附件2：企业版杀毒软件技术参数

## 1、采购产品和服务一览表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **型号** | **数量** | **单位** | **服务期限** |
| 1 | 系统管理控制中心 | B/S架构管理 | 1 | 套 | 三年服务 |
| 2 | Windows终端防病毒授权 | 防病毒功能+补丁功能+运维管控功能 | 1200 | 个 | 三年服务 |
| 3 | Windows服务器防病毒授权 | 防病毒功能+补丁功能 | 130 | 个 | 三年服务 |
| 4 | Linux服务器防病毒授权 | 防病毒功能 | 20 | 个 | 三年服务 |
| 备注：需国产品牌杀毒软件。 |

## 2、产品清单及指标要求

### 1）系统管理控制中心（B/S架构管理）

|  |  |  |
| --- | --- | --- |
| **序号** | **指标** | **指标要求** |
| 1 | 终端操作系统 | 操作系统至少支持Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10 /windows 11。产品全功能支持简体中文/繁体中体/英语自由切换。 |
| 2 | 系统管理 | 控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、硬件资产管理以及各种报表和查询等功能； |
| 3 | 客户端提供控制中心管理所需的相关数据信息，通讯可选择非明文方式；客户端执行最终的木马病毒查杀、漏洞修复等安全操作； |
| 4 | 管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性。(提供功能截图) |
| 5 | 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。(提供功能截图) |
| 6 | 产品支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；要求客户端程序具备自保功能，避免被恶意篡改 |
| 7 | 支持自动分组，按IP地址、CPU数量、MEM容量、主机名、计算机工作组等参数进行自动动态调整分组。(提供功能截图) |
| 8 | 要求支持服务器端病毒库的定时更新和手动更新两种升级模式。 |
| 9 | 支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率 |

### 2）Windows终端防病毒（提供1200个Windows客户端授权）

|  |  |  |
| --- | --- | --- |
| **序号** | **指标** | **指标要求** |
| 1 | 病毒、恶意代码、木马防护 | 支持病毒木马威胁的快速扫描、全盘扫描、强力扫描、文件专杀、隔离区恢复、系统修复、插件管理 |
| 2 | 最后一次全盘扫描时间，记录终端最后一次完成全盘扫描的时间(提供功能截图) |
| 3 | 立体防护系统，包含浏览器防护，系统防护，入口防护和隔离防护4大类。其中浏览器防护可对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置 |
| 4 | 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。(提供功能截图) |
| 5 | 支持仅利用多个非工作时间时间段完成一次全盘扫描(提供功能截图) |
| 6 | 要求产品具备公有云检测能力，并且公有云特征储备超过140亿 |
| 7 | 为阻止入侵者关闭或者破坏客户端防护、以及放行勒索病毒，将阻止客户端退出和卸载，终端无法添加信任和开发者信任，客户端无法关闭自我保护，禁止应用程序加载驱动（提供证明截图） |
| 8 | 补丁分发与漏洞修复 | 要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、功能性补丁等修复类型； |
| 9 | 支持补丁下载安装顺序设置，可以有效节省漏洞修复时间与减少CPU占用； |
| 10 | 要求产品具有简化补丁运维工作，支持补丁灰度发布，支持设置对特定分组优先进行补丁分发，自定义测试一段时间后再全网升级，实现补丁自动化运维 |
| 11 | 终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁 |
| 12 | 支持影响到编辑Office文档时提醒，可取消此次修复任务。（提供产品界面截图） |
| 13 | 支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞CVE编号、漏洞CNNVD编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。 |
| 14 | 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。（提供产品界面截图） |
| 15 | 运维管控功能 | 支持终端在内网环境下的远程控制；（提供产品界面截图） |
| 16 | 支持远程操作时锁定屏幕、截取屏幕，远程锁定屏幕后需要输入解锁密码才可再次使用； |
| 17 | 支持对单点维护功能，可远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行（执行路径+执行参数）、内存占用、支持远程结束进程。支持远程查看计算机各个网卡配置信息。 |
| 18 | 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。(提供功能截图) |
| 19 | 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。(提供功能截图) |
| 20 | 支持冗余有线网卡、无线网卡、3G网卡、MODEM、ADSL、ISDN等设备的外联控制；违规外联发生时可针对内外网连接状态分别设置违规处理措施 |
| 21 | 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。（提供产品界面截图） |
| 22 | 支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID和设备来源。（提供产品界面截图） |
| 23 | 资质 | 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》内网主机监测（一级）资质证书复印件并加盖厂商公章 |
| 24 | 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》资质证书复印件并加盖厂商公章 |
| 25 | 近四年IDC终端安全市场排名前三。（提供相关证明材料） |
| 26 | 生产厂商应具备国家信息安全服务资质安全运营类一级（提供有效证书的复印件，并加盖设备原厂商公章） |
| 27 | 提供原厂授权函及售后服务承诺函原件。 |

### 3）Windows服务器防病毒（提供130个Windows服务器授权）

|  |  |  |
| --- | --- | --- |
| **序号** | **指标** | **指标要求** |
| 1 | 服务器病毒防护 | 支持病毒木马威胁的快速扫描、全盘扫描、强力扫描、文件专杀、隔离区恢复、系统修复、插件管理 |
| 2 | 支持仅利用多个非工作时间时间段完成一次全盘扫描(提供功能截图) |
| 3 | 文件系统实时防护，提供实时防护拦截病毒的完整分析（包含实时防护概况趋势、处理结果分布、病毒类型TOP10、检出终端TOP10、病毒名称TOP10、病毒文件TOP10、病毒路径TOP10、勒索程序TOP10、挖矿木马TOP10、WebShell木马TOP10） |
| 4 | 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。（提供产品界面截图） |
| 5 | 支持对终端当扫描到感染型病毒、顽固木马时，扫描时不允许终端用户暂停或停止扫描任务。（提供产品界面截图） |
| 6 | 补丁分发与漏洞修复 | 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。（提供产品界面截图） |
| 7 | 支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复。(提供功能截图) |
| 8 | 支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞CVE编号、漏洞CNNVD编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。 |
| 9 | 支持管理员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，根据企业环境，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。 |
| 10 | 资质 | 提供销售许可证复印件并加盖厂商公章 |
| 11 | 提供软件著作权复印件并加盖厂商公章 |
| 12 | 近四年IDC终端安全市场排名前三。（提供相关证明材料） |
| 13 | 生产厂商应具备国家信息安全服务资质安全运营类一级（提供有效证书的复印件，并加盖设备原厂商公章） |
| 14 | 提供原厂授权函及售后服务承诺函原件。 |

## 4）Linux服务器防病毒（提供20个Linux服务器授权）

|  |  |  |
| --- | --- | --- |
| **序号** | **指标** | **指标要求** |
| 1 | 服务器病毒防护 | 病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本 |
| 2 | 最后一次全盘扫描时间，记录终端最后一次完成全盘扫描的时间(提供功能截图) |
| 3 | 查杀未处理，一键处理指定终端上存在的被用户忽略的病毒，且不需要再次扫描。（提供功能截图） |
| 4 | 病毒防护日志包含：病毒查杀日志、查杀任务日志、系统防护日志、按分组、按终端、按时间。（提供功能截图） |
| 5 | 病毒防护日志包含：病毒查杀日志、查杀任务日志、系统防护日志、按分组、按终端、按时间。（提供功能截图） |
| 6 | 实时防护分析：提供实时防护拦截病毒的完整分析（包含实时防护概况趋势、处理结果分布、病毒类型TOP10、检出终端TOP10、病毒名称TOP10、病毒文件TOP10、病毒路径TOP10、勒索程序TOP10、挖矿木马TOP10、WebShell木马TOP10）（提供功能截图） |
| 7 | 支持手动导入、导出黑白名单，添加黑白名单。支持通过文件导入添加黑白名单。 |
| 8 | 病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。（提供功能截图） |
| 9 | 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。（提供功能截图） |
| 10 | 支持不少于两个杀毒引擎混合使用，提高病毒检出率。（提供功能截图） |
| 11 | 资质 | 提供销售许可证复印件并加盖厂商公章 |
| 12 | 提供软件著作权复印件并加盖厂商公章 |
| 13 | 近四年IDC终端安全市场排名前三。（提供相关证明材料） |
| 14 | 生产厂商应具备国家信息安全服务资质安全运营类一级（提供有效证书的复印件，并加盖设备原厂商公章） |
| 15 | 提供原厂授权函及售后服务承诺函原件。 |

## 3、实施周期

合同签订后，1个月内实施完成。

## 4、服务

1. 提供服务期间内的免费上门服务，包括终端及服务器的首次上门安装调试。
2. 由经验丰富的专业技术工程师保障 7×24 小时的电话支持、邮件支持、远程服务等，对系统发生故障的维修、技术支援响应时间不应超过1小时，需提供现场服务的不超过24小时。
3. 定期巡检、甲方回访和给予技术指导，采用远程或电话支持巡检相结合的方式进行，每年至少提供四次上门巡检服务，并出具巡检报告。