**霍邱县第二人民医院网络防病毒系统续保服务项目采购**

**招标文件**

**招标编号：HQEYXXH-2021003**

**采购人：霍邱县第二人民医院**

**2021年8月**

**霍邱县第二人民医院网络防病毒系统续保服务项目采购公告**

根据《皖软件正〔2021〕3号关于推进全省公立医院软件正版化工作专项督导通知》的要求，现对我院网络防病毒系统续保服务项目进行院内招标采购。

一、项目概况

1、项目名称：网络防病毒系统续保服务项目

2、项目编号：HQEYXXH-2021003

3、项目单位：霍邱县第二人民医院

4、项目预算：54000.00元（最高限价）

5、项目数量：180套

6、授权方式：5年授权

二、投标供应商资格

1、符合《中华人民共和国政府采购法》第二十二条规定；

2、投标人须是在中华人民共和国境内注册的，具有独立企业法人资格且营业执照在有效期内生产商或代理商。

3、投标人存在以下不良信用记录情形之一的，不得推荐为中标候选人，不得确定为中标人：

(1）投标人被人民法院列入失信被执行人的；

(2）投标人或其法定代表人被人民检察院列入行贿犯罪档案的；

(3）投标人被工商行政管理部门列入企业经营异常名录的；

(4）投标人被税务部门列入重大税收违法案件当事人名单的；

(5）投标人被政府采购监管部门列入政府采购严重违法失信行为记录名单的。

4、投标人须具有有效的营业执照（三证合一），且营业执照经营范围须涵盖本次采购内容。

5、标的只有一家供应商响应时且投标文件满足询价文件全部实质性要求，现场改为单一来源采购。

6、本项目不接受联合体投标。

三、开标时间及地点：

1.开标时间：2021年8月31日 10:00

2.开标地点：霍邱县第二人民医院住院部十六楼小会议室

四、开标方式

本项目无需报名，投标供应商于2021年8月31日（北京时间，下同）10：00前到霍邱县第二人民医院住院部大楼十六楼小会议室，密封报价和营业执照（复印件），符合条件的最低报价方作为中标方。

五、评审方法：

1、本次院内采购活动将采用最低评标价法评审。

最低评标价法：以价格为主要因素确定成交候选供应商，即在全部满足询价文件实质性要求（包含资格条件、技术指标及规格、质保期以及询价过程中对以上内容的补充和修改等）前提下，根据各家报价由低到高排出成交候选供应商。

若出现报价相同的情况，则采取询价小组抽签方式确定成交单位。

2、在询价过程中，出现下列情形之一的，应予废标：

1）出现影响采购公正的违法、违规行为的；

2）供应商的报价均超过预算金额，采购人不能支付的；

3）因重大变故，采购任务取消的；

4）其他经询价小组一致认定应予废标情形的。

六、发布媒介
    霍邱县第二人民医院网站（[http://www.hqey.cn](http://www.hqey.cn/)），请投标供应商关注霍邱县第二人民医院官网《公告通知》栏目中关于本项目的补遗等内容。
  七、特别说明
    投标供应商参加本项目必须携带近3天内核酸检测阴性报告。

八、联系方式：

霍邱县第二人民医院（霍邱县城关镇蓼南路与海河路交叉口）

联系人： 李先生  联系电话：0564-6018610

**网络防病毒系统参数要求**

|  |  |
| --- | --- |
| **功能指标** | **功能描述** |
| 系统要求 | ★产品支持各类Windows 32/64位操作系统(Windows 7、Windows 8、Windows 10、Windows Server 2003、Windows Server 2008、Windows Server 2012等），支持苹果Mac OS系统、支持各类32/64 Linux系统（Red hat、SUSE、Cent OS等），支持各类移动操作系统（苹果IOS、安卓、塞班、黑莓OS等）。需提供支持Mac系统、Linux系统产品官网截图证明。 |
| 病毒处理和修复能力 | ★支持文件、邮件、即时通讯和网页的反病毒功能模块，必须支持Linux系统实时防病毒功能，即有病毒传入系统立即拦截，提供支持Linux产品实时防病毒功能技术截图证明。 |
| ★具备系统监控主动防御技术，当恶意行为对系统关键区域比如注册表进破坏或修改后，可回滚病毒在操作系统上执行的恶意操作，如通过系统监控主动防御技术发现未知勒索病毒进行拦截的同时能够回滚还原被勒索病毒加密破坏的文件，提供产品具备回滚技术功能截图。 |
| 支持压缩文件扫描，包含多级嵌套压缩文件，能够做到压缩包内清毒，支持加密压缩文件扫描。 |
| 产品具备云安全网络技术，云辅助技术可提高对未知病毒的响应速度并减少误报，同时有效抵御零日漏洞攻击。 |
| ★支持使用受信任的系统证书，通过证书提高系统安全性，支持个人及企业信任证书、受信任根证书颁发机构、智能卡受信任的根、受信任的设备、第三方根证书颁发机构等多种选择，提供产品支持使用证书系统的技术功能截图。 |
| 防火墙和反网络攻击 | 支持网络数据包规则的防火墙功能，通过建立防火墙策略规则对特定端口选定数据协议发送和接收网络流量。 |
| 支持根据应用程序建立网络访问规则，对特定应用程序的网络活动评估和限制，阻止不合法的应用程序网络连接。 |
| ★具备H-IPS（主机入侵防御系统），提供反网络攻击的功能，检测和抵御危险的网络活动和网络攻击，并自动将攻击源加入攻击列表，产品必须能够阻止诸如“永恒之蓝”等漏洞利用方式的攻击行为，提供产品能够检测和阻断“永恒之蓝”漏洞攻击（漏洞编号MS17-010）的技术功能截图证明。 |
| 合规性管理 | ★支持访问保护多样化的权限锁定功能，支持对操作系统启动设置、系统文件关键设置、系统服务、进程访问、入侵进程（安装钩子、注入代码、重复句柄等）、使用浏览器命令行或浏览器接口等多种方式进行访问保护，提供产品针对代码注入、重复句柄等权限安全设定技术功能截图。 |
| 支持移动存储介质控制，如控制U盘、移动硬盘、手机等设备接入终端，避免移动介质传播病毒的风险，支持外接设备认证功能，即特定的U盘可以使用其他则不可以，提供产品控制USB接口和配置信任移动设备功能截图；。 |
| ★支持漏洞扫描功能，漏洞扫描需包含针对系统漏洞和应用程序（Flash、JAVA等）漏洞评估，并支持补丁分类操作和集中统计进行补丁分发功能。 |
| 安全管理及升级更新 | ★实现统一平台、统一管理和统一流程，考虑到未来云计算平台的搭建和应用，原厂商须具备虚拟化安全的解决方案，且管控中心能够管理包括物理（Windows、Linux、Mac OS等操作系统）、移动（Android、IOS等操作系统）和虚拟化（VMware、Citrix、Hyper-V）在内的所有安全产品，并集中定制物理、移动和虚拟化的策略配置和报告输出，提供集中管理技术功能截图。 |
| ★具有减少网络负载功能，管理控制中心可针对IP子网或者IP段进行数据传输速度的控制，通过建立相关配置规则，可对最大传输速率和时间等参数进行定义，提供技术功能截图。 |
| 丰富的报表功能，包括：保护状态、感染最严重的情况、客户端被网络攻击的情况、终端产品版本和病毒库版本等。 |
| ★支持多种事件导出方式联动SOC、SIEM等大数据系统平台，支持RFC5424、Spluk（CEF格式）、Arcsight（CEF格式）及QRadar（LEEF格式），提供产品技术功能截图。 |
| 资质及服务 | ★提供180个防病毒系统授权和5年软件版本及特征库免费升级服务。 |
| ★公安部计算机信息系统安全专用产品的销售许可证。 |
| 公安部计算机病毒防治产品检验中心检验报告，检测结果为一级品。 |
| 国家版权局计算机软件著作权登记证书。 |