附件

软件采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 软件大类 | 软件名称 | 购买年限 | 数量 | 备注 |
| 终端安全管理系统 | 终端安全控制中心 | 软件为永久授权，含3年升级维护费，3年后每年维保费以磋商确定 | 1套 |  |
| 终端安全管理客户端授权 | 1000套 |
| 终端安全产品安装服务 | / |
| 服务器安全管理系统 | 服务器安全管理系统管理控制中心 | 1套 |
| 服务器安全管理系统客户端功能授权 | 200套 |
| 服务器安全产品安装服务 | / |

软件技术要求

|  |  |  |
| --- | --- | --- |
| **序号** | **设备名称** | **技术参数** |
| 1 | **终端安全管理系统** | 1.终端安全控制中心可实现终端安全客户端的集中管理，包括终端统一部署、策略配置、任务分发、集中监控、日志报表等终端安全管理功能，支持Windows Server 2008 R2/2012/2012 R2/2016的64位版本（简体中文版）；  2.支持CentOS 7、Redhat 7等Linux系统；提供终端安全管理客户端授权≥1000点，包含三年升级服务。  3.客户端支持Windows XP\_SP3及以上/Windows 操作系统安全防护，并通过控制中心对全网终端进行健康状况监测、统一杀毒、统一漏洞修复、统一管控、弹窗管理、硬件资产管理以及各种报表和查询等功能；  4.支持对单个客户端进行维护，终端视角查看终端基本信息，包括计算机名、型号、IP、MAC地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态；所功能应用策略情况；硬件信息展示，包括CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息；实时进程信息展示，包括进程名称、PID、进程用户名、命令行、占用内存、CPU占用、MD5等信息；  5.★为了满足多语言使用需求，产品全功能支持简体中文/繁体中体/英语自由切换。（提供产品截图证明并加盖厂商公章）  6.支持定时公告功能，可配置开机显示、周期显示和立即推送。  7.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、IM防护、局域网文件防护、网页安全防护、勒索软件防护。支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁。  8.★补丁修复支持预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据网络环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。（提供产品截图证明并加盖厂商公章）  9.★支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。（提供产品截图证明并加盖厂商公章）  10.支持对网卡进行防护，支持阻止终端修改IP地址、使用动态IP地址、热点创建和IPV6地址使用等，可自定义提示内容和生效时间。支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理。  11.支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。  12.★支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机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、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间；（提供产品截图证明并加盖厂商公章）  13.支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。（提供产品截图证明并加盖厂商公章）  14.支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。  15.★产品具备该软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书。提供公安部颁发的《计算机信息系统安全专用产品销售许可证》和检测报告。提供连续通过国际权威杀毒软件评测机构Virus Bulleti测评认证（VB100）三次以上认证证明文件。 |
| 2 | **服务器安全管理系统** | 1. 服务器安全管理系统管理控制中心，可实现对客户端的统一运维管理、安全策略维护及全网安全日志分析、威胁溯源;提供服务器安全管理系统客户端功能授权≥200点，提供完整的系统加固和防护能力，包括资产梳理、风险发现、病毒扫描、安全基线、入侵检测、系统加固、应用防护、EDR、溯源分析等高级功能，包含三年升级使用授权。  为了满足多操作系统安全需求，产品需具备良好的系统兼容性，需支持Windows、Linux和国产化操作系统部署：  2. 客户端需支持自我防护技术，即使客户端被意外关闭，防护依然有效；  3. 支持对服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产管理，并提供搜索及导出功能；  4. 支持对服务行为进行状态学习，可添加命令执行、文件创建、网络连接三种服务行为例外的白名单，针对学习行为之外的行为进行告警，支持对行为进行信任、例外操作（提供产品截图证明并加盖厂商公章）  5. 采用主动的方式进行自动化病毒查杀，可支持多引擎技术识别并查杀最新病毒；可支持病毒文件自动隔离、自动删除、不处理三种方式。并可将病毒查杀的结果导出报告；  6. 支持自动学习并梳理出内网端口访问情况，并提供端口处置（提供产品截图证明并加盖厂商公章）  7. 可对服务器的软件漏洞进行综合扫描，并可对扫描方式、扫描周期进行设置，并以报告的形式展示软件漏洞扫描结果；  8. 支持CIS、等级保护二级、三级检查，满足等保二级及等保三级要求，同时支持自定义基线检查任务。  9. ★支持系统内核加固，对非法创建文件、非法更改系统设置、非法创建可执行文件、非法提权等恶意行为进行监控和防护。（提供产品截图证明并加盖厂商公章）  10.★支持驱动级防篡改，可以保护整个目录、网页或文件不被恶意修改或者变更，支持监控和控制文件读取、写入、删除、链接、创建、执行、重命名等操作，支持对目录、进程进行例外设置。（提供产品截图证明并加盖厂商公章）  11. ★支持RASP（Runtime Application Self Protection）运行时应用自我保护技术，可对ASP、.Net、PHP、Java四种语言进行RASP防护，支持通过对应用系统流量、上下文、行为进行持续监控，有效抵御一句话木马、变形/未活动/加密Webshell、SQL注入、命令执行、文件上传、任意文件读写、反序列化、Struts2漏洞等各类高级Web应用攻击（提供产品截图证明并加盖厂商公章）  12. 支持统计并展示服务器的可疑威胁及告警信息，包括：可疑威胁事件统计、可疑威胁分布、可疑问些趋势，以及具体的威胁事件列表，并可对威胁事件进行研判。  13. 支持记录当前所有服务器产生的事件日志，并提供筛选的功能和自定义时间段筛选查询，用户可通过安全日志快速锁定问题服务器，并进行相应处理。同时支持对安全事件进行溯源分析，对安全事件的等级、攻击类型、ATT&CK ID、ATT攻击阶段进行匹配。（提供产品截图证明并加盖厂商公章）  14. ★支持对应用漏洞防护的设置，可有效拦截各类WEB入侵，包括：SQL注入类、XSS防护、Web服务器溢出攻击防护、文件名解析漏洞防护、禁止浏览畸形文件、自动屏蔽扫描器、X-Forwarded-For防护、请求类型控制、禁止下载特定类型文件、网站浏览实时防护、HTTP请求头防护等。同时可对一句话木马利用工具进行防护，包括：ASP、PHP、ASPX等语言，并可禁止使用PHP://inpu、禁止使用PHP://fillter，以及SVN信息保护设置（提供产品截图证明并加盖厂商公章）  15. ★产品具备计算机信息系统安全专用产品销售许可证（主机文件监测(基本级)）；具备攻击代码检测机制的权威机构证明文件；产品拥有自主知识产权，非OEM产品，具备中华人民共和国国家版权局计算机软件著作权登记证书。 |
| 3 | **售后服务** | 1. 集中进行涉及平台使用的各项培训，以及提供使用手册； 2. 发生故障时第一时间响应及时排查故障，提供7x24小时电话响应，及时远程支持，4小时内抵达现场处置。 3. 提供7x24小时技术支持，解决系统使用过程中的技术性、功能使用性问题的咨询指导服务。 4. 发生网络安全事件时，保证4小时内到现场协助处置。 5. 提供一个月一次现场终端安全巡检服务。 |