**网络防病毒系统（标准版）招标参数**

|  |
| --- |
| **功能描述** |
| ★产品支持各类Windows 32/64位操作系统(Windows 7、Windows 8、Windows 10、Windows 11、Windows Server 2008、Windows Server 2012、Windows Server 2016、Windows Server 2019等），支持各类32/64 Linux系统（Red hat、SUSE、Cent OS等）。 |
| ★支持文件、邮件和网页的反病毒功能模块，必须支持Linux系统实时防病毒功能，即有恶意代码传入系统立即拦截，提供支持Linux系统实时防病毒功能技术截图证明。 |
| ★支持远程擦除客户端指定文件夹下的文件，支持客户端满足脱管超过时限等条件时自动擦除，确保设备遗失等场景下的数据安全 |
| ★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，可回滚病毒在操作系统上执行的恶意操作，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立即还原被勒索病毒加密破坏的文件，提供产品具备回滚还原技术功能截图。 |
| 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，支持加密压缩文件扫描。 |
| 产品具备云安全网络技术，云辅助技术可提高对未知病毒的响应速度并减少误报，同时有效抵御最新零日漏洞攻击。 |
| ★支持使用受信任的系统证书，通过证书提高系统安全性，支持个人及企业信任证书、受信任根证书颁发机构、智能卡受信任的根、受信任的设备、第三方根证书颁发机构等多种选择，提供产品支持使用证书系统的技术功能截图。 |
| 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。 |
| ★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技术功能截图。 |
| 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。 |
| ★支持收集有关安装在客户端计算机上的应用程序相关信息，可提供客户端软硬件信息清单。 |
| ★实现统一平台、统一管理和统一流程，管控中心能够管理包括物理（Windows、Linux、Mac OS等操作系统）、移动（Android、IOS等操作系统）和虚拟化（VMware、Citrix、Hyper-V）在内的所有安全产品，并集中定制物理、移动和虚拟化的策略配置和报告输出，提供集中管理技术功能截图。 |
| ★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，提供技术功能截图。 |
| 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。 |
| ★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、Splunk（CEF格式）、Arcsight（CEF格式）及QRadar（LEEF格式），提供产品技术功能截图。 |
| ★提供XXX个防病毒系统授权和3年软件版本及特征库免费升级服务。 |
|  |