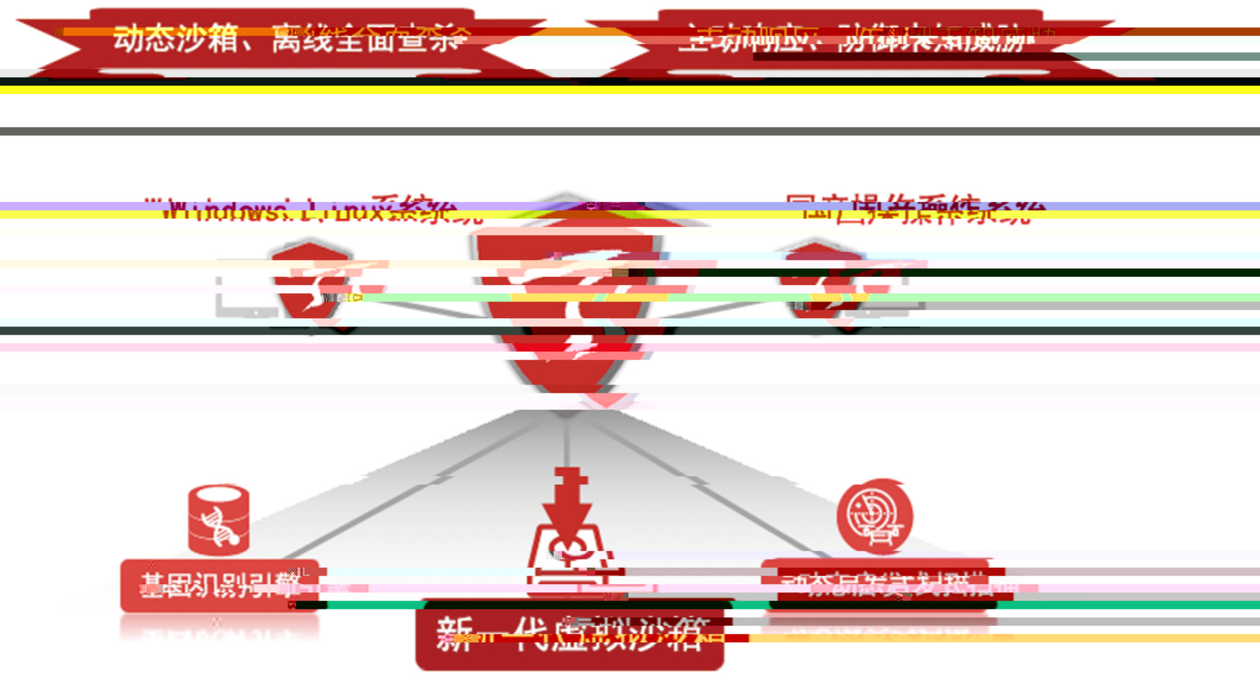
天融信终端威胁防御系统

www.topsec.com.cn

产品概述

终端威胁防御系统（简称EDR）是一套立体化的终端安全防护解决方案，集成病毒查杀、漏洞修复、系统加固、网络防御、终端管控、资产管理、风险态势感知等多种功能于同时满足的虚拟沙盒技术对威胁行为深度分析，结合静态特征检测、主动防御、微隔离等主动防御技术，有效检测、阻断、完全追溯未知威胁，多维度防御病毒传播和横向感染，全面提升用户的终端安全管理能力。



产品特点

终端态势 全局可视

通过智能化的企业管理中心，对终端进行统一管理，实现防护系统的整体控制及终端威胁集中展示，帮助用户掌握全网终端安全态势。

基因识别 轻量高效

通过特征码查壳脱壳、恶意代码DNA识别、恶意代码DNA片段重组等技术减少特征库冗余数据对已知病毒和变种病毒精准识别，有效节省CPU和服务器资源。

虚拟沙盒 精准分析

通过强大的自主知识产权反病毒引擎检测技术，及时发现恶意代码，基于虚拟沙盒的分析引擎，还原病毒样本的攻击行为，精准识别未知病毒威胁。

主动防御 多维防护

防御：虚拟补丁技术、恶意行为监控、勒索病毒诱捕、黑客入侵拦截等，针对所有的威胁入口设计强有力的防御策略，阻断终端的威胁行为。

终端行为全面管控

移动存储介质管理：标签化管理，细化U盘等使用权限。

设备管控：限制光驱、打印机、网络适配器等设备接入终端。

外联监控：检测终端连接互联网行为进行阻断等管控措施。

远程协助：通过管理平台远程控制终端电脑，提高运维效率。

系统监控：对进程/服务、帐号和软件类型的监控。

文档安全：关键字检测防止数据泄露，跟踪文档的各种操作行为，方便追溯。

与防火墙、态势感知、上网行为管理联动处置，形成终端防护、边界防护、智能展示为一体的安全解决方案，为企业客户提供全面的立体防御。

典型应用

管理端

管理中心对终端进行集中管控、策略下发、漏洞修复、病毒库升级等统一管理，实现对全网终端防病毒系统的运行状态实时可视化，保障网络整体安全。

客户端

客户端执行管理中心下发的任务和安全策略，自动执行终端进行全方位的病毒查杀和防御，收集安全事件上报给管理中心。