SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

深信服统一端点安全管理系统aES

智防护、真联动、全场景

端点安全建设风险与挑战

挑战一：
传统安全产品
无法应对端侧新威胁

在高级攻击技术平民化及黑灰产产业化的趋势下，越来越多的威胁利用高级攻击手法如加密、混淆、白利用等来逃避检测，传统安全防护措施基本失效。

挑战二：
威胁处置不彻底，
安全事件难以有效闭环

网络侧及终端侧安全产品检测机制不同，导致无法协同处置安全威胁，网侧发现威胁而端侧无法定位威胁根因，查不到、处置不干净等问题频发，难以有效闭环。

挑战三：
端点安全管理成本高，
难统一分析管理

PC、服务器、容器等安全需求需要不同的安全产品来满足，在带来管理成本提升的同时，面对攻击的横向渗透行为，也难以跨平台分析攻击路径和影响面。

深信服 aES 产品简介

深信服 aES 是应用于 PC、主机、容器等端点设备的统一安全管理系统，能够对于网络钓鱼、勒索病毒、0day、APT 等多种攻击方式进行有效检测和防护，致力于为用户打造全场景安全效果最好的新一代端点安全软件。

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

优势能力

钓鱼攻击阻断

- **精准检测钓鱼攻击：**全面采集强 / 弱攻击行为信号，由 AI 赋能还原攻击情境，精准判定钓鱼事件。
- **自动阻断钓鱼攻击：**自动提取钓鱼攻击产生的关键点如恶意行为、文件、驻留项等，并自动阻断和清除。

勒索病毒防护

- **秒级自动阻断：**基于动静结合的双 AI 引擎，秒级捕获勒索攻击并阻断告警。
- **自动增量备份：**AI 检测可疑勒索行为，触发增量备份，将目录内文件备份至特殊加密空间。
- **一键回滚恢复：**勒索病毒被查杀后，一键即可将被加密的文件回滚恢复至未加密状态。

0day 漏洞检测

- **主机行为画像自学习：**通过无监督学习，基于历史访问行为、文件、网络和进程行为数据，建立业务白行为画像。
- **以白鉴黑，发现可疑行为：**通过白行为画像比对，以白鉴黑发现可疑的 0day 漏洞攻击行为，进入留观区预警。
- **告警削减，检测 0Day：**通过 NoDR 技术削减 90%+ 告警误报，实现 0Day 精准检测。

APT 攻击防护

- **行为关联和聚类，APT 信号无所遁形：**持续行为采集，对 APT 攻击行为针对性标记、关联和回溯，任何 APT 信号无所遁形。
- **专项引擎将 APT 攻击遏制于萌芽：**精准识别和自动化阻断如钓鱼、勒索、0day 等伴随 APT 出现的攻击，遏制 APT 攻击于萌芽。

失陷主机处置

- **失陷主机恶意进程定位：**结合网络侧设备告警信息，由端侧定位发起外联的恶意进程及其关联项。
- **阻断恶意程序外联及横向：**通过端侧和网络侧联动，在网络侧安全设备上一键即可遏制失陷主机外联及横向行为。
- **清除恶意文件及关联项：**结合网络侧和端侧能力，一键删除恶意文件、关联注册表项、计划任务等，彻底清除威胁。

核心价值

智防护
安全防护效果好

AI 自动防护技术，能够自动防护勒索病毒、网络钓鱼、0day 等多种攻击类型，帮助用户快速阻断安全威胁，降低因安全事件带来的损失。

真联动
产品联动易闭环

安全产品之间强强联合，实现 1+1>2 的安全效果，解决用户威胁定位难、处置不彻底、闭环效率低等问题，实现安全事件有效闭环。

全场景
不同场景适用强

国内率先落地“一端一中心”，PC、服务器、容器及信创环境等全场景端点融合管理，支持 SAAS 化轻交付，极大增强了全网端点的安全可见性和管理的便捷性。

市场认可

品牌影响

- 国内首家连续 3 次满分通过国际权威机构 AV-TEST TOP 认证的企业级终端安全产品
- 自研 SAVE 人工智能引擎获得国际知名检测平台 VirusTotal 认证

用户选择

- 累计超过 1400W+ 终端部署
- 16000+ 用户的信赖
- 7*24 小时持续威胁响应

扫码了解 aES 更多详情

致力于为用户打造全场景，安全效果最好的端点安全产品！