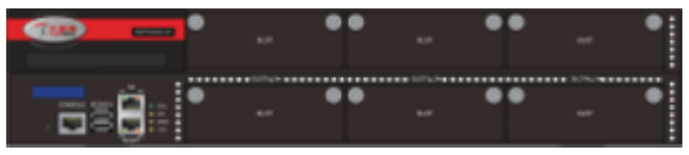
天融信僵尸网络木马和蠕虫监测与处置系统TopTVD

www.topsec.com.cn

产品概述

天融信僵尸网络木马和蠕虫监测与处置系统（以下简称TopTVD）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，即九合一全流量检测探针。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、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网络威胁。



产品特点

九合一检测探针

TopTVD产品是集攻击检测、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，TopTVD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。

未知恶意程序检测

TopTVD产品首创应用TAI-1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。TAI-1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。TAI-1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。

嵌入式威胁情报

TopTVD产品的威胁情报库是由天融信安全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680万高可靠的威胁情报数据。嵌入式威胁情报库情报来源可靠精准、情报种类丰富、更新速度快、独立性强。

多维知识库支撑

TopTVD产品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。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。

全流量元数据挖掘

TopTVD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。

典型应用

旁路部署

对于规模较小、结构简单的网络环境，TopTVD通常是在网络出口处或核心网络节点处旁路部署。对于规模较大、结构复杂的网络环境，TopTVD可在客户下级单位、分支机构等多个网络出口处部署。TopTVD旁路部署在不影响网络的前提下，做到对客户网络环境中多种威胁事件监测。

产品规格

型号	TVD-71358	TVD-7155A	TVD-72354	TVD-96424
固定接口	6*GE&4*SFP	6*GE&4*SFP&2*SFP+	4*SFP+	≥1*GE
USB接口	2个			≥2个
产品形态	2U			6U
尺寸(宽深高)	426*500*89mm			442*522.5*265.9mm
冗余电源	是			最多支持4块电源
净重	13.39Kg	14.39Kg	13.39Kg	满配置约53Kg
毛重	16.90Kg	17.90Kg	16.90Kg	满配置约83Kg
电压	220V			100-240V AC； -36V-~-72V DC；
频率	47-63Hz			50-60Hz
电流	4.5-2A			
功率	300W MAX			参考具体配置
运行温度	0℃—40℃			0℃—40℃
存储温度	-20℃~70℃			-20℃~70℃
相对湿度	20%—90%，非冷凝			10%—95%，非冷凝

功能列表

检测能力	支持对web攻击、漏洞攻击、注入攻击、扫描攻击、跨站攻击、溢出攻击等入侵行为检测。
	支持对木马、病毒、蠕虫、勒索软件、钓鱼软件等恶意文件检测。
	支持本地威胁情报，包括恶意IP、恶意域名、恶意URL、恶意文件等情报。
	支持对僵尸主机异常通信行为监测。
取证能力	支持捕获存留威胁原始报文以及恶意样本文件。

产品资质

证书名称	认证机构
计算机信息系统安全专用产品销售许可证	中华人民共和国公安部
计算机软件著作权登记证书	国家版权局