计算机终端安全管理系统市场调研询价技术要求

1.网络安全准入系统

|  |  |
| --- | --- |
| **功能需求** | **技术参数要求** |
| 基本要求 | 网络安全准入系统软件和硬件设备，提供三年质保服务。 |
| 授权要求 | 提供不少于1000点准入授权。 |
| 入网控制 | 产品支持多种认证控制方式，支持802.1x、portal、DHCP、MAB MAC、WebAuth等认证方式，支持无线和有线环境下的准入控制。 |
| 支持健康合规检查策略，采用动态检测技术，需支持多种检查机制，至少支持入网检查、定时检查、周期检查机制，针对接入内部网络的计算机终端实行多种安全检查策略，支持分组策略下发控制，拦截不安全终端接入网络。 |
| 支持多种逃生机制，包括一键认证放行、第三方服务器异常自动放行等，确保非正常情况下不影响用户网络的稳定运行；  |
| 支持进程检查、域检查、文件检查、补丁检查、U盘运行检查、注册表检查、软件检查、操作系统检查、非法外联检查、防火墙检查等安全基线检查。 |
| 系统管理 | 为保证运维方便，要求网络安全准入系统与终端安全管理系统在同一个控制中心进行管理维护。 |

2.虚拟化安全管理系统

|  |  |
| --- | --- |
| **功能需求** | **技术参数要求** |
| 基本要求 | 虚拟化安全管理系统，提供三年质保服务。 |
| 授权要求 | 提供不少于70点服务器客户端服务授权 |
| 客户端要求 | 采用轻量级Agent部署，无需依赖虚拟化平台API即可实现安全防护；客户端支持Windows类、Linux类、物理服务器、虚拟服务器。 |
| 病毒查杀要求 | 产品支持普通病毒木马查杀，宏病毒、勒索病毒、注册表病毒、间谍软件、僵尸远程软件等特定恶意文件的查杀；对网络映射驱动器、移动存储路径、共享目录、局域网路径等扩展路径也能够进行扫描查杀。 |
| 针对压缩文件处理，支持压缩文件数量、压缩层级、压缩包大小进行精确扫描，系统除文件、文件夹例外，还需支持单独的病毒黑白名单的管理运维。 |
| 提供防护策略控制可避免启动风暴和查杀风暴。 |
| 提供勒索病毒防御功能，支持针对已知勒索病毒家族及其变种免疫防御。 |

3.终端安全管理系统

|  |  |
| --- | --- |
| **功能需求** | **技术参数要求** |
| 基本要求 | 终端安全管理系统，提供三年质保服务。 |
| 客户端要求 | 客户端软件要求支持Windows XP/Windows 7/Windows 8/Windows 10/Windows 11，Windows Server 2003/2008/2012/2016/2019，支持32位/64位操作系统。 |
| 授权要求 | 配置不少于1000点PC端授权、不少于30点Windows Server授权、不少于20点Linux Server授权。 |
| 病毒查杀 | 支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、局域网文件防护、网页安全防护、勒索软件防护。 |
| 支持勒索病毒免疫防护，同时支持诱饵文件防护、预防勒索病毒变种 |
| 支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。 |
| 补丁分发 | 支持对Windows操作系统、IE、.NET Framework、Office、硬件驱动等软件进行补丁修复。 |
| 支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。 |
| 运维管控 | 支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口）设置使用权限。 |
| 支持终端禁止修改IP、MAC，禁止创建WiFi，禁止使用无线网卡 |
| 支持对长时间运行、定时关机、空闲节能等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、睡眠处理。 |
| 支持对终端进行远程桌面协助，支持文件分发和自动运行。 |
| 主机防火墙 | 具备支持主机防火墙功能，包括基于数据包流向、协议、端口和IP的访问控制。 |
| XP加固 | 支持针对Windows XP系统可带来安全隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护。 |
| 移动存储管理 | 支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、取消注册、导出注册列表等； |
| 支持多级环境下U盘漫游功能；支持移动存储介质外出管理，并可以设置外出使用权限与有效时间； |