# 天融信入侵检测系统TopSentry

www.topsec.com.cn

## 产品概述

天融信入侵检测系统（以下简称TopSentry产品）是一款旁路监听网络流量，精准发现并详细审计网络中漏洞攻击、DDoS攻击等风险隐患的网络安全监控产品。同时，TopSentry产品具有上网行为监控功能，发现客户风险网络访问、资源滥用行为，辅助管理员对网络使用进行规范管理，并可结合与防火墙联动阻断功能，进一步实现对攻击的有效拦截，全面监控、保护客户网络安全。

## 产品特点

### 全面检测

准确检测发现网络中包括：溢出攻击、RPC攻击、WEBCGI攻击、拒绝服务、木马、蠕虫、系统漏洞等在内的11大类网络攻击行为。同时，结合上网行为管理等模块，扩展网络安全监控范围，实现对全网威胁的立体化监控效果。

### 深度分析

采用基于目标主机的流检测引擎，结合协议分析、模式匹配、统计阀值和流量异常监视等综合技术手段来深入分析判断L2~L7层的网络入侵行为，并具有多种抗逃逸算法，可精准、深度发现网络中的攻击威胁，保证TopSentry产品的高检测率。

### 高效计算

采用天融信多核处理硬件平台，基于先进的独创专利技术SmartAMP并行处理架构，通过处理器动态负载均衡技术，实现最大化利用运算空间，并结合独创的SecDFA核心加速算法，实现了对网络数据流的高性能实时检测效果。

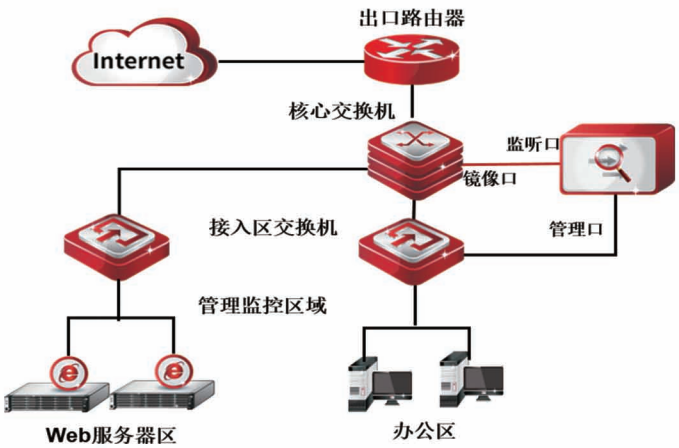
### 详尽审计

详细审计攻击事件五元组、攻击内容，攻击特征码以及攻击报文等信息，为攻击溯源提供有效的依据。同时，具有分析报表功能，对大量的攻击事件进行进一步分析，让管理员对网络中复杂的攻击状态一目了然。

## 典型应用

### 旁路部署

面对复杂多变的网络环境，企业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。此时在企业网络的出入口和重点服务器处分别部署入侵检测系统，时刻掌握企业的重要信息资产网络整体的安全水平。



## 产品规格

| 型号 | TS-53228 | TS-53528 | TS-53628 | TS-6371C | TS-73660 | TS-73552 | TS-73752 |
|---|---|---|---|---|---|---|---|
| 固定接口 | 6GE&4SFP | 6GE&4SFP | 6GE&4SFP | 6GE&4SFP&4SFP+ | / | 2SFP+ | 2SFP+ |
| USB接口 | 2 | | | | | | |
| 产品形态 | 2U | | | | | | |
| 尺寸(宽深高) | 426* 560 *89 mm | | | | 426* 550 *89 mm | | |
| 冗余电源 | 是 | | | | | | |
| 净重 | 12.43Kg | | | | 11.89Kg | 12.89Kg | |
| 毛重 | 18Kg | | | 18.32Kg | 15.40Kg | 16.40Kg | |
| 电压 | 100~240VAC | | | | | | |
| 频率 | 50~60HZ | | | | 47~63HZ | | |
| 电流 | 5-2.5A | | | | 4.5-2A | | |
| 功率 | 75W | | | | 300W | | |
| 运行温度 | 0~40℃ | | | | | | |
| 存储温度 | -20~70℃ | | | | | | |
| 相对湿度 | 10~95%，非冷凝 | | | | | | |

## 功能列表

| | |
|---|---|
| 入侵防御检测 | 超过6000条攻击规则 |
| | 全面检测溢出攻击（BufferOverflow）、RPC攻击（RPC）、WEBCGI攻击（WebAccess）、拒绝服务（DDOS）、木马（TrojanHorse）、蠕虫（VirusWorm）、扫描（Scan）、HTTP攻击类（HTTP）、系统漏洞类（system） |
| 上网行为检测 | 内网实时监控 |
| | 超过1000万条URL地址分类库，可以实时监测对主页的访问<br>基于应用（网络视频、聊天等）的细粒度监测，可以轻松对应用进行限流、禁止、限定时间段 |
| DoS/DDoS检测 | 支持CC攻击检测 |
| | DNS异常包检测、DHCP攻击检测 |
| | 非法报文攻击：tcp_sscan、ip_option等；统计型报文攻击：Synflood、Icmpflood、Udpflood |
| | 支持flood阀值自学习功能，学习时间可设置 |
| | 支持flood服务器阈值、服务器高压阈值、单机阈值设置 |

## 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 |
| 国家信息安全测评信息技术产品安全测评证书EAL3+ | 中国信息安全测评中心 |