天融信终端威胁防御系统TopEDR

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、风险态势展示等功能；采用领先的虚拟沙盒技术对威胁行为深度分析，结合勒索诱捕、虚拟补丁、微隔离等主动防御技术，有效解决勒索、挖矿、免杀逃逸等威胁，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，协助用户掌握全网终端安全态势。

基因识别 轻量准确

通过特征高度复用、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PC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核心底层技术，及时发现恶意代码，基于虚拟沙盒的分析引擎，还原病毒本质的攻击行为，精准识别未知病毒威胁。

主动防御 多层防护

对于无文本或漏洞利用等攻击，EDR通过系统核心位置防御、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独特的防护策略，实时感知终端的威胁行为。

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断网等管控措施。

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、账号和软件等实时监控。

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。

协同联动 全面护航

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，为企业客户提供更全面的立体化防护。

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，实现对整个防护系统的有效控制和安全态势可视化，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，有效的对全网终端进行全方位的病毒查杀和防护，收集安全事件上报给管理中心。