

天融信终端威胁防御系统TOP-UTM

产品概述

终端威胁防御系统(简称ETD)是一套立体化的终端综合防护解决方案,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、风险评估等威胁感知和响应能力,通过拟沙盒技术对威胁行为深度分析,结合病毒威胁情报库、微隔离等主动防御技术,有效阻断病毒传播、防止病毒逃逸等威胁,多维度防御病毒传播和横向感染,全面提升用户终端安全管理能力。

动态沙箱、离线全面查杀

主动响应、防御未知威胁



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态势及终端威胁集中展示,辅助用户掌握全网终端安全态势。

基因识别 精准溯源

通过特征高度复用、恶意代码DNA识别、恶意代码DNA片段匹配等技术,减少病毒样本数量,提升病毒识别精度,精准识别病毒威胁,有效节省CPU和服务器资源。

虚拟沙箱 精准分析

通过强大的基因识别引擎及病毒引擎,及时发现恶意代码,基于虚拟沙箱的分析引擎,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 预防威胁

通过主动防御引擎,对恶意行为进行拦截、阻断、防御,防止病毒传播、恶意行为扩散、勒索病毒传播、黑客入侵、拦截等,针对所有的威胁入口设计精准的防御策略,防止威胁终端的威胁行为。

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时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、权限、操作等进行实时监控。
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。

统一防护 全面防御

与防火墙、态势感知、上网行为管理等联动处置,形成终端防护、边界防护、智能展示为一体的安全解决方案,为企业用户提供全方位的安全防护。

