**达州市中心医院**

**《智慧医院服务器及配套设备采购》**

**项目技术要求**

**一、商务要求**

**1.1产品质量要求**

（一）中标供应商交付货物时须提供制造厂商正规渠道货物来源证明，以保证货物质量，否则，追究相应损失责任。

(二)中标供应商提供的设备必须是相应设备合法生产厂家的合格产品，必须符合国家检测标准以及出厂标准，必须是全新设备（包括零部件），采购单位凭检验合格证验货，拒收验收不合格产品，一切损失概由供应商负责。供应商所供产品送到采购单位之前须是未拆封、未使用，设备及零部件表面无划伤的产品。

（三）质保期 （验收合格后开始计算）：硬件部份保修：不得小于36个月，设备保修期内实行三包，软件部份保修： 不得小于12个月，质保期内，提供运维服务和软件版本免费升级服务。

**1.2、售后服务要求**

（一）在质保期内，当出现硬件问题时，须提供硬件保修或更换服务，硬件维修：硬件维修时间不得超过15天；硬件更换：如维修过程中，因产品质量问题无法维修好，须提供整机更换或零配件更换，所有更换的设备必须是全新设备或零配件。

（二）服务要求：在质保服务期内，中标供应商须提供24小时服务热线电话和紧急联系人，采购人有任何疑惑或问题，可用电话或其他形式通知，在5分钟内给予响应，在10分钟内到达现场，30分钟内排除故障。

**1.3、到货地点及验收**

（一）交货地点：采购人指定地点。

（二）设备运抵安装现场后，采购人将首先查验货物来源证明，核实货物来源渠道,保证货物质量，并与中标供应商共同开箱验收，验收时发现短缺、破损、型号不符、非原厂生产产品等，中标供应商必须立即补发或更换。

（四）安装：

(1)安装、调试时使用的工具、设备由中标供应商提供。

(2)设备安装调试由中标供应商负责，安装调试过程中需要的配件由中标供应商负责，中标供应商应严格按照采购人的施工要求进行，同时，采购人有权派出技术人员参加，中标供应商有义务对其进行指导。

（五）验收：

货到后由采购人根据技术参数指标进行逐条验收，确认无误后，进行验收。

**1.4、付款方式**

（一）签订合同时不付预付款，如产品验收时与采购方要求不符或以次冲好、贴牌生产的无条件全额退货，并赔偿采购方损失；

（二）设施、设备安装调试完成并最终验收合格后，一次性支付。

**二、技术要求**

| 序号 | 设备名称 | 参数要求 | 数量 | 单位 |
| --- | --- | --- | --- | --- |
| 1 | 服务器 | 1.外形：2U机架式服务器,含导轨。  2.配置≥2颗处理器,单颗主频≥3.0GHz、核数≥18核、线程≥36、≥205W。  3.内存：≥384GB (12x32GB) DDR4-2933 支持最大内存≥3TB，支持最大NVDIMM内存≥192GB。  4. ≥2块480G 2.5寸SATA SSD 固态硬盘，含BOSS卡；  5. ≥6块3.84T 2.5寸 U.2 SSD固态硬盘, 最高可配12个可从正面拆卸的Express Flash NVMe PCIe 固态硬盘(PCIe 3.0)。  6.配置智能阵列控制器，≥8GB缓存，支持RAID 0/1/5/6/10/50/60。  7. ≥8个PCIe 第三代插槽。  8. 支持SD卡数量≥2，SD卡可组成RAID 1级别，保证虚拟化平台高可用性。  9. 支持U.2 SSD数量≥24。  10. 支持双宽GPU数量≥3，单宽GPU数量≥6。  11. 配置2端口千兆网卡，双口万兆光口网卡\*3张/满配本端及对端模块及配套尾纤。  12. 高效能节能冗余1100W电源1+1、支持直流电源、冗余电源风扇，支持热插拔，支持PMBus电源监控标准，满足80PLUS标准管理。  13. 配置远程管理卡模块，可提供远程管理功能，支持远程虚拟介质。服务器内置配置管理工具，集成在系统内，可通过单访问点提供“立即启动”，是部署操作系统以及内置驱动程序安装、固件更新、硬件配置和问题诊断程序的一站式中心；提供服务器管理软件：主板内部集成可管理存储空间，集成管理软件及驱动，可实现在线升级，提供快速无盘布署和管理功能；单界面即可完成所有管理服务的管理软件；支持BMC，IPMI 2.0, Redfish。  14. 利用以加密方式签名的固件程序包和安全启动确保数据安全，借助服务器锁定防止未经授权的更改或恶意更改， 通过系统擦除快速、安全地从存储介质中擦除所有数据，其中包括硬盘驱动器、 固态驱动器和系统内存。  15. 支持移动端Wifi/Bluetooth方式统一管理服务器。 | 2 | 台 |
| 2 | 模块 | 1. 速率：≥10G； 2. 接口：双LC； 3. 类型：单模； 4. 通过交换机监控模块流量、温度。 | 16 | 个 |
| 3 | 服务器安  全管理系统 | 1.配置2点防护授权，支持主流windows server 和SUSE、Red Hat、Ubuntu、CentOS、debian等常见官方发布版本的Linux内核的操作系统。  2.针对服务器和网站的目录及文件进行全面巡检扫描，对服务器和网站存在的安全隐患进行检查并修复。“服务器安全”主要针对计划任务、账户（登录账户、克隆账户、隐藏账户）及服务器安全管理系统各功能开启状态进行检查和修复；“网站安全”主要针对网页木马、网站挂马和暗链进行检查和清除。  3.通过服务器内核加固技术，加强操作系统自身对抗恶意代码和黑客攻击的能力，抵御非法提权、非法创建可执行文件等黑客行为，有效降低无补丁可打、无法打补丁带来的的安全风险。  4.支持对磁盘所有文件的监控和防护，包括读取、写入、删除、创建、执行、链接、重命名、完整性等关于文件操作的监控和防护。并且支持通配符设置，支持监控和防护两种模式，文件监控和防护生成的相关日志信息，会在系统防护日志里进行展示。  5.具有系统自身应用程序的保护功能、禁止修改应用程序关键文件。  6.支持通过在web应用(IIS、Apache、nginx、tomcat等)中插入waf探针的方式，高效过滤网络流量，防止黑客利用web应用漏洞或网站漏洞攻击服务器。  7.通过匹配漏洞攻击特征库对用户输入进行过滤，从而实现防止攻击保护网站的目的。根据不同检测对象（URL、Cookie、Post）进行具体防护规则的配置（开启与关闭）。  8.Agent提供监控点bypass功能，能够快速关停监控模块，方便问题处理或调试。  9.agent进程被终止后，监控与防护功能仍然生效，不影响安全防护效果。Windows与Linux产品功能一致，无差异。  10.黑白名单工具分为黑名单和白名单。黑名单框用来展示被系统拦截并禁用的IP列表，可以从黑名单中删除禁用名单（解禁限制IP）。白名单用于添加例外的IP，也可以批量导入。白名单中IP操作将不做拦截。  11.为保证服务器漏洞防护效果，产品制造商具备向国家信息安全漏洞共享平台（CNVD漏洞库）漏洞报送贡献能力，2021全年或2022全年需向其报送漏洞信息总数达到60000条以上。（提供CNVD颁发的证明材料或官网截图证明）  12.支持采用语境关联分析引擎技术对服务器网络异常行为进行分析识别，以保证网络威胁的检测能力及效率。（提供国家知识产权局、国家版权局、公安部、工信部之中任意一家出具的证明材料复印件并加盖投标人公章） | 1 | 套 |