**采购文件**

 **（货物类）**

**深圳市儿童医院**

**评标信息**

价格分计算（每个供应商可进行两次报价，以第二次报价为最终报价）：价格分=[1-（投标报价-最低价）/最低价]×价格分权重。

当价格分<0时，取0。

最低价是指所有有效报价中最低的投标报价(**注：投标人的报价明显低于其他投标人的报价，有可能影响产品质量或者不能诚信履约的，应在评标现场提供书面说明和相关证明材料；不能证明其报价合理性的，将其作为无效投标处理**）。

评审委员会在评标时，应按照以下量化的评审因素，对各投标文件进行分析和比较：

**本项目详细评分细则如下表：**

|  |  |  |
| --- | --- | --- |
| 序号 | 评分项 | 权重 |
| 一 | 价格部分 | 30分 |
| 二 | 技术部分 | 48分 |
|  | 序号 | 评分因素 | 权重 | 评分方式 | 评分准则 |
| 1 | 技术响应情况 | 45 | 专家评分 | 投标人应如实填写《技术规格偏离表》，评审委员会根据技术需求参数响应情况进行打分，各项技术参数指标及要求全部满足的得45分，带“▲”为重要参数，每负偏离一项扣10分，其他参数（每个最小排号的参数）每负偏离一项扣5分，扣完为止。正偏离不加分。（重要参数不能超过参数总项的10%）注：对带三角号（“▲”）的重要技术参数投标人必须提供相关证明材料（技术白皮书、彩页、产品说明书或检测报告等），否则按负偏离进行扣分。 |
| 2 | 技术保障措施 | 3 | 专家打分 | 在投标文件中详细说明保障措施（包括技术团队、技术方案、技术人员、场地、车辆等），评审委员会根据响应情况进行横向比较，优3分，良2分，中1分，差0分。 |
| 三 | 商务部分 | 17 |
|  | 1 | 免费保修期内售后服务条款偏离情况 | 5 | 专家评分 | (1)投标人应如实填写《免费保修期内售后服务条款偏离表》，评审委员会根据响应情况进行打分。满足免费保修期的得3分。(2)其他要求全部满足要求的得2分，每负偏离一项扣1分。以上两项合计5分。 |
| 2 | 免费保修期外售后服务条款偏离情况 | 5 | 专家评分 | 投标人应如实填写《免费保修期外售后服务条款偏离表》，评审委员会根据响应情况进行打分，每负偏离一项扣1分，扣完为止。 |
| 3 | 投标人自主知识产权产品（创新、设计）偏离情况 | 3 | 专家评分 | 1.要求提供有效的产权（专利）证书等证明材料作为得分依据。2.以上资料均要求提供扫描件（或官方网站截图），原件备查。评分中出现无证明资料或专家无法凭所提供资料判断是否得分的情况，一律作不得分处理。全部满足要求的得3分，每负偏离一项扣1分,扣完为止。 |
| 4 | 其他商务要求偏离情况 | 4 | 专家评分 | 投标人应如实填写《其他商务条款偏离表》，评审委员会根据响应情况进行打分，全部满足要求的得4分，每负偏离一项扣2分,扣完为止。 |
| 四 | 诚信情况 | 5 |
|  | 序号 | 评分因素 | 权重 | 评分方式 | 评分准则 |
| 1 | 诚信情况 | 5 | 专家评分 | 评审标准：依据深财购[2017]42号文的有关规定，本项目将对投标人诚信进行评审：（1）投标人不存在不诚信情况且按照要求提供承诺函的，得5分。（2）投标人存在不诚信情况或未按规定提供承诺函的，得0分。 |

注：1、每项得分均不能超过该项最高分值，得分精确至小数点后两位。

2、缺项或不合格，则该项为0分。

3、重要参数不得超过技术参数总数的10%。

# 采购需求文件

|  |  |
| --- | --- |
| **项目背景** | 深圳市儿童医院目前有大量的服务器和终端计算机，但病毒等恶意程序通过多种途径进入到医院内网和外网中，院内很多计算机安装使用了杀毒软件，虽然可以对病毒起到一定的防御作用，但目前杀毒软件在查杀病毒效果上并不理想甚至无法彻底清除恶意程序。为了配合医院快速发展的步伐和业务增长的趋势，因此需要在医院网络中部署一套安全防护解决方案，解决方案可以集中管理和防护所有物理终端、服务器等系统安全。对计算机网络安全以及病毒防御实行整体的安全策略，保障医院办公自动化系统、数据库系统、网站邮件系统、网络管理中心应用服务HIS、LISPACS、CIS等业务系统的基础安全。 |
| **货物清单**  |

| **系统名称**  | **数量** | **单位** | **总预算金额(元)** | **备注** |
| --- | --- | --- | --- | --- |
| **防病毒软件** | **1** | **套** | **50万** | **无** |
|  |

 |
| **项目交付** | **项目交付清单：**

|  |  |  |
| --- | --- | --- |
| 序号 | 项目清单 | 数量 |
| 1 | 杀毒软件 | 2000点 三年维保 |
| 2 | 客户端以及服务器实施和净网服务 | 2000点 |
| 3 | 原厂软件升级服务及技术支持 | 3年 |
| 4 | 现场服务（第一年提供一周一次现场服务以及应急响应服务。） | 3年 |
| 5 | 常规技术支持服务（第二年和第三年提供远程技术支持和应急响应服务。） |
| 6 | 原厂安全专家全院信息安全知识培训服务 | 3年，每年一次 |
| 7 | 针对防病毒服务器主机安全漏洞扫描服务  | 3年，第一年两次，第二年和第三年各一次 |

 |
| **技术要求** |

|  |  |  |
| --- | --- | --- |
| **序号** | **货物名称** | **招标技术要求** |
| 1 | 项目整体要求 | 1.1▲所投杀毒软件提供产品软件销售许可证扫描件并加盖原厂公章。 |
| 1.2▲防病毒软件客户端数量2000个，三年原厂维保服务。 |
| 1.3▲投标厂商能提供至少十家三级甲等医院使用产品的成功案例。 |
| 1.4▲产品支持的操作系统支持客户端（Windows 10各种版本，MacOS 10.12-10.15及后续版本，CentOS 7以上，Debian 9以上，Ubuntu16以上，RHEL 7以上）、服务器操作系统（Windows 2008 R2以后，CentOS5.5以上，ubunt14以上所有版本 ），以上版本包括64和32位系统。 |
| 2 | 产品成熟度 | 2.1▲投标产品需要通过国际上知名和权威的防病毒认证机构VB100的认证，且连续通过70次或以上。 |
| 2.2▲中央国家机关政府采购中心的入围品牌 |
| 2.3▲经销商投标须提供原厂项目授权函及售后服务承诺函，并加盖公章。 |
| 3 | 安装部署 | 3.1杀毒软件提供多种方式的安装。必须支持网页安装、远程推送安装、MSI方式安装、共享安装、登录脚本安装、域组策略安装等。 |
| 3.2WINDOWS客户端杀毒软件必须具备一键中英文界面切换功能。 |
| 3.3产品必须提供密码保护功能，防止软件自行卸载、退出和更改设置。 |
| 3.4自动识别服务器或桌面系统，提供不同的防护功能。 |
| 3.5产品必须具备从本地或管理端检测和卸载不兼容软件功能，以避免系统冲突。 |
| 3.6管理中心可以通过打包防病毒客户端和其他应用软件安装包（如：WINRAR、Office等软件），并在需要的时候推送安装到目前Windows操作系统里。 |
| 4 | 病毒查杀 | 4.1具备实时监控病毒、木马、广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等功能； |
| 4.2▲产品具备本地独立沙箱服务器与端点杀毒的联动功能，在不安装EDR插件的情况下实现联动杀毒功能。(提供产品功能截图和厂商盖章证明) |
| 4.3具备勒索病毒加密回滚还原功能，该测试还包含不开启杀毒功能。 |
| 4.4通过主动防御技术拦截未知威胁，并且当前时间还原已被加密的文件体现安全防护能力和技术领先型，漏洞曝露阻挡，自动漏洞利用防护功能。 |
| 4.5▲产品集成EDR模块，可实现网络安全溯源、端点安全事件审计调查提供产品功能截图和厂商盖章证明) |
| 4.6产品必须具备iSwift或类似扫描技术，以大幅减少扫描时间和资源占用。 |
| 4.7支持存档和压缩格式包内病毒扫描和清除功能。 |
| 4.8病毒处理方式必须支持智能和自定义的处理方式。根据不同的病毒类型，采取不同的处理策略。 |
| 4.9必须具备主机入侵防护和IDS/IPS功能，响应可疑网络传输行为，阻止漏洞和零日攻击。 |
| 4.10可基于应用程序网络行为创建防火墙规则，可为每个WINDOWS系统设定不同的规则。 |
| 4.11产品支持主动防御技术，主动防御使用BSS行为流特征码，检测到恶意软件活动时可选择操作。  |
| 4.12产品支持只扫描新建和被修改的文件，以提高扫描效率。 |
| 4.13产品必须支持反网络攻击，检测到攻击时可将攻击计算机加入到阻止计算机列表，可自定义阻止的时间。 |
| 4.14产品必须具备邮件协议防御功能，支持标准邮件协议POP3/SMTP/IMAP/NNTP。 |
| 4.15产品必须具备启发式检测功能，可对文件、邮件、网页等进行检测。 |
| 4.16支持扫描内存和正在运行的文件，能够扫描和清除内存和文件中的病毒和蠕虫。 |
| 4.17支持自动隔离感染文件功能。 |
| 4.18产品必须支持云扫描技术，并在产品界面可查看相关数据。 |
| 4.19▲产品必须具备系统解锁或退出屏保后自动暂停扫描任务功能，以减少扫描负载。(提供产品功能截图和厂商盖章证明) |
| 5 | 端点控制 | 5.1▲产品具备允许/禁止应用程序启动功能，防止安装使用未经许可的应用程序。(提供产品功能截图和厂商盖章证明) |
| 5.2产品提供操作系统和应用程序漏洞检测和修复功能。 |
| 5.3产品具备网页控制功能，可以基于网页地址、网页类型、数据类型、时间和系统账户定制不同策略。 |
| 5.4▲支持按总线类型对外接设备进行精细化控制，包括：串行总线、并行总线、USB总线等。(提供产品功能截图和厂商盖章证明) |
| 5.5▲授权指定的程序对文档的创建、读取、修改、删除的权限，防止勒索病毒对重要文档加密。(提供产品功能截图和厂商盖章证明) |
| 6 | 管理控制 | 6.1管理控制中心必须支持WEB和MMC界面管理方式，支持SSL加密通讯连接。 |
| 6.2▲采用一个管理中心模式，支持5级以上主从管理架构，避免大型网络环境下管理中心负载过大，以及分支机构较多情况下的统一管理。(提供产品功能截图和厂商盖章证明) |
| 6.3通过逻辑分组监控客户端状态，对不同的客户端实行不同的安全策略，并能根据不同的用户权限对管理控制平台进行分级授权。 |
| 6.4具有病毒日志查询与统计功能，查询机制包括按时间（日、周或任意时间段）、IP地址、计算机名、病毒名称、病毒类型进行查询。 |
| 6.5具备客户端快速定位功能，可按IP、IP段、系统信息、计算机感染病毒情况、安装防病毒程序等进行定位。 |
| 6.6具备远程协助功能，管理中心可直接运行指定工具、获取客户端系统信息、运行的程序信息、进程日志等。 |
| 6.7管理控制中心支持广播消息推送功能。 |
| 6.8可配置管理控制中心的通知方式，包括Email、可执行程序、SMS、SNMP等多种途径。 |
| 6.9具备网络扫描功能，快速锁定未被保护的电脑。 |
| 6.10可在指定时间段对管理控制中心的访问流量大小做自定义管理，避免高峰期杀毒软件对网络流量的过度占用。 |
| 6.11具备客户端隔离和备份区中文件统一上传至管理控制中心功能，管理员可统一处理。 |
| 6.12具备客户端已安装程序信息收集功能，将其作为客户端分类、客户端入组、程序启动权限的依据。 |
| 6.13管理控制中心具备统计客户端硬件信息功能。 |
| 6.14▲管理控制中心必须具备统一配置客户端应用程序启动规则、应用程序权限规则、设备接入规则、网页浏览规则功能。(提供产品功能截图和厂商盖章证明) |
| 6.15管理控制中心统一收集漏洞信息，必须支持按漏洞优先级为全部或单个客户端进行修复。 |
| 6.16安全产品可为内网第三方程序做补丁管理，建立分发更新服务器。 |
| 6.17客户端系统进行补丁分发安装和修复后可选择需要执行的操作如不重启、重启和提示用户操作，避免影响使用。 |
| 6.18客户端系统分发补丁修复可配置运行计划，计划设定可按时、天、周等周期自动运行。 |
| 6.19可以建立自动迁移规则，客户端根据条件自动分组，包括IP地址段，计算机名、操作系统类型、代理状态、虚拟机类型、已安装应用程序等。 |
| 6.20▲一个管理控制中心能够管理包括物理平台（Windows、Linux等操作系统）、移动平台和虚拟化平台（VMware、Citrix、Hyper-V、OpenStack）在内的所有终端防护产品。（提供集中管理功能截图和厂商盖章证明） |
| 7 | 升级更新 | 7.1在服务期内，提供免费的防病毒库更新和产品升级信息服务。 |
| 7.2在国内拥有更新服务器，以保证程序自动选择最快的更新服务器，使用最快的速度获取最新的防病毒数据库。 |
| 7.3支持断点续传，避免因网络中断或系统故障而造成更新失败，重复更新。 |
| 7.4支持防病毒数据库回滚功能，当更新出现故障时，可恢复到上一次更新时的正常状态。 |
| 7.5要求管理控制中心更新后，能够有效、及时、自动地完成全网客户端的更新。 |
| 7.6要求厂商有快速的反应能力，防病毒数据数据库要求常规平均每个小时更新一次，支持在线或离线下载最新防病毒数据库和组件。 |
| 7.7▲要求厂商防病毒数据库条数至少要达到1300万条以上。(提供产品功能截图和厂商盖章证明) |
| 7.8▲在服务期内，提供免费服务端、客户端版本升级服务。 |
| **8** | 实施服务 | 8.1▲需三个月内完成客户端、服务器部署实施和净网服务。 |
| 8.2▲项目实施团队要求全部由拥有行业经验和项目经验资深的工程师组成防病毒实施项目团队，至少五人以上，全部持有相关安全和项目认证证书，其中有一人具有CISP证书，一人具有CISSP证书，一人具有PMP证书，实施团队成员全部具有杀毒产品的专业技术认证证书。 |
| 8.3需对客户端常用系统软件和业务系统的兼容性测试。 |
| 8.4根据医院各科室和合规监管实际需求，提供多元化的客户端安全策略。 |
| 8.5对挂号自助机、报告打印机、胶片打印机、CT、B超、MRI、检验科和高压氧仓进行实时防御。 |
| 8.6项目管理：注重统筹医院各科室和信息科协调，保障业务客户端正常业务，平滑过渡，提高科室满意度。 |
| 8.7项目报告：在项目实施过程中，严格实行项目报告制度，具体如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 报告 | 准备人 | 频度 | 接收人 |
| 1 | 项目周报 | 项目经理 | 每周一次 | 项目领导小组质量经理 |
| 2 | 个人周报 | 项目组成员 | 每周一次 | 项目经理 |
| 3 | 项目月报告 | 项目经理 | 每月末 | 项目领导小组质量经理 |
| 4 | 里程碑报告 | 项目经理 | 每个里程碑结束 | 项目领导小组质量经理 |
| 5 | 项目验收报告 | 项目经理 | 项目结束 | 项目领导小组质量经理 |
| 6 | 例外事件报告 | 项目经理 | 当意外事件发生时 | 项目领导小组质量经理 |

 |
| 8.8项目实施成果体现：客户端防病毒软件有效实时防护率达95%以上，真正净网率达90%以上。 |
| **9** | 项目整体售后服务 | 9.1▲需提供防病毒系统整体原厂质保期3年。 |
| 9.2▲需提供杀毒软件的原厂售后服务承诺函。 |
| 9.3▲需提供3年原厂技术支持和系统免费升级服务。 |
| 9.4▲需提供第一年每周一次现场技术支持服务以及应急响应服务。 |
| 9.4.1▲需提供7×24小时电话技术支持，五分钟内电话响应，1小时内提供应急技术支持响应，紧急情况下2小时内到达现场处理，对安全事件进行及时处理。 |
| 9.4.2▲需提供一年每季度一次的杀毒服务器和客户端系统巡检服务，巡检报告发送给深圳市儿童医院信息科指定电子邮箱，每次具体巡检时间由双方共同约定协商。 |
| 9.4.3▲需一年提供不低于二次的每次1天，每天1人的现场值守服务，以配合病毒突发和升级视察工作。 |
| 9.4.4从项目验收合格之日起计算，提供三年防病毒软件的远程技术支持的防病毒服务。 |
| 9.4.5▲一年中针对紧急安全事件，向深圳市儿童医院提供事件调查服务，并出具事件调查报告（RCA报告）；  |
| 9.4.6▲一年中当大规模病毒安全事件出现时，需要派出1到8人安全应急团队，2小时之内到达现场。 |
| 9.4.7满意度调查服务：一年中每月提供一次满意度调查服务。 |
| 9.5▲需提供第二年和第三年远程技术支持服务以及应急响应服务。 |
| 9.5.1提供7\*24小时远程服务，解答使用中遇到的问题，对于通过电话、网络、远程手段无法解决的紧急问题，24小时内到达现场解决问题。 |
| 9.6▲需提供原厂专家全院信息安全知识培训服务，一共三年，每年一次。 |
| 9.7▲需提供第一年两次针对反病毒服务器的主机安全漏洞扫描服务，第二年和第三年各提供一次针对反病毒服务器的主机安全漏洞扫描服务。 |

 |
| **商务需求**  |

|  |  |  |
| --- | --- | --- |
| **序号** | **目录** | **商务需求（根据货物种类不同自行改写）** |
| **（一）免费保修期内售后服务要求** |
| **1** | 免费保护期 | 软件免费维保期 三年，时间自最终验收合格并交付使用之日起计算。 |
| **2** | 维护响应及故障解决时间 | 在保修期内，提供7\*24小时远程服务，解答使用中遇到的问题，对于通过电话、网络、远程手段无法解决的紧急问题，24小时内到达现场解决问题。 |
| 3 | 产权合法性 | 供应商保证所使用软件的合法性，任何知识产权纠纷与用户无关。 |
| 4 | 相关培训 | 有专业人员对软件使用人员进行专业的培训，并对维护工程师进行维护培训。 |
| **6** | 其他 | 投标人应按其投标文件中的承诺，进行其他售后服务工作。 |
| **（二）免费维护期外售后服务要求** |
| **1** | 维护响应 |  免费维护期后，如需乙方进行维护，维护费用另行再议 |
| 2 |  产权合法性 |  供应商保证所使用软件的合法性，任何知识产权纠纷与用户无关。 |
| 3 |  相关培训 |  免费维保期后，如需乙方专业人员对软件使用人员进行专业的培训，并对维护工程师进行维护培训。培训费用另行再议。 |
| **（三）其他商务要求** |
| 1 | 关于交货 | 1.1签订合同后 30 天（日历日）内。 |
| 1.2投标人按要求完成软件安装、调试、上线运行。 |
| 2 | 关于验收 | 1.1 在乙方安装实施完成软件正式投入运行一个月后进行项目验收，甲方接到申请验收报告后10个工作日内无正当理由不组织验收，或验收后5个工作日内不予批准且不能提出修改意见，视作验收报告已被批准，即应办理结算手续。 |
| 1.2当满足以下条件时，采购人才向中标人签发货物验收报告：a、中标人已按照合同规定提供了全部产品及完整的技术资料。b、货物符合招标文件技术规格书的要求，性能满足要求。c、货物具备产品合格证 |
| 3 | 关于付款 | 1、付款条件：合同签订并收到全额发票后30天内向中标方方支付货款30%预付，系统上线并验收合格后凭验收单支付至全款的95%，验收合格一年后支付余款5%。2、由于供应商的原因，未能按照约定工期完成上线，导致项目延期，每迟一天罚款合同总额的0.5%； 3、由于采购人的原因，未按约定条款向供货商支付,则须按约定的付款时间起算,每迟一天罚款拖欠金额的0.5%； |
|  |  |  |

 |

 **项目投标文件**

**开标一览表**

**采购编号： SEYXX-XXK- 2020036**

**投标人名称（公章)：**

**投标人代表（签字）：**

**投标日期： 年 月 日**

开标一览表格式

### 一、开标一览表

项目编号：

|  |  |  |
| --- | --- | --- |
| 项目编号 | 供应商名称 | 软件名称 |
|  |  |  |
| 品牌 | 型号及规格 | 产地 | 生产商名称 | 数量 |
|  |  |  |  |  |
| 投标总价（人民币/元） | 交货日期 | 备注 |
|  |  |  |

注：

1、价格应按“采购文件”中规定的货币单位填写。

 2、投标人如果需要对报价或其它内容加以说明，可在备注栏填写。

投标人名称（公章）：

投标人代表（签字)：

日 期：

**二、法定代表人授权委托书**

**本授权书声明：**

注册于 （公司地址） （公司名称） （法定代表人姓名、职务）代表本公司授权 （被授权人的姓名、职务）为本公司的合法代理人，以本公司名义负责处理在深圳市儿童医院软件采购活动中相关谈判采购事务。

本授权书于 年 月 日签字生效，特此声明。

供应商法定代表人签字（盖章）：

被授权人签字（盖章）：

企业公章：

**法人代表**

**居民身份证复印件粘贴处**

（请加盖骑缝章）

**被授权人**

**居民身份证复印件粘贴处**

（请加盖骑缝章）

**被授权人**

**居民身份证复印件粘贴处**

（请加盖骑缝章）

**法人代表**

**居民身份证复印件粘贴处**

（请加盖骑缝章）

技术规格偏离表格式

**三、技术规格偏离表**

**注：▲参数为重要参数，投标人必须提供相关证明材料（技术白皮书、彩页、产品说明书或检测报告等），否则按负偏离进行扣分，但不作为废标条款。**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 招标技术要求 | 投标技术响应 | 偏离情况 | 说明 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

提示：

1、“招标技术要求”一栏应填写招标文件“具体技术要求”的内容。如“具体技术要求”内容空白，则“招标技术要求”一栏应填写招标文件相关的全部技术要求内容)

2、“投标技术响应”一栏必须详细填写投标产品的具体参数，并应对照招标技术要求一一对应响应。

3、“偏离情况”一栏应如实填写“正偏离”、“负偏离”或“无偏离”。

4、投标产品的技术参数应尽可能提供相应的证明资料，以证明投标人响应的真实性。证明资料包括制造商公布的产品说明书、产品彩页和我国政府机构出具的产品检验和核准证件等。投标人应在“说明”一栏中列出技术参数的证明资料名称，并指明该证明资料在投标文件中的具体位置。

5、证明资料要求（可提交复印件）：

（1）产品说明书或彩页应为制造商公布或出具的中文产品说明书或彩页；提供外文说明书或彩页的，须同时提供对应中文翻译说明，评标依据以中文翻译内容为准，外文说明书或彩页仅供参考；产品说明书或彩页的尺寸和清晰度应该能够被阅读、识别和判断；

（2）我国政府机构出具的产品检验和核准证件应为证件正面、背面和附件标注的全部具体内容；产品检验和核准证件的尺寸和清晰度应该能够被阅读、识别和判断。

未达到以上提供要求的，评审小组有权认定为不合格响应，其相关分数予以扣减或作废标处理。

6、评审小组有权对以谋取中标为目的的技术规格模糊响应（如有意照搬照抄招标文件的技术要求）或虚假响应予以认定，并视情况报医院相关监督管理部门予以处罚。

商务需求偏离表格式

**四、商务需求偏离表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 目录 | 招标商务条款 | 投标商务条款 | 偏离情况 | 说明 |
| （一）免费保修期内售后服务条款偏离表 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| …… |  |  |  |  |  |
| （一）免费保修期外售后服务条款偏离表 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| …… |  |  |  |  |  |
| （三）其他商务条款偏离表 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| …… |  |  |  |  |  |

提示：

1、“招标商务条款”一栏必须填写招标文件“商务需求”的内容（如有），并分别对应“（一）免费保修期内售后服务要求、（二）免费保修期外售后服务要求、（三）其他商务要求”的内容进行填写。

2、“投标商务条款”一栏必须详细填写投标商务条款的内容。

3、“偏离情况”栏中应如实填写“正偏离”、“负偏离”或“无偏离”。

4、交货期条款为不可负偏离条款，投标文件响应为“负偏离”的，投标文件将按废标处理。

5、开标一览表中填写的“交货期”必须与本表填写的“交货期”一致。如填写不一致，以开标一览表填写的“交货期”为准。

投标分项报价表格式

**五、投标分项报价表**

单位：元

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **型号/规格** | **原产地** | **品牌** | **数量** | **单价** | **合价** | **备注** |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| ３ |  |  |  |  |  |  |  |  |
| ４ |  |  |  |  |  |  |  |  |
| ５ |  |  |  |  |  |  |  |  |
| ６ |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **总 计** |  |

注：

1、单价、合价和投标总价为包干价，即三者均应包含设备的价款、包装、运输、装卸、安装、调试、技术指导、培训、咨询、服务、保险、税费、检测、验收合格交付使用之前以及技术和售后服务等其他各项有关费用。

2、开标一览表的投标总价必须与本报价表的投标总价一致。

3、“原产地”是指该产品的实际生产加工地，而非品牌总公司所在地。

**（二）零配件、消耗品和延续保修合同报价清单（不包括在投标总价内）**

**注：价格最高的前5项零配件、消耗品和延续保修合同的报价明细必须填写于此清单中。如耗材价格较贵并长期使用则按需求分类报价评分。**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 规格及型号 | 原产地 | 品牌 | 数量 | 单价(元) |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务名称 | 服务内容 | 价格（元） |
| 1 | 延续保修合同 |  |  |
|  |  |  |  |

**（三）供应商认为需要涉及的其他内容报价清单**

投标人名称（公章）：

投标人代表（签字）：

日 期：

货物说明一览表格式

**六、货物说明一览表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **型号/规格** | **数量** | **其他** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

提示：提供制造商出具的产品中文说明书、彩页、照片等相关资料。

**七、诚信情况承诺函**

致：深圳市儿童医院

我司参加贵院 招标项目投标，在此郑重承诺：

1、我司未在政府采购活动中出现以下情形之一：

* 1. 被纪检监察部门立案调查，违法违规事实成立的；
	2. 未按规定签订、履行采购合同，造成严重后果的；
	3. 隐瞒真实情况，提供虚假资料的；
	4. 以非法手段排斥其他供应商参与竞争的；
	5. 与其他采购参加人串通投标的；
	6. 在采购活动中应当回避而未回避的；
	7. 恶意投诉的；
	8. 向采购项目相关人行贿或者提供其他不当利益的；
	9. 阻碍、抗拒主管部门监督检查的；
	10. 在政府采购主管部门履约检查中不及格或评价为差的；

（十一）主管部门认定的其他情形。

2、我司已清楚不得作虚假承诺。如违反上述要求作出虚假承诺，其投标将作废，被列入不良记录名单并在网上曝光，一年内不得参加我院投标。

投标人名称（公章）：

投标人代表（签字）：

日 期：

**八、产品质量保证书**

本公司销售的产品是经由国家相关部门严格审核获准进入市场。

为保证您安全、放心地使用本产品，我公司对产品的质量和服务郑重承诺：

1. 使用本产品的患者均能得到公司高质量的售前、售中、售后服务。
2. 因产品质量缺陷造成的伤害和损失（经国家法定权威部门鉴定，情况属实），则与医院无关，由本公司与产品生产厂家负责赔偿责任。
3. 因使用本产品而导致的医患纠纷，在未明确责任前，本公司愿意协助医院积极处理。

销售公司（盖章）：

代表签名：

身份证号：

日 期：

**九、投标人认为需要补充的其他资料（如有）**

# 采购需求文件

|  |  |
| --- | --- |
| **项目背景** | 深圳市儿童医院目前有大量的服务器和终端计算机，但病毒等恶意程序通过多种途径进入到医院内网和外网中，院内很多计算机安装使用了杀毒软件，虽然可以对病毒起到一定的防御作用，但目前杀毒软件在查杀病毒效果上并不理想甚至无法彻底清除恶意程序。为了配合医院快速发展的步伐和业务增长的趋势，因此需要在医院网络中部署一套安全防护解决方案，解决方案可以集中管理和防护所有物理终端、服务器等系统安全。对计算机网络安全以及病毒防御实行整体的安全策略，保障医院办公自动化系统、数据库系统、网站邮件系统、网络管理中心应用服务HIS、LISPACS、CIS等业务系统的基础安全。 |
| **货物清单**  |

| **系统名称**  | **数量** | **单位** | **总预算金额(元)** | **备注** |
| --- | --- | --- | --- | --- |
| **防病毒软件** | **1** | **套** | **50万** | **无** |
|  |

 |
| **项目交付** | **项目交付清单：**

|  |  |  |
| --- | --- | --- |
| 序号 | 项目清单 | 数量 |
| 1 | 杀毒软件 | 2000点 三年维保 |
| 2 | 客户端以及服务器实施和净网服务 | 2000点 |
| 3 | 原厂软件升级服务及技术支持 | 3年 |
| 4 | 现场服务（第一年提供一周一次现场服务以及应急响应服务。） | 3年 |
| 5 | 常规技术支持服务（第二年和第三年提供远程技术支持和应急响应服务。） |
| 6 | 原厂安全专家全院信息安全知识培训服务 | 3年，每年一次 |
| 7 | 针对防病毒服务器主机安全漏洞扫描服务  | 3年，第一年两次，第二年和第三年各一次 |

 |
| **技术要求** |

|  |  |  |
| --- | --- | --- |
| **序号** | **货物名称** | **招标技术要求** |
| 1 | 项目整体要求 | 1.1▲所投杀毒软件提供产品软件销售许可证扫描件并加盖原厂公章。 |
| 1.2▲防病毒软件客户端数量2000个，三年原厂维保服务。 |
| 1.3▲投标厂商能提供至少十家三级甲等医院使用产品的成功案例。 |
| 1.4▲产品支持的操作系统支持客户端（Windows 10各种版本，MacOS 10.12-10.15及后续版本，CentOS 7以上，Debian 9以上，Ubuntu16以上，RHEL 7以上）、服务器操作系统（Windows 2008 R2以后，CentOS5.5以上，ubunt14以上所有版本 ），以上版本包括64和32位系统。 |
| 2 | 产品成熟度 | 2.1▲投标产品需要通过国际上知名和权威的防病毒认证机构VB100的认证，且连续通过70次或以上。 |
| 2.2▲中央国家机关政府采购中心的入围品牌 |
| 2.3▲经销商投标须提供原厂项目授权函及售后服务承诺函，并加盖公章。 |
| 3 | 安装部署 | 3.1杀毒软件提供多种方式的安装。必须支持网页安装、远程推送安装、MSI方式安装、共享安装、登录脚本安装、域组策略安装等。 |
| 3.2WINDOWS客户端杀毒软件必须具备一键中英文界面切换功能。 |
| 3.3产品必须提供密码保护功能，防止软件自行卸载、退出和更改设置。 |
| 3.4自动识别服务器或桌面系统，提供不同的防护功能。 |
| 3.5产品必须具备从本地或管理端检测和卸载不兼容软件功能，以避免系统冲突。 |
| 3.6管理中心可以通过打包防病毒客户端和其他应用软件安装包（如：WINRAR、Office等软件），并在需要的时候推送安装到目前Windows操作系统里。 |
| 4 | 病毒查杀 | 4.1具备实时监控病毒、木马、广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等功能； |
| 4.2▲产品具备本地独立沙箱服务器与端点杀毒的联动功能，在不安装EDR插件的情况下实现联动杀毒功能。(提供产品功能截图和厂商盖章证明) |
| 4.3具备勒索病毒加密回滚还原功能，该测试还包含不开启杀毒功能。 |
| 4.4通过主动防御技术拦截未知威胁，并且当前时间还原已被加密的文件体现安全防护能力和技术领先型，漏洞曝露阻挡，自动漏洞利用防护功能。 |
| 4.5▲产品集成EDR模块，可实现网络安全溯源、端点安全事件审计调查提供产品功能截图和厂商盖章证明) |
| 4.6产品必须具备iSwift或类似扫描技术，以大幅减少扫描时间和资源占用。 |
| 4.7支持存档和压缩格式包内病毒扫描和清除功能。 |
| 4.8病毒处理方式必须支持智能和自定义的处理方式。根据不同的病毒类型，采取不同的处理策略。 |
| 4.9必须具备主机入侵防护和IDS/IPS功能，响应可疑网络传输行为，阻止漏洞和零日攻击。 |
| 4.10可基于应用程序网络行为创建防火墙规则，可为每个WINDOWS系统设定不同的规则。 |
| 4.11产品支持主动防御技术，主动防御使用BSS行为流特征码，检测到恶意软件活动时可选择操作。  |
| 4.12产品支持只扫描新建和被修改的文件，以提高扫描效率。 |
| 4.13产品必须支持反网络攻击，检测到攻击时可将攻击计算机加入到阻止计算机列表，可自定义阻止的时间。 |
| 4.14产品必须具备邮件协议防御功能，支持标准邮件协议POP3/SMTP/IMAP/NNTP。 |
| 4.15产品必须具备启发式检测功能，可对文件、邮件、网页等进行检测。 |
| 4.16支持扫描内存和正在运行的文件，能够扫描和清除内存和文件中的病毒和蠕虫。 |
| 4.17支持自动隔离感染文件功能。 |
| 4.18产品必须支持云扫描技术，并在产品界面可查看相关数据。 |
| 4.19▲产品必须具备系统解锁或退出屏保后自动暂停扫描任务功能，以减少扫描负载。(提供产品功能截图和厂商盖章证明) |
| 5 | 端点控制 | 5.1▲产品具备允许/禁止应用程序启动功能，防止安装使用未经许可的应用程序。(提供产品功能截图和厂商盖章证明) |
| 5.2产品提供操作系统和应用程序漏洞检测和修复功能。 |
| 5.3产品具备网页控制功能，可以基于网页地址、网页类型、数据类型、时间和系统账户定制不同策略。 |
| 5.4▲支持按总线类型对外接设备进行精细化控制，包括：串行总线、并行总线、USB总线等。(提供产品功能截图和厂商盖章证明) |
| 5.5▲授权指定的程序对文档的创建、读取、修改、删除的权限，防止勒索病毒对重要文档加密。(提供产品功能截图和厂商盖章证明) |
| 6 | 管理控制 | 6.1管理控制中心必须支持WEB和MMC界面管理方式，支持SSL加密通讯连接。 |
| 6.2▲采用一个管理中心模式，支持5级以上主从管理架构，避免大型网络环境下管理中心负载过大，以及分支机构较多情况下的统一管理。(提供产品功能截图和厂商盖章证明) |
| 6.3通过逻辑分组监控客户端状态，对不同的客户端实行不同的安全策略，并能根据不同的用户权限对管理控制平台进行分级授权。 |
| 6.4具有病毒日志查询与统计功能，查询机制包括按时间（日、周或任意时间段）、IP地址、计算机名、病毒名称、病毒类型进行查询。 |
| 6.5具备客户端快速定位功能，可按IP、IP段、系统信息、计算机感染病毒情况、安装防病毒程序等进行定位。 |
| 6.6具备远程协助功能，管理中心可直接运行指定工具、获取客户端系统信息、运行的程序信息、进程日志等。 |
| 6.7管理控制中心支持广播消息推送功能。 |
| 6.8可配置管理控制中心的通知方式，包括Email、可执行程序、SMS、SNMP等多种途径。 |
| 6.9具备网络扫描功能，快速锁定未被保护的电脑。 |
| 6.10可在指定时间段对管理控制中心的访问流量大小做自定义管理，避免高峰期杀毒软件对网络流量的过度占用。 |
| 6.11具备客户端隔离和备份区中文件统一上传至管理控制中心功能，管理员可统一处理。 |
| 6.12具备客户端已安装程序信息收集功能，将其作为客户端分类、客户端入组、程序启动权限的依据。 |
| 6.13管理控制中心具备统计客户端硬件信息功能。 |
| 6.14▲管理控制中心必须具备统一配置客户端应用程序启动规则、应用程序权限规则、设备接入规则、网页浏览规则功能。(提供产品功能截图和厂商盖章证明) |
| 6.15管理控制中心统一收集漏洞信息，必须支持按漏洞优先级为全部或单个客户端进行修复。 |
| 6.16安全产品可为内网第三方程序做补丁管理，建立分发更新服务器。 |
| 6.17客户端系统进行补丁分发安装和修复后可选择需要执行的操作如不重启、重启和提示用户操作，避免影响使用。 |
| 6.18客户端系统分发补丁修复可配置运行计划，计划设定可按时、天、周等周期自动运行。 |
| 6.19可以建立自动迁移规则，客户端根据条件自动分组，包括IP地址段，计算机名、操作系统类型、代理状态、虚拟机类型、已安装应用程序等。 |
| 6.20▲一个管理控制中心能够管理包括物理平台（Windows、Linux等操作系统）、移动平台和虚拟化平台（VMware、Citrix、Hyper-V、OpenStack）在内的所有终端防护产品。（提供集中管理功能截图和厂商盖章证明） |
| 7 | 升级更新 | 7.1在服务期内，提供免费的防病毒库更新和产品升级信息服务。 |
| 7.2在国内拥有更新服务器，以保证程序自动选择最快的更新服务器，使用最快的速度获取最新的防病毒数据库。 |
| 7.3支持断点续传，避免因网络中断或系统故障而造成更新失败，重复更新。 |
| 7.4支持防病毒数据库回滚功能，当更新出现故障时，可恢复到上一次更新时的正常状态。 |
| 7.5要求管理控制中心更新后，能够有效、及时、自动地完成全网客户端的更新。 |
| 7.6要求厂商有快速的反应能力，防病毒数据数据库要求常规平均每个小时更新一次，支持在线或离线下载最新防病毒数据库和组件。 |
| 7.7▲要求厂商防病毒数据库条数至少要达到1300万条以上。(提供产品功能截图和厂商盖章证明) |
| 7.8▲在服务期内，提供免费服务端、客户端版本升级服务。 |
| **8** | 实施服务 | 8.1▲需三个月内完成客户端、服务器部署实施和净网服务。 |
| 8.2▲项目实施团队要求全部由拥有行业经验和项目经验资深的工程师组成防病毒实施项目团队，至少五人以上，全部持有相关安全和项目认证证书，其中有一人具有CISP证书，一人具有CISSP证书，一人具有PMP证书，实施团队成员全部具有杀毒产品的专业技术认证证书。 |
| 8.3需对客户端常用系统软件和业务系统的兼容性测试。 |
| 8.4根据医院各科室和合规监管实际需求，提供多元化的客户端安全策略。 |
| 8.5对挂号自助机、报告打印机、胶片打印机、CT、B超、MRI、检验科和高压氧仓进行实时防御。 |
| 8.6项目管理：注重统筹医院各科室和信息科协调，保障业务客户端正常业务，平滑过渡，提高科室满意度。 |
| 8.7项目报告：在项目实施过程中，严格实行项目报告制度，具体如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 报告 | 准备人 | 频度 | 接收人 |
| 1 | 项目周报 | 项目经理 | 每周一次 | 项目领导小组质量经理 |
| 2 | 个人周报 | 项目组成员 | 每周一次 | 项目经理 |
| 3 | 项目月报告 | 项目经理 | 每月末 | 项目领导小组质量经理 |
| 4 | 里程碑报告 | 项目经理 | 每个里程碑结束 | 项目领导小组质量经理 |
| 5 | 项目验收报告 | 项目经理 | 项目结束 | 项目领导小组质量经理 |
| 6 | 例外事件报告 | 项目经理 | 当意外事件发生时 | 项目领导小组质量经理 |

 |
| 8.8项目实施成果体现：客户端防病毒软件有效实时防护率达95%以上，真正净网率达90%以上。 |
| **9** | 项目整体售后服务 | 9.1▲需提供防病毒系统整体原厂质保期3年。 |
| 9.2▲需提供杀毒软件的原厂售后服务承诺函。 |
| 9.3▲需提供3年原厂技术支持和系统免费升级服务。 |
| 9.4▲需提供第一年每周一次现场技术支持服务以及应急响应服务。 |
| 9.4.1▲需提供7×24小时电话技术支持，五分钟内电话响应，1小时内提供应急技术支持响应，紧急情况下2小时内到达现场处理，对安全事件进行及时处理。 |
| 9.4.2▲需提供一年每季度一次的杀毒服务器和客户端系统巡检服务，巡检报告发送给深圳市儿童医院信息科指定电子邮箱，每次具体巡检时间由双方共同约定协商。 |
| 9.4.3▲需一年提供不低于二次的每次1天，每天1人的现场值守服务，以配合病毒突发和升级视察工作。 |
| 9.4.4从项目验收合格之日起计算，提供三年防病毒软件的远程技术支持的防病毒服务。 |
| 9.4.5▲一年中针对紧急安全事件，向深圳市儿童医院提供事件调查服务，并出具事件调查报告（RCA报告）；  |
| 9.4.6▲一年中当大规模病毒安全事件出现时，需要派出1到8人安全应急团队，2小时之内到达现场。 |
| 9.4.7满意度调查服务：一年中每月提供一次满意度调查服务。 |
| 9.5▲需提供第二年和第三年远程技术支持服务以及应急响应服务。 |
| 9.5.1提供7\*24小时远程服务，解答使用中遇到的问题，对于通过电话、网络、远程手段无法解决的紧急问题，24小时内到达现场解决问题。 |
| 9.6▲需提供原厂专家全院信息安全知识培训服务，一共三年，每年一次。 |
| 9.7▲需提供第一年两次针对反病毒服务器的主机安全漏洞扫描服务，第二年和第三年各提供一次针对反病毒服务器的主机安全漏洞扫描服务。 |

 |
| **商务需求**  |

|  |  |  |
| --- | --- | --- |
| **序号** | **目录** | **商务需求（根据货物种类不同自行改写）** |
| **（一）免费保修期内售后服务要求** |
| **1** | 免费保护期 | 软件免费维保期 三年，时间自最终验收合格并交付使用之日起计算。 |
| **2** | 维护响应及故障解决时间 | 在保修期内，提供7\*24小时远程服务，解答使用中遇到的问题，对于通过电话、网络、远程手段无法解决的紧急问题，24小时内到达现场解决问题。 |
| 3 | 产权合法性 | 供应商保证所使用软件的合法性，任何知识产权纠纷与用户无关。 |
| 4 | 相关培训 | 有专业人员对软件使用人员进行专业的培训，并对维护工程师进行维护培训。 |
| **6** | 其他 | 投标人应按其投标文件中的承诺，进行其他售后服务工作。 |
| **（二）免费维护期外售后服务要求** |
| **1** | 维护响应 |  免费维护期后，如需乙方进行维护，维护费用另行再议 |
| 2 |  产权合法性 |  供应商保证所使用软件的合法性，任何知识产权纠纷与用户无关。 |
| 3 |  相关培训 |  免费维保期后，如需乙方专业人员对软件使用人员进行专业的培训，并对维护工程师进行维护培训。培训费用另行再议。 |
| **（三）其他商务要求** |
| 1 | 关于交货 | 1.1签订合同后 30 天（日历日）内。 |
| 1.2投标人按要求完成软件安装、调试、上线运行。 |
| 2 | 关于验收 | 1.1 在乙方安装实施完成软件正式投入运行一个月后进行项目验收，甲方接到申请验收报告后10个工作日内无正当理由不组织验收，或验收后5个工作日内不予批准且不能提出修改意见，视作验收报告已被批准，即应办理结算手续。 |
| 1.2当满足以下条件时，采购人才向中标人签发货物验收报告：a、中标人已按照合同规定提供了全部产品及完整的技术资料。b、货物符合招标文件技术规格书的要求，性能满足要求。c、货物具备产品合格证 |
| 3 | 关于付款 | 1、付款条件：合同签订并收到全额发票后30天内向中标方方支付货款30%预付，系统上线并验收合格后凭验收单支付至全款的95%，验收合格一年后支付余款5%。2、由于供应商的原因，未能按照约定工期完成上线，导致项目延期，每迟一天罚款合同总额的0.5%； 3、由于采购人的原因，未按约定条款向供货商支付,则须按约定的付款时间起算,每迟一天罚款拖欠金额的0.5%； |
|  |  |  |

 |

第二节 具体技术要求

重要提示：

投标人须如实填写《技术规格偏离表》，并按招标文件的要求提供相关证明资料，包括产品原厂说明书或产品彩页等。提供的证明资料与投标响应情况不相符的，视为《技术规格偏离表》填写不实。

### 具体技术要求表

|  |  |  |
| --- | --- | --- |
| **序号** | **货物名称** | **招标技术要求** |
| 1 | 项目整体要求 | 1.1▲所投杀毒软件提供产品软件销售许可证扫描件并加盖原厂公章。 |
| 1.2▲防病毒软件客户端数量2000个，三年原厂维保服务。 |
| 1.3▲投标厂商能提供至少十家三级甲等医院使用产品的成功案例。 |
| 1.4▲产品支持的操作系统支持客户端（Windows 10各种版本，MacOS 10.12-10.15及后续版本，CentOS 7以上，Debian 9以上，Ubuntu16以上，RHEL 7以上）、服务器操作系统（Windows 2008 R2以后，CentOS5.5以上，ubunt14以上所有版本 ），以上版本包括64和32位系统。 |
| 2 | 产品成熟度 | 2.1▲投标产品需要通过国际上知名和权威的防病毒认证机构VB100的认证，且连续通过70次或以上。 |
| 2.2▲中央国家机关政府采购中心的入围品牌 |
| 2.3▲经销商投标须提供原厂项目授权函及售后服务承诺函，并加盖公章。 |
| 3 | 安装部署 | 3.1杀毒软件提供多种方式的安装。必须支持网页安装、远程推送安装、MSI方式安装、共享安装、登录脚本安装、域组策略安装等。 |
| 3.2WINDOWS客户端杀毒软件必须具备一键中英文界面切换功能。 |
| 3.3产品必须提供密码保护功能，防止软件自行卸载、退出和更改设置。 |
| 3.4自动识别服务器或桌面系统，提供不同的防护功能。 |
| 3.5产品必须具备从本地或管理端检测和卸载不兼容软件功能，以避免系统冲突。 |
| 3.6管理中心可以通过打包防病毒客户端和其他应用软件安装包（如：WINRAR、Office等软件），并在需要的时候推送安装到目前Windows操作系统里。 |
| 4 | 病毒查杀 | 4.1具备实时监控病毒、木马、广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等功能； |
| 4.2▲产品具备本地独立沙箱服务器与端点杀毒的联动功能，在不安装EDR插件的情况下实现联动杀毒功能。(提供产品功能截图和厂商盖章证明) |
| 4.3具备勒索病毒加密回滚还原功能，该测试还包含不开启杀毒功能。 |
| 4.4通过主动防御技术拦截未知威胁，并且当前时间还原已被加密的文件体现安全防护能力和技术领先型，漏洞曝露阻挡，自动漏洞利用防护功能。 |
| 4.5▲产品集成EDR模块，可实现网络安全溯源、端点安全事件审计调查提供产品功能截图和厂商盖章证明) |
| 4.6产品必须具备iSwift或类似扫描技术，以大幅减少扫描时间和资源占用。 |
| 4.7支持存档和压缩格式包内病毒扫描和清除功能。 |
| 4.8病毒处理方式必须支持智能和自定义的处理方式。根据不同的病毒类型，采取不同的处理策略。 |
| 4.9必须具备主机入侵防护和IDS/IPS功能，响应可疑网络传输行为，阻止漏洞和零日攻击。 |
| 4.10可基于应用程序网络行为创建防火墙规则，可为每个WINDOWS系统设定不同的规则。 |
| 4.11产品支持主动防御技术，主动防御使用BSS行为流特征码，检测到恶意软件活动时可选择操作。  |
| 4.12产品支持只扫描新建和被修改的文件，以提高扫描效率。 |
| 4.13产品必须支持反网络攻击，检测到攻击时可将攻击计算机加入到阻止计算机列表，可自定义阻止的时间。 |
| 4.14产品必须具备邮件协议防御功能，支持标准邮件协议POP3/SMTP/IMAP/NNTP。 |
| 4.15产品必须具备启发式检测功能，可对文件、邮件、网页等进行检测。 |
| 4.16支持扫描内存和正在运行的文件，能够扫描和清除内存和文件中的病毒和蠕虫。 |
| 4.17支持自动隔离感染文件功能。 |
| 4.18产品必须支持云扫描技术，并在产品界面可查看相关数据。 |
| 4.19▲产品必须具备系统解锁或退出屏保后自动暂停扫描任务功能，以减少扫描负载。(提供产品功能截图和厂商盖章证明) |
| 5 | 端点控制 | 5.1▲产品具备允许/禁止应用程序启动功能，防止安装使用未经许可的应用程序。(提供产品功能截图和厂商盖章证明) |
| 5.2产品提供操作系统和应用程序漏洞检测和修复功能。 |
| 5.3产品具备网页控制功能，可以基于网页地址、网页类型、数据类型、时间和系统账户定制不同策略。 |
| 5.4▲支持按总线类型对外接设备进行精细化控制，包括：串行总线、并行总线、USB总线等。(提供产品功能截图和厂商盖章证明) |
| 5.5▲授权指定的程序对文档的创建、读取、修改、删除的权限，防止勒索病毒对重要文档加密。(提供产品功能截图和厂商盖章证明) |
| 6 | 管理控制 | 6.1管理控制中心必须支持WEB和MMC界面管理方式，支持SSL加密通讯连接。 |
| 6.2▲采用一个管理中心模式，支持5级以上主从管理架构，避免大型网络环境下管理中心负载过大，以及分支机构较多情况下的统一管理。(提供产品功能截图和厂商盖章证明) |
| 6.3通过逻辑分组监控客户端状态，对不同的客户端实行不同的安全策略，并能根据不同的用户权限对管理控制平台进行分级授权。 |
| 6.4具有病毒日志查询与统计功能，查询机制包括按时间（日、周或任意时间段）、IP地址、计算机名、病毒名称、病毒类型进行查询。 |
| 6.5具备客户端快速定位功能，可按IP、IP段、系统信息、计算机感染病毒情况、安装防病毒程序等进行定位。 |
| 6.6具备远程协助功能，管理中心可直接运行指定工具、获取客户端系统信息、运行的程序信息、进程日志等。 |
| 6.7管理控制中心支持广播消息推送功能。 |
| 6.8可配置管理控制中心的通知方式，包括Email、可执行程序、SMS、SNMP等多种途径。 |
| 6.9具备网络扫描功能，快速锁定未被保护的电脑。 |
| 6.10可在指定时间段对管理控制中心的访问流量大小做自定义管理，避免高峰期杀毒软件对网络流量的过度占用。 |
| 6.11具备客户端隔离和备份区中文件统一上传至管理控制中心功能，管理员可统一处理。 |
| 6.12具备客户端已安装程序信息收集功能，将其作为客户端分类、客户端入组、程序启动权限的依据。 |
| 6.13管理控制中心具备统计客户端硬件信息功能。 |
| 6.14▲管理控制中心必须具备统一配置客户端应用程序启动规则、应用程序权限规则、设备接入规则、网页浏览规则功能。(提供产品功能截图和厂商盖章证明) |
| 6.15管理控制中心统一收集漏洞信息，必须支持按漏洞优先级为全部或单个客户端进行修复。 |
| 6.16安全产品可为内网第三方程序做补丁管理，建立分发更新服务器。 |
| 6.17客户端系统进行补丁分发安装和修复后可选择需要执行的操作如不重启、重启和提示用户操作，避免影响使用。 |
| 6.18客户端系统分发补丁修复可配置运行计划，计划设定可按时、天、周等周期自动运行。 |
| 6.19可以建立自动迁移规则，客户端根据条件自动分组，包括IP地址段，计算机名、操作系统类型、代理状态、虚拟机类型、已安装应用程序等。 |
| 6.20▲一个管理控制中心能够管理包括物理平台（Windows、Linux等操作系统）、移动平台和虚拟化平台（VMware、Citrix、Hyper-V、OpenStack）在内的所有终端防护产品。（提供集中管理功能截图和厂商盖章证明） |
| 7 | 升级更新 | 7.1在服务期内，提供免费的防病毒库更新和产品升级信息服务。 |
| 7.2在国内拥有更新服务器，以保证程序自动选择最快的更新服务器，使用最快的速度获取最新的防病毒数据库。 |
| 7.3支持断点续传，避免因网络中断或系统故障而造成更新失败，重复更新。 |
| 7.4支持防病毒数据库回滚功能，当更新出现故障时，可恢复到上一次更新时的正常状态。 |
| 7.5要求管理控制中心更新后，能够有效、及时、自动地完成全网客户端的更新。 |
| 7.6要求厂商有快速的反应能力，防病毒数据数据库要求常规平均每个小时更新一次，支持在线或离线下载最新防病毒数据库和组件。 |
| 7.7▲要求厂商防病毒数据库条数至少要达到1300万条以上。(提供产品功能截图和厂商盖章证明) |
| 7.8▲在服务期内，提供免费服务端、客户端版本升级服务。 |
| **8** | 实施服务 | 8.1▲需三个月内完成客户端、服务器部署实施和净网服务。 |
| 8.2▲项目实施团队要求全部由拥有行业经验和项目经验资深的工程师组成防病毒实施项目团队，至少五人以上，全部持有相关安全和项目认证证书，其中有一人具有CISP证书，一人具有CISSP证书，一人具有PMP证书，实施团队成员全部具有杀毒产品的专业技术认证证书。 |
| 8.3需对客户端常用系统软件和业务系统的兼容性测试。 |
| 8.4根据医院各科室和合规监管实际需求，提供多元化的客户端安全策略。 |
| 8.5对挂号自助机、报告打印机、胶片打印机、CT、B超、MRI、检验科和高压氧仓进行实时防御。 |
| 8.6项目管理：注重统筹医院各科室和信息科协调，保障业务客户端正常业务，平滑过渡，提高科室满意度。 |
| 8.7项目报告：在项目实施过程中，严格实行项目报告制度，具体如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 报告 | 准备人 | 频度 | 接收人 |
| 1 | 项目周报 | 项目经理 | 每周一次 | 项目领导小组质量经理 |
| 2 | 个人周报 | 项目组成员 | 每周一次 | 项目经理 |
| 3 | 项目月报告 | 项目经理 | 每月末 | 项目领导小组质量经理 |
| 4 | 里程碑报告 | 项目经理 | 每个里程碑结束 | 项目领导小组质量经理 |
| 5 | 项目验收报告 | 项目经理 | 项目结束 | 项目领导小组质量经理 |
| 6 | 例外事件报告 | 项目经理 | 当意外事件发生时 | 项目领导小组质量经理 |

 |
| 8.8项目实施成果体现：客户端防病毒软件有效实时防护率达95%以上，真正净网率达90%以上。 |
| **9** | 项目整体售后服务 | 9.1▲需提供防病毒系统整体原厂质保期3年。 |
| 9.2▲需提供杀毒软件的原厂售后服务承诺函。 |
| 9.3▲需提供3年原厂技术支持和系统免费升级服务。 |
| 9.4▲需提供第一年每周一次现场技术支持服务以及应急响应服务。 |
| 9.4.1▲需提供7×24小时电话技术支持，五分钟内电话响应，1小时内提供应急技术支持响应，紧急情况下2小时内到达现场处理，对安全事件进行及时处理。 |
| 9.4.2▲需提供一年每季度一次的杀毒服务器和客户端系统巡检服务，巡检报告发送给深圳市儿童医院信息科指定电子邮箱，每次具体巡检时间由双方共同约定协商。 |
| 9.4.3▲需一年提供不低于二次的每次1天，每天1人的现场值守服务，以配合病毒突发和升级视察工作。 |
| 9.4.4从项目验收合格之日起计算，提供三年防病毒软件的远程技术支持的防病毒服务。 |
| 9.4.5▲一年中针对紧急安全事件，向深圳市儿童医院提供事件调查服务，并出具事件调查报告（RCA报告）；  |
| 9.4.6▲一年中当大规模病毒安全事件出现时，需要派出1到8人安全应急团队，2小时之内到达现场。 |
| 9.4.7满意度调查服务：一年中每月提供一次满意度调查服务。 |
| 9.5▲需提供第二年和第三年远程技术支持服务以及应急响应服务。 |
| 9.5.1提供7\*24小时远程服务，解答使用中遇到的问题，对于通过电话、网络、远程手段无法解决的紧急问题，24小时内到达现场解决问题。 |
| 9.6▲需提供原厂专家全院信息安全知识培训服务，一共三年，每年一次。 |
| 9.7▲需提供第一年两次针对反病毒服务器的主机安全漏洞扫描服务，第二年和第三年各提供一次针对反病毒服务器的主机安全漏洞扫描服务。 |

### 提示：若招标文件本节表格内容空白，则投标人应根据招标文件相关全部技术要求填写“技术规格偏离表”。