SANGFOR
深信服科技

深信服让IT更简单，更安全，更有价值!

深圳市南山区学苑大道1001号南山智园A1栋
售前咨询：400-806-6868　售后服务：400-630-6430
邮编：518055　邮箱：market@sangfor.com.cn

深信服官方微信

深信服移动官网

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

深信服EDR快速使用指南

轻量易用，实时保护，东西向可视可控

深信服EDR快速使用指南

让产品帮您快速带来价值

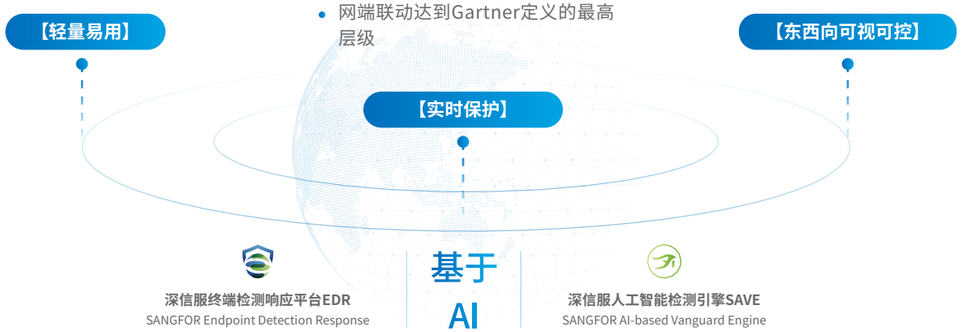
深信服EDR是一款轻量易用、实时保护、东西向可视可控的下一代终端安全产品

预防	漏洞补丁管理	系统安全基线核查	微隔离流量可视	微隔离流量可控	USB管控	一键端口封堵
防护	勒索诱饵防护	无文件攻击专防	进程黑白名单	全球热点威胁同步	远程登录防护	轻补丁漏洞免疫
检测	文件实时监控	Webshell检测	暴力破解检测	违规外联监控	流行病毒快速检测框架	SAVE引擎
响应	宏病毒修复	僵尸网络举证	进程溯源	终端隔离	清除&移除	终端围剿式查杀
运营	资产信息清点	可视化首页&报表	警报	API接口支持	网端联动	批量部署

客户端轻量化业务无感知，无需复杂配置，半自动化安全运维

- 基于威胁攻击链多达30个功能构建多层次防御
- 恶性病毒（感染型病毒，宏病毒，CAD病毒，勒索病毒等影响业务连续性的病毒）清除修复能力强
- 网端联动达到Gartner定义的最高层级

创新微隔离技术基于业务维度让终端间流量可视可控，同时做到简单落地，高效运维



市场成绩

- 实际安装超过400W终端
- 5000+客户的最优选择
- 7*24小时持续威胁响应
- 全球威胁情报实时同步
- 老旧系统（Win7、XP等）持续支持

第三方评测

深信服EDR成功入围微软官方终端安全软件**推荐名录**，获得了**兼容Windows**的微软WHQL徽标认证，其人工智能引擎SAVE也入围了**国际权威**的Virustotal检测平台，技术能力位居业界前沿。


赛可达实验室-东方之星证书


微软官方Windows 10/8/8.1推荐防病毒软件


赛可达优秀产品奖SKD AWARDS


微软的WHQL徽标认证


中国反网络病毒联盟成员单位


SAVE引擎入围Virustotal检测平台

在您使用之前，来看看EDR交付的5000家客户中，最高频使用的八大功能

TOP 1 威胁检测与快速处置

客户大大

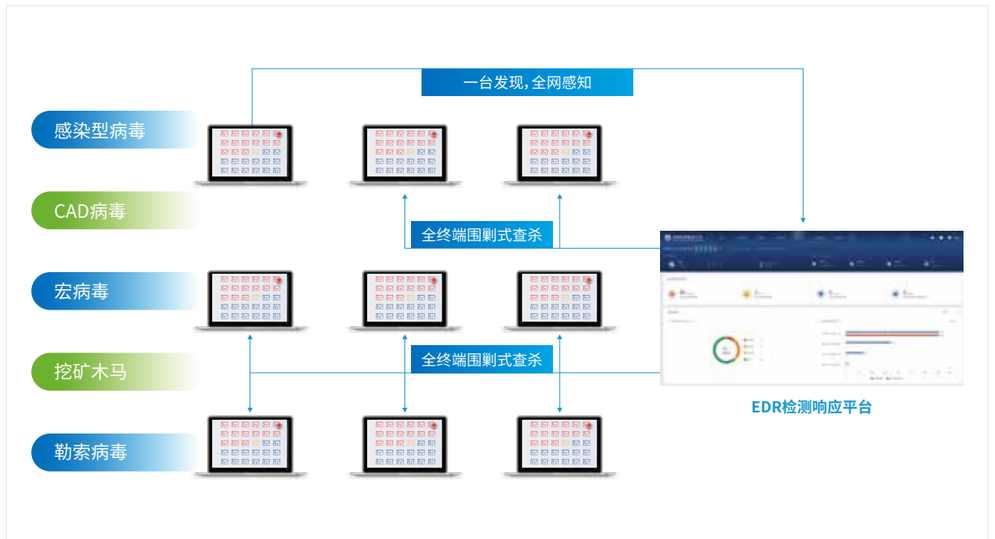
病毒千千万，担心我们内网系统会中毒，导致我们业务中断，能否快速有效的检测和修复病毒？

信服君

当然没问题，EDR 基于 AI 的漏斗型检测框架，统一配置下发病毒查杀策略，能够有效地针对恶性病毒（感染性病毒、CAD 病毒、宏病毒、勒索病毒等）进行快速处置修复，实现业务“零”干扰的安全防护！

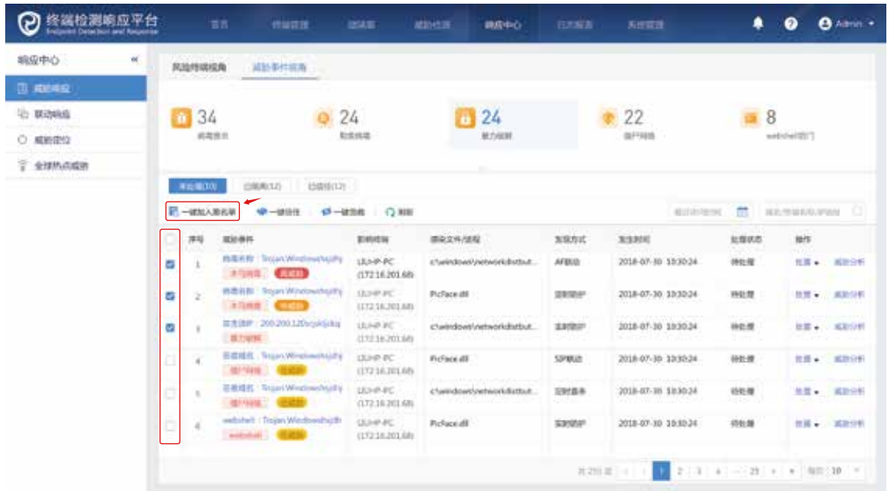
威胁检测

打开【终端管理】->【策略中心】->【病毒查杀】->【扫描配置】进行多引擎扫描策略配置，如下图。



一键威胁处置（含威胁分析百科）

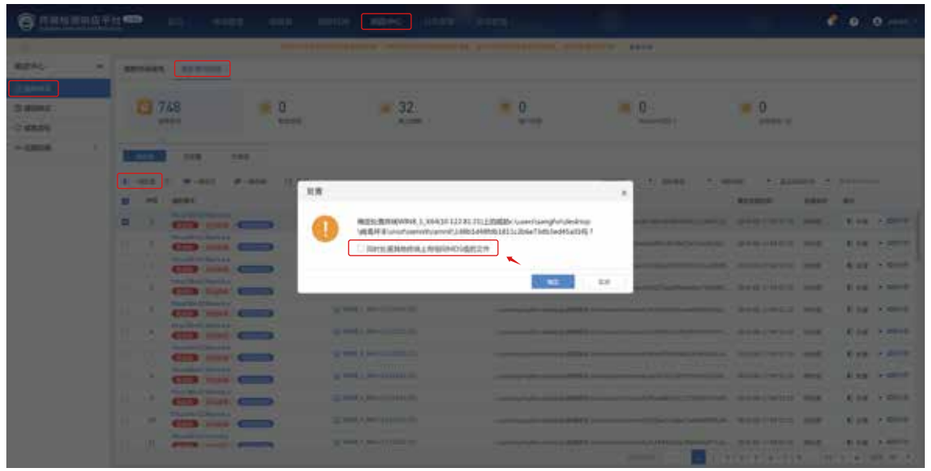
打开【响应中心】->【威胁响应】->【威胁事件视角】，批量选中威胁事件，点击【一键处置】，进行批量处置威胁，如下图。



点击具体威胁事件右侧的【威胁分析】，跳转至深信服威胁情报网站，对威胁文件进行详细分析。

围剿式查杀

打开【响应中心】->【威胁响应】->【威胁事件视角】，选中威胁事件，点击【一键处置】，弹出“一键处置”对话框，启用“同时处置其他终端上有相同MD5值的文件”，点击【确定】下发终端围剿式查杀，如下图。



TOP 2 资产便捷管理

客户大大

我们的终端设备信息资产摸不清、风险也看不见，怎么办？

EDR 多维度采集终端资产信息，友好的可视化界面，轻松实现终端资产的安全与运维！

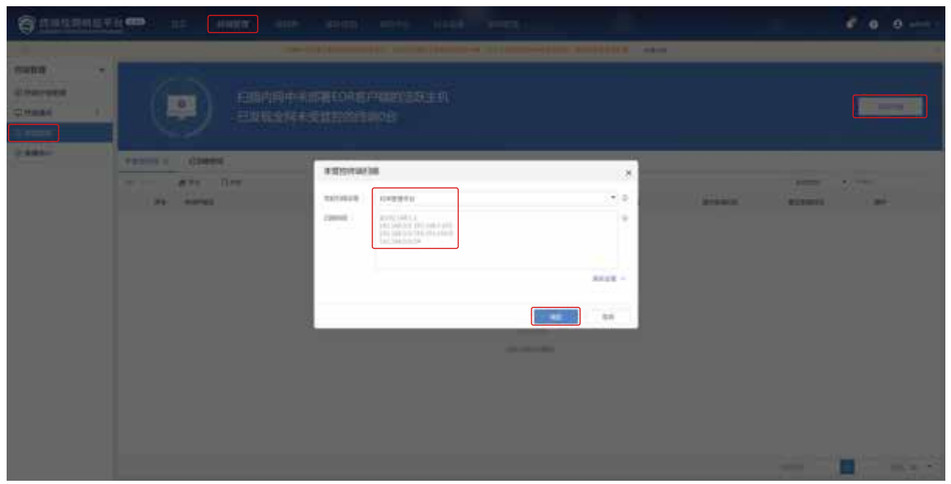
信服君

资产信息梳理

打开【终端管理】->【终端清点】->【操作系统】【应用软件】【监听端口】【终端账户】。

终端发现

打开【终端管理】->【终端发现】，点击【立即扫描】，弹出“未管控终端扫描”对话框，设置“发起扫描设备”为“EDR管理平台”，填写内网扫描网段，点击【确定】进行扫描。



TOP 3 漏洞快速修复

客户大大

管理员扫描出一大堆漏洞，需要打一大堆补丁，打完补丁还要重启服务，非常影响业务。要如何从这么多补丁中选择并快速修复漏洞，不影响我们正常业务呢？

EDR 帮助管理员摆脱复杂补丁选择，通过深信服团队对补丁精心筛选优化，并基于轻补丁漏洞免疫技术，实现轻、快、好、省的漏洞修复！

信服君

标签化补丁说明，让漏洞修补不再盲目

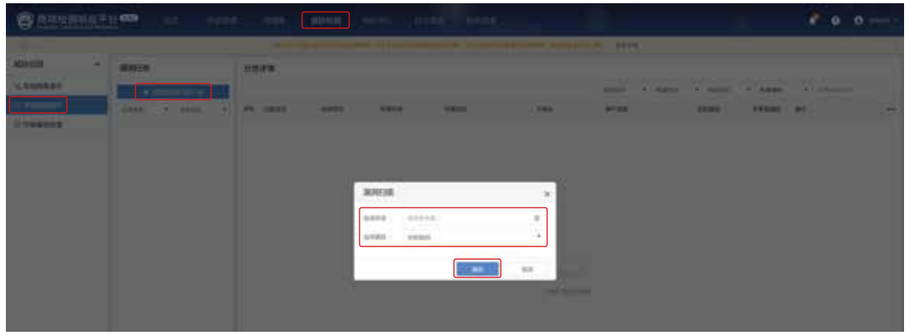
深信服精选补丁库，兼容稳定有保障

安全基石
终端兼容性安全实验室

打造EDR终端安全兼容性实验室，遵循着**【没有稳定兼容，一切安全都是空谈】**建设了基于**2000+**物理机、**8000+**虚拟机的兼容性环境。保障最优补丁筛选，适应复杂环境下发。

漏洞修复

打开【威胁检测】->【终端漏洞查补】，点击【添加漏洞扫描任务】，弹出“漏洞扫描”对话框，设置扫描的终端，点击【确定】下发漏洞扫描。



轻补丁漏洞免疫

【响应中心】->【轻补丁漏洞免疫】，客户端无需下载安装补丁、重启服务器，即可实现业务无感知的漏洞修复。

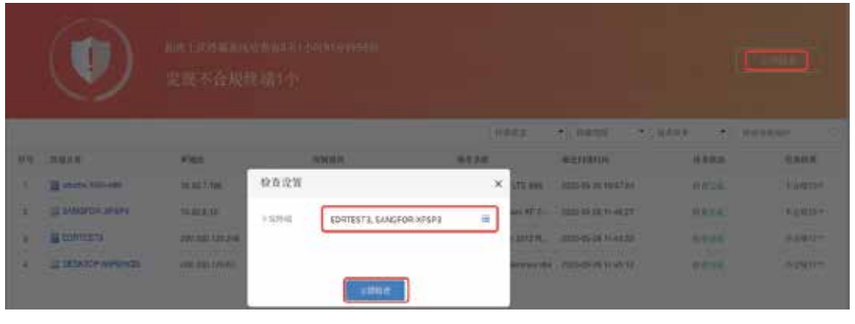
TOP 4 基线合规检查

客户大大：网络安全法颁布，要求越来越严，不知道我们内网的终端是否过了等保 2.0 的要求？

信服君：别担心，EDR 来给您做“合规体检”，对标等保 2.0，给终端进行主机安全基线的全面检查和改进建议。

终端基线核查

打开【威胁检测】->【终端基线检查】，点击【立即检查】，弹出“检查设置”对话框，设置需要进行基线检查的终端，点击【立即检查】下发基线检查操作，如下图。



TOP 5 AI进程自学习

客户大大

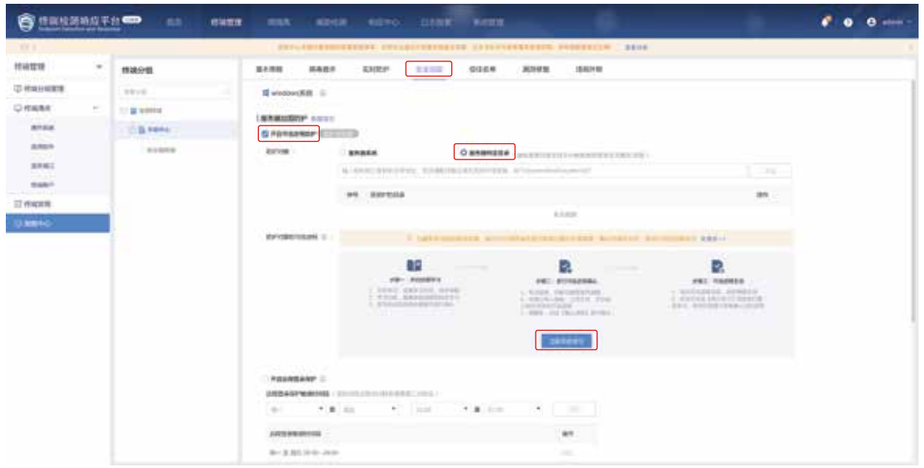
服务器常常起一些我们不常用的新进程，我们担心这些进程承载了一些病毒，存在安全隐患，能不能实现对这些可疑进程的阻拦？

EDR 通过 AI 进程自学习，轻松定义进程黑白名单，可疑操作通通拦截，降低业务受影响的风险。

信服君

进程自学习加固

打开【终端管理】->【策略中心】，设置服务器组的安全加固策略，选中“开启可信进程防护”，防护对象选择“服务器系统”，点击【立即开启学习】进行可信进程学习，学习结束，服务系统可信进程防护生效，如下图。



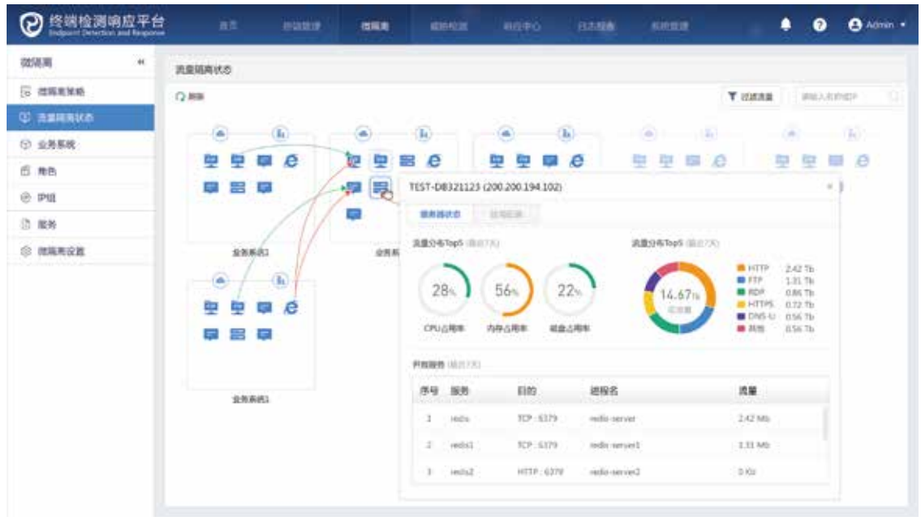
TOP 6 微隔离

客户大大

勒索病毒又通过 445 端口传播了，导致我们内网威胁泛滥。终端和终端间的访问关系到底是啥样?能不能批量控制威胁的传播?

信服君

EDR 微隔离细粒度管控东西向业务流，流量访问关系看得见，风险控得住。



终端流量可控

开【微隔离】->【微隔离策略】，新增拒绝访问服务器445端口策略，并开启右上角“策略生效开关”，如下图。

终端流量可视

打开【微隔离】->【流量状态】，开启流量上报开关，如下图。

TOP 7 勒索病毒攻击链立体防护

客户大大

我们已经装了杀毒软件了，为什么勒索病毒还是防不住？

EDR 基于勒索病毒供给链立体防护方案，全面阻止勒索勒索病毒。

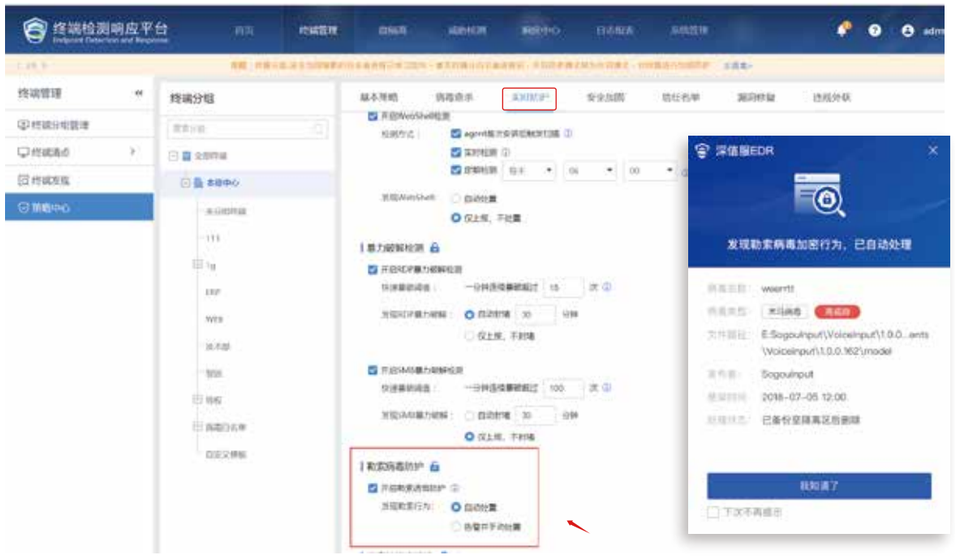
信服君

勒索诱饵

打开【首页】->【勒索病毒防御】即可看到全流程防护功能。

其中，勒索诱捕作为针对性功能可快速防御勒索病毒加密。

当检测到勒索病毒时，自动隔离勒索病毒，并弹框告警，如下图。



TOP 8 多维度风险报告自动导出

客户大大

能不能自动形成一个文档，可以从整体分析全网安全状况？

EDR 自动化导出多维度风险报告，快速了解业务与网络的安全风险

信服君

打开【日志报表】->【风险报告】，导出最近1个月的报表，如下图。

识别二维码

可查看EDR品牌白皮书、行业案例集等更多产品资料