**技术要求参数**

|  |
| --- |
| 杀毒软件病毒更新授权 |
| 序号 | 指标项 | 技术需求指标 |
| 1 | 数量要求 | 1. ★提供虚拟化平台安全防护90个宿主机安全防护续费授权。
 |
| 2 | 兼容性 | 1. 提供卡巴斯基3年软件版本及特征库免费升级服务；
2. 与VMware vShield完全集成，提供实时的无代理反恶意程序保护，无需在虚拟机操作系统上安装任何安全代理软件，通过专属安全虚拟机SVA与VMware接口技术集成联动进行病毒防护，和传统防病毒客户端模式的产品相比，专属安全虚拟机SVA的无代理防护模式能减少对系统硬件资源的利用率；
3. 基于vShield Endpoint和NSX环境的无代理防病毒功能，也可以同时提供不基于vShield Endpoint和NSX的轻代理防护模式，并支持更多虚拟化系统，支持包含VMware、Citrix、Hyper-v、华为、红帽、KVM等虚拟化平台轻量代理模式，即客户端代理程序远小于传统代理程序，通过轻代理和安全虚拟机SVA联动进行安全防护，轻代理客户端本地不进行病毒扫描操作也无需更新病毒库，轻代理模式消除虚拟化环境中反病毒带来的扫描风暴、病毒库更新风暴等问题，并可实现两种模式虚拟化防病毒系统的集中管理；
4. 无代理模式反病毒程序部署过程中不能对主机或虚拟机进行重启，以保障虚拟化平台业务的连续性；
 |
| 3 | 病毒防护 | 1. 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；
2. ★轻代理模式下支持邮件和网页反病毒，支持下列协议：POP3/SMTP/IMAP/MAPI/NNTP（**要求提供功能截图，并加盖原厂商公章）；**
3. ★轻代理模式可提供主动防御技术，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（**提供产品功能截图；并加盖原厂商公章**）；
4. ★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数据（要求提供功能截图，并加盖原厂商公章）；
 |
| 4 | 攻击防护 | 1. 无代理模式反网络攻击：够与VMware NSX接口技术集成，在虚拟分布交换机模式下提供IDS/IPS的反网络攻击防护功能；
2. 支持网络数据包规则的防火墙功能，通过建立防火墙策略规则对特定端口选定数据协议发送和接收网络流量；支持根据应用程序建立网络访问规则，对特定应用程序的网络活动评估和限制，阻止不合法的应用程序网络连接；
3. ★具备主机IPS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；（**要求提供功能截图，并加盖原厂商公章）；**
 |
| 5 | 工作站台合规性控制 | 1. ★轻代理模式支持对应用程序进分类操作，为终端用户定制应用程序权限规则，包含应用程序系统权限规则和网络策略，权限控制至少包含启动、系统服务、进程控制、入侵中安装钩子、注入代码、低级别磁盘防护等权限控制功能（要求提供功能截图，并加盖原厂商公章）；

控制客户端禁止读取U盘/写入U盘，能控制客户端禁止读取CDROM/写入CDROM等，能控制客户端禁止除USB键盘、USB鼠标外的其它USB设备的使用（更精细化的外设控制），能对以下控制（USB、网络、CDROM、接口等）进行计划管理（定时开放、禁用）； |
| 6 | 安全管理控制及安全日志报告 | 1. ★考虑未来的安全产品扩容，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）在内的所有终端防护产品，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（**要求提供功能截图，并加盖原厂商公章）；**
2. ★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，并支持多种事件导出方式联动SOC系统、SIEM系统或其他威胁感知系统，支持RFC5424、Spluk（CEF格式）、Arcsight（CEF格式）及QRadar（LEEF格式）等（**要求提供功能截图，并加盖原厂商公章）；**
 |
| 7 | 病毒库、规则库和产品的升级与更新 | 1. 支持以SVA安全虚拟机为单位的方式进行升级，虚拟机客户端不需单独升级；
2. 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；
3. ★反病毒数据库条目数≥1200万（要求提供功能截图，并加盖原厂商公章）；
 |
| 8 | 服务要求 | 1. ★用户可以通过视频、语音、文字提交问题，服务工程师提供工单响应支持, 回答提问和协助解决发现到的安全风险事件，**提供服务平台系统功能截图**；服务平台预警服务，用户可以通过服务平台系统实时看到防病毒系统的威胁数据展示，增加威胁可见性，**提供服务平台系统功能截图**
 |
| 9 | 商务资质 | 1. ★产品具有质量保证体系ISO9001认证资质；
2. ★提供公安部计算机病毒防治产品检验中心检验报告；
3. ★提供公安部计算机信息系统安全专用产品的销售许可证。
 |