentry 具备带外管理能力，提供图形化与命令行两种管理方式，能够根据不同应用需求与网络环境，针对网络、系统、对象、策略、LIC、用户等内容进行配置，并可实施运行监控、日志查询以及报表维护导出等操作。

TopSentry 提供恶意样本及攻击取证文件外发能力，可用于第三方分析平台以及其他威胁分析工具的进一步研判工作。

4 特点与优势

4.1 攻击检测 全面精准

TopSentry 具备专业的攻击检测引擎，集合攻击检测、WEB 安全检测、DDoS 检测、弱口令检测、暴力破解检测等功能，实现对网络威胁全方位、深层次检测的效果。TopSentry 采用协议分析、模式识别、阈值统计和流量异常监视等综合技术手段，深入分析 L2~L7 层网络入侵行为，准确发现多种网络攻击，其中包括扫描探测、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、物联网漏洞攻击等在内 17 大类网络攻击行为，此外，TopSentry 能够对攻击事件信息记录留存，包括请求响应信息、原始报文、攻击特征、漏洞描述、解决方法等，并可对安全事件进行攻击报文取证。同时，TopSentry 具有防逃逸检测能力，做到从根源上检测逃逸行为攻击。TopSentry 全方位深层次的攻击检测能力，可持续对抗不断出现的各类安全威胁。



4.2 僵尸主机 精准定位

TopSentry 支持对僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT 等多种僵尸主机行为检测，可快速、精准定位僵尸主机。TopSentry 通过僵尸主机和控制主机之间的异常通信挖掘僵尸网络，采用多种方式判断，包括从僵尸主机的 C&C 通信过程中提取行为特征，支持 11000 种以上的僵尸主机行为特征库；支持服务器非法外联监测，可检测

内部主动的恶意外联行为；此外，TopSentry 对通信协议采用智能分析的手段，能够有效识别僵尸主机是否使用通用知名端口进行隐蔽通信的威胁，有效避免信息泄露等风险。对被检测到的僵尸主机异常行为，TopSentry 支持对异常行为报文取证、事件记录，事件记录包括攻击源/目的信息、事件应用协议、事件描述等，可进一步分析研判。TopSentry 丰富多维的检测手段+详细全面的日志记录，能够快速、有效定位僵尸主机，规避僵尸主机所带来的危害。

4.3 威胁情报 独立可靠

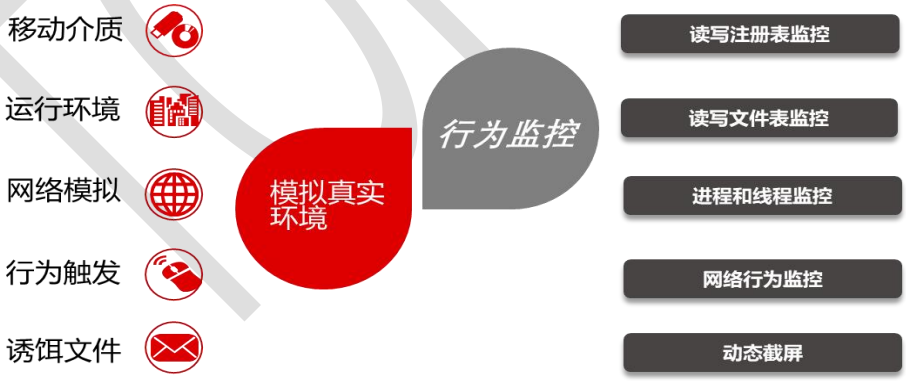
TopSentry 具备独立、可靠的威胁情报能力。TopSentry 采用本地嵌入威胁情报库的方式，无需和第三方威胁情报平台联动即可独立实现威胁情报能力。TopSentry 的威胁情报库是由天融信安全服务产品线听风者实验室分析生产，包含 800 多万高可靠的威胁情报数据，情报数量丰富，具有恶意 IP、恶意 URL、恶意域名、恶意文件等多种情报类型。天融信专业团队不断挖掘、研究、跟踪最新情报，保证我们威胁情报来源可靠。TopSentry 威胁情报功能的应用，能够有效提高威胁检测效率，并帮助企业全面了解网络信息系统所面临的威胁情况，为威胁检测工作提供有力参考依据，提升安全性。

支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本、MD5 进行一键检索。

4.4 全能沙箱

系统集成 Windows、Linux、、MacOS、Android 主流操作系统环境，能够深度检测可执行文件、文档文件、压缩文件、脚本文件、图片、音频、视频等百余种文件类型，检测已知和未知恶意程序。

通过模拟用户的真实环境，寻找虚拟机和真实环境的差异性，可对用户交互差异性、运行环境差异性、业务逻辑差异性三大类多种逃逸手段和逃逸行为进行检测。通过模拟用户的移动介质、运行环境、网络模拟、行为触发等，监控稳健运行过程中是否有读写注册表操作、读写文件操作、网络行为监控、进程和线程监控操作、其它危害系统的行为等。



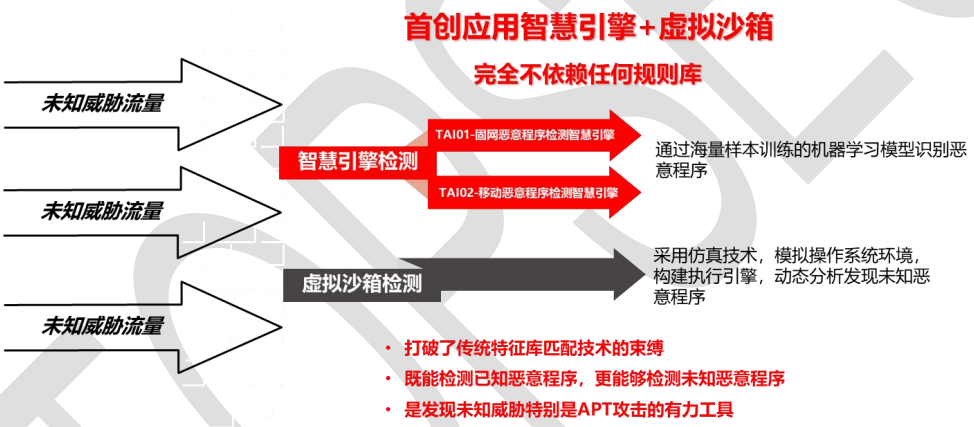
4.5 平滑升级 无缝满检

TopSentry 具备权威的攻击规则库，并可支持在规则库升级过程中，不中断安全策略的正常检测，做到“平滑升级，无缝检测”。天融信公司具有专业攻防研究实验室，充分与国际厂商和国家权威机构合作，不断跟踪、分析、研究最新发现的安全漏洞，生成拥有自主知识产权的规则库并应用于 TopSentry，使其能够全面、有效保护企业信息化资产。规则库以

周为单位定期更新，如遇紧急事件，规则库可第一时间升级，从而确保 TopSentry 及时有效的检测已知网络威胁。此外，在规则库升级过程完成之前，TopSentry 使用之前的备份规则库进行威胁防护，升级完成后自动切换至新规则库，从而完成规则库的“主备无缝切换”，安全事件可第一时间检测。在规则库升级期间，TopSentry 设备界面操作无抖动或延迟现象，客户网络的业务处理无感知，实现升级过程中检测功能的“无缝衔接”。

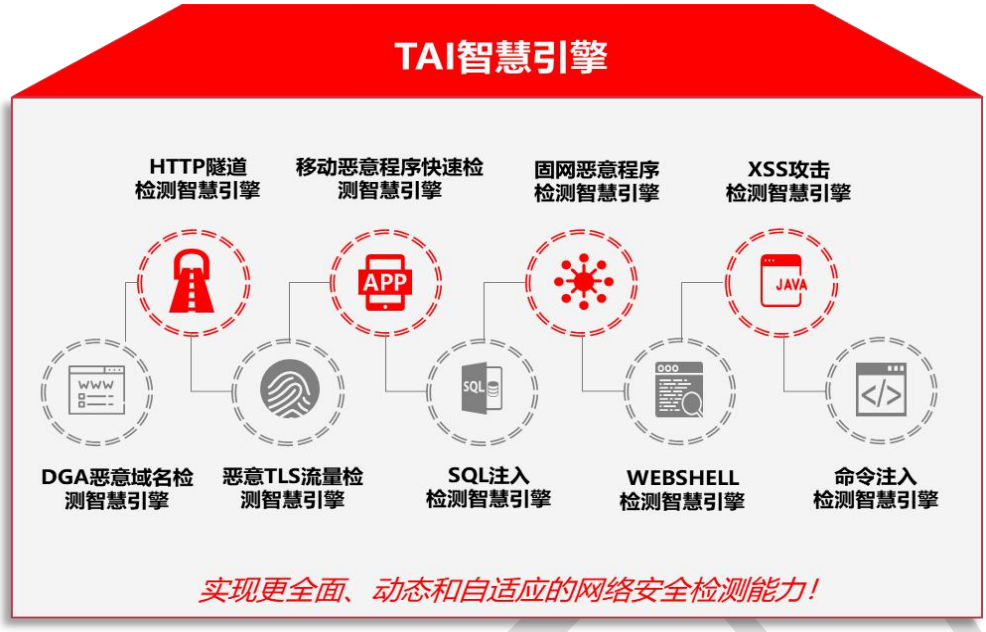
4.6 未知威胁 多维挖掘

TopSentry 应用智慧引擎，结合沙箱的检测技术，在不依赖任何规则库情况下，达到高效、精准的未知威胁检测能力。智慧引擎通过海量样本训练的机器学习模型识别未知威胁。沙箱检测采用仿真技术，模拟操作系统环境，构建执行引擎，动态化分析发现未知威胁。隐蔽隧道检测可识别是否使用通用知名端口进行隐蔽通信的威胁。智慧引擎+沙箱的方式，打破了传统特征匹配技术的束缚，既能检测已知威胁，更能发现未知威胁，让未知威胁特别是 APT 攻击无处遁形。



4.7 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，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。


TAI智慧引擎
HTTP隧道
检测智慧引擎
移动恶意程序快速检
测智慧引擎
固网恶意程序
检测智慧引擎
XSS攻击
检测智慧引擎
APP
JAVA
SQL
WWW
DGA恶意域名检
测智慧引擎
恶意TLS流量检
测智慧引擎
SQL注入
检测智慧引擎
WEBSHELL
检测智慧引擎
命令注入
检测智慧引擎
实现更全面、动态和自适应的网络安全检测能力！

5 系统功能

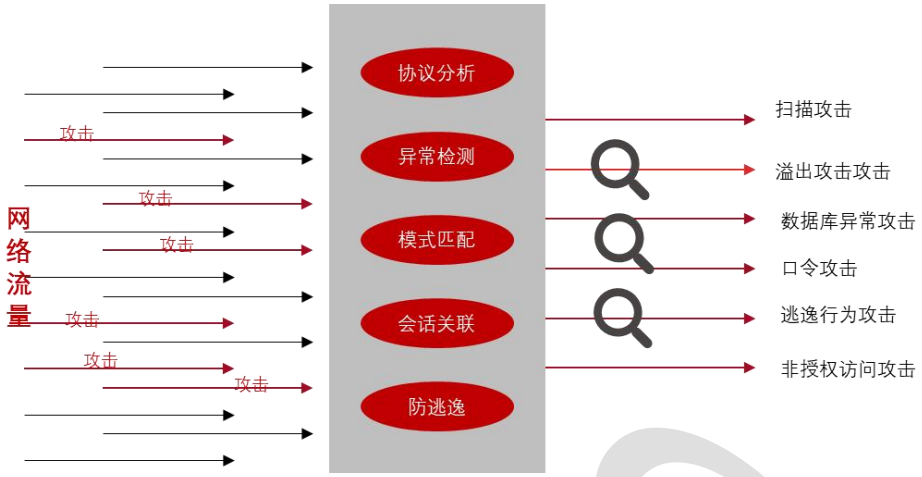
TopSentry 通过旁路部署方式，能够实时检测多种网络入侵攻击行为，并具有应用识别管控、DDoS 检测，web 安全防御，异常流量检测，可支持僵尸主机监控、威胁情报监控、恶意程序检测、URL 访问检测、流量审计、黑白名单监控、联动检测等功能，为用户提供了综合性的网络安全检测解决方案。

5.1 攻击检测

网络信息系统所面临的威胁是来自多方面的，利用网络信息系统存在的漏洞和安全缺陷对系统和应用资源进行攻击的行为层出不穷，对于入侵防御系统而言，需要针对上述行为进行全面有效防御。TopSentry 具备专业的攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段，深入分析 L2~L7 层网络入侵行为，准确发现并阻断多种网络攻击，其中包括：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、物联网漏洞攻击等在内的 17 大类网络攻击行为。为帮助用户快速、准确检索网络攻击相关的检测规则库，TopSentry 提供预定义分类规则功能，能够按照攻击类型、操作系统、风险等级、受影响的业务、流行程度等条件分类网络攻击的检测规则，并设定安全策略，有效增加攻击检测防御功能的易用性。

同时，TopSentry 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和其他的攻击行为检测。

- **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。

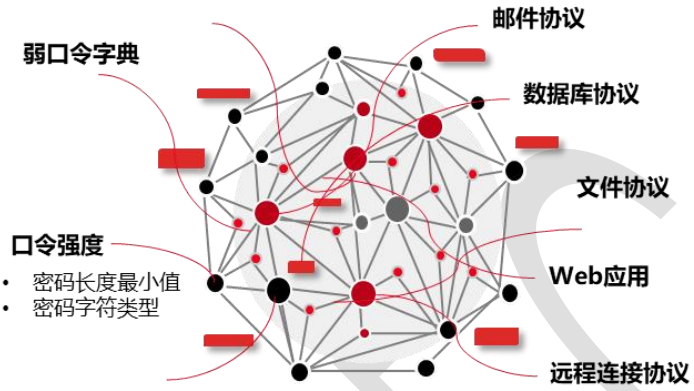


TopSentry 具备专业、权威的攻击检测规则库，产品已获得 CVE、CNNVD 兼容性认证。同时，天融信公司具有专业攻防研究实验室，充分与国际厂商和国家权威机构合作，不断跟踪、分析、研究最新发现的安全漏洞，生成拥有自主知识产权的攻击检测规则库并应用于 TopSentry，使其能够全面、有效保护企业信息化资产。规则库以周为单位定期更新，如遇紧急事件实时更新，从而确保 TopSentry 及时有效的防御已知网络攻击。

TopSentry 具有完整的 IPv4/IPv6 协议栈，能够兼容并识别 IPv4/IPv6 封包下的攻击，有效适应当今网络 IPv6 普及趋势。

5.1.1 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。

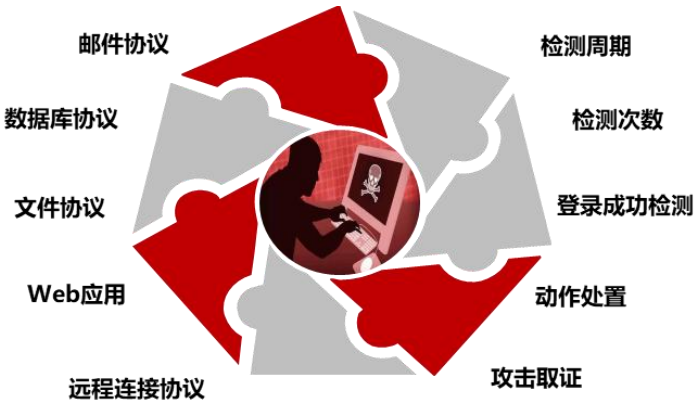


TopSentry 的弱口令检测是根据密码字典和口令强度双重模式实现对弱口令的攻击检测，设备检测到密码符合弱口令字典或者密码符合配置的密码强度，则会判断为弱口令。可支持对邮件协议、文件协议、远程连接协议、数据库协议、web 应用多种协议识别检测，有效应对弱口令攻击行为。

5.1.2 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。

TopSentry 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。

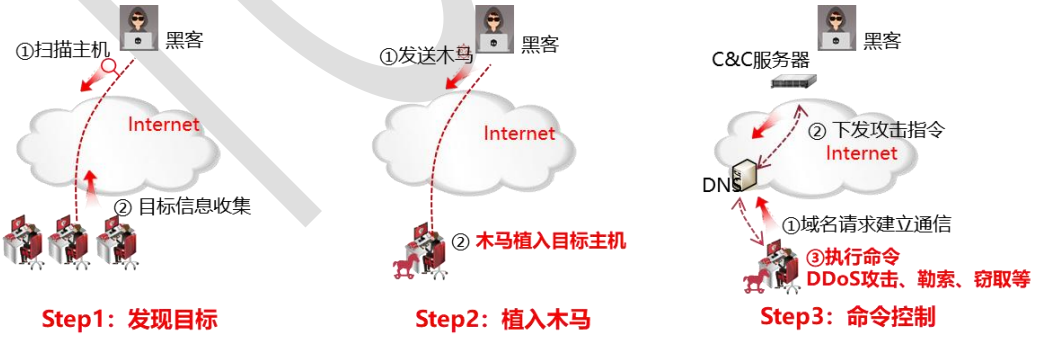


5.2 僵尸主机行为检测

在网络信息系统中，感染木马程序的主机即成为了僵尸主机，黑客可随意通过程序控制被感染计算机进行非授权操作，如开展拒绝服务攻击或大批量发送垃圾邮件等行为，而这些非授权操作往往不易被用户所察觉，可带来的危害却显而易见。

对于上述威胁隐患，TopSentry 支持对木马、蠕虫病毒的活跃周期，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。TopSentry 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。

TopSentry 能够监控超过 11000 种僵尸主机，内容涵盖僵尸网络、木马控制、蠕虫、挖矿、勒索、移动木马控制等类型，一旦命中，系统即告警、旁路阻断，同时，TopSentry 还可抓取僵尸主机的 pcap 文件，用于取证及进一步的分析研判。TopSentry 可详细记录包括：源 IP、源 MAC、源端口、目的 IP、目的 MAC、目的端口、协议、事件、关联 URL 等日志信息，详细全面的日志记录，能够有效发现定位僵尸主机，规避僵尸主机所带来的危害。



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

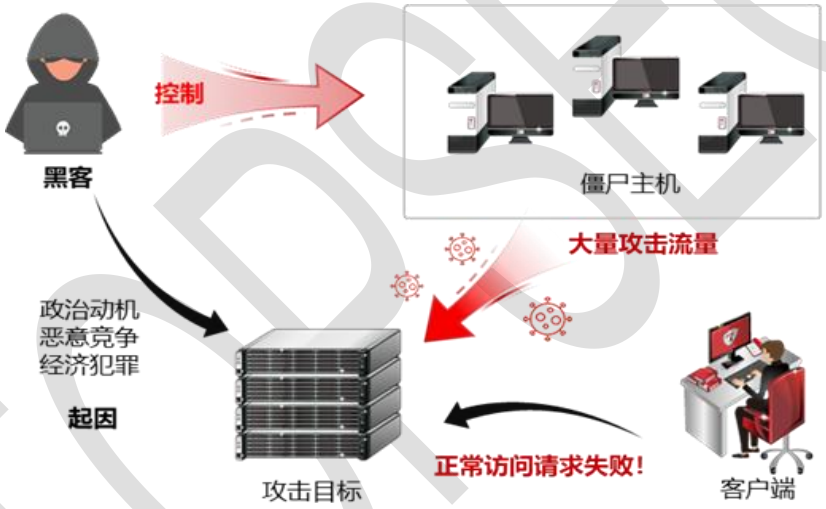
判断是否已经成为僵尸主机

5.3 DDoS 检测

企业核心业务的正常运行与服务支撑，是保障正常工作并创造经济利益的关键所在，网络信息系统中一旦充斥着分布式拒绝服务攻击，其网络带宽及系统资源充分消耗，将直接导致网络或系统负荷直至瘫痪，停止正常的网络服务，网络服务的终止使用户网站无法正常访问与操作，严重影响用户正常使用的同时，造成不可估量的经济损失。

针对危害巨大的 DDoS 攻击，TopSentry 具备全面且细粒度的 DDoS 检测功能，通过构建统计性攻击模型和异常包攻击模型，能够全面检测 ICMP Flood、UDP Flood、TCP SYN/ACK/RST/FIN Flood、TCP SYNACK Flood、TCP FRAG Flood、TCP NULL FLAG Flood、HTTP Flood、HTTPS Flood、DNS REQUERY Flood、DNS REPLY Flood 等多达几十种 DOS/DDOS 攻击行为。

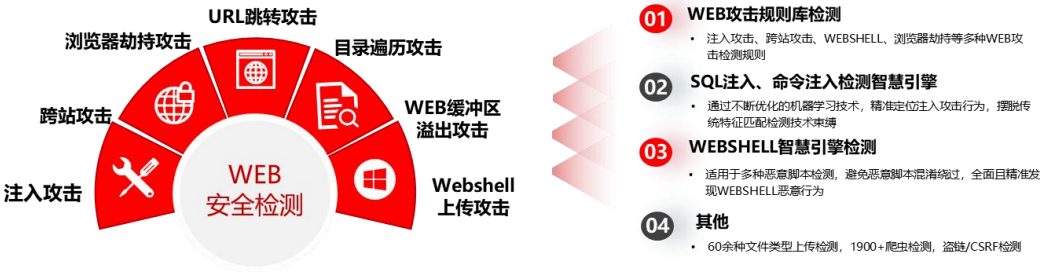
除上述功能之外，TopSentry 的 DDoS 检测模块还具有先进、易用的智能学习功能，可根据设定周期内流量学习结果生成检测阈值，有效监测未知 DDoS 攻击。



5.4 WEB 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。



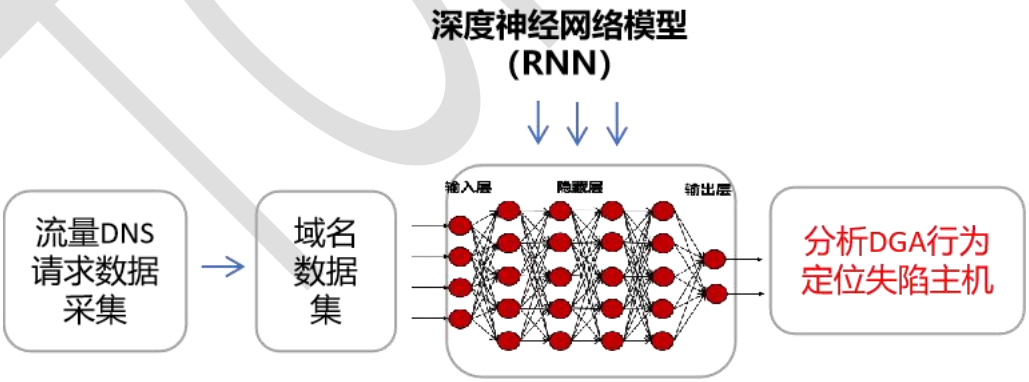
5.5 异常流量检测

5.5.1 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。

5.5.2 DGA 域名检测

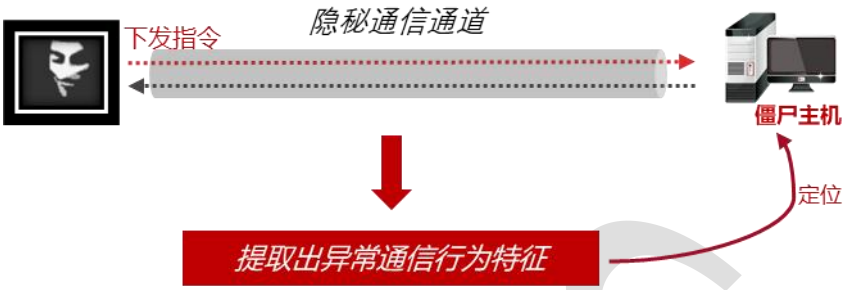
TopSentry 可通过 AI 深度学习技术中的循环神经网络（Recurrent Neural Network, RNN），对海量恶意域名样本充分训练生成检测模型来识别网络中伪随机域名，解决 DGA 域名算法逆向破解难题，实现对隐秘性高的 DGA 恶意域名进行深入检测。RNN 具有自动提取样本特征的能力，可挖掘其内在的字符分布统计特征，将传统方法的分类精度大幅度提升，实现检测率高，误报率，漏报率低。



5.5.3 隐蔽隧道检测

TopSentry 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。



5.6 应用识别

应用程序是保障用户正常工作办公的重要组成之一，在信息系统中，网络不规范使用所导致的网速骤降问题比比皆是，而应用层攻击事件更是防不胜防，故深度应用识别能力，是应用层安全防护的基础，亦是规范化用户上网，确保正常网络访问的有力保障。

TopSentry 提供深度且全面的应用识别功能，能识别包括：P2P 下载、P2P 音频、P2P 视频、即时通讯、语音电话、网上银行、电子商务、财经软件、网络游戏、社交网络、网页视频、网页音频、网络硬盘、网页邮箱、加密隧道、标准协议、远程控制、数据库、移动应用、HTTP 应用、软件更新、IM 文件传输、工控物联网等 5000 多种应用。全面的应用识别功能，能够发现从而检测应用漏洞利用攻击，保障网络安全。

应用识别管控功能采用深度识别技术，能够智能分析应用协议交互过程，在应用协议交互过程进行智能分析，而非简单依据服务端口的技术手段来判断应用协议类型，对采用动态变化服务端口或者使用标准协议端口隐藏传输内容的应用也能够准确识别和控制。

5.7 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。

TopSentry 的威胁情功能报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。

TopSentry 威胁情报库是从海量的威胁情报数据中提取出 800+万高可信威胁，所检测威胁类型多维，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。威胁情报功能的应用，能够有效提高威胁检测效率，并帮助企业全面了解网络信息系统所面临的威胁情况，为威胁检测工作提供有力参考依据，提升安全性。

同时，支持与天融信云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本、MD5 进行一键搜索，查看包括但不限于基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名。

5.8 病毒检测

在网络信息系统中，病毒威胁通常会通过共享、邮件等方式广泛传播，信息系统主机一旦感染木马、病毒，将会导致用户隐私、机密文件、账号信息窃取泄露、电脑数据破坏、内存/磁盘空间消耗等事件产生。另外，受感染主机被利用发动网络攻击等事件亦普遍存在，业务被迫中止、正常工作无法进行，病毒所造成的严重危害显而易见。

TopSentry 的病毒加检测功能具有两种方式：

◆ 依靠威胁情报检测已知病毒文件

TopSentry 的威胁情报库中具有恶意文件威胁情报信息，包含蠕虫、木马、间谍软件、灰色软件、恶意广告、后门程序、垃圾邮件、勒索软件、钓鱼等多种病毒情报类型，能够深层检测文档文件、压缩文件、执行文件、移动端文件、图片文件等多种文件类型中包含的病毒信息，实时发现流行的各种网络病毒。

◆ 依靠恶意程序检测未知病毒文件

TopSentry 通过机器学习引擎、沙箱引擎和联动天融信 APT 安全监测系统（APT-61158-ATD），能够深层检测 HTTP、FTP、SMTP、POP3、IMAP、SMB、NFS 等协议中传输的文件，发现并阻断包括计算机病毒、木马、蠕虫、混合攻击程序、间谍软件、恶意广告、勒索软件、流氓推广、移动恶意程序、灰色软件等多种类型的病毒文件。

另外，TopSentry 具备病毒样本捕获能力，可还原 exe、dll、elf、so、apk 等类型文件，并可根据需要，进一步实施文件鉴定，检测恶意程序名称、文件类型、风险等级、MD5 等信息， 能够全面解析病毒样本信息。

5.9 URL 访问

对于网络信息系统而言，其中的威胁会来自内外不同方向，由内至外的威胁更具主动性，如企业员工误访问挂马网站、钓鱼网站、恶意代码网站等情况，造成信息恶意传播、国家机密以及企业敏感信息泄漏等一系列问题。除此外，随意浏览访问与工作无关的网站，亦会导致网络资源滥用情况发生，整体工作效率无从保障。

TopSentry 支持 URL 访问检测功能，内置全面且细粒度的 URL 分类库，包括搜索引擎、社交网络、网上购物、科学技术、求职招聘、生活资讯、新闻及门户、休闲娱乐、财经、流

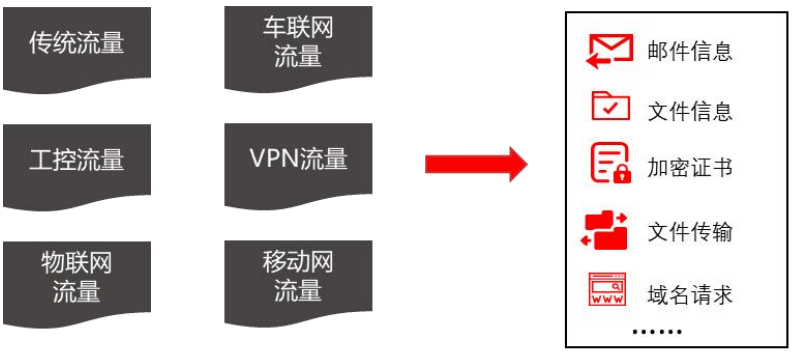
媒体、P2P 资源、下载、教育、邮件和存储、传统行业、政策法规、网络安全、成人内容、非法及不良、其它等超过 1000 万个 URL 地址分类库，能够有效针对网站访问行为进行检测，全面规避风险，确保合规化网站访问行为。

TopSentry 的 URL 检测功能，能够按周期统计内网用户的上网行为以及告警情况，限制用户对违规站点的访问，并详细展示违规事件主机与事件详情，以便在发生安全事件时，快速定位到问题源头，有效威慑和遏制内网用户的各种违反安全策略行为。

5.10流量审计

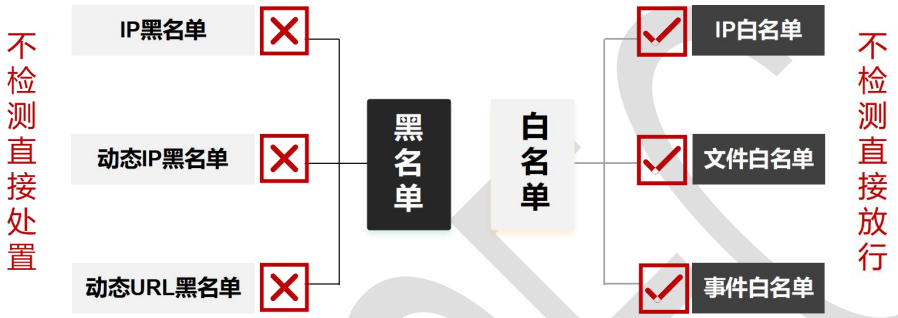
在企业的网络环境中，除已知与未知威胁之外，还充斥着网络访问与使用所导致的重要信息泄露、违规网站访问、邮件非法传播数据等一系列问题，日趋复杂的信息系统中，针对违规用户行为给网络所带来的潜在威胁，需要具备全面的网络行为审计能力。

TopSentry 提供综合性的网络流量审计功能，可基于 TCP/UDP、ICMP、HTTP、邮件、文件、FTP、DNS、NFS、SMB、SSL 等不同协议进行网络行为审计，审计包括网站访问、域名访问、邮件收发、文件传输等行为，综合性的流量审计功能，可使企业积极响应政策合规审计要求，全面监测用户网络行为及通信内容，及时发现违规行为，并提取日志，更为后续全面的安全态势分析提供多维有力依据。



5.11黑白名单

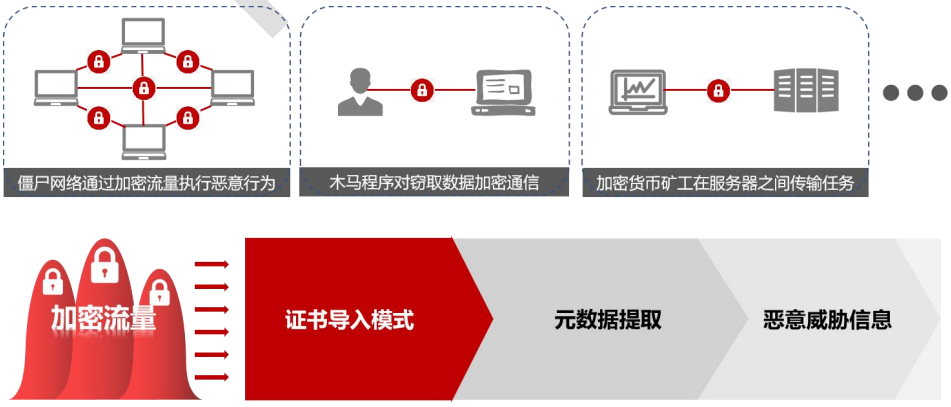
为最大化增加入侵检测系统的检测效率，TopSentry 提供黑白名单监控功能，系统可基于单 IP 地址、端口、URL、事件告警、XFF 字段等选择加入对应名单，加入黑名单的 IP 地址所发送的数据包将直接被系统告警、旁路阻断等响应，而加入到白名单的 IP 地址，系统不对其进行检测。针对 IP 黑名单监控功能，系统提供手动和自动两种添加方式，不同方式添加的 IP 将采取不同策略删除。同时，系统还支持文件白名单能力，对一些不安全且必须传输的文件，不检测直接放过。



5.12加密流量

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。

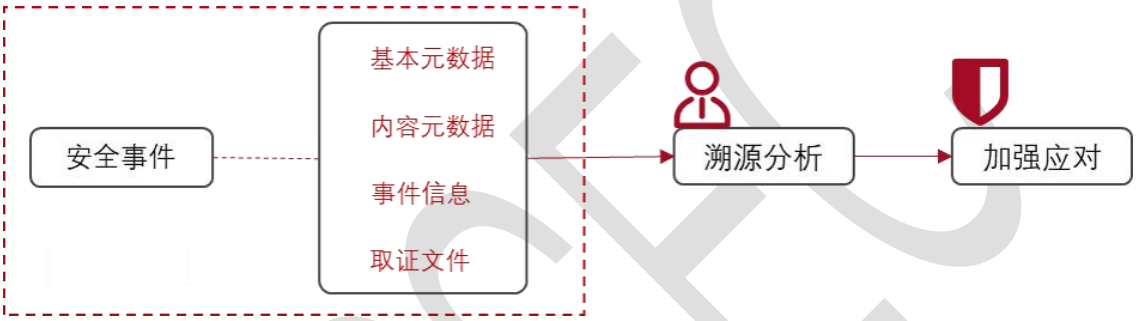
TopSentry 可通过导入证书+无证书检测相结合的方式，直接对加密流量进行解密处理，实现对加密流量元数据的深度提取，检测恶意威胁信息。设备通过智慧引擎检测、异常握手检测、非法证书检测、内网流量检测等多种方式发现恶意程序的加密通信，实现无证书检测加密通信的效果。由天融信安全研究团队通过对恶意程序行为进行深入分析，提取出恶意程序加密通信的指纹特征，从而生成指纹特征库。TopSentry 的加密检测引擎对加密流量的报文深度解析，从中筛选出潜在的恶意加密流量，提取报文中的摘要信息，通过将摘要与指纹特征库匹配的方式，确认恶意程序的通信行为，从而让恶意程序加密通信无处遁形。



5.13溯源取证

TopSentry 支持对入侵攻击、异常行为、恶意程序等威胁事件进行取证记录，支持报文取证和样本文件取证。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，兼容 wireshark 等工具，支持查看会话数量，会话时间、源/目的 IP、协议、会话信息等。

此外，TopSentry 还具有攻击有效性研判能力，通过回包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。支持将威胁事件日志信息和取证文件相互关联，通过对威胁基本信息检索即可获取威胁详情。



5.14日志报表

系统全面的威胁检测功能，与之相匹配的是相关告警事件多维度直观展示能力，TopSentry 提供详尽的安全事件审计及分析报表功能，系统可实时图形化展示攻击、恶意程序、僵尸主机、URL 检测、网络流量、系统状态等信息，并根据不同安全事件，详细审计包括：时间、协议、源 IP、源端口、目的 IP、目的端口、级别、动作、规则编号、事件描述、应用协议、事件详情等信息，为后续事件分析提供有效依据。另 TopSentry 可根据不同事件提供多维度统计分析功能，以安全事件 Top10、受影响业务、类型、分布、趋势、结果等维度图形化方式展示，使用户更为直观掌握网络信息系统中复杂的威胁状态。

TopSentry 提供丰富易于配置的报表功能，可为管理员在系统海量事件日志中提取有用信息，该功能配置简单，可根据策略设置，自动对庞大的网络安全事件进行智能统计分析汇总，提取有效分析值。通过各种事件的汇总信息，加以图表的直观展示方式，使管理员能够很快掌握某一段时间内的威胁状况、网络运行状态等有效信息，有效减轻管理员工作量的同时，使其轻松了解全网的攻击形势及网络资产的安全态势。

5.15威胁分析

TopSentry 提供威胁视角和运维视角分析，威胁视角按照受害者、攻击者、威胁事件、恶意文件(扩展功能)、攻击类型、攻击主机、受害主机、应用类型、恶意程序类型(扩展功能)

等维度进行综合分析，支持数据下钻查看威胁详情。运维视角分析能够帮助运维人员了解设备运行状态。(提供截图证明)支持威胁分析功能，威胁分析展示包括:威胁事件的失陷/成功/尝试/失败等攻击结果、攻击事件级别、攻击类型分布、攻击阶段、事件详情等信息。(提供截图证明)支持攻击者视角分析，按照时间范围、攻击者 IP、事件类型、处置状态、来源(境外、境内、内网)、攻击者所属国家等条件综合分析攻击者信息。

支持受害者视角分析，按照时间范围、受害者 IP、事件类型、处置状态、攻击结果、应用协议等条件综合分析受害者信息。

支持文件视角分析，按照时间范围、级别、攻击结果、文件 MD5、攻击者 IP、受害者 IP、来源(境外、内网)、类型等条件综合分析恶意文件信息。

5.16多维联动

天融信入侵检测系统提供了防火墙联动、终端安全管理系统联动和集中管理联动功能，全方位保障用户的网络安全。

- 防火墙联动：

通过防火墙联动功能，可以实现由 TopSentry 进行监听，由联动防火墙进行阻断的安全策略；

- 集中管理平台联动：

通过集中管理联动功能，对入侵检测系统进行集中管理。通过集中管理平台统一管理入侵检测系统，包括账号密码、系统配置、安全策略、自定义情报等。

- 终端安全管理系统联动：

通过终端安全管理系统联动功能，可快速锁定受害者信息，将受害主机告知终端安全管理系统，对受害主机进行全面扫描。通过联动获取终端资产信息，以资产为视角，深入分析威胁全过程。

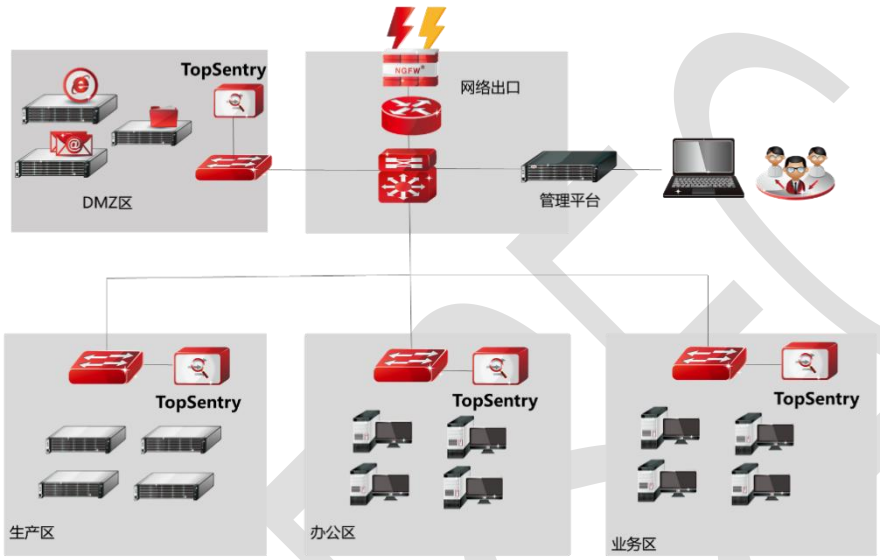
5.17日志告警

设备具备多种告警方式，包括:邮件、声音、本地、串口、SNMP 多种告警类型。支持针对不同类别告警信息进行配置，包括:安全告警(攻击检测、僵尸主机、恶意程序、威胁情报、WEB 防护、异常流量、DDoS 检测、URL 过滤、黑名单等）、分析、管理、系统、硬件、容错、测试等。

支持通过 syslog、Kafka、邮件等方式将日志数据、告警数据等发送给第三方平台。

6 部署方案

面对复杂多变的网络环境，单位不仅需要有针对重点区域监控，还需要针对内部整个网络的全面监控。可在网络的出入口或者重点服务器区均可部署入侵检测系统，时刻掌握企业的重要信息资产网络整体的安全水平。



7 产品规格

型号	TS-54328-FT	TS-3542A-FT	TS-74453-HG
CPU	飞腾 D2000（2.3GHz，8 核）	飞腾 D2000（2.3GHz，8 核）	海光 7390(3.3GHZ,32 核) *2
操作系统	银河麒麟 V10 （内核版本 4.19.90）	银河麒麟 V10 （内核版本 4.19.90）	统信服务器操作系统 V20 （内核版本 4.19）
数据库	人大金仓	人大金仓	人大金仓
硬盘	128G SSD 系统盘+4T SATA 存储盘	128G SSD 系统盘+4T SATA 存储盘	960G SSD 系统盘+16T SATA 存储盘
内存	32G	32G	128G
固定接口	6GE&4SFP&4SFP+	6GE&4SFP&2SFP+	2GE&4SFP+
可扩展槽位	1 个	2 个	1 个
USB 接口	2 个	2 个	2 个
产品形态	硬件	硬件	硬件
尺寸(宽深高)	440*510*89（2U）	440*510*89（2U）	440*510*89（2U）
冗余电源	是	是	是
净重	12Kg	11.6Kg	11.38Kg
毛重	16.4Kg	16Kg	16.5Kg
电压	100~240VAC/240VDC	100~240VAC/240VDC	100~240VAC/240VDC
频率	50~60HZ	50~60HZ	50~60HZ
电流	7A MAX	7A MAX	7A MAX
功率	550W	550W	350W
运行温度	0~40℃	0~40℃	0~40℃
存储温度	-40~55℃	-40~55℃	-40~55℃
相对湿度	10~90%，非冷凝	10~90%，非冷凝	10~90%，非冷凝

8 产品资质

详细要求
《网络关键设备和网络安全专用产品安全认证证书》
《涉密信息系统产品检测证书》
《计算机软件著作权登记证书》
《国家信息安全漏洞库兼容性资质证书》
《国家信息安全测评信息技术产品安全测评证书》
IPV6 Ready Phase-2 金牌认证
CVE Compatibility Certificate
具备军用信息安全产品认证证书
具备南大通用产品兼容性认证
具备飞腾产品适配证明
具备海光产品适配证明
具备麒麟软件 NeoCertify 认证证明
支持 GCB010-2017<安全管理接口技术要求>
支持 GCB007-2017 <安全审计服务规范>

声明

1. 本文档所提到的产品功能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。

RELIABLE NETWORK
SAFE WORLD
TOPSEC