**虚拟化服务器杀毒软件技术参数**

|  |
| --- |
| **★项目范围**提供虚拟化平台不少于240虚拟主机安全防护授权；支持各种Windows及Linux服务器；提供3年软件版本及特征库免费升级服务；★杀毒软件系统控制端，里面有大量的配置和策略，同一品牌可以统一管理，配置可以利旧。不用单独再次部署额外控制端，分配额外管理员进行日常维护管理，只需要简单继续安装扩容的授权即可。 |
| 一、病毒防护  无代理和轻代理两种模式，支持压缩文件扫描，包含多级嵌套压缩文件，能够做到压缩包内清毒；无需更新病毒数据库并将病毒扫描开销负载到安全虚拟机SVA完成，消除虚拟化环境病毒扫描风暴、更新风暴等问题；须支持VMware、Citrix、Microsoft Hyper-v、华为、H3C、深信服、红帽、KVM等多种虚拟化系统； |
| ★轻代理模式提供更完善的安全防护体系，支持邮件和网页反病毒，至少支持下列协议：POP3/SMTP/IMAP/MAPI/NNTP，提供产品功能截图； |
| ★轻代理提供主动防御技术，安全防护能力高于无代理模式，产品具备系统监控主动防御技术，当恶意行为对系统关键区域比如注册表进破坏或修改后，可回滚恶意软件在操作系统上执行的操作，如通过系统监控主动防御技术发现未知勒索病毒进行拦截的同时能够回滚还原被勒索病毒加密破坏的文件，提供产品技术功能截图； |
| 产品支持云安全网络，能够在第一时间抵御最新威胁和零日漏洞，并可在产品界面可查看相关安全信誉数据； |
| 二、攻击防护 无代理模式反网络攻击：能够与VMware NSX接口技术集成，提供IDS/IPS的反网络攻击防护功能，有效拦截针对系统和第三方应用程序的漏洞利用攻击； |
| ★轻代理模式具备反网络攻击虚拟补丁功能，检测和抵御危险的网络活动和网络攻击，支持漏洞入侵防护技术，即系统未修补补丁程序可实现补丁自动热修复无需再安装补丁，并自动将攻击源加入攻击列表，黑客入侵拦截功能，能对永恒之蓝、暴力破解、端口扫描等网络攻击流量具有防护功能；提供拦截永恒之蓝漏洞攻击的技术功能截图证明； |
| 三、合规控制及审计 ★支持访问保护多样化的权限锁定功能，支持对操作系统启动设置、系统文件关键设置、系统服务、进程访问、入侵进程（安装钩子、注入代码、重复句柄等）、使用浏览器命令行或浏览器接口等多种方式进行访问保护，提供产品针对代码注入、重复句柄等权限安全设定功能截图； |
| 支持移动存储介质控制，如控制U盘、移动硬盘、手机等设备接入终端，避免移动介质传播病毒的风险，支持外接设备认证功能，即特定的U盘可以使用其他则不可以，提供产品控制USB接口和配置信任移动设备功能截图； |
| 四、安全管理控制及安全日志报告★考虑要与现有终端反病毒兼容，可实现统一平台、统一管理和统一流程，一个管理控制中心能够管理包括物理平台（Windows、Linux等操作系统）、移动平台（Android、Apple iOS等操作系统）和虚拟化平台（VMware、Citrix、Hyper-V）在内的所有安全防护产品，并集中定制物理、移动和虚拟化平台的策略管理和报告输出，提供产品集中管理功能截图； |
| ★支持多种事件导出方式联动SOC、SIEM等大数据系统平台，支持RFC5424、Spluk（CEF格式）、Arcsight（CEF格式）及QRadar（LEEF格式）等，提供产品技术功能截图； |
| 丰富的报表功能，包括：保护状态、感染最严重的情况、客户端被网络攻击的情况、终端产品版本和病毒库版本等； |
| 五、病毒库、规则库和产品的升级与更新支持以SVA安全虚拟机为单位的方式进行升级，同时轻代理客户端也无须更新病毒库，消除反病毒风暴隐患，节约虚拟化性能开销； |
| ★具有减少网络负载功能，管理控制中心可针对IP子网或者IP段进行数据传输速度的控制，通过建立相关配置规则，可对最大传输速率和时间等参数进行定义，最佳优化虚拟化网络传输环境，提供技术功能截图； |
| 六、商务资质 |
| ★防病毒软件需提供公安部监制的销售许可证（应包含无代理和轻代理） |