按照采购单位提供的技术要求拟制。关键性技术指标参数前标记“★”符号，一般性指标参数前不作标记。

带“★”和“▲”条款需提供技术支持材料【①技术要求中明确的技术支持材料以具体项目为准；②未明确的技术支持材料可以从（不限于）以下支持材料选择：产品规格表、产品宣传彩页、技术白皮书、制造商官方网站发布的产品信息、说明书等或检测机构出具的检测报告等技术材料支持的（定制产品除外）；③定制产品的技术支持材料可提供响应承诺。】

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **需求名称** | **参数 性质** | **需求具体内容** | **备注（证明材料等其他要求）** |
|
| **技术要求** | | | | |
| 1 | 基本要求 | ★ | 为我中心PC端和服务器端安装一套可实现对客户端集中管理，具有统一部署、策略配置、任务分发、集中监控、日志报表、终端管控、补丁管理、移动存储管理、病毒防控等功能的终端防护软件 具体需求： （1）控制中心系统软件1套； （2）Windows PC端授权点位 3000个； （3）server授权点位（Windows、Linux）400个； （4）银河麒麟V10终端授权点位 200个。 | 企业承诺 |
| 2 | 控制中心系统软件 | ★ | 支持主流 Windows Server 及 Linux 操作系统，Windows版支持单机模式部署，Linux 版支持集群模式部署，中英双语界面；可实现对客户端的集中管理，包括静默安装（支持软件（文件）分发带参数运行）、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。 | 企业承诺或产品截图 |
| 3 | NAC准入 | ★ | 支持现有NAC准入设备配套升级，或提供与投标系统配套的NAC准入设备。 | 企业承诺或产品截图 |
| 4 | Windows PC端 |  | 3000个点位授权，病毒防护、补丁管理、防火墙、文件分发、软件统计、威胁处置、安检合规、准入认证客户端、文件审计、网络管控、进程管理、能耗管理、违规外联、外设管理、移动存储、服务管理、远程协助、桌面加固、行为审计、外发管控、高级威胁防御、垃圾清理、启动项管理、高级违规外联等功能。 |  |
| 4.1 | 终端管控 功能 |  | 支持终端维护、外设管理、进程管理、违规外联、能耗管理、网络管控、远程协助、软件管理、停服系统加固等； 支持XP、win7 32位/64位、win10 32位/64位 客户端操作系统。 |  |
| 4.1.1 | 终端维护 | ▲ | 支持批量和单个客户端维护，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、软件安装信息、在线状态、资产品牌、设备出厂日期等； 硬件信息展示，包括CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息等； 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； 网络信息展示，包括IP获取方式、IP地址、子网掩码、默认网关、DNS等信息。 | 企业承诺或产品截图 |
| 4.1.2 | 外设管理 | ▲ | 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、1394、PCMIA）设置使用权限，并支持生效时间设置； 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和设备来源等； 可禁止使用大容量USB存储设备（大容量设备自持自定义大小阈值）； 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，通过添加例外或加黑。 | 企业承诺或产品截图 |
| 4.1.3 | 进程管理 |  | 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； 支持终端进程红名单、黑名单、白名单功能，可保护核心进程不被结束。 |  |
| 4.1.4 | 违规外联 | ▲ | 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； 支持例外白名单添加； 支持违规外联监控加。 报警方式：发送邮件，告警接受服务器放置在互联网侧，内网终端或服务器外接至互联网后自动将关键信息（IP地址，MAC地址，账号，等信息）上传至互联网服务器端，互联网服务器可由用户自行部署。 | 企业承诺或产品截图 |
| 4.1.5 | 能耗管理 |  | 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。 |  |
| 4.1.6 | 网络管控 | ▲ | 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。 | 企业承诺或产品截图 |
| 4.1.7 | 文件审计 | ▲ | 支持记录终端用户对于文件操作的审计，操作类型包括新建、移动、复制、删除和重命名； 支持记录全部/指定 文件路径下的文件操作审计； 支持记录全部/指定 文件后缀的文件操作审计； 支持审计日志下载。 | 企业承诺或产品截图 |
| 4.1.8 | 安全水印 |  | 支持文件水印、屏幕水印； 支持在指定应用区域或全屏展示自定义水印信息，包括当前日期、用户名、当前时间、IP地址、MAC、操作系统账号、计算机名、使用人、手机尾号和资产责任人等； 屏幕水印可调整显示区域为全屏显示和进程区域显示； 可调整水印密度、大小、角度、透明度、水印内容顺序、换行显示； 支持对应用区域显示水印页面添加新的进程； 支持打印水印，支持打印结果附带图片背景水印，支持页眉页脚位置附带水印信息，可选择“左”、“中”、“右”位置显示，支持以二维码的方式展示水印信息； 支持截屏暗水印，屏幕上无任何输出，截屏后的图片可溯源用户、终端等信息。 |  |
| 4.1.9 | 软件管理 |  | 支持软件资产统计、软件分发、软件版本管理等功能，可配合软件云中心、自定义本地软件库搭建企业私有的应用商店。 |  |
| 4.1.10 | 远程协助 | ▲ | 支持终端远程协助，可设置需要终端同意和不需要终端同意。 | 企业承诺或产品截图 |
| 4.2 | 停服系统加固 | ▲ | 支持针对Windows XP、Windows 7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。 | 企业承诺或产品截图 |
| 4.2.1 | 补丁管理功能 |  | 支持终端系统漏洞发现、补丁智能修复等功能；支持主流 Windows PC 客户端操作系统。 |  |
| 4.2.2 | 补丁类型 | ▲ | 支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC等软件进行补丁修复；支持按补丁类型和级别修复，补丁级别需包括：安全更新、重要补丁、功能补丁、可选补丁等，支持仅安装指定补丁设置。 | 企业承诺或产品截图 |
| 4.2.3 | 漏洞修复设置 |  | 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； 支持影响到编辑Office文档时提醒，可取消此次修复任务；允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。 |  |
| 4.2.4 | 补丁日志 |  | 支持展示终端信息、补丁号、补丁级别、补丁类型、安装日期、事件上报时间、事件类型、详细描述； 支持按终端统计补丁安装和生效情况，支持按照终端维度统计，统计每台终端的各个级别的补丁未安装数量，以及已安装、已安装未生效、已排除的总数量，并支持导出统计报表； 支持对停服系统补丁管理，支持统计即将停服的操作系统，显示操作系统、版本类型、系统位数、停服日期、终端数和升级建议，可直接下发策略进行升级； 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。 |  |
| 4.3 | 移动存储管理功能 | ▲ | 支持对移动存储介质进行身份注册、适用范围和读写权限控制等功能； 支持主流 Windows PC 客户端操作系统。 | 企业承诺或产品截图 |
| 4.4 | 防病毒功能 | ▲ | 支持现有安全平台联动杀毒，需提供接口； 支持多引擎协同，可对病毒、木马、恶意软件等进行查杀，提供主动防御功能；  支持主机网络访问控制，提供基于常用的网络协议以及端口层的访问控制功能； 支持主流 Windows PC 客户端操作系统。 支持开启病毒防护功能的最低配置适用于院内大多数计算机硬件配置。 | 企业承诺或产品截图 |
| 4.4.1 | 主动防御 | ▲ | 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、网页安全防护、勒索软件防护等； 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。 | 企业承诺或产品截图 |
| 4.4.2 | 网络防护 | ▲ | 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； 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； 支持僵尸网络攻击防护，对流出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后门攻击等威胁； 支持防护对流出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后门攻击等威胁。 | 企业承诺或产品截图 |
| 4.4.3 | 杀毒引擎 | ▲ | 支持不少于三个杀毒引擎混合使用，提高病毒检出率。 | 企业承诺或产品截图 |
| 4.4.4 | 病毒扫描 | ▲ | 支持信任区设置，病毒扫描或实时防护时不扫描目录或文件； 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，支持多层压缩包的扫描，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，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； 支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务； 支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式； 支持仅利用多个非工作时间时间段完成一次全盘扫描。 | 企业承诺或产品截图 |
| 4.4.5 | 病毒查杀日志 | ▲ | 支持病毒防护日志（查杀日志、防护日志）查看与下载，病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。 | 企业承诺或产品截图 |
| 4.4.6 | 黑白名单 | ▲ | 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； 支持通过文件数字签名添加黑白名单管理。 | 企业承诺或产品截图 |
| 5 | Windows Server端 |  | Windows server 授权点位300个，病毒防护、补丁管理、文件分发、软件统计、威胁处置、高级威胁防御等 |  |
| 5.1 | 防病毒 功能 |  | 支持现有安全平台联动杀毒，需提供接口； 支持多引擎协同，可对病毒、木马、恶意软件等进行查杀，提供主动防御功能； 支持主流 Windows Server 、Linux等操作系统。 |  |
| 5.1.1 | 主动防御 | ▲ | 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、网页安全防护、勒索软件防护等； 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。 | 企业承诺或产品截图 |
| 5.1.2 | 杀毒引擎 | ▲ | 支持不少于三个杀毒引擎混合使用，提高病毒检出率。 | 企业承诺或产品截图 |
| 5.1.3 | 病毒扫描 | ▲ | 支持信任区设置，病毒扫描或实时防护时不扫描目录或文件； 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，支持多层压缩包的扫描，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，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； 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； 支持仅利用多个非工作时间时间段完成一次全盘扫描。 | 企业承诺或产品截图 |
| 5.1.4 | 病毒查杀日志 | ▲ | 支持病毒防护日志（查杀日志、防护日志）查看与下载，病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。 | 企业承诺或产品截图 |
| 5.1.5 | 黑白名单 | ▲ | 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。 | 企业承诺或产品截图 |
| 5.2 | 补丁管理功能 |  | 支持终端系统漏洞发现、补丁智能修复等功能； 支持主流 Windows Server操作系统。 |  |
| 5.2.1 | 补丁类型 | ▲ | 支持对Windows Server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； 支持按补丁类型和级别修复，补丁级别需包括：安全更新、重要补丁、功能补丁、可选补丁。支持仅安装指定补丁设置。 | 企业承诺或产品截图 |
| 5.2.2 | 漏洞修复设置 | ▲ | 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； 支持影响到编辑Office文档时提醒，可取消此次修复任务； 允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。 | 企业承诺或产品截图 |
| 5.2.3 | 补丁日志 |  | 支持展示终端信息、补丁号、补丁级别、补丁类型、安装日期、事件上报时间、事件类型、结果、详细描述； 支持按终端统计补丁安装和生效情况，支持按照终端维度统计，统计每台终端的各个级别的补丁未安装数量，以及已安装、已安装未生效、已排除的总数量，并支持导出统计报表； 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。 |  |
| 5.3 | BD引擎（防病毒扩展引擎）功能 | ▲ | 支持基于 BitDefender 引擎进行病毒查杀； 支持主流 Windows Server操作系统。 | 企业承诺或产品截图 |
| 5.4 | Linux服务器 | ▲ | Linux 服务器授权点位100个，包括病毒防护、威胁处置 | 企业承诺或产品截图 |
| 6 | 银河麒麟V10 |  | 200个点位授权 |  |
| 6.1 | 终端管控 功能 |  | 支持终端维护、外设管理、软件管理、补丁管理、移动存储管理、数据防泄漏等； 支持银河麒麟V10(龙芯、飞腾、X86)、银河麒麟(龙芯、飞腾、X86)V10.1、UOS20 sp1(龙芯、龙芯3A5000、鲲鹏920、麒麟9006C、飞腾、X86、兆芯)、中科方德（龙芯、飞腾、申威、X86），TencentOS Server3等其它国产系统。 |  |
| 6.1.1 | 终端维护 | ▲ | 支持批量和单个客户端维护，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、软件安装信息、在线状态、资产品牌、设备出厂日期等； 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； 网络信息展示，包括IP获取方式、IP地址、子网掩码、默认网关、DNS等信息。 | 企业承诺或产品截图 |
| 6.1.2 | 外设管理 | ▲ | 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、1394、PCMIA）设置使用权限，并支持生效时间设置； 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和设备来源等； 可禁止使用大容量USB存储设备（大容量设备自持自定义大小阈值）； 支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径等。 | 企业承诺或产品截图 |
| 6.1.3 | 软件管理 | ▲ | 支持软件资产统计、软件分发、软件版本管理等功能，可配合软件云中心、自定义本地软件库搭建企业私有的应用商店。 | 企业承诺或产品截图 |
| 6.1.4 | 补丁管理 |  | 支持对信创桌面系统终端提供补丁管理功能。 |  |
| 6.1.5 | 移动存储管理 | ▲ | 支持对信创终端移动存储介质的注册、授权、管理及审计的安全管理。 | 企业承诺或产品截图 |
| 6.1.6 | 数据防泄漏 | ▲ | 支持对信创终端提供DLP功能。 | 企业承诺或产品截图 |
| 6.2 | 防病毒 功能 |  | 支持现有安全平台联动杀毒，需提供接口； 支持多引擎协同，可对病毒、木马、恶意软件等进行查杀，提供主动防御功能； 支持银河麒麟V10(龙芯、飞腾、X86)、银河麒麟(龙芯、飞腾、X86)V10.1、UOS20 sp1(龙芯、龙芯3A5000、鲲鹏920、麒麟9006C、飞腾、X86、兆芯)、中科方德（龙芯、飞腾、申威、X86），TencentOS Server3等其它国产系统。 |  |
| 6.2.1 | 主动防御 | ▲ | 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、网页安全防护、勒索软件防护等； 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。 | 企业承诺或产品截图 |
| 6.2.2 | 杀毒引擎 | ▲ | 支持不少于三个杀毒引擎混合使用，提高病毒检出率。 | 企业承诺或产品截图 |
| 6.2.3 | 病毒扫描 | ▲ | 支持信任区设置，病毒扫描或实时防护时不扫描目录或文件； 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，支持多层压缩包的扫描，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，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； 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； 支持仅利用多个非工作时间时间段完成一次全盘扫描。 | 企业承诺或产品截图 |
| 6.2.4 | 病毒查杀日志 | ▲ | 支持病毒防护日志（查杀日志、防护日志）查看与下载，病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间等。 | 企业承诺或产品截图 |
| 6.2.5 | 黑白名单 | ▲ | 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。 | 企业承诺或产品截图 |
| **商务要求** | | | | |
| 1 | 交货时间、交货地点 | ★ | 合同签订后3个月内交付，交付地点由甲方指定。 | 企业承诺 |
| 2 | 付款及结算方式 | ★ | 签订合同且安装软件后，支付合同金额的40%；验收合格后，支付合同金额的60%； | 企业承诺 |
| 3 | 履约保证金、质量保证金 | ★ | 合同签订前向财务缴纳合同额5%的履约保证金，验收合格后转为质量保证金，保修期满且合同内约定的其他条目均履约完成后无息退还。 | 企业承诺 |
| 4 | 产品包装和运输要求 | ★ | 按照国家、行业相关标准规范，产品确保包装完好，运输确保不对产品造成损伤。 | 企业承诺 |
| 5 | 售后服务1 （质保） | ★ | 保修年限不低于3年，全年故障停机时间不高于5%（按365日/年计算)。每月不低于1次巡检，每年不少于12次巡检，且节假日前安排保障服务，提交纸质巡检报告。 | 企业承诺 |
| 6 | 售后服务2 （质保） | ★ | 保修期内免费提供定期维护保养服务，免费升级和维护软件，免费提供使用培训。 | 企业承诺 |
| 7 | 售后服务3 （质保） | ★ | 提供不少于3人次、7天的工程师维修培训。 | 企业承诺 |
| 8 | 售后服务4 （响应时间） | ★ | 维修响应时间0.5小时，维修到达现场时间≤4小时。 | 企业承诺 |
| 9 | 知识产权 | ★ | 报价供应商应当保证采购单位在使用该物资或其任何一部分时，不受第三方侵权指控。同时，报价供应商不得向第三方泄露采购机构提供的技术文件等材料。 基于项目合同履行形成的知识产权和其他权益，其权属归采购单位所有，法律另有规定的除外。 | 企业承诺 |
| **说明：1.加注“★”号的技术指标为关键指标，≥1项未达到招标文件要求，即做废标处理**  **2.加注“▲”号的技术指标为重要指标**  **3.加注“★”、“▲”号的技术指标均需投标企业提供证明材料（证明材料为“企业承诺”的，在技术商务指标参数响应偏离表中体现即可）** | | | | |