①指标按重要性分为“★”、“#”。★代表实质性指标，不满足该指标项将导致投标被拒绝，#代表重要指标。

②“证明材料要求”项可填“是”和“否”。填“是”的，投标人/响应人须提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或第三方机构检验报告或其他相关证明材料，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。

③除技术、服务、实施方案需求中明确要求投标人承诺的事项外，其他要求提供证明材料的指标中，提供投标人承诺作为应答的不予认定。

### 杀毒软件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** | **证明材料要求** |
| **1** | ★ |  | 包含一套控制中心管理软件，500点终端，一年病毒库升级维保服务 | 否 |
| 2 |  |  | 控制中心支持根据客户端点数的增加支持横向扩展，操作系统支持Windows Server 2008 R2/2012/2012 R2/2016的64位版本（简体中文版）；支持CentOS 7、Redhat 7等Linux系统。 | 否 |
| 3 | # | 支持单个页面展示终端部署统计、终端安全趋势、终端状态（文件防护开启率、未安装补丁终端率、终端病毒更新率和终端版本更新率）、终端程序版本、终端在线统计、病毒库版本分布、安全更新和重要补丁安全趋势等信息，均可通过图形化展示。 | 是 |
| 3 | # | 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。 | 是 |
| 4 |  | 客户端要求 | 支持操作系统Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10；Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019SUSE Linux/Red Hat Linux/CentOS/Ubuntu。 | 否 |
| 5 | # | 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，终端防退出密码和终端防卸载密码支持哈希算法和国密算法。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。 | 是 |
| 6 | # | 产品全功能支持简体中文/繁体中体/英语自由切换 | 是 |
| 7 | # | 软件管理 | 支持内置软件库，需包含1000款以上应用软件，类别包括：下载工具、主题壁纸、办公软件、压缩刻录、图形图像、安全杀毒、教育学习、浏览器、系统工具、编程开发、网络应用、网银、聊天工具、视频软件、输入法、远程工具、阅读翻译、音乐软件等，以保证软件安装包无捆绑和病毒。 | 是 |
| 8 | # | 管制中心支持上传本地软件，支持本地软件应用平台，为终端用户提供本地软件下载。支持软件的上传、更新、上架、下架、回退、删除管理精细操作，包含软件名称、软件描述、软件状态、软件版本、软件大小、上传日期、更新时间、上架状态、分类等信息。 | 是 |
| 9 |  | 支持统一配置终端下载软件存储位置、软件安装包保留时间、更新提醒间隔等设置。支持定制分类名称，关闭云中心。 | 否 |
| 10 | # | 支持多个管理员同时对一台终端分发软件，终端可以并发安装。 | 是 |
| 11 |  | 病毒防护 | 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。 | 否 |
| 12 | # | 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。 | 是 |
| 13 |  | 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。 | 是 |
| 14 |  | 补丁管理 | 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。 | 否 |
| 15 | # | 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、发布状态、文件数量、发现补丁次数、已安装补丁次数、忽略补丁次数、卸载补丁次数、未更新补丁库。并支持导出统计报表。 | 是 |
| 16 | # | 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。 | 是 |
| 17 |  | 主机防火墙 | 支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标IP，支持输入IP范围。 | 否 |
| 18 | # | 终端管控 | 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。 | 是 |
| 19 |  | 支持统计终端的出口地址列表，搜集终端连接的无线信号信息统一展示，标识出ssid可连通互联网，可连通服务器的情况，汇总展示内网终端上报的进程信息，支持设置进程匹配规则，其它业务可直接调用创建好的进程规则或者进程分组。 | 是 |
| 20 | # | 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。 | 是 |
| 21 |  | EDR功能 | 支持IOC、IOA规则库，匹配规则后后进行告警，包含风险等级、告警类型、告警详情、技术点、战术点、发现时间、计算机名、终端本地IP、MAC地址、分组、状态等信息。 | 否 |
| 22 |  | 支持对恶意文件进行处置，保证文件不能再次运行和执行，处置动作包括终止进程、终止进程并隔离、终止进程并删除、恢复隔离进程文件。 | 否 |
| 23 | # | 支持对指定终端当下的状态进行深入调查，包括终端登录日志、启动项、计划任务、正在运行的服务等，以及最近一段时间内终端的行为数据信息。 | 是 |
| 24 | # | 支持对全网终端进行威胁事件风险性评估，并支持一键响应处置能力。 | 是 |
| 25 |  | 支持跟威胁感知系统类设备进行处置联动，联动接口处置接口包含：终端隔离、取消隔离、全盘扫描。 | 否 |
| 26 |  | 产品资质 | 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》。 | 是 |
| 27 |  | 具备信息技术产品安全测试证书。 | 是 |
| 28 | # | 连续通过国际权威杀毒软件评测机构Virus Bulleti测评认证（VB100）七次以上认证。 | 是 |
| 29 | # | 近三年IDC终端安全市场排名前三。 | 是 |
| 30 | # | 入围中央国家机关2021年“终端安全软件”名录。 | 是 |