**采购需求**

**安阳市肿瘤医院**

**云资源及配套服务采购方案**

**安阳市肿瘤医院**

**2025 年 3 月**

一、 项目目标

本项目旨在购买一个技术上高度安全可靠的云资源服务。云资源池应位于安阳市区域，所用资源为安阳市肿瘤医院专属，且必须为专属资源池、不与其他单位共用。通过网络专线与医院内各机房连接。

二、 项目需求

1.安全可靠架构：采用安全可靠的云平台，以确保在关键的云管理层面实现技术安全可靠。

2.模块化设计：采用模块化设计理念，确保系统的各个组件可以独立更新和替换，而不会影响到整体架构的稳定性和安全性。

3.自主研发的关键技术：在系统的关键部分应用自主研发的技术，如云计算基础设施的设备芯片采用国产自研。

4.兼容性：确保系统兼容性，特别是对操作系统、数据库和中间件等方面的兼容，确保整个业务系统安全稳定的运行。

5.可扩展性和弹性：设计时应考虑到未来的可扩展性和弹性，以便于在业务需求变化时，可以无缝升级和扩展。

6.数据主权和隐私保护：确保数据存储、处理和传输过程符合《中国人民共和国数据安全法》的相关规定，保障用户数据的主权和隐私。

三、软件支持服务

为满足院方使用，云平台需提供院方未列出的其他配套软件包括但不限于云平台管理系统、虚拟化组件、安全组件等以保障云平台的正常运维，平台运维整体由响应人负责操作和技术指导。

四、机房要求

云平台的主机房应部署在安阳本地，响应人如在安阳本地无自有机房，需承诺云平台部署在安阳本地。云平台机房应具备：

1.双路不间断供电，每年持续电力供应时间在 99.99%以上，以确保应用系统可持续工作，满足采购人对于信息化工作的高要求，机房空间和供电在满足本期资源需求规模基础上。

2.适应业务发展的扩展能力。

3.机房同地点处的办公场地，满足日常运维值班，设备安装调试，后期业务系统迁移等工作需要。

4.较高性能的安防、环境监控、灭火系统等基础设施服务，机房抗震烈度不低于 7 度。

5.环境智能监控，实现对设备电流量的监控、机房温度监控、机房湿度监控。

以上要求为机房服务的基本要求，应按照云平台的要求进行建设，满足安全可靠、节能环保、扩展灵活等建设原则，应保证提供不间断的云服务，可用性应在 99.99% 以上。

五、资源需求

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 类型 | 名称 | 规格 | 单位 | 数量 | 备注 |
| 业务区 | vCPU | vCPU | 核 | 2000 | 1.超分比≤2; 2.除数据库服务器外，其他服务器主频≥2.4GHz。 |
| 内存 | 内存 | G | 8000 |  |
| 存储(SSD) | 全闪独立存储 | T | 60 |  |
| 文件存储 | 文件存储功能 | T | 100 |  |
| 影像存储 | 影像存储功能 | T | 300 |  |
| 核心交换机 | 1.交换容量≥1070Tbps，包转发率≥345000Mpps，以官网最小值为准； 2.设备支持主控板槽位数≥2，独立交换矩阵槽位≥4，业务板槽位≥6，电源模块槽位数≥4； 3.支持跨设备链路聚合（DRNI/M-LAG），支持无损升级，支持快速收敛（流量无丢包），支持一致性检查； 4.支持VXLAN多种方式接入，支持VXLAN二三层互通,支持EVPN，支持基于IPv4/IPv6 Underlay 的 VXLAN 三层 Anycast 分布式网关(包括 IPv4 VXLAN over IPv4、IPv4 VXLAN over IPv6、IPv6 VXLAN over IPv4、IPv6 VXLAN over IPv6)，支持基于 IPv4/IPv6 Underlay 的 VXLAN 三层集中式网关； 5.支持CoPP，支持CPU保护，支持ARP防攻击，支持自动防御，支持IP source guard(MAC地址攻击防范)，支持 Attack source tracing，支持DAI，支持DDOS 攻击防御，支持ND Snooping，支持协议报文黑名单； 6.支持纵向虚拟化功能，支持一键配置下发、智能版本升级、一键命令下发，支持终端管理，融合监控摄像头质量管理，指纹库等功能； 7.支持全端口MACsec加密技术，密钥长度为256bits； 8.提供三年原厂质保服务。 | | | | |
| 万兆交换机 | 1.交换容量≥4.8Tbps，包转发率≥2000Mpps（官网最小值），支持≥4个风扇模块槽位，≥2个电源模块槽位； 2.支持ISSU（不中断业务升级）、OAM（操作、管理和维护）； 3.支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持SP、WDRR、SP+WDRR等多种模式； 4.支持基于端口、流的M:N复制，M口和N口最大53，支持GRE隧道剥离封装，支持同源同宿，支持报文截断，支持源端口标识，支持增加时间戳及以太网头，识别指定报文，修改mac地址或IP地址后复制转发； 5.提供三年原厂质保服务。 | | | | |
| 数据库  服务器 | 1.2颗X86 CPU，主频：≥2.5GHz；核心数：≥16核； 2.内存：≥8\*32GB 2Rx4 DDR4； 3.系统盘：≥2\* 480GB SSD； 4.RAID卡模块,带4GB缓存； 5.网卡≥4个10GE光接口(含光模块）,≥4个千兆电接口；机身提供≥6个USB接口； 6.支持通过服务U盘下载服务器设备故障诊断日志； 7.快速定位故障硬盘：提供不局限于存储控制卡连接硬盘、背板直连主板（即板载硬盘）的硬盘点灯功能，提升硬盘运维效率； 8.冗余交流电源(支持高压直流)； 9.仅数据库使用以上配置； 10.提供3年原厂质保服务。 | | | | |

|  |  |  |
| --- | --- | --- |
|  | 设备  名称 | 性能参数 |
| 管理中心设备 | NGFW防火墙 | 1.吞吐量：应选择高性能的防火墙，以满足100台服务器的网络流量需求。吞吐量≥1Gbps的防火墙； 2.并发连接数：支持高并发连接数，至少支持100万以上的并发连接； 3.处理能力：能够快速处理网络流量，确保低延迟和高吞吐量； 4.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式； 5.集成入侵检测系统（IDS）和入侵防御系统（IPS），能够实时监测并防御常见的网络攻击，如端口扫描、木马后门攻击、拒绝服务攻击等； 6.支持防病毒功能，能够检测和清除恶意代码； 7.为确保高可用性，建议选择具备冗余电源和接口的防火墙设备； 8.产品支持3种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证； 9.产品支持应用管控功能，应用特征识别库数量大于9000种； 10.产品支持基于网络区域、网络对象、MAC地址、服务、应用等维度进行访问控制策略设置； 11.产品支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型； 12.产品支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上（需提供产品功能截图，并加盖原厂公章）； 13.产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略，需提供产品相关功能截图，并提供第三方检测机构出具关于“勒索病毒”的相关证书证明功能有效性； 14.产品支持管控非法、违规网站的访问行为，具备海量的URL分类库；支持基于文件传输方式、文件类型等维度的管控策略配置；支持https解密功能，支持TCP代理和SSL代理； 15.产品内置不低于13000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则（需提供产品功能截图，并加盖原厂公章）； 16.产品支持与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理，支持检测到某主机有僵木蠕毒的C2通信时，手动或自动化将恶意域名信息下发到终端安全软件做C2通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离（需提供产品功能截图，并加盖原厂公章）； 17.产品支持管理员双因子认证，可以通过用户密码和Key等不同方式登陆产品管理界面； 18.配置3年IPS、AV特征库升级授权； 19.提供三年原厂质保服务。 |
| 堡垒机 | 1.授权资产：至少支持100个节点（根据实际需求可扩展到300个节点）； 2.用户管理：支持多角色划分（如系统管理员、部门管理员、运维员、审计管理员、密码管理员等），内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范，并支持细粒度权限管理； 3.身份认证：支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、短信认证，并支持各种认证方式和静态口令组合认证； 4.访问控制：基于状态的访问控制，能够根据会话状态信息为数据流提供明确的允许/拒绝访问能力，控制粒度为端口级。支持在授权基础上设定双人复核登陆，登录时必须经过第二人授权后才能登录，第二人可通过远程授权或同终端授权两种方式实现授权； 5.操作审计：对所有通过堡垒机进行的操作进行详细记录和审计，详细记录用户行为，包括登录时间、操作命令、操作结果等，支持将审计日志发送到专用的日志服务器； 6.会话管理：实时监控和控制用户会话，必要时可强制断开会话。还应包含可临时分配账号，账号使用时间的功能，如超过设定使用时间账号会自动失效； 7.具备录屏功能（需提供产品功能截图，并加盖原厂公章）； 7.提供三年原厂软件升级和质保服务。 |
| 数据库审计 | 1.性能参数：峰值SQL处理能力≥10000条/s, 日志存储能力≥10亿条/天, 存储存储期限≥12个月, 审计处理能力≥2Gbps,，存储空间≥2TB； 2.支持对多种数据库进行审计，如Oracle（Tdata）、SQL-Server、DB2、MySQL（Tdsql）、Informix、Sybase、Cache、PostgreSQL；国产化数据库：MongDB、K-DB，达梦、人大金仓（需提供产品功能截图，并加盖原厂公章）； 3.审计范围：覆盖到每个拥有数据库的服务器，满足院方所需，数量不得低于200个； 4.支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌； 5.精细化日志秒级查询通过SQL串模式抽取保障磁盘IO的读写性能，分离式存储SQL语句保障数据审计速度快（需提供产品功能截图，并加盖原厂公章）； 6.自定义报表拖拽。通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果； 7.内置大量SQL安全规则。包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp\_addrolemember提权、web端sp\_addrolemember提权、查询内置敏感表、篡改内置敏感表等（需提供产品功能截图，并加盖原厂公章）； 8.支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断； 9.可以对SQL语句进行安全检测，并识别当前的SQL操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施； 10.支持以时间、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL模版为条件的数据库风险查询； 11.支持Syslog告警、SNMP trap告警、邮件告警，短信告警；支持WEB界面备份及日志恢复导入工作；支持自动与手动两种备份归档方式； 12.提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能（需提供产品功能截图，并加盖原厂公章）； 13.支持SNMP方式，提供系统运行状态给第三方网管系统；支持Syslog方式向外发送审计日志； 14.提供三年原厂质保服务。 |
| 日志审计 | 1.性能参数：每秒日志处理能力（EPS）≥3000, 存储存储期限≥12个月, 包含主机审计许可证书数量≥200； 2.支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射（需提供产品功能截图，并加盖原厂公章）； 3.支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志； 4.支持TLS加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量（需提供产品功能截图，并加盖原厂公章）； 5.支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件； 6.支持将检索查询的条件收藏为查询模版，支持查询模版创建、导入导出、删除功能，支持历史搜索记录功能； 7.支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上，支持自定义关联分析规则； 8.支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件； 9.支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景； 10.支持个性化定制，支持全系统更换logo与系统名称，支持一键恢复默认； 11.支持POC测试工具一键生成数据,验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险（需提供截图证明并加盖原厂公章）； 12.提供三年原厂软件升级（包含但不限于攻击检测规则库）及质保服务。 |
| 漏洞扫描 | 1.性能参数：系统漏扫授权IP数≥200，WEB漏扫授权URL数≥100；系统漏扫最大并发IP数≥200，WEB漏扫最大并发URL数≥50； 2.漏洞扫描支持指定登录用户名和口令进行本地漏扫检查； 3.采用有自主知识产权的安全操作系统，采用B/S设计架构，并采用SSL加密通信方式，无须安装客户端，用户可通过浏览器远程方便的对产品进行管理； 4.支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情； 5.支持常见的WEB应用弱点检测，支持主流安全漏洞扫描，如：SQL注入、跨站脚本攻击、网页木马、系统命令执行漏洞、信息泄露、资源位置预测漏洞、目录遍历漏洞、配置不当漏洞、弱密码、内容欺骗漏洞、外链、暗链等类型漏洞； 6.支持按“一个中心、三重防护”的架构展示检测结果，每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认； 7.可自定义扫描时间段，设置禁止扫描时间段后，该时间段内的周期任务、一次执行任务将无法自动执行。可选择多个例外任务，禁扫时间段不会影响例外任务执行； 8.以列表的方式展示告警，支持告警策略自定义、告警声音设置，不同级别设置不同音效； 9.产品支持对系统漏洞、SQL注入漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、SQL注入漏洞、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表（需提供截图证明，并加盖公章）； 10.配置管理功能，支持将当前系统环境信息中，自定义信息完整导出，可在新环境导入，已做环境迁移； 11.系统内置对应基线问题、安全经验等知识。并支持自定义创建增加知识； 12.要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务一级资质，提供有效证书复印件并加盖公章； 13.提供三年原厂软件升级及质保服务。 |
| 态势感知 | 1.性能参数：流量处理能力≥2G，日志处理能力（EPS每秒）≥8000； 2.支持安全态势的可视化呈现，帮助客户更直观的看清风险、看懂威胁，提供综合态势大屏、分支安全态势、安全事件态势、通报预警态势大屏、物联网安全态势大屏、全球网络攻击态势、资产态势、重大活动网络安全指挥调度大屏、设备运行态势、外联风险监控态势等不少于17块大屏展示界面（需提供截图证明，并加盖原厂公章）； 3.支持主机类资产识别，能够识别资产数据来源、IP地址、主机名、MAC地址、基线异常、操作系统、操作系统详请、主机类型、服务与端口、状态、责任人、EDR状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP类型、识别方式、首次发现时间等； 4.支持跨三层取MAC地址，识别资产MAC地址，并能够解决不同资产IP冲突问题，以及DHCP场景IP变更的问题； 5.支持整体展示服务器脆弱性风险分析、热点漏洞情况、脆弱性风险详情（漏洞风险、配置风险、弱密码、web明文传输、可用性风险），支持第三方漏扫报告导入和解析，可按资产组分类上传，支持上传文件； 6.支持弱密码主动扫描，支持SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL等扫描协议，支持自定义扫描周期、发包频率、扫描时间段、扫描优先级、扫描对象等； 7.支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置； 8.支持对800+网络安全设备接入类型，接入方式支持文件、数据库、API、Syslog、FTP、Snmp trap、Kafka、WMI、webservice、winlogbeat等方式进日志行接入； 9.支持勒索专项检测页面，帮助客户更好的应对日益严峻的勒索风险，支持对勒索主题的安全告警进行统一展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类； 10.支持综合安全风险、主机安全风险、脆弱性感知、外部威胁感知、工单报告、摘要报告、处置报告多种方式呈现，可快速生成月度、季度、年度报表，摘要报告支持至少三种导出方式，至少包含ppt、pdf、doc； 11.支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序； 12.支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，重新发起识别后，资产数据能够及时更新（提供第三方权威机构检测报告证明，至少包含报告首页，对应功能测试页和报告尾页，并加盖原厂公章）； 13.支持挖矿专项检测，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测； 14.支持通过网络侧与终端侧关联聚合，可以实现进程级取证，失陷主机定位，并以可视化图谱直观清晰地展示出完整的攻击链（需提供截图证明，并加盖原厂公章 15.支持与院方采购的杀毒软件等设备联动，实现一键查杀等功能（需提供截图证明，并加盖原厂公章）； 16.院方能随时通过管理平台实时对软硬件进行动态监控，监控软硬件资源占用情况； 17.提供三年原厂升级和质保服务。 |
| 威胁检测探针 | 1.网络层吞吐量≥1Gbps，应用层吞吐量≥350Mbps； 2.支持旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响； 3.支持自动识别内网的服务器及其开放的服务与端口，支持以列表形式显示资产IP、提供的服务及其开放的端口、设备类型、操作系统等信息； 4.支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测等（提供产品功能截图证明材料，并加盖公章）； 5.支持多种类型弱口令策略可选；支持自定义FTP弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等； 6.支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞、自定义WAF规则、WAF云防护等网站攻击检测； 7.支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Media漏洞攻击、Network Device、Shellcode漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击、IPS云防护等服务漏洞攻击检测； 8.支持检测出网络中的网络拓扑设备进行绘制，更直观可视化查看网络整体情况； 9.审计白名单支持源目IP、源目端口和日志类型、日志来源； 10.支持基于IP和域名的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断； 11.内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、白名单库； 12.为保障产品的可靠性，所投产品的生产厂商具备中国通信企业协会的企业行业信用（系统集成领域）AAA级等级证书，提供证书复印件并加盖公章； 13.提供三年原厂升级和质保服务。 |
| 动态密码管理 | 1.基本要求：标准机架设备，国产化CPU+国产化操作系统，≥6个千兆电口，≥4个千兆光口，≥2个万兆光口，≥16GB内存，≥4TB硬盘，冗余电源。≥300路图形会话或≥1000路字符会话并发，配置≥500授权资产许可，配置国密硬件加密卡，配置10个动态密码卡； 2.支持的协议和应用：支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin、X11；可通过应用发布的方式进行协议扩展，如数据库、浏览器等客户端工具； 3.自动收集和自动授权：支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权（提供功能截图及国家权威机构证明并加盖原厂公章）； 4.专用客户端运维：支持Windows/macOS操作系统，UOS /麒麟等国产操作系统下C/S架构的设备专用客户端，可通过此专用客户端登录设备，对设备进行简单的管理及运维资产操作（提供截图）； 5.命令审批：支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令（提供功能截图及国家权威机构证明并加盖原厂公章）； 6.密码及登录策略：支持设置用户密码的长度、复杂度、相关度和检查历史密码；支持密码过期前告警；支持用户密码错误策略的自定义调整，对用户及来源IP进行锁定，防止暴力破解； 7.访问策略：支持旁路部署方式，采用B/S方式进行管理，支持根据运维用户、运维对象、管理方式等条件设置访问控制策略，并可对指定运维操作命令设置报警和阻断动作。该产品自身具备身份鉴别功能，支持对用户操作生成会话审计日志，能够对运维操作进行审计回放，会话可以实时监控（提供公安部出具的检测报告扫描件并加盖原厂商公章）； 8.国密和非国密兼容模式：支持国密和非国密通信兼容模式，在开启国密通信的同时兼容普通加密通信，能够满足在国密兼容模式下，使用国密浏览器时协商国密通信，使用普通浏览器时协商普通加密通信的相关能力； 9.身份鉴别：支持使用基于国密算法的动态令牌、国密USBkey对设备的登录实行双因素认证。以满足对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性。针对国密动态令牌、国密USBkey可提供国家密码局颁发的《商用密码产品认证证书》及加盖公章的厂商授权书； 10.提供三年原厂升级与质保服务。 |
| 计算环境设备 | NGFW防火墙 | 1.吞吐量：应选择高性能的防火墙，以满足100台服务器的网络流量需求。吞吐量≥1Gbps的防火墙； 2.并发连接数：支持高并发连接数，至少支持100万以上的并发连接； 3.处理能力：能够快速处理网络流量，确保低延迟和高吞吐量； 4.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式； 5.集成入侵检测系统（IDS）和入侵防御系统（IPS），能够实时监测并防御常见的网络攻击，如端口扫描、木马后门攻击、拒绝服务攻击等； 6.支持防病毒功能，能够检测和清除恶意代码； 7.为确保高可用性，建议选择具备冗余电源和接口的防火墙设备； 8.产品支持3种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证； 9.产品支持应用管控功能，应用特征识别库数量大于9000种； 10.产品支持基于网络区域、网络对象、MAC地址、服务、应用等维度进行访问控制策略设置； 11.产品支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型； 12.产品支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上（需提供产品功能截图，并加盖原厂公章）； 13.产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略，需提供产品相关功能截图，并提供第三方检测机构出具关于“勒索病毒”的相关证书证明功能有效性； 14.产品支持管控非法、违规网站的访问行为，具备海量的URL分类库；支持基于文件传输方式、文件类型等维度的管控策略配置；支持https解密功能，支持TCP代理和SSL代理； 15.产品内置不低于13000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则（需提供产品功能截图，并加盖原厂公章）； 16.产品支持与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理，支持检测到某主机有僵木蠕毒的C2通信时，手动或自动化将恶意域名信息下发到终端安全软件做C2通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离（需提供产品功能截图，并加盖原厂公章）； 17.产品支持管理员双因子认证，可以通过用户密码和Key等不同方式登陆产品管理界面； 18.配置WEB应用防护功能模块： 1）防护对象：支持对Web应用进行防护，包括但不限于HTTP/HTTPS流量； 2）防护规则：内置Web核心防护规则，能够防御SQL注入、XSS跨站脚本、代码执行、WebShell上传、命令注入等常见Web攻击； 3）防护模式：支持拦截模式和检测模式，可根据业务需求选择适合的防护模式； 4）规则模板：提供默认规则模板，用户可自定义规则模板以满足特定业务需求； 5）白名单功能：支持白名单功能，允许放行具有指定特征的请求，避免误拦截； 6）CC防护：支持CC攻击防护，可自定义规则进行频率限制，缓解高频请求攻击； 7）扫描防护：能够识别并阻止扫描器对网站的大规模扫描行为； 8）IP黑名单：支持自定义IP黑名单，拦截来自特定IP地址或地址段的请求； 9）自定义规则：允许用户基于HTTP请求特征或特征组合，对符合条件的请求执行拦截、验证、记录日志等操作； 10）区域封禁：支持一键封禁来自特定区域的客户端IP； 11）网页防篡改：支持网页防篡改功能，锁定重要页面，防止恶意篡改； 12）信息泄露防护：支持对网站返回内容中的敏感信息进行过滤和脱敏显示； 19.配置3年IPS、AV、Web特征库升级授权； 20.提供三年原厂质保服务。 |
| 杀毒软件 | 1.软件规格：提供控制中心一套，可实现对客户端的统一运维管理、安全策略维护、消息中心、手机令牌、报表中心功能等，配置不少于200套杀毒软件授权； 2.资产梳理：提供Windows、Linux服务器统一的资产展示能力。支持跨系统、跨资产类型、跨主机进行快捷搜索。对搜索匹配到的资产关键字进行高亮标记，统计搜索到的资产数量，并提供搜索高级查询语法规则和快捷保存搜索条件以方便搜索； 3.入侵检测：支持对攻击者发起的恶意扫描行为进行识别，可防护端口扫描和扫描器扫描行为，以攻击和受害两种视角展示扫描信息包括：发生时间、受害IP、攻击IP、攻击类型、扫描端口、扫描次数、在威胁情报中是否为黑IP等信息。支持报告并记录相应的安全事件，包括:端口扫描、强力攻击、缓冲区溢出攻击、可疑连接攻击，记录的内容包括事件名称、攻击源地址、目的地址、事件发生时间、重要级别等信息； 4.风险评估：所投产品应支持统计总风险及各类风险数量，展示影响服务器信息。通过各类图表展示安全评分趋势、风险项趋势、账户风险类型分布、口令风险应用排行、漏洞风险项数量、配置风险排行等相关统计信息，便于用户快速了解风险整体情况； 5.漏洞扫描：支持检测的漏洞数量应不低于4000个。厂商应提供推荐扫描的漏洞项，形成模板供客户快速选择；同时支持按照漏洞名称、漏洞编号、漏洞等级、漏洞类型、系统类型、应用名称、检测原理、披露时间、存在EXP、本地提权、内核风险、修复影响、是否可防护等信息搜索或筛选特定漏洞进行扫描；  6.安全基线：产品应支持两次基线扫描任务的结果比对，比对前后不合规项比率、不合规服务器比率的偏差，并列出前后偏差的服务器列表； 7.防病毒：杀毒引擎数量应不少于4种，其中自研杀毒引擎不低于1种； 8.Webshell：支持Webshell的实时监测，支持批量开启关闭实时监测； 9.微隔离：产品微隔离能力在Windows、Linux、国产化多种系统上，应保持同样的功能，实现同等水平的微隔离效果； 10.勒索场景化防护：产品应支持针对勒索攻击事件可独立展示告警和防护配置，同时产品预置Linux和Windows系统勒索防护配置模版，可一键下发防护策略； 11.微蜜罐：产品应支持端口蜜罐能力，在配置时可以自定义触发端口后的返回文本信息，可迷惑攻击者提高防护能力以及为取证提供支持； 12.系统加固：通过对Linux和Windows操作系统深度解析提供对操作系统加固能力，具体防护项覆盖系统关键文件、系统重要服务、系统网络访问方面，且加固条数不少于60项； 13.性能监控：产品支持对服务器CPU使用率、内存使用率、磁盘使用率、客户端内存使用率、客户端CPU使用率进行监控； 14.主机IPS（虚拟补丁）：支持从服务器角度聚合展示该服务器上存在的漏洞，并统计有风险的服务器数量、存在危急和高危漏洞服务器的数量、支持打虚拟补丁和支持实体补丁的服务器数量； 15.服务器被病毒入侵后的所有损失由中标方承担； 16.提供三年原厂升级（包括但不限于病毒特征库）和质保服务。 |
| 应用负载均衡 | 1.性能要求：吞吐量≥1Gbps，不限制新建和并发； 2.支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应时间、加权最小流量、按主机加权最小流量、源IP源端口哈希、源IP哈希、URI哈希和HOST哈希等； 3.支持外部应用监视器健康检查功能，同时可配置间隔时间、超时时间，同时可通过Web页面执行命令，并且能开启/关闭调试日志功能； 4.支持HTTP被动健康检查，可配置指定检查URL、响应状态码、响应超时时间、统计时间以及可设置异常URL上限，并且能开启/关闭调试日志功能； 5.支持TCP被动健康检查，可配置统计时间、监视类型、保护时间等，并且能开启/关闭调试日志功能； 6.支持配置每台的业务主机的并发连接数、新建连接数和每秒请求数限制，同时可配置每个虚拟服务的单个IP或所有IP的最大新建和最大并发限制；（需提供产品功能截图，并加盖原厂公章） 7.可针对单个虚拟服务配置对称路由、QoS策略、HTTP2策略和HTTP防护策略等； 8.支持HTTP2网关部署，在不改变web服务器的情况下将对外服务协议从HTTP1.1/1.0升级至HTTP/2，提升终端用户使用体验和业务安全性；支持HTTP2策略，可设置每连接最大流量数、空闲超时时间、接收窗口大小和头部表大小等； 9.支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的WebP或JPEG格式，优化加速效果；（需提供产品功能截图，并加盖原厂公章） 10.服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU温度、CPU和内存占用率、新建连接数、并发连接数、吞吐情况、SSL新建和SSL吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量；（需提供产品功能截图，并加盖原厂公章） 11.支持双机热备部署方式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换； 12.支持在同一个虚拟服务下同时配置多个IPv4和IPv6地址；（需提供产品功能截图，并加盖原厂公章） 13.提供三年原厂升级与质保服务。 |
| 区域边界设备 | 上网行为管理 | 1.部署要求：部署在相对独立的网络区域，确保内外网的物理隔离； 2.网络环境：确保网络环境的稳定性和安全性，支持高速网络连接； 3.流量监控与管理：实时监控网络流量，分析和记录用户的上网行为，识别异常活动并采取控制措施； 4.策略控制：实现对上网行为的细粒度控制，如限制特定网站、应用的访问，或根据时间段进行访问控制； 5.日志记录与审计：详细记录用户的上网行为日志，定期进行审计，生成报表，确保日志信息的完整性和安全性； 6.安全预警与响应：设定安全预警规则，及时发现并响应潜在的安全威胁，具备自动化的报警机制； 7.访问控制策略：根据用户角色和访问权限设定不同的访问控制策略，可基于用户、部门、时间等条件制定访问规则； 8.内容过滤策略：配置内容过滤规则，阻止访问不合规的网站和内容，可通过关键字、网址分类等方式进行过滤； 9.数据安全策略：设置数据加密和备份策略，保护用户数据的机密性和完整性，确保日志数据的加密存储和安全传输； 10.安全审计策略：配置审计策略，定期生成和分析安全审计报告，确保所有操作和事件都可以被追踪和检查； 11.应急响应策略：建立应急响应机制和处理流程，以应对可能出现的安全事件，包括事件的检测、报告、分析和处理； 12.提供三年原厂升级与质保服务。 |
| NGFW防火墙 | 1.吞吐量：应选择高性能的防火墙，以满足100台服务器的网络流量需求。吞吐量≥1Gbps的防火墙； 2.并发连接数：支持高并发连接数，至少支持100万以上的并发连接； 3.处理能力：能够快速处理网络流量，确保低延迟和高吞吐量； 4.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式； 5.集成入侵检测系统（IDS）和入侵防御系统（IPS），能够实时监控网络流量，识别并报告潜在的安全威胁，支持监测端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等，支持记录攻击源IP、攻击类型、攻击目的、攻击时间，并在发生严重入侵时提供报警； 6.支持防病毒功能，能够检测和清除恶意代码； 7.为确保高可用性，建议选择具备冗余电源和接口的防火墙设备； 8.产品支持3种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证； 9.产品支持应用管控功能，应用特征识别库数量大于9000种； 10.产品支持基于网络区域、网络对象、MAC地址、服务、应用等维度进行访问控制策略设置； 11.产品支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型； 12.产品支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上（需提供产品功能截图，并加盖原厂公章）； 13.产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略，需提供产品相关功能截图，并提供第三方检测机构出具关于“勒索病毒”的相关证书证明功能有效性； 14.产品支持管控非法、违规网站的访问行为，具备海量的URL分类库；支持基于文件传输方式、文件类型等维度的管控策略配置；支持https解密功能，支持TCP代理和SSL代理； 15.产品内置不低于13000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则（需提供产品功能截图，并加盖原厂公章）； 16.产品支持与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理，支持检测到某主机有僵木蠕毒的C2通信时，手动或自动化将恶意域名信息下发到终端安全软件做C2通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离（需提供产品功能截图，并加盖原厂公章）； 17.产品支持管理员双因子认证，可以通过用户密码和Key等不同方式登陆产品管理界面； 18.配置3年IPS、AV特征库升级授权； 19.提供三年原厂质保服务。 |
| VPN | 1.部署位置：部署在接入边界NGFW设备上； 2.支持的VPN类型：支持SSL VPN功能，用于远程安全接入；. 3.加密算法：支持强加密算法，如AES-256，确保数据传输的保密性和完整性； 4.身份认证：支持多种身份认证方式，如用户名/密码、数字证书、双因素认证等；. 5.并发连接数：根据实际需求配置，确保满足远程用户并发接入的需求； 6.带宽管理：支持带宽管理功能，合理分配VPN连接的带宽资源； 7.日志记录：详细记录VPN连接的登录、访问和断开等日志信息，便于审计和追溯； 8.安全策略：配置访问控制策略，限制VPN用户的访问权限，确保只有授权用户才能访问特定资源； 9.高可用性：支持主备设备配置，实现故障切换，确保VPN服务的高可用性； 10.提供三年原厂升级与质保服务。 |
| 网闸 | 1、性能参数≥吞吐量：5Gbps，并发连接数≥20W； 2、采用“2+1”结构，内外端机都采用安全的LINUX操作系统，内外端机之间采用FPGA隔离卡及光纤线路连接； 3、设备内外端之间不允许有任何TCP/IP等网络协议，在采用专用隔离卡的基础上，使用API进行原始数据交换，支持各类上层应用的数据摆渡； 4、支持基于TCP、UDP协议的非标准应用协议以及IP、SMTP、POP3、MULTICAST、网络协议等； 5、支持基于FTP、NFS、SFTP、Samba等方式的文件同步； 6、支持基于五元组（源地址、源端口、目的地址、目的端口、协议）的访问控制机制； 7、自带的防病毒能对来往应用数据进行病毒查杀，有效的保护了来往的数据、文件、音视频、图片的安全；（提供产品功能截图证明材料，并加盖公章） 8、支持Oracle、SQLServer、DB2、MySql及国产达梦、人大金仓等主流同构异构数据库同步功能，并且支持基于向导式的数据库同步任务配置；（提供产品功能截图证明材料，并加盖公章） |
| 数据脱敏系统 | 1.性能参数：提供峰值不小于25000条SQL/秒的动态脱敏性能； 2.支持Oracle，MySQL，SQL Server，PostgreSQL，DB2，informix，GaussDB，神通，人大金仓，达梦，GBASE，Greenplum，TeraData，HIVE，HBASE，HDFS，MongoDB，TiDB，ClickHouse，ODPS等数据库； 3.支持数据库到数据库、数据库到文件、文件到文件、文件到数据库等多种数据分发方式的脱敏； 4.支持对已脱敏的数据进行逆向脱敏查询，得到真实数据，便于用户校验数据的可使用性； 5.支持敏感数据自动发现，系统内置敏感数据特征库，包含但不限于以下种类的隐私数据类型：身份证号、三证合一码、电子邮箱、车牌号、手机号、固定电话、军队证件、银行卡号、时间、日期、邮政编码、车架号、台湾居民来往大陆通行证、港澳居民来往大陆通行证、护照号、保单号、中文姓名、企业单位名称、中文地址等； 6.支持自定义文件脱敏模板，用户上传需要脱敏的文件后通过选择模板即可完成敏感数据确认、脱敏算法选择、脱敏方案选择等任务，进行快捷高效脱敏； 7.支持周期调度作业任务，可根据需求设定任务单次或多次调度执行的时间，进行任务定时脱敏； 8.支持多种脱敏算法，仿真、置空、加密、随机、遮蔽、K匿名、令牌化、洗牌、截断、字符乱序； 9.系统支持脱敏敏感数据的同时增加水印信息，提高敏感数据多渠道分发的安全指标； 10.提供系统管理员、安全管理员和审计管理员来管理脱敏设备； 11.提供三年原厂升级与质保服务。 |
| 容灾 |  | 1.资源要求：提供不低于784核vCPU、3608G内存、137000GB高性能存储可用资源（本资源为单独部署资源，不包含在总资源中）； 2.性能要求：CPU主频不低于2.4GHz； 3.容灾方式最低为双机热备（满足三甲复审和电子病历五级评审等要求，包括但不限于以下系统：HIS、LIS、EMR、PCAS、RIS），投标人提供承诺函； 4.为了确保本次项目业务的数据安全性，本次采购的云服务需采用硬件独享的模式，云厂商需要提供物理资源独享方案，同时满足用户资源物理隔离、安全合规等； 5.为提高数据传输效率、减少对云上带宽的消耗，本容灾服务需要支持压缩传输功能，对同步到备站点的数据先压缩再进行传输，并可以根据实际带宽启用、禁用压缩传输功能； 6.为了保证能提供可靠的备份数据管理功能，并满足我单位对数据保留周期的要求。要求支持容灾服务可对异地容灾的备份数据设置保留周期操作，可以按照不同时间周期，最高可保留30年内全部备份文件； 7.当主站点恢复正常后，为了方便业务回迁操作，提升恢复速度，我单位要求所提供的容灾服务能够支持一键回迁功能，且能够根据业务需求选择回迁全量数据或增量数据； 8.由于我院本地需容灾数据量较大，为了提升首次数据同步速率，降低对带宽要求，要求容灾服务支持种子文件功能，用户可以在主站点使用种子文件功能将需要容灾的云主机备份制作成种子文件存放到外置存储（U盘，移动硬盘）中，使用物理方式将存储介质运输到云厂商提供的容灾数据中心，然后导入主站点云主机的种子文件，以此来提到容灾首次数据同步的速度，降低对带宽的要求（需提供产品功能截图，并加盖厂商公章）； 9.为资源容灾提供容灾向导。主备容灾云主机底层同架构，互联互通，可实现云间大二层网络，实现部分业务主机房，部分业务在备机房仍然能够互相访问，不需要修改DNS等复杂配置，一键完成容灾演练和容灾切换。在网络条件能满足情况下，容灾RPO≈0和RTO分钟级容灾等级（需提供产品功能截图，并加盖厂商公章）； 10.为保证容灾效果，同时满足合规要求，厂商需提供容灾演练方案，并每年提供至少1次的容灾演练服务（需提供承诺函，并加盖厂商公章）； 11.为提高数据传输效率、减少对带宽的消耗，灾备软件需要支持压缩传输功能，对同步到备站点的数据先压缩再进行传输； 12.确保数据在不同场景下的高效保护与快速恢复，持续数据保护CDP软件模块需采用无代理的方案，避免对虚拟机的稳定性和性能产生影响； 13.支持快速浏览指定CDP备份内的文件，可快速的从CDP备份中找回数据文件（windows文件系统），查看虚拟机文件目录的操作可做安全审计（需提供截图证明，并加盖厂商公章）； 14.支持数据找回RPO为秒级； 15.需厂商提供各项资源配置单价，若合同期内需要增加资源配置，应按照资源单价进行统一收费； 16.支持原厂三年质保服务。 |
| 纯业务异地数据备份 |  | 1.本服务可支持不限制虚拟机数量的整机备份服务，提供不少于30TB备份空间（需提供承诺函并加盖厂商公章）； 2.提供云备份资源机房所在位置满足机房两地三中心； 3.提供无需第二机房的异地备份服务，支持按需购买，灵活扩容，无需自己运维（需提供承诺函并加盖厂商公章）； 4.为了保证数据能够能够完整恢复，需提供数据验证服务和远程应急恢复； 5.提供基于磁盘数据块复制技术的整机备份，无需了解主机业务系统类型、部署方法、业务系统间的数据交互机制、数据结构/逻辑关系和数据库的品牌/版本； 6.为了防止因定时备份执行过程对生产主机造成性能影响，需保证执行定时备份保护过程中备份进程最高CPU占用不超过3%,内存不能高于1G（提供截图，并加盖原厂公章）； 7.可自建隔离私有虚拟化验证环境，无论备份任务是否停止，可同时选一个备份任务的多个备份点执行虚拟化验证备份数据的一致性和可靠性，在灾难发生时采用二分法快速定位出最佳数据恢复的备份历史点（提供截图，并加盖原厂公章）； 8.演练时，演练目标机无需预置任何演练环境（目标机无操作系统、目标机和原机操作系统不一致、目标机无应用系统、目标机无数据库等）可即时开展对指定业务模拟故障后的演练重建功能； 9.支持以邮件、企业微信告警的方式，针对于备份存储系统的软件故障、存储空间、备份任务、操作状态等信息及时通知管理员； 10.备份机房也需满足三级等保机房要求； 11.备份软件费用由中标方承担； 12.提供三年原厂质保服务。 |
| 专线 |  | 1.4根专线分别从不同的方向迁入机房； 2.容灾专线需单独走线。 |
| 服务 | 售后服务 | 1.方便医院后期运维管理需要，提供不少于100个服务器/虚拟机迁移授权服务； 2.提供同品牌自研的迁移工具，无需采购第三方迁移服务，支持原主机和异构目标机之间的自动化迁移功能； 3.支持在线增量迁移、全量迁移，且是迁移期间不中断业务的热迁移，仅最后一次增量数据迁移需要停虚拟机； 4.支持目标机无需预置任何迁移环境，目标机无操作系统、目标机和原机操作系统不一致、目标机无应用系统、目标机无数据库等； 5.迁移过程中对源机业务影响小，可以动态调整源机IO占用、网络带宽占用，确保迁移过程不影响源主机正常运行； 6.提供整体灾备重建迁移，支持任意秒历史点回退切换，确保迁移到正常系统状态； 7.合同终止后，如需进行数据迁移，需无偿协助院方进行数据迁移，并确保不再使用的数据被彻底销毁；  8.如院方需要新增资源，分配时间不能超过3天，紧急情况下不能超过1天。 |
| 安全托管服务 | 1.服务要求（要求供应商提供承诺函加盖公章）： （1）为单位提供网络安全运维服务，不少于3年的服务期限，提供7\*24H线上安全运维服务，服务资产数量≥50。服务方需要提供安全运营服务过程中必要的配套工具，包括但不限于安全评估工具等； （2）投标方应当具备云端检测和分析平台，通过采集我方安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为我方提供7\*24小时持续不间断的安全威胁分析鉴定。 2.安全现状评估： （1）漏洞风险评估：对操作系统、数据库、Web应用进行漏洞扫描及风险评估； （2）弱口令风险评估：对IT资产及应用进行弱口令风险排查； （3）针对业务系统可能存在的攻击行为判断是否成功，以及业务现有的攻击风险点； （4）失陷主机分析：对现有IT资产进行分析后，识别已经失陷的资产，并给出针对性修复建议； （5）中标公司每月提供一次机房设备巡检，巡检设备包括但不限于服务器、存储、操作系统、数据库、中间件等（要求供应商提供承诺函加盖公章）。 3.漏洞管理： （1）从资产重要性、威胁情报、漏洞等级等多个维度对单位内的漏洞风险进行排序，并提供修复指导建议； （2）对识别的漏洞风险进行验证，验证漏洞利用可能性及可能造成的影响面。针对已经验证的漏洞，由安全专家跟进漏洞状态，并为我方生成相应的工单，可视化处理的进度； （3）要求投标方可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到99%，要求供应商提供承诺函加盖公章； （4）中标公司每半年提供一次服务器漏扫，如发现漏洞应在15个工作日修复（尤其是中高危漏洞）。 4.威胁管理： （1）全年365天7\*24H实时监测网络安全状态，一旦有攻击事件发生，便生成相应的工单，进行跟进处理； （2）全年365天7\*24H实时监测网络安全状态，对病毒等安全事件生成工单，进行跟进处理。 5.服务质量承诺（要求供应商提供承诺函加盖公章）： （1）从安全日志产生到事件通告的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于15分钟，一般事件的通告时间少于30分钟； （2）安全事件经过服务人员的确认后，通告给招标方的各类安全事件的准确率不低于99%（即误报不能超过1%）； （3）投标方应当承诺，服务范围内的所有安全事件的闭环处置比例达到100%； （4）投标方应当满足重大事故应启动应急响应机制，工作时间15分钟之内云端专家进行响应，非工作时间30分钟之内云端专家进行响应，8小时内上门处置。 |
| 专项服务 | 服务内容包括： 1.中标公司要根据医院发展给出专业的资源重整方案； 2.中标公司负责我院在贵公司的服务器和存储的数据安全，并根据院方需求配合资源分配，不得以任何借口拒绝； 3.中标公司负责我院在移动公司所有数据的迁移，产生的任何费用由中标公司承担（如果需要部署裸光纤移动公司配合）； 4.管家服务：提供专属管家7x24小时省心服务，范围：问题咨询、突发事件保障、配置变更、周期巡检、巡检风险处理、巡检报告； 5.交付服务：业务上云评估咨询服务、上云迁移服务、上云实施服务、专线接入服务、物理设备托管接入服务、培训服务、备案支持服务； 6.响应支持：应急响应、基础服务（帮助与文档、订阅支持、生命周期管理、续费延期服务）、响应方式（官网在线咨询、电话支持、工单支持）； 7.基础安全能力：提供弱密码检测与辅助闭环，公网暴露面的高危端口发现与辅助闭环，协助勒索数据恢复； 8.监控服务：云资源异常事件监控支持、云资源用量与性能监控支持、支持业务拨测任务与告警管理工具、业务拨测配额免费提供、外网暴露云主机安全风险检查、安全防护风险检查、威胁情报通知。 还包括如下代维服务内容： 1.云资源风险主动服务：针对托管云云资源监控告警、数据保障风险告警的主动式运维服务承接，从定制化告警策略配置、提前预测风险、主动介入处置并闭环等，提供告警事件与风险的一站式全栈管理服务支持；  2.安全风险主动服务：针对托管云云上安全风险主动式运维服务支持，分别从安全组件配置风险检查、云平台配置风险检查、外网暴露面风险检查、咸胁情报对业务影响分析等维度及时进行风险检测，并提供主动通知及修复建议； 3.监控服务医院大屏端：医院信息中心必须部署我院云资源在云端的运行提供可视化屏幕监测（包含硬件和线路）。 |

**六、报价表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 类型 | 名称 | 规格 | 单位 | 数量 | 单价（元/1年） | 3年小计 | 备注 |
| 业务区 | vCPU | vCPU | 核 | 2000 |  |  |  |
| 内存 | 内存 | G | 8000 |  |  |  |
| 存储(SSD) | 全闪独立存储 | T | 60 |  |  |  |
| 文件存储 | 文件存储功能 | T | 100 |  |  |  |
| 影像存储 | 影像存储功能 | T | 300 |  |  |  |
| 总价 |  |  |  |  |  |  |  |

**七、扩容单价**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 类型 | 名称 | 规格 | 单位 | 数量 | 单价（元/1年） | 3年小计 | 备注 |
| 业务区 | vCPU | vCPU | 核 |  |  |  |  |
| 内存 | 内存 | G |  |  |  |  |
| 存储(SSD) | 全闪独立存储 | T |  |  |  |  |
| 文件存储 | 文件存储功能 | T |  |  |  |  |
| 影像存储 | 影像存储功能 | T |  |  |  |  |

备注：

1.以上价格均为含税报价。

2.如果按单价乘以数量所得的结果与总价不一致，以价格低的为准。

3.表中数量为系统上线最小资源量，“单价（元/1 年）”列为合同签订后生效周期。

内每年租赁价格，“总价（元/5 年）”用于评审标准中价格得分的计算。

4.表中所表述的规格、数量皆为扣除折损后采购人需要的实际可用规格数量。

5.扩容部分按照实际使用量核算。

响应单位： （盖单位章）

年 月 日