**第三部分：项目需求**

**一、项目概述：**

（1）采购清单：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目名称** | **单位** | **数量** |
| 1 | 虚拟化杀毒 | 套 | 1 |
| 2 | 终端安全管理 | 套 | 1 |
| 3 | 终端准入系统 | 套 | 1 |
| 4 | 集成服务 | 套 | 1 |

**二、技术要求：**

**1、虚拟化杀毒**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 架构要求 | 系统需要支持B/S架构，管理员可只通过浏览器登录控制中心，即可对系统进行管理。 |
| 授权数量 | ★提供服务器安全管理系统管理控制中心软件，提供单颗 CPU 防病毒功能和防火墙功能,3年服务授权,包括:7X24小时远程电话支持服务、病毒库升级服务、软件升级服务。12 CPU 许可或不低于 300 个虚拟机的授权，含3年病毒库升级和质保服务。 |
| 部署要求 | ▲系统需支持无代理部署模式及有代理部署模式，以便结合管理需求选择相应部署模式**（提供能够体现上述功能及配置选项的截图证明加盖公章。）** |
| 需支持一套管控中心统一管理，包括有代理、无代理部署模式统一管理；物理服务器、虚拟服务器统一管理；Windows、Linux、信创操作系统统一管理；私有云、公有云、容器环境统一管理； |
| 操作系统支持 | 支持windows/linux主流操作系统（不限于下）：1、Windows Server 2003、2008、2012、2016、2019；2、Windows 7、Windows 8、Windows 10、Windows Vista；3、RedHat Enterprise Linux 6.0-7.7、CentOS6.0-8.4、Ubuntu 10.04-20.04、SUSE 11、12、15 、中兴新支点NewStart、BC-linux、Oracle Serve、Deepin、RE-DCOS、NeoKylin Linux等操作系统。 |
| 资产管理 | ★提供十五类资产的清点能力，包括服务器资产、账号资产、端口资产、网络连接、进程资产、软件应用、web服务、web站点、数据库、Jar包、系统安装包、启动服务、计划任务、环境变量、内核模块。 |
| 病毒查杀 | 采用主动的方式进行自动化病毒查杀，支持多引擎联动防护Bitdefender、QOWL、云查杀、支持灵活开启或停用引擎；支持病毒文件自动隔离、自动删除、修复、监控多种处理方式。支持病毒查杀的结果生成报告。提供防护策略控制可避免启动风暴和查杀风暴。 |
| ▲支持人工智能引擎**（提供能够体现上述功能及配置选项的截图证明加盖公章。）** |
| 支持提供病毒防护等级设置、支持对操作系统资源占用进行配置； |
| ★提供基于“诱饵”行为监测的勒索病毒防御，Windows平台支持针对已知勒索病毒家族及其变种，通过内存抢占模式，实现该类病毒免疫，同时保护Windows系统还原点，禁止还原点被恶意删除，保障系统业务恢复。 |
| 风险发现 | 提供风险发现功能，通过风险扫描功能对服务器的弱口令风险、webshell、安全补丁、漏洞风险，系统配置风险进行检测，发现服务器上的风险异常。支持安全风险评级，可直观展现评级与分数，支持按风险等级、TOP5风险、易受攻击TPO5等维度提供可视化呈现。 |
| Webshell检测 | ▲支持webshell实时防护。**（提供能够体现上述功能及配置选项的截图证明加盖公章。）** |
| 系统加固 | 提供应用程序控制功能，可基于黑白名单方式对授信/风险程序进行控制。当主机完整性发生变化时，提供报警以及追踪痕迹功能。支持提供系统补丁管理功能，针对扫描、识别的漏洞风险，可提供漏洞修复建议。 |
| 微隔离 | 提供防火墙功能，支持虚拟机/终端系统的双向控制。可提供对威胁情报实时分析网络流量功能，检测出失陷主机并提供监控及阻止失陷主机与恶意域名的连接功能。系统需支持对DDoS等异常流量进行拦截和清洗能力。 |
| 入侵防御 | 系统应支持入侵防御功能，可针对出入虚拟机的流量进行检测识别，防御网络攻击及入侵行为，通过真实漏洞利用流量的特征来检测或阻止漏洞利用(虚拟补丁防护能力) |

**2、终端安全管理**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 产品要求 | ★软件形态，管理中心系统软件，支持主流 WindowsServer 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。可实现对天擎客户端的集中管理，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。含防病毒(不含第三方扩展引擎)补丁管理、主机防火墙、终端管控功能。支持主流 Windows PC 客户端操作系统，包含500个授权数，默认包含 3年更新服务。 |
| 控制中心要求 | 控制中心支持单机部署和集群部署两种方式，控制中心根据客户端点数的增加支持横向扩展；控制中心支持安装在虚拟机上；操作系统支持Windows Server 2012/2012 R2/2016的64位版本（简体中文版）；支持CentOS 7系统； |
| ubuntu操作系统 | ★ubuntu系统终禁止修改ip功能；ubuntu系统终桌面上显示ip地址，管理员可以自定义显示信息，以及显示的颜色；远程协助:Windows管理端可以直接远程协助ubuntu终端，并互传文件；ubuntu系统终端，一旦外联立刻断掉外网，用户联系信息科解禁 |
| 客户端要求 | 操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10；Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019；macOS X 10.11/macOS X 10.12/macOS X 10.13/macOS X 10.14/macOS X 10.15/macOS X 10.16/macOS X 11.0；CentOS 5~8/Red Hat Enterprise Linux 5~8； |
| 语言要求 | ▲产品全功能支持简体中文/繁体中体/英语自由切换。**（提供能够体现上述功能及配置选项的截图扫描证明加盖公章。）** |
| 控制中心管理 | 支持控制中心迁移、数据备份、数据恢复；支持多升级服务器； |
| 支持不同分组，客户端轻量化模式一键切换功能。  |
| 客户端管理 | 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。 |
| 病毒防护概况 | 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 |
| 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。 |
| 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。 |
| 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。**（提供能够体现上述功能及配置选项的截图证明加盖公章。）** |
| ★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。 |
| 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、IM防护、局域网文件防护、网页安全防护、勒索软件防护。 |
| 网络防护 | 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。 |
| 终端病毒处理弹窗 | 客户端弹窗支持免打扰模式和智能模式，使用免打扰模式可以对不能弹窗的终端设备中避免弹窗。使用智能模式是智能调整弹窗，对已知的病毒自动处理，对未知的病毒提示处理。 |
| 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。 |
| 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、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。 |
| 支持精细配置按照操作系统版本修复漏洞，支持精细配置按照Office版本修复漏洞。 |
| 灰度发布 | ★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。 |
| 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。**（提供能够体现上述功能及配置选项的截图证明加盖公章。）** |
| 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、签名、产品名称、公司名称等，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。 |
| 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。 |

**3、终端准入系统**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 终端准入管理系统 | ▲可以为管理员提供丰富的终端安全管理功能，包括终端管理、网络准入核心管理模块；两个核心管理模块需要完整体现在同一管理平台，为了保证管理的及时性，系统管理界面要求为C/S架构，不接受WEB管理界面。**（提供截图证明加盖公章。）** |
| 网络准入 | ★网络准入设备为1U机架式准入设备，采用嵌入式Linux系统，配备6个千兆网口支持，并发数≥100000；最大吞吐量5Gbps，提供500个终端准入授权，支持Bypass功能； 支持旁路、干路、策略路由等多种方式接入。 |
| 入网合规检测 | 系统自带默认安全合规检测库，支持操作系统版本检测，系统防火墙开启检测，来宾帐户检查，系统垃圾文件检查，系统共享检测，机器名称检测检测，是否开启屏保检测，安装补丁检测，进程检测、软件检测等；软件检测包括安装指定软件不能入网，或者不安装指定软件不能入网。计算机入网后，在使用的过程中，合规检测也及时生效，在这个过程中，当发现终端计算机合规检测不合格时，立即阻止终端接入网络，同时在终端计算机上有详细的违规信息弹窗提示，并可以对于当前终端的违规情况进行评分；在系统的管理界面中也有该违规信息的详细展示。 |
| 802.1X协议 | 实现认证过的客户端才能接入交换机。终端使用者，可以进行登录与注销操作。支持与GUEST-VLAN联动，未登录的客户端，自动加入GUEST-VLAN，只有登录成功的客户端，才能加入网络 |
| 网络资产测绘 | 系统可以对于网络资产进行测绘梳理，无需在终端安装任何程序，可以探测所有在用IP，并且识别出设备类型，如计算机、打印机、摄像头、交换机、路由器、移动设备、防火墙、存储、虚拟化等网络设备，并可以进行各类设备数量统计。同时可以对于内网中的设备操作系统进行识别梳理，识别包括Window、Linux、安卓、MACOS、嵌入式系统等操作系统，并生成相关统计报表。 |
| IP可视化 | 系统可以以图形形式展示每个网段中所有IP地址占用情况，未占用和以占用以不同颜色图形标识。**（提供截图截图证明加盖公章。）** |
| 入网认证 | 包括安装客户端合规入网，强制注册入网，管理员审批入网，用户名/密码，UKey认证入网，手机短信认证入网，指纹仪认证等。 |
| 入网信息查询 | 理员可以查询所有入网用户的信息，包括：姓名、部门、入网时间、入网认证方式等信息。 |
| 网络管理 | 可以通过SNMP协议对于网络终端接入交换机的情况进行展示和管理；系统可以展示每个交换上设备的面板，以不同颜色标注交换机是否连接终端，可以展示交换机每个端口连接的终端设备的IP地址 |
| 系统功能 | 可以为管理员提供丰富的终端安全管理功能，包括日志审计、移动介质管理、外设管理、补丁管理、运维管理、水印管理等核心管理功能；提供150个终端管理授权。 |
| 系统构架 | 系统设计为C/S构架，满足更好的远程运维需求，管理员需通过控制台程序对终端进行管理。 |
| 系统兼容性 | 系统能兼容Windows各系统，支持国产系统。 |
| 远程屏幕协助 | 管理员可以快速接管（在1秒钟内接管终端电脑屏幕）远程监看或者（控制效果流畅 ）客户端的计算机。当对终端计算机进行远程控制时，客户互传终端计算机中的文件，针对终端为双屏的电脑，管理员可以点击主/副屏切换进行控制，客户端本地也可以邀请管理员远程操作自己的电脑。 |
| 远程协助安卓设备 | ▲管理员可以对于医院的PDA、诊间叫号屏等安卓系统相关设备进行远程屏幕控制，管理员可以在一秒内接管安卓设备的屏幕，控制速度快，无卡顿。**（提供截图截图证明加盖公章。）** |
| 安卓应用商店 | 为了让员工都安装指定的App，IT管理员可以把这些App放到应用商店中。员工将会自动收到系统提示，通过点击进行App安装。当IT管理员在应用商店中更新了现有的App，员工也可立刻收到提示信息，从而确保员工的App即刻符合最新的医院合规。 |
| 安卓端管理 | 系统具备软硬件资产管理，系统具备WIFI白名单功能，具备APP白名单功能，支持安卓系统全部版本。 |
| 安卓安全桌面 | 管理员可设置移动终端使用一个固定的安全桌面。在此安全桌面上仅可展示管理员规定的应用，非指定应用将不被展示在安全桌面中，确保移动终端设备专机专用。 |
| 桌面助手 | 管理员开启桌面助手策略，终端计算机桌面底层一直展示半透明窗口，管理员可以配置窗口上多个快捷方式的网址和打开浏览器名称，用户点击每个快捷方式会打开相应系统。管理员可以以九宫格的形式设置桌面助手的固定展示位置。**（提供截图截图证明加盖公章。）** |
| 截屏工具 | ▲客户端软件自带截屏工具，截屏工具在桌面助手中展示，点击可以进行截图。**（提供截图截图证明加盖公章。）** |
| 桌面IP展示 | 支持桌面展示机器名称、IP、MAC、日期、工作组以及自定义内容。显示的文字字体、大小、颜色均可设置，管理员可以通过九宫格的方式设置显示位置。 |
| 内网聊天 | 终端用户可以登录自带的聊天模块功能，可以选择医院的其他用户发送、接收即时消息，支持文件发送和接收，可以查看历史消息。 |
| 多屏墙 | 管理员可以实时查看多个计算机的电脑屏幕，最大支持64屏同时监看；可灵活设置监控屏数和自动循环播放的时间。**（提供截图截图证明加盖公章。）** |
| 系统盘自动还原 | ▲对于终端计算机提供系统盘还原功能，每次计算机重启，对于系统盘的写入信息，全部丢弃，系统盘恢复原状。**（提供截图截图证明加盖公章。）** |
| U盘管理 | 可以设置禁止使用U盘，可以为U盘设置只读，只写权限。U盘插入报警。对于鼠标键盘等USB非存储设备不禁用。支持制作注册U盘，制作后的例外U盘，可以在单位内部按权使用。客户端本地也可向管理员申请例外U盘，管理人员可以收到申请消息，并进行审批。 |
| 硬件资产管理 | 管理者可以查询硬件资产统计报表，自动收集硬件资产的变更情况。包括CPU、内存、硬盘、打印设备、串口设备等。可以对于硬件资产信息进行自定义操作，包括设置维保日期，责任人，机器品牌，配备时间，配备方式。 |
| 软件资产管理 | 管理者可以查询软件统计报表，自动收集软件的变更情况。可以统计安全软件名称、安装日期、版本号、发布者。 |
| 杀毒软件检测 | 管理员可以按计算机模式查看所有客户端的杀毒软件状况，包括是否安装杀毒软件、杀毒软件状态、杀毒软件版本号等。 |
| Windows补丁管理 | 系统可以搜集当前终端计算机的系统漏洞，以折线图的形式展现近一周内全网终端的漏洞数和趋势；以这线图的形式展示最近一周全网终端修复漏洞数；系统可以展示全部补丁信息，管理员可以根据补丁编号、补丁名称、补丁支持的操作系统进行搜索，选择需要的补丁；管理员可以查看每个补丁，在那些计算机上安装了；管理员可以查看所有补丁安装的信息，包括安装成功、安装失败、忽略信息。管理员可以设置补丁的分发速度和分发时间。管理员可以设置补丁的分发部门和分发终端。**（提供截图截图证明加盖公章。）** |
| 自动同步时间 | 客户端自动同步服务器时间。**（提供截图截图证明加盖公章。）** |
| 文件外发记录/控制 | 客户端会自动记录用户文档外发行为。包括QQ外发、USB外发、浏览器外发等，同时可以记录外发的源文件。禁止用户通过浏览器外发文件。禁止QQ外发文件。禁止阿里旺旺外发文件。禁止微信电脑版外发文件。禁止MSN外发文件。禁止U盘外发文件。禁止拷贝文件到USB设备。禁止拷贝文件到共享目录。禁止拷贝文件到网络硬盘。禁止从USB拷贝文件到本地计算机。禁止从共享目录拷贝文件到本地计算机。从网络硬盘拷贝文件到本地计算机。限制USB设备拷贝文件的大小。 |
| 系统提供大屏幕展示功能 | 以WEB形式展现，支持4K电视机屏幕完美呈现，可以在同一个屏幕上动态展示以下数据：分别以饼状图展示操作系统分布情况、计算机品牌分布情况、杀毒软件分布情况；以仪表盘的形式服务器的CPU、内存使用状态;以跑马灯的形式展示全网终端的健康度；大屏幕可以展示终端计算机维保在各个年段的计算机数量，年段定义按需求设置。**（提供截图证明扫描截图证明加盖公章。）** |
| 软件安装 | 管理员可以对计算机实行远程推送安装软件。以任务的形式提交到服务器，对于在线的计算机立刻安装，对于不在线的计算机，开机后自动执行安装任务。分发时间可自行设置开始时间与结束时间，分发速度也可限制。 |
| 屏幕保护 | 可以远程批量统一分发客户端桌面屏保；管理员可以在系统中上传制作好的屏幕保护文件，以及无操作多长时间后启动屏保。 |
| 桌面背景 | 可以远程批量统一分发客户端桌面背景。 |
| 禁用外设 | 禁止终端计算机使用软驱，光驱，红外，蓝牙，MODEM，声卡，COM口，禁用图形图像设备，禁用便携式设备，禁用无线网卡。 |
| 资质 | 提供计算机软件著作登记证书和公安部销售许可证。 |
| 其他 | ★保障用户利益，中标供应商应在签订采购合同前到达采购人指定位置测试主要指标功能是否满足项目建设的需求，对于提供虛假参数谋取中标的行为，经测试查实后将取消其中标资格，并按相关要求赔偿采购方相关损失。 |

**4、集成服务**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 集成服务 | 提供涵盖虚拟化杀毒、终端杀毒、终端准入和桌面管理的集成服务。部署虚拟化杀毒，为虚拟机环境提供高效的病毒防护，通过隔离病毒活动，防止其扩散到物理主机或其他虚拟机，确保业务连续性和数据安全。部署终端杀毒软件，在终端层面提供全面的杀毒解决方案，这包括实时监控、定期扫描、威胁分析和清除等功能，确保终端设备免受病毒、木马、蠕虫等恶意软件的侵害；实施严格的终端准入控制，确保只有符合安全策略的设备才能接入企业网络。这包括设备认证、访问权限控制、行为审计等，有效防止非法设备或未经授权的用户访问敏感数据；提供全面的桌面管理服务，包括软件分发、补丁管理、配置管理、资产管理等。通过集中化的管理，企业可以实现对终端设备的快速响应和有效控制，提高运维效率，降低管理成本。 |

**三、综合评分标准**

| **评审因素** | **评审标准** |
| --- | --- |
| **价格****（30分）** | 价格分采用低价优先法计算，即满足竞争性比选文件要求且响应价格最低的响应报价为评审基准价，其价格分为满分30分。其他供应商的价格分按照下列公式计算，保留小数点后2位：响应报价得分=（评审基准价／响应报价）×30注：评审委员会认为供应商的报价明显低于其他通过符合性审查供应商的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评审现场合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，评审委员会应当将其作为无效处理。 |
| **技术要求响应****（30分）** | 评审委员会根据比选响应文件中《技术要求响应/偏离表》，结合比选响应文件提供的佐证材料等进行评审：响应产品的技术指标全部满足竞争性比选文件《第三部分：项目需求》技术要求的得满分30分。加注“★”符号的为关键参数，不接受任何一项的负偏离或者不满足。加注“▲”符号的为重要参数，有一项负偏离或不满足扣2分；扣完为止。未加注“▲”符号的为一般指标有一项负偏离或不满足扣1分；扣完为止。 |
| **商务要求响应****（3分）** | 评审委员会根据比选响应文件中《商务要求响应/偏离表》进行评审：完全满足竞争性比选文件《第三部分：项目需求》商务要求的得满分3分。加注“★”符号的为关键参数，不接受任何一项的负偏离或者不满足。未加注“★”符号的为一般指标有一项负偏离或不满足扣1分；扣完为止。 |
| **企业履约能力****（9分）** | 投标人具备有效期内的信息安全管理、信息技术服务管理、业务连续性管理体系、信息系统安全集成、信息系统安全运维、三级及以上ITSS信息技术运行维护等证书的有一个得1.5分，最多得9分；**注：需提以上相关供有效证书扫描或相关证明材料。** |
| **集成方案****（10分）** | 评估项目方案的实施计划是否合理，包括时间表、里程碑、人员分工等方面，是否具备可操作性和可控制性等，项目实施计划优秀的得5分、合理的得3分，其他不得分；评估项目方案的售后服务支持体系是否完善，包括技术支持、培训、维护等方面，是否能够确保项目的长期稳定运行等，售后服务支持体系完善优秀的得5分、合理的得3分，其他不得分； |
| **拟投入项目组人员能力（9分）** | 1、项目负责人具有注册信息安全专业人员证书、系统集成项目管理工程师证书，中级及以上网络工程师证书，有一个得1分，满分得3分。2、项目组成员（除项目负责人）具有ITSS服务项目经理、信息安全保障人员认证、网络认证工程师、虚拟机数据保护工程师、网络安全技术能力、数据库工程师、虚拟化工程师等相关证书的，每有1人得1分，最高得6分。**注：以上人员不重复计分，需提供相关证书复印件，并加盖投标人公章及投标人为项目组成员近三个月内任意一个月缴纳的带二维码的社保证明材料。** |
| **维保应急能力（4分）** | 根据国家对等级医院建设标准要求，提供通过互联互通四级甲等用户的真实应急演练报告，一个用户的多份报告算一份，每提供一份得1分，最高不超过4分。**注：提供的报告需有用户盖章复印件并提供联系方式备查。** |
| **业绩（5分）** | 投标人2021年01月01日以来（合同签订时间为准），承担过类似业绩，每提供1个得1分；本项最多得5分。注：提供合同复印件并提供联系方式备查。 |