杭州市第七人民医院

浙西院区信息化基础设备建设项目

招标文件

 **（电子招投标）**

编号:HSZB-2022-445

杭州市第七人民医院

浙江豪圣建设项目管理有限公司

二〇二二年九月二十八日

**目 录**

**[第一部分 招标公告 3](#_Toc26721)**

**[第二部分 投标人须知 8](#_Toc9395)**

**[第三部分 采购需求 26](#_Toc13068)**

**[第四部分 评标办法 100](#_Toc5463)**

**[第五部分 拟签订的合同文本 108](#_Toc17651)**

**[第六部分 应提交的有关格式范例 123](#_Toc23700)**

**第一部分 招标公告**

项目概况

杭州市第七人民医院浙西院区信息化基础设备建设项目招标项目的潜在投标人应在政采云平台（[https://www.zcygov.cn/）获取（下载）招标文件，并于2022年10月19日13点30分00秒](https://www.zcygov.cn/%EF%BC%89%E8%8E%B7%E5%8F%96%EF%BC%88%E4%B8%8B%E8%BD%BD%EF%BC%89%E6%8B%9B%E6%A0%87%E6%96%87%E4%BB%B6%EF%BC%8C%E5%B9%B6%E4%BA%8E2021%E5%B9%B4)（北京时间）前递交（上传）投标文件。

**一、项目基本情况**

 **项目编号：**HSZB-2022-445

  **项目名称：**杭州市第七人民医院浙西院区信息化基础设备建设项目

  **预算金额（元）：**7805100.00

**最高限价（元）：**7805100.00

**采购需求：**杭州市第七人民医院浙西院区信息化基础设备建设项目，主要内容：杭州市第七人民医院浙西院区信息化基础设备建设。详见招标文件第三部分采购需求。

**合同履约期限：2023年12月前完成建设，投入正常运行，运行6个月后系统无问题，进行项目验收。**

**本项目接受联合体投标：**[x] **是，**[ ] **否**。

**注：不得限制大中型企业与小微企业组成联合体参与投标。**

**二、申请人的资格要求：**

1. 满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

 2.落实政府采购政策需满足的资格要求：

[x] 无；

[ ] 专门面向中小企业

[ ] 货物全部由符合政策要求的中小企业制造，提供中小企业声明函；

[ ] 货物全部由符合政策要求的小微企业制造，提供中小企业声明函；

[ ] 服务全部由符合政策要求的中小企业承接，提供中小企业声明函；

[ ] 服务全部由符合政策要求的小微企业承接，提供中小企业声明函；

[ ] 要求以联合体形式参加，提供联合协议和中小企业声明函，联合协议中中小企业合同金额应当达到 %，小微企业合同金额应当达到 %;如果供应商本身提供所有标的均由中小企业制造、承建或承接，视同符合了资格条件，无需再与其他中小企业组成联合体参加政府采购活动，无需提供联合协议；

[ ] 要求合同分包，提供分包意向协议和中小企业声明函，分包意向协议中中小企业合同金额应当达到达到 % ，小微企业合同金额应当达到 % ;如果供应商本身提供所有标的均由中小企业制造、承建或承接，视同符合了资格条件，无需再向中小企业分包，无需提供分包意向协议；

3.本项目的特定资格要求：无；

4.单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动；为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后不得再参加该采购项目的其他采购活动。

**三、获取招标文件**

**时间：**/至2022年10月19日，每天上午00:00至12:00 ，下午12:00至23:59（北京时间，线上获取法定节假日均可，线下获取文件法定节假日除外）

**地点（网址）：**政采云平台（https://www.zcygov.cn/）

**方式：**供应商登录政采云平台https://www.zcygov.cn/在线申请获取采购文件（进入“项目采购”应用，在获取采购文件菜单中选择项目，申请获取采购文件）。

**售价（元）：**0

**四、提交投标文件截止时间、开标时间和地点**

**提交投标文件截止时间：** 2022年10月19日13点30分 （北京时间）

**投标地点（网址）：**政采云平台（https://www.zcygov.cn/）

**开标时间：**2022年10月19日13点30分

**开标地点（网址）：**政采云平台（https://www.zcygov.cn/）

**五、公告期限**

自本公告发布之日起5个工作日。

**六、其他补充事宜**

 1.《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》 （浙财采监（2022）3号）、《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）、《浙江省财政厅关于进一步加大政府采购 支持中小企业力度 助力扎实稳住经济 的通知》（浙财采监〔2022〕8号）已分别于2022年1月29日、2022年2月1日和2022年7月1日开始实施，此前有关规定与上述文件内容不一致的，按上述文件要求执行。

 2.根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表:鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政府服务网-政府采购投诉处理-在线办理。

3.供应商认为招标文件使自己的权益受到损害的，可以自获取招标文件之日或者招标文件公告期限届满之日（公告期限届满后获取招标文件的，以公告期限届满之日为准）起7个工作日内，以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

4.其他事项：（1）需要落实的政府采购政策：包括节约资源、保护环境、支持创新、促进中小企业发展等。详见招标文件的第二部分总则。（2）电子招投标的说明：①电子招投标：本项目以数据电文形式，依托“政府采购云平台（www.zcygov.cn）”进行招投标活动，不接受纸质投标文件；②投标准备：注册账号--点击“商家入驻”，进行政府采购供应商资料填写；申领CA数字证书---申领流程详见“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”；安装“政采云电子交易客户端”----前往“浙江政府采购网-下载专区-电子交易客户端”进行下载并安装；③招标文件的获取：使用账号登录或者使用CA登录政采云平台；进入“项目采购”应用，在获取采购文件菜单中选择项目，获取招标文件；④投标文件的制作：在“政采云电子交易客户端”中完成“填写基本信息”、“导入投标文件”、“标书关联”、“标书检查”、“电子签名”、“生成电子标书”等操作；⑤采购人、采购机构将依托政采云平台完成本项目的电子交易活动，平台不接受未按上述方式获取招标文件的供应商进行投标活动； ⑥对未按上述方式获取招标文件的供应商对该文件提出的质疑，采购人或采购代理机构将不予处理；⑦不提供招标文件纸质版；⑧投标文件的传输递交：投标人在投标截止时间前将加密的投标文件上传至政府采购云平台，还可以在投标截止时间前直接提交或者以邮政快递方式递交备份投标文件1份。备份投标文件的制作、存储、密封详见招标文件第二部分第15点—“备份投标文件”；⑨投标文件的解密：投标人按照平台提示和招标文件的规定在半小时内完成在线解密。通过“政府采购云平台”上传递交的投标文件无法按时解密，投标供应商递交了备份投标文件的，以备份投标文件为依据，否则视为投标文件撤回。通过“政府采购云平台”上传递交的投标文件已按时解密的，备份投标文件自动失效。投标人仅提交备份投标文件，未在电子交易平台传输递交投标文件的，投标无效；⑩具体操作指南：详见政采云平台“服务中心-帮助文档-项目采购-操作流程-电子招投标-政府采购项目电子交易管理操作指南-供应商”。（3）招标文件公告期限与招标公告的公告期限一致。

**七、对本次采购提出询问、质疑、投诉，请按以下方式联系**

 1.采购人信息

 名 称：杭州市第七人民医院

 地 址：杭州市天目山路305号

传 真： /

项目联系人（询问）：周易

 项目联系方式（询问）：0571-85126511

 质疑联系人：章俊航

 质疑联系方式：0571-85127350

 2.采购代理机构信息

名 称：浙江豪圣建设项目管理有限公司

地 址：杭州市拱墅区大关路179号远洋国际中心A座17楼1706室

 传 真：/

 项目联系人（询问）：刘先生、曹剑斌、陈敏娇

 项目联系方式（询问）：0571-87981527

 质疑联系人：刘先成

 质疑联系方式：0571-56386096

 3.同级政府采购监督管理部门

 名 称：杭州市财政局政府采购监管处

 地 址：杭州市中河中路152号614办公室

 传 真：0571-89580456

 联系人 ：厉先生

监督投诉电话：0571-89580456

若对项目采购电子交易系统操作有疑问，可登录政采云（https://www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线400-881-7190获取热线服务帮助。

CA问题联系电话（人工）：汇信CA 400-888-4636；天谷CA 400-087-8198。

**第二部分 投标人须知**

**前附表**

| **序号** | **事项** | **本项目的特别规定** |
| --- | --- | --- |
| 1 | **项目属性与核心产品** | [x] A货物类，单一产品或核心产品为： 超融合系统。[ ] B服务类。 |
| 2 | **采购标的对应的中小企业划分标准所属行业** | （1）标的： 超融合系统 ，属于 工业 行业；（2）标的： 服务器负载均衡 ，属于 工业 行；（3）标的： Pacs系统服务器 ，属于 工业 行业；（4）标的： Pacs系统存储 ，属于 工业 行业；（5）标的： 数据库一体机平台 ，属于 工业 行业；（6）标的： 总分院一体化容灾系统节点（分院） ，属于 工业 行业；（7）标的： 总分院一体化容灾存储节点（分院） ，属于 工业 行业；（8）标的： 准入设备 ，属于 工业 行业 ；制造商为 （企业名称）；（9）标的： 虚拟化安全 ，属于 工业 行业；（10）标的： 防病毒设备 ，属于 工业 行业；（11）标的： 数据库审计 ，属于 工业 行业；（12）标的： 桌面管理 ，属于 工业 行业；（13）标的： 堡垒主机设备 ，属于 工业 行业；（14）标的： VPN设备 ，属于 工业 行业；（15）标的： 上网行为管理设备 ，属于 工业 行业；（16）标的： 日志审计设备 ，属于 工业 行业；（17）标的： 态势感知设备 ，属于 工业 行业； |
| 1. 标的： 漏洞扫描设备 ，属于 工业 行业；
2. 标的： 数据库内控管理设备 ，属于 工业 行业；
3. 标的： 信息交换设备 ，属于 工业 行业；
4. 标的： 驻点工程师 ，属于 软件和信息技术服务业 行业；
5. 标的： 台式电脑 ，属于 工业 行业；
6. 标的： 笔记本电脑 ，属于 工业 行业；
7. 标的： 黑白激光打印机（单面） ，属于 工业 行业；
8. 标的： 黑白激光打印机（双面网络） ，属于 工业 行业；
9. 标的： 彩色激光打印机 ，属于 工业 行业；
10. 标的： 多功能一体机 ，属于 工业 行业；
11. 标的： 针式打印机 ，属于 工业 行业；
12. 标的： 热敏打印机（热敏处方） ，属于 工业 行业；
13. 标的： 条码打印机（热敏标签） ，属于 工业 行业；
14. 标的： 立式扫码枪备 ，属于 工业 行业；
15. 标的： 手持扫码枪 ，属于 工业 行业；
16. 标的： 医生PAD ，属于 工业 行业；
17. 标的： 护理PDA ，属于 工业 行业；
18. 标的： 护理移动推车 ，属于 工业 行业；
19. 标的： 床边结算推车 ，属于 工业 行业；
20. 标的： 摄像头 ，属于 工业 行业；
21. 标的： 碎纸机 ，属于 工业 行业；
22. 标的： 复印机 ，属于 工业 行业；
23. 标的： 读卡器（实体插卡） ，属于 工业 行业；
 |
| 1. 标的： 电子卡读卡器 ，属于 工业 行业；
2. 标的： 自助挂号机 ，属于 工业 行业；
3. 标的： 自助检验单打印机 ，属于 工业 行业；
4. 标的： 自助发票打印机 ，属于 工业 行业；
5. 标的： 省专线市医保线路 ，属于 信息传输业 行业；
6. 标的： 视联网线路 ，属于 信息传输业 行业；
7. 标的： 卫生专网线路 ，属于 信息传输业 行业；
8. 标的： 互联网宽带线路 ，属于 信息传输业 行业；
9. 标的： 公众互联网宽带线路 ，属于 信息传输业 行业；
 |
| 3 | **是否允许采购进口产品** | [x] 本项目不允许采购进口产品。[ ] 可以就 采购进口产品。 |
| 4 | **分包** | [x]  A同意将非主体、非关键性的 验收、培训、售后服务 工作分包。[ ]  B不同意分包。注：不得限制大中型企业向小微企业合理分包。 |
| 5 | **开标前答疑会或现场考察** | [x] A不组织。[ ] B组织，时间： ,地点： ，联系人： ，联系方式： 。 |
| 6 | **样品提供** | [x] A不要求提供。[ ] B要求提供，（1）样品： ；（2）样品制作的标准和要求： ；（3）样品的评审方法以及评审标准：详见评标办法；（4）是否需要随样品提交检测报告：[x] 否；[ ] 是，检测机构的要求： ；检测内容： 。（5）提供样品的时间： ；地点： ；联系人： ，联系电话： 。请投标人在上述时间内提供样品并按规定位置安装完毕。超过截止时间的，采购人或采购代理机构将不予接收，并将清场并封闭样品现场。 (6)采购活动结束后，对于未中标人提供的样品，采购人、采购机构将通知未中标人在规定的时间内取回，逾期未取回的，采购人、采购机构不负保管义务；对于中标人提供的样品，采购人将进行保管、封存，并作为履约验收的参考。（7）制作、运输、安装和保管样品所发生的一切费用由投标人自理。 |
| 7 | **方案讲解演示** | [ ] A不组织。[x] **B组织。****（1）演示内容及讲解过程录制视频，总共演示时间不超过5分钟，以.mp4格式，存储于U盘或光盘。演示U盘或光盘以EMS或顺丰邮寄形式在响应文件提交截止时间前递交，演示U盘应当密封包装并在包装上标注演示U盘、项目名称、标项、供应商名称并加盖公章。未按文件要求提供演示U盘造成评审专家无法正常评审的风险由供应商自行承担。（演示U盘或光盘请单独封装），能够清晰展示演示项目内容即可。注：因投标人自身原因导致无法演示或者演示效果不理想的，责任自负。** |
| 8 | **投标人应当提供的资格、资信证明文件** | （1）资格证明文件：见招标文件第二部分11.1。投标人未提供有效的资格证明文件的，视为投标人不具备招标文件中规定的资格要求，投标无效。 |
| （2）资信证明文件：根据招标文件第四部分评标标准提供。 |
| 9 | **节能产品、环境标志产品** | 采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。 |
| 10 | **报价要求** | 有关本项目实施所需的所有费用（含税费）均计入报价。开标一览表（报价表）是报价的唯一载体。投标文件中价格全部采用人民币报价。招标文件未列明，而投标人认为必需的费用也需列入报价。**提醒：验收时检测费用由采购人承担，不包含在投标总价中。****投标报价出现下列情形的，投标无效：****投标文件出现不是唯一的、有选择性投标报价的；****投标报价超过招标文件中规定的预算金额或者最高限价的;****报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，未能按要求提供书面说明或者提交相关证明材料证明其报价合理性的;****投标人对根据修正原则修正后的报价不确认的。** |
| 11 | **中小企业信用融资** | 为支持和促进中小企业发展，进一步发挥政府采购政策功能，杭州市财政局与省银保监局、市地方金融监督管理局、市经信局共同出台了《杭州市政府采购支持中小企业信用融资管理办法》，供应商若有融资意向，详见《政府采购支持中小企业信用融资相关事项通知》，或登录杭州市政府采购网“中小企业信用融资”模块，查看信用融资政策文件及各相关银行服务方案。 |
| 供应商中标后也可在“政采云”平台申请政采贷：操作路径：登录政采云平台 - 金融服务中心 -【融资服务】，可在热门申请中选择产品直接申请，也可点击云智贷匹配适合产品进行申请，或者在可申请项目中根据该项目进行申请。 |
| 12 | **备份投标文件送达地点和签收人员**  | 备份投标文件送达地点：杭州市拱墅区大关路179号远洋国际中心A座17楼1706室 ；备份投标文件签收人员联系电话： 0571-87981527 。**采购人、采购机构不强制或变相强制投标人提交备份投标文件。** |
| 13 | **特别说明** | **联合体或者以分包方式履行合同的，联合体各方（供应商与分包供应商）分别提供与联合体协议（分包意向协议）中规定的分工内容相应的业绩证明材料，业绩数量以提供材料较少的一方为准。** |
| 14 | **招标代理服务费** | **本项目招标代理服务费按计价格[2002]1980号文件规定的取费标准的80%计取，不足2000元时按2000元收取，以中标价为计算基数。由中标人在领取中标通知书时支付给招标代理机构。该费用在投标文件中不单列，由中标人在投标总报价中综合考虑。** |

**一、总则**

**1. 适用范围**

本招标文件适用于该项目的招标、投标、开标、资格审查及信用信息查询、评标、定标、合同、验收等行为（法律、法规另有规定的，从其规定）。

**2.定义**

2.1 “采购人”系指招标公告中载明的本项目的采购人。

2.2 “采购机构”系指招标公告中载明的本项目的采购机构。

2.3 “投标人”系指是指响应招标、参加投标竞争的法人、其他组织或者自然人。

2.4 “负责人”系指法人企业的法定负责人，或其他组织为法律、行政法规规定代表单位行使职权的主要负责人，或自然人本人。

2.5“电子签名”系指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据；“公章”系指单位法定名称章。因特殊原因需要使用冠以法定名称的业务专用章的，投标时须提供《业务专用章使用说明函》（附件4）。

2.6“电子交易平台”是指本项目政府采购活动所依托的政府采购云平台（https://www.zcygov.cn/）。

2.7 “▲” 系指实质性要求条款，“[x] ” 系指适用本项目的要求，“[ ] ” 系指不适用本项目的要求。

**3.** **采购项目需要落实的政府采购政策**

3.1 本项目原则上采购本国生产的货物、工程和服务，不允许采购进口产品。除非采购人采购进口产品，已经在采购活动开始前向财政部门提出申请并获得财政部门审核同意，且在采购需求中明确规定可以采购进口产品（但如果因信息不对称等原因，仍有满足需求的国内产品要求参与采购竞争的，采购人、采购机构不会对其加以限制，仍将按照公平竞争原则实施采购）；优先采购向我国企业转让技术、与我国企业签订消化吸收再创新方案的供应商的进口产品。

3.2 支持绿色发展

3.2.1采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。投标人须按招标文件要求提供相关产品认证证书。▲**采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人未按招标文件要求提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的，投标无效。**

3.2.2 修缮、装修类项目采购建材的，采购人应将绿色建筑和绿色建材性能、指标等作为实质性条件纳入招标文件和合同。

3.2.3为助力打好污染防治攻坚战，推广使用绿色包装，政府采购货物、工程和服务项目中涉及商品包装和快递包装的，供应商提供产品及相关快递服务的具体包装要求要参考《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》。

3.3支持中小企业发展

3.3.1中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。

符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

3.3.2在政府采购活动中，投标人提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

3.3.2.1在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

3.3.2.2在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

3.3.2.3在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

在货物采购项目中，投标人提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

3.3.3对于未预留份额专门面向中小企业的政府采购货物或服务项目，以及预留份额政府采购货物或服务项目中的非预留部分标项，对小型和微型企业的投标报价给予20%的扣除，用扣除后的价格参与评审。接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的政府采购货物或服务项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体或者大中型企业的报价给予6%的扣除，用扣除后的价格参加评审。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

3.3.4符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供《残疾人福利性单位声明函》（附件1）的残疾人福利性单位视同小型、微型企业；

3.3.5符合《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）规定的监狱企业并提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业证明文件的，视同为小型、微型企业。

3.3.6可享受中小企业扶持政策的投标人应按照招标文件格式要求提供《中小企业声明函》，投标人提供的《中小企业声明函》与实际情况不符的，不享受中小企业扶持政策。声明内容不实的，属于提供虚假材料谋取中标、成交的，依法承担法律责任。

3.3.7中小企业享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

3.4支持创新发展

3.4.1 采购人优先采购被认定为首台套产品和“制造精品”的自主创新产品。

3.4.2首台套产品被纳入《首台套产品推广应用指导目录》之日起3年内，以及产品核心技术高于国内领先水平，并具有明晰自主知识产权的“制造精品”产品，自认定之日起2年内视同已具备相应销售业绩，参加政府采购活动时业绩分值为满分。

3.5中小企业信用融资：为支持和促进中小企业发展，进一步发挥政府采购政策功能，杭州市财政局与省银保监局、市金融办、市经信局共同出台了《杭州市政府采购支持中小企业信用融资管理办法》，供应商若有融资意向，详见《政府采购支持中小企业信用融资相关事项通知》，或登录杭州市政府采购网“中小企业信用融资”模块，查看信用融资政策文件及各相关银行服务方案。

3.5平等对待内外资企业和符合条件的破产重整企业

平等对待内外资企业和符合条件的破产重整企业，切实保障企业公平竞争，平等维护企业的合法利益。

**4. 询问、质疑、投诉**

4.1供应商询问

供应商对政府采购活动事项有疑问的，可以提出询问，采购人或者采购代理机构应当在3个工作日内对供应商依法提出的询问作出答复，但答复的内容不得涉及商业秘密。供应商提出的询问超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知供应商向采购人提出。

4.2供应商质疑

4.2.1提出质疑的供应商应当是参与所质疑项目采购活动的供应商。潜在供应商已依法获取其可质疑的招标文件的，可以对该文件提出质疑。

4.2.2供应商认为招标文件、采购过程和中标结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向采购人或者采购机构提出质疑，否则，采购人或者采购机构不予受理：

4.2.2.1对招标文件提出质疑的，质疑期限为供应商获得招标文件之日或者招标文件公告期限届满之日起计算。

4.2.2.2对采购过程提出质疑的，质疑期限为各采购程序环节结束之日起计算。4.2.2.3对采购结果提出质疑的，质疑期限自采购结果公告期限届满之日起计算。

4.2.3供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

　　4.2.3.1供应商的姓名或者名称、地址、邮编、联系人及联系电话；

　　4.2.3.2质疑项目的名称、编号；

　　4.2.3.3具体、明确的质疑事项和与质疑事项相关的请求；

　　4.2.3.4事实依据；

　　4.2.3.5必要的法律依据；

4.2.3.6提出质疑的日期。

供应商提交的质疑函需一式三份。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

质疑函范本及制作说明详见附件2。

4.2.4对同一采购程序环节的质疑，供应商须在法定质疑期内一次性提出。

4.2.5采购人或者采购机构应当在收到供应商的书面质疑后七个工作日内作出答复，并以书面形式通知质疑供应商和其他与质疑处理结果有利害关系的政府采购当事人，但答复的内容不得涉及商业秘密。根据《杭州市财政局关于进一步加强政府采购信息公开优化营商环境的通知》（杭财采监〔2021〕17号）,采购人或者采购机构在质疑回复后5个工作日内，在浙江政府采购网的“其他公告”栏目公开质疑答复，答复内容应当完整。质疑函作为附件上传。

4.2.6询问或者质疑事项可能影响采购结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

4.3供应商投诉

4.3.1质疑供应商对采购人、采购机构的答复不满意或者采购人、采购机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门提出投诉。

4.3.2供应商投诉的事项不得超出已质疑事项的范围，基于质疑答复内容提出的投诉事项除外。

4.3.3供应商投诉应当有明确的请求和必要的证明材料。

4.3.5 以联合体形式参加政府采购活动的，其投诉应当由组成联合体的所有供应商共同提出。

投诉书范本及制作说明详见附件3。

4.4在线质疑、投诉。

根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表；鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政府服务网-政府采购投诉处理-在线办理。

**二、招标文件的构成、澄清、修改**

**5．招标文件的构成**

5.1 招标文件包括下列文件及附件：

5.1.1招标公告；

5.1.2投标人须知；

5.1.3采购需求；

5.1.4评标办法；

5.1.5拟签订的合同文本；

5.1.6应提交的有关格式范例。

5.2与本项目有关的澄清或者修改的内容为招标文件的组成部分。

**6. 招标文件的澄清、修改**

6.1已获取招标文件的潜在投标人，若有问题需要澄清，应于投标截止时间前，以书面形式向采购机构提出。

6.2 采购机构对招标文件进行澄清或修改的，将同时通过电子交易平台通知已获取招标文件的潜在投标人。依法应当公告的，将按规定公告，同时视情况延长投标截止时间和开标时间。该澄清或者修改的内容为招标文件的组成部分。

**三、投标**

**7. 招标文件的获取**

详见招标公告中获取招标文件的时间期限、地点、方式及招标文件售价。

**8.开标前答疑会或现场考察**

采购人组织潜在投标人现场考察或者召开开标前答疑会的，潜在投标人按第二部分投标人须知前附表的规定参加现场考察或者开标前答疑会。

**9.投标保证金**

本项目不需缴纳投标保证金。

**10. 投标文件的语言**

投标文件及投标人与采购有关的来往通知、函件和文件均应使用中文。

**11. 投标文件的组成**

11.1**资格文件**：

11.1.1符合参加政府采购活动应当具备的一般条件的承诺函；

11.1.2落实政府采购政策需满足的资格要求；

11.1.3本项目的特定资格要求。

11.2 商务技术文件：

11.2.1投标函；

11.2.2授权委托书或法定代表人（单位负责人、自然人本人）身份证明；

11.2.3联合协议；

11.2.4分包意向协议；

11.2.5符合性审查资料；

11.2.6评标标准相应的商务技术资料；

11.2.7投标标的清单；

11.2.8商务技术偏离表；

11.2.9政府采购供应商廉洁自律承诺书；

11.3**报价文件：**

11.3.1开标一览表（报价表）；

11.3.2中小企业声明函。

**投标文件含有采购人不能接受的附加条件的，投标无效；**

**投标人提供虚假材料投标的，投标无效。**

**12. 投标文件的编制**

12.1投标文件分为资格文件、商务技术文件、报价文件三部分。各投标人在编制投标文件时请按照招标文件第六部分规定的格式进行，混乱的编排导致投标文件被误读或评标委员会查找不到有效文件是投标人的风险。

12.2投标人进行电子投标应安装客户端软件—“政采云电子交易客户端”，并按照招标文件和电子交易平台的要求编制并加密投标文件。投标人未按规定加密的投标文件，电子交易平台将拒收并提示。

12.3使用“政采云电子交易客户端”需要提前申领CA数字证书，申领流程请自行前往“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”进行查阅。

**13.投标文件的签署、盖章**

13.1投标文件按照招标文件第六部分格式要求进行签署、盖章。**▲投标人的投标文件未按照招标文件要求签署、盖章的，其投标无效**。

13.2为确保网上操作合法、有效和安全，投标人应当在投标截止时间前完成在“政府采购云平台”的身份认证，确保在电子投标过程中能够对相关数据电文进行加密和使用电子签名。

13.3招标文件对投标文件签署、盖章的要求适用于电子签名。

**14. 投标文件的提交、补充、修改、撤回**

14.1 供应商应当在投标截止时间前完成投标文件的传输递交，并可以补充、修改或者撤回投标文件。补充或者修改投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。投标截止时间后递交的投标文件，电子交易平台将拒收。

14.2电子交易平台收到投标文件，将妥善保存并即时向供应商发出确认回执通知。在投标截止时间前，除供应商补充、修改或者撤回投标文件外，任何单位和个人不得解密或提取投标文件。

14.3采购人、采购机构可以视情况延长投标文件提交的截止时间。在上述情况下，采购机构与投标人以前在投标截止期方面的全部权利、责任和义务，将适用于延长至新的投标截止期。

**15.备份投标文件**

 15.1投标人在电子交易平台传输递交投标文件后，还可以在投标截止时间前直接提交或者以邮政快递方式递交备份投标文件1份，**但采购人、采购机构不强制或变相强制投标人提交备份投标文件。**

15.2备份投标文件须在“政采云投标客户端”制作生成，并储存在DVD光盘中。备份投标文件应当密封包装并在包装上加盖公章并注明投标项目名称，投标人名称(联合体投标的，包装物封面需注明联合体投标，并注明联合体成员各方的名称和联合协议中约定的牵头人的名称)。**不符合上述制作、存储、密封规定的备份投标文件将被视为无效或者被拒绝接收。**

15.3直接提交备份投标文件的，投标人应于投标截止时间前在招标公告中载明的开标地点将备份投标文件提交给采购机构，采购机构将拒绝接受逾期送达的备份投标文件。

15.4以邮政快递方式递交备份投标文件的，投标人应先将备份投标文件按要求密封和标记，再进行邮政快递包装后邮寄。备份投标文件须在投标截止时间之前送达招标文件第二部分投标人须知前附表规定的备份投标文件送达地点；送达时间以签收人签收时间为准。采购机构将拒绝接受逾期送达的备份投标文件。邮寄过程中，电子备份投标文件发生泄露、遗失、损坏或延期送达等情况的，由投标人自行负责。

**15.5投标人仅提交备份投标文件，未在电子交易平台传输递交投标文件的，投标无效。**

**16.投标文件的无效处理**

有招标文件第四部分4.2规定的情形之一的，投标无效：

**17.投标有效期**

17.1投标有效期为从提交投标文件的截止之日起90天。▲**投标人的投标文件中承诺的投标有效期少于招标文件中载明的投标有效期的，投标无效。**

17.2投标文件合格投递后，自投标截止日期起，在投标有效期内有效。

17.3在原定投标有效期满之前，如果出现特殊情况，采购机构可以以书面形式通知投标人延长投标有效期。投标人同意延长的，不得要求或被允许修改其投标文件，投标人拒绝延长的，其投标无效。

**四、开标、资格审查与信用信息查询**

**18.开标**

18.1采购机构按照招标文件规定的时间通过电子交易平台组织开标，所有投标人均应当准时在线参加。投标人不足3家的，不得开标。

　18.2开标时，电子交易平台按开标时间自动提取所有投标文件。采购机构依托电子交易平台发起开始解密指令，投标人按照平台提示和招标文件的规定在半小时内完成在线解密。

　18.3**投标文件未按时解密，投标人提供了备份投标文件的，以备份投标文件作为依据，否则视为投标文件撤回。投标文件已按时解密的，备份投标文件自动失效。**

**19、资格审查**

19.1开标后，采购人或采购机构将依法对投标人的资格进行审查。

19.2采购人或采购机构依据法律法规和招标文件的规定，对投标人的基本资格条件、特定资格条件进行审查。

19.3投标人未按照招标文件要求提供与基本资格条件、特定资格条件相应的有效资格证明材料的，视为投标人不具备招标文件中规定的资格要求，其投标无效。

19.4对未通过资格审查的投标人，采购人或采购机构告知其未通过的原因。

19.5合格投标人不足3家的，不再评标。

**20、信用信息查询**

20.1信用信息查询渠道及截止时间：采购机构将通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道查询投标人投标截止时间当天的信用记录。

20.2信用信息查询记录和证据留存的具体方式：现场查询的投标人的信用记录、查询结果经确认后将与采购文件一起存档。

20.3信用信息的使用规则：经查询列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人将被拒绝参与政府采购活动。

20.4联合体信用信息查询：两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

**五、评标**

**21.** 评标委员会将根据招标文件和有关规定，履行评标工作职责，并按照评标方法及评分标准，全面衡量各投标人对招标文件的响应情况。对实质上响应招标文件的投标人，按照评审因素的量化指标排出推荐中标的投标人的先后顺序，并按顺序提出授标建议。**详见招标文件第四部分评标办法。**

**六、定 标**

**22. 确定中标供应商**

政府采购项目实行全流程电子化，评审报告送交、采购结果确定和结果公告均在线完成。为进一步提升采购结果确定效率，采购代理机构应当依法及时将评审报告在线送交采购人。采购单位应当自收到评审报告之日起2个工作日内在线确定中标或者成交供应商。中标、成交通知书和中标、成交结果公告应当在规定时间内同时发出。

**23. 中标通知与中标结果公告**

23.1自中标人确定之日起2个工作日内，采购机构通过电子交易平台向中标人发出中标通知书，同时编制发布采购结果公告。采购机构也可以以纸质形式进行中标通知。

23.2中标结果公告内容包括采购人及其委托的采购机构的名称、地址、联系方式，项目名称和项目编号，中标人名称、地址和中标金额，主要中标标的的名称、规格型号、数量、单价、服务要求，开标记录、未中标情况说明、中标公告期限以及评审专家名单、评分汇总及明细。

23.3公告期限为1个工作日。

**七、合同授予**

**24.** 合同主要条款详见第五部分拟签订的合同文本。

**25. 合同的签订**

25.1 采购人与中标人应当通过电子交易平台在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同，并在签订之日起2个工作日内将政府采购合同在浙江政府采购网上公告。鼓励有条件的采购人视情缩减采购合同签订时限，提高采购效率，杜绝“冷、硬、横、推”等不当行为。除不可抗力等特殊情况外，原则上应当在中标通知书发出之日起10个工作日内，与中标供应商按照采购文件确定的事项签订政府采购合同。

25.2中标人按规定的日期、时间、地点，由法定代表人或其授权代表与采购人代表签订合同。如中标人为联合体的，由联合体成员各方法定代表人或其授权代表与采购人代表签订合同。

25.3如签订合同并生效后，供应商无故拒绝或延期，除按照合同条款处理外，列入不良行为记录一次，并给予通报。

25.4中标供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标或者成交候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。

25.5采购合同由采购人与中标供应商根据招标文件、投标文件等内容通过政府采购电子交易平台在线签订，自动备案。

**26. 履约保证金**

拟签订的合同文本要求中标供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。杭州市政府采购网公布的供应商履约评价为满分的供应商，采购单位应当免收履约保证金。确需收取履约保证金的，履约保证金缴纳最高比例由不超过合同金额的1%。采购单位鼓励供应商采取履约保函形式提供信用保证；供应商提供保函的，采购单位不得拒收。项目验收结束后应及时退还，延迟退还的，应当按照合同约定和法律规定承担相应的赔偿责任。

供应商可登录政采云平台-【金融服务】—【我的项目】—【已备案合同】以保函形式提供：1、供应商在合同列表选择需要投保的合同，点击[保函推荐]。2、在弹框里查看推荐的保函产品，供应商自行选择保函产品，点击[立即申请]。3、在弹框里填写保函申请信息。具体步骤：选择产品—填写供应商信息—选择中标项目—确认信息—等待保险/保函受理—确认保单—支付保费—成功出单。政采云金融专线400-903-9583。

**八、电子交易活动的中止**

2**7. 电子交易活动的中止。**采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购机构可中止电子交易活动：

27.1电子交易平台发生故障而无法登录访问的；

27.2电子交易平台应用或数据库出现错误，不能进行正常操作的；

27.3电子交易平台发现严重安全漏洞，有潜在泄密危险的；

27.4病毒发作导致不能进行正常操作的；

27.5其他无法保证电子交易的公平、公正和安全的情况。

28.出现以上情形，不影响采购公平、公正性的，采购组织机构可以待上述情形消除后继续组织电子交易活动，也可以决定某些环节以纸质形式进行；影响或可能影响采购公平、公正性的，应当重新采购。

**九、验收**

**29.验收**

29.1采购人组织对供应商履约的验收。大型或者复杂的政府采购项目，应当邀请国家认可的质量检测机构参加验收工作。验收方成员应当在验收书上签字，并承担相应的法律责任。如果发现与合同中要求不符，供应商须承担由此发生的一切损失和费用，并接受相应的处理。

29.2采购人可以邀请参加本项目的其他投标人或者第三方机构参与验收。参与验收的投标人或者第三方机构的意见作为验收书的参考资料一并存档。

29.3严格按照采购合同开展履约验收。采购人成立验收小组，按照采购合同的约定对供应商履约情况进行验收。验收时，按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料应当存档备查。

29.4验收合格的项目，采购人将根据采购合同的约定及时向供应商支付采购资金、退还履约保证金。验收不合格的项目，采购人将依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。供应商在履约过程中有政府采购法律法规规定的违法违规情形的，采购人应当及时报告本级财政部门。

**第三部分 采购需求**

**一、项目概况**

杭州市第七人民医院浙西院区即将投入使用，随着医疗业务信息化的不断完善，作为浙江西部三甲精神专科医院，将为浙江西部人民群众提供优质的医疗服务。医院整体的信息化建设必不可少，如何向患者提供高效便捷的服务也成为未来智能化、信息化医院建设的主要方向。

浙西院区按照三级甲等精神专科医院建设，总用地200亩，项目实行整体规划、分批供地、分期实施，项目分二期建设，一期用地127亩，开设床位500张；二期用地73亩，开设300张床位。

项目位于杭州建德市寿昌镇十八桥村郑山自然村区块，一期总建筑面积47478平方米，其中，地上建筑面积35018平方米，地下建筑面积12460平方米。

随着我院浙西院区工程的竣工，新院区即将投入运营，医院面临着第二次创业的大好形势，在这一时期实施医院信息化建设有其重要意义。

**二、设备采购内容**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 单位 | 数量 | 备注 |
| 第一部分：数据中心建设 |
| 1 | 超融合系统 | 详见设备技术要求 | 套 | 1 | 　 |
| 2 | 服务器负载均衡 | 详见设备技术要求 | 套 | 2 | 　 |
| 3 | Pacs系统 | 服务器 | 详见设备技术要求 | 台 | 2 | 　 |
| 4 | 存储 | 详见设备技术要求 | 台 | 1 | 　 |
| 5 | 数据库一体机平台 | 详见设备技术要求 | 套 | 1 | 　 |
| 6 | 总分院一体化容灾系统节点（分院） | 详见设备技术要求 | 套 | 1 | 　 |
| 7 | 总分院一体化容灾存储节点（分院） | 详见设备技术要求 | 套 | 1 | 　 |
| 第二部分：安全建设 |
| 8 | 准入设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 9 | 虚拟化安全 | 详见设备技术要求 | 套 | 1 | 　 |
| 10 | 防病毒设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 11 | 数据库审计 | 详见设备技术要求 | 套 | 1 | 　 |
| 12 | 桌面管理 | 详见设备技术要求 | 套 | 1 | 　 |
| 13 | 堡垒主机设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 14 | VPN设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 15 | 上网行为管理设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 16 | 日志审计设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 17 | 态势感知设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 18 | 漏洞扫描设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 19 | 数据库内控管理设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 20 | 信息交换设备 | 详见设备技术要求 | 套 | 1 | 　 |
| 21 | 驻点工程师 | 详见设备技术要求 | 项 | 1 | 　 |
| 22 | 时间同步服务器 | 详见设备技术要求 | 项 | 1 |  |
| 第三部分：终端 |
| 23 | 台式电脑 | 详见设备技术要求 | 台 | 191 | 　 |
| 24 | 办公软件 | 详见设备技术要求 | 套 | 191 |  |
| 25 | 笔记本电脑 | 详见设备技术要求 | 台 | 3 | 　 |
| 26 | 黑白激光打印机（单面） | 详见设备技术要求 | 台 | 15 | 　 |
| 27 | 黑白激光打印机（双面网络） | 详见设备技术要求 | 台 | 72 | 　 |
| 28 | 彩色激光打印机 | 详见设备技术要求 | 台 | 2 | 　 |
| 29 | 多功能一体机 | 详见设备技术要求 | 台 | 15 | 　 |
| 30 | 针式打印机 | 详见设备技术要求 | 台 | 28 | 　 |
| 31 | 热敏打印机（热敏处方） | 详见设备技术要求 | 台 | 16 | 　 |
| 32 | 条码打印机（热敏标签） | 详见设备技术要求 | 台 | 41 | 　 |
| 33 | 立式扫码枪 | 详见设备技术要求 | 台 | 12 | 　 |
| 34 | 手持扫码枪 | 详见设备技术要求 | 台 | 7 | 　 |
| 35 | 医生PAD | 详见设备技术要求 | 台 | 14 | 　 |
| 36 | 护理PDA | 详见设备技术要求 | 台 | 21 | 　 |
| 37 | 护理移动推车 | 详见设备技术要求 | 台 | 5 | 　 |
| 38 | 床边结算推车 | 详见设备技术要求 | 台 | 1 | 　 |
| 39 | 摄像头 | 详见设备技术要求 | 台 | 35 | 　 |
| 40 | 碎纸机 | 详见设备技术要求 | 台 | 3 | 　 |
| 41 | 复印机 | 详见设备技术要求 | 台 | 2 | 　 |
| 42 | 读卡器（实体插卡） | 详见设备技术要求 | 台 | 55 | 　 |
| 43 | 电子卡读卡器 | 详见设备技术要求 | 台 | 41 | 　 |
| 44 | 自助挂号机 | 详见设备技术要求 | 台 | 10 | 　 |
| 45 | 自助检验单打印机 | 详见设备技术要求 | 台 | 4 | 　 |
| 46 | 自助发票打印机 | 详见设备技术要求 | 台 | 2 | 　 |
| 第四部分：线路 |
| 47 | 省专线市医保线路 | 省专线市医保线路 | 年 | 1 | 　 |
| 48 | 视联网线路 | 视联网线路 | 年 | 1 | 　 |
| 49 | 卫生专网线路 | 卫生专网线路 | 年 | 1 | 　 |
| 50 | 互联网宽带线路 | 50M线路 | 年 | 1 | 　 |
| 51 | 公众互联网宽带线路 | 50M线路 | 年 | 1 | 　 |

## 三、设备技术要求

## A、第一部分

## 3.1超融合系统（核心产品）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 硬件参数要求 | 超融合设备：6台，单台配置如下：CPU≥Gold 6226R 2.9 GHz，CPU个数≥2，内存≥512GB，硬盘要求≥2\*240GB SSD，10\*3.84T SSD，标配盘位数≥12，电源：冗余电源，接口≥6个千兆电口+4个万兆光口，4个万兆光模块。软件要求如下：提供1个授权销售key。包含服务器虚拟化、网络虚拟化、存储虚拟化、云计算管理平台软件授权、安全虚拟化授权各12套。 |
| 虚拟化功能参数 | 冗余性：冗余电源、风扇、控制器、缓存断电保护功能 |
| 虚拟化软件应基于KVM开发，可维护性好，部署时无需绑定安装OpenStack相关组件 |
| 虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，以保障系统平台的安全性 |
| 支持虚拟机的无代理备份，能提供至少100个虚拟机的高性能备份功能，无备份数据容量限制，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复 |
| 支持虚拟机卡死及蓝屏的检测功能并实现自动重启，无需人工干预，减少运维工作量（需提供产品功能截图证明） |
| 支持灵活的告警管理及阈值配置功能，提供告警开关 |
| 支持虚拟机分组视图的功能，管理员可根据部门或者业务类型等将虚拟机划分到不同的目录，进行统一管理 |
| 支持漏洞及版本信息巡检，推送补丁及升级信息，并支持补丁管理、更新、回滚（需提供产品功能截图） |
| 提供热添加CPU、内存、磁盘、网卡的功能，无需中断或停机即可实现虚拟资源的在线添加 |
| 提供集群文件系统功能，通过集群文件系统为虚拟机提供存储资源，允许多个虚机镜像使用同一个虚拟存储卷，简化虚拟机的部署和管理 |
| 主机资源告警项支持主机CPU利用率、主机内存利用率，主机交换分区利用率，主机CPU温度异常，主机网口丢包率，并检测异常状态持续时间；支持主机网关不通，主机网口掉线，主机离线，数据通信口不通的监控告警，用户可自定义告警项并支持通过邮件和短信进行告警（需提供产品功能截图证明） |
| ★支持无代理跨物理主机的虚拟机USB映射，需要使用USB KEY时，无需再虚拟机上安装客户端插件，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的USB资源，对于业务的自适应能力、使用便捷性更佳（需提供产品功能截图证明） |
| 支持以EXCEL表格的方式导出虚拟机的配置信息，包括名称、IP、CPU内存磁盘配置、使用率信息 |
| 当虚拟机Windows、Linux操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性 |
| 支持虚拟机跨集群的虚拟机迁移，支持在不停机的状态下跨集群迁移 |
| 为尽可能保障数据中心断电场景下的业务，支持UPS联动，并在市电断电通过UPS临时供应电量，当UPS电量多低时，按照虚拟机优先级先将不重要的虚拟机进行软关机 |
| 支持设置告警类型（紧急和普通）、告警内容（集群、主机、虚拟机、CPU、内存、磁盘），针对告警信息平台可自动给出告警处理建议，同时支持将告警信息以短信和邮件方式发送给管理员（需提供产品功能截图证明） |
| 每个虚拟机都可以安装独立的操作系统，为获得良好的兼容性操作系统支持需要包括Windows、 Linux，并且支持国产操作系统（包括但不限于：红旗linux、中标麒麟、中标普华、深度linux等） |
| 支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源，确保业务持续高效运行 |
| 支持配置集群动态资源调度功能，系统支持自动评估物理主机的负载情况，当物理主机负载过高时，自动将该物理主机上的虚拟机迁移到其他负载较低的主机上，确保业务持续高效运行和集群主机负载均衡 |
| 支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源，确保业务持续高效运行 |
| 支持UPS QoS（UPS联动），为尽可能保障数据中心断电场景下的业务，可在市电断电时通过UPS临时供应电量，当UPS电量过低时，按照虚拟机优先级先将不重要的虚拟机进行软关机（需提供产品功能截图） |
| 支持虚拟机的无代理备份，能提供至少100个虚拟机的高性能备份功能，无备份数据容量限制，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复 |
| 存储虚拟化 | 支持存储分卷功能，以物理主机为单位划分为不同的存储卷，可将集群内全闪存的磁盘组成一个高性能存储池，满足高性能应用需求，将混闪磁盘组成一个大容量存储池，满足低性能大容量应用需求。所有类型不同性能磁盘均可支持分区，包含NL-SAS，SATA，SSD，SAS等。**（需要投标人对本功能项进行演示，提供演示视频。）** |
| 支持磁盘亚健康监测，包括PCIE SSD寿命告警、硬盘卡、慢的检测和告警、IO错误告警、RAID卡错误告警等。 |
| 故障快速恢复：保障硬盘失效后的故障时间短，快速恢复数据，减少风险； |
| 物理硬件出现故障时业务能够实现自动漂移，保障业务系统快速恢复 |
| 支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性（需提供产品功能截图证明） |
| 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响 |
| 支持多副本冗余功能，支持2个或以上副本，副本互斥地保存在集群的不同节点，当1个或多个主机或者磁盘故障，确保数据依旧正常访问。 |
| 支持数据写入优化机制，将高速SSD作为写缓存，数据先写到SSD，再回写到机械硬盘，提升写IO性能 |
| 在可视化的WEB管理平台上，可以查看虚拟分布式存储对应的容量大小、容量使用率、实时的IOPS读写次数、IOPS读写数据量等信息，方便为IT管理做为有效的决策依据。（需提供产品功能截图证明） |
| 当硬盘寿命到期、硬盘坏道数量过多，硬盘处于亚健康状态时，支持进入磁盘维护模式，在系统隔离硬盘之前，会对数据进行全面的巡检，确保硬盘隔离时业务不受影响。 |
| 为了更好地进行运维，准确识别出接下来会出现坏道的硬盘，支持智能坏道预测，实现故障前预测并处理，规避故障风险（需提供产品功能截图证明）  |
| ★为了便于部署关键业务系统，虚拟存储可支持Oracle RAC，支持共享盘，及共享块设备，支持向导式安装，降低部署复杂度（需提供产品功能截图） |
| 全自动化的分布式存储配置，和虚拟化平台紧密耦合，为虚拟机提供存储资源 |
| 采用分布式的软件定义存储架构，在通用x86服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点；通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out架构），扩容过程保证业务零中断 |
| 支持2个或以上多副本冗余功能，副本互斥地保存在集群的不同节点. 当1个或多个主机或者磁盘故障，确保数据依旧正常访问 |
| 支持对虚拟机业务按照小时/天/周自定义设置定时快照策略，以便业务发生故障时可以快速回滚覆盖原虚拟机或者通过对快照进行克隆的方式生成全新虚拟机，进而恢复至业务健康状态 |
| 支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能 |
| 支持条带化功能，实现分布式raid0的性能提升效果，并且支持以虚拟磁盘为单位设置不同的条带数（需提供产品功能截图证明） |
| 支持多种克隆方式，实现虚拟机秒级启动，可根据需求选择克隆方式，包括节省空间的基于源虚拟机镜像文件生成链接克隆虚拟机；和保证业务高性能的基于源虚拟机镜像文件生成链接克隆虚拟机, 后进行源虚拟机数据的完整拷贝 |
| 支持多种存储配置；磁盘预分配根据业务需求分配固定的物理存储空间、磁盘精简分配根据应用实际写需要时才分配相应的物理存储空间，磁盘动态分配机制根据业务动态需求分配存储资源，实现预分配的高性能和提高磁盘利用率 |
| 为保证集群业务或者oracle rac数据库业务的快照一致性，以便故障时业务可通过快照恢复，支持对虚拟机配置一致性组，对整个一致性组进行快照 |
| 支持坏道扫描功能，由用户设置扫描的时间段定期对集群的硬盘进行扫描，及时发现潜藏的坏道 |
| 为了更好地进行运维，支持智能坏道预测，准确识别出接下来会出现坏道的硬盘，实现故障前预测并处理，规避故障风险 |
| 支持针对卡慢盘、异常只读盘的自动检测、自动隔离及手动隔离，隔离分为临时拔盘、永久拔盘（注：永久拔盘后，需要手动替换磁盘，原有磁盘离线后无法上线），消除磁盘异常对业务的影响（需提供产品功能截图） |
| 支持磁盘亚健康监测，包括PCIE SSD寿命告警、硬盘卡、慢的检测和告警、IO错误告警、RAID卡错误告警等，支持邮件和短信告警 |
| 支持对虚拟机或虚拟磁盘设置不同的缓存QoS能力，区分出高性能虚拟机、普通性能虚拟机和低性能虚拟机 |
| 分布式存储能够提供超高性能，性能随着节点数增加线性增长，能够提供百万级IOPS和12GB/s以上的带宽能力 |
| 支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，且重建速度最快可达30min/TB以上，快速恢复副本的完整性和冗余度，确保用户数据的可靠性和安全性 |
| 支持存储业务网的自动负载均衡功能，自动分流存储业务流量，减轻单点压力 |
| 支持智能预测硬盘寿命，并预估硬盘剩余可使用时间，进行实时预警，提醒用户在寿命到期之前可实现在对业务无影响的情况下安全更换硬盘（需提供产品功能截图证明）  |
| 网络虚拟化 | 通过License激活的方式，实现网络虚拟化功能（虚拟应用负载均衡、虚拟路由器、虚拟应用防火墙、分布式虚拟交换机），支持Vxlan网络和现有的Vlan网络对接，实现虚拟化平台与原有网络的兼容性。 |
| 主动探测业务系统，实时监控业务可用性，监控策略包括SMTP、FTP、POP3、HTTP、自定义端口协议等，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障 |
| 本次配置虚拟路由器100台，虚拟路由器支持HA功能，当虚拟路由器运行的主机出现故障时，保障业务的高可靠性，可以实现故障自动恢复。 |
| 可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上 |
| 支持对Weblogic、sqlserver、oracle数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析 |
| 网络硬件检测（网络可通、网卡掉线、光模块、闪断、网卡） |
| 提供虚拟机报表功能，可以导出TOPN的虚拟机进行1年以内的性能分析与趋势分析报表，可以自定义报表模板 |
| 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、关闭、开启虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。（需提供产品功能截图证明） |
| 支持链路聚合，为网络中的每个虚拟机提供内置的负载均衡能力和网络故障切换，实现更高的硬件可用性和容错能力 |
| 可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上 |
| 支持创建分布式虚拟防火墙，基于虚拟机构建安全防火墙，当虚拟机在不同的物理节点之间迁移时，安全策略随之移动 |
| 提供虚拟路由器、虚拟交换机等设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，方便快速排查问题保障业务的高连续性，并且能够排查到acl策略配置错误等层面。  |
| 云管平台 | 提供统一的镜像管理功能，实现各个可用区上镜像的统一创建和管理，可实现一键快速生成云主机，要求可提供网络设备镜像，方便快速的部署虚拟化安全的组件 |
| 云资源的申请需要通过管理员审批方可使用，云操作系统支持多级审批流程，可以根据用户实际组织进行自定义 |
| 支持业务整体可靠性指标的集中展示，包括业务可靠性、平台可靠性和硬件可靠性，方便管理员能直观地掌握整个数据中心的可靠性状态。（需提供对应大屏展示功能截图） |
| 云平台采用冗余架构设计，避免出现单点故障  |
| 为有效保护客户投资，云安全服务平台需集成于虚拟化平台中，一体化方式交付，无需第三方平台承载，部署运维更便捷 |
| 平台支持模板化的组件部署模式，至少支持等保合规安全模板 |
| ★云计算管理平台，和底层资源池部分的（计算虚拟化、存储虚拟化、网络虚拟化）均为同一厂商品牌提供，并可以支持扩展同一品牌的网络功能虚拟化、虚拟应用防火墙、虚拟应用负载均衡等功能组件，以保障平台的扩展性和兼容性（需提供通过序列号方式扩展产品功能的截图） |
| 支持常见数据库、中间件、大数据平台的一键部署，包括但不限于RabbitMQ、Redis、MongoDB、Kafka、MySQL、CDH等应用的可视化快速部署，可对应用进行参数配置、应用监控、平台告警的全生命周期管理 |
| 支持以可视化的方式展示云平台可靠性，包括硬件可靠性、业务可靠性、平台可靠性三个层面，对CPU、存储、内存、多副本状态、数据重建状态等进行监控，对异常情况进行告警展示，方便管理员掌握云平台的整体情况 |
| 为简化用户运维管理，支持在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备 |
| 支持上传或利用现有云主机创建镜像，可对关联资源池、镜像进行管理、等操作，可通过镜像实现一键快速创建云主机及安全组件 |
| 支持与安全产品联动，实现当发生僵尸网络、挖矿安全事故、勒索病毒时，实现自动隔离中毒云主机，并提供故障前一刻的业务安全状态供恢复，将安全事故损失最小化，也支持将病毒虚拟机进行关机或挂起，避免挖坑云主机消耗整个平台的性能。（需提供产品功能截图） |
| 平台具备独立的日志中心，支持关键安全组件的全量日志审计，支持syslog/WMI接收第三方日志，支持日志统一检索、备份、恢复等操作，支持磁盘按需扩展 |
| 支持创建云主机时设置使用时长，在云主机使用时长到期后可进行延期操作 |
| 安全虚拟化 | 支持安全事件展示，包括勒索病毒，暴力破解，后门等；支持安全事件报表分析；支持按优先级排序展示虚拟机安全状态，包括操作系统、内部应用、安全事件、是否开启防护等，支持搜索筛选；支持安全告警展示；支持安全事件处置记录展示；支持病毒扫描记录展示；支持查看虚拟机安全防护状态 |
| 支持虚拟化平台自动安装agent代理进行虚拟主机防护 |
| 可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率，并提供一键威胁处置  |
| 支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离（需要投标人对本功能项进行演示，提供演示视频。） |
| 提供向导化勒索病毒处理流程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（需提供产品功能截图证明） |
| 支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截（需提供产品功能截图证明） |
| 支持防暴力破解，统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置，支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、最后攻击时间、发现方式、攻击内容、攻击历史  |
| 主机安全防护 | ★配置主机安全防护软件，配置9个虚拟机防护授权许可。主机安全防护软件需要与本超融合系统为同一品牌，提供主机安全防护软件的相关计算机软件著作权登记证书 |
| 采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能  |
| 支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量（需提供产品功能截图证明） |
| 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数 （需提供产品截图证明 ） |
| 支持按“最近7天”、“最近30天”、“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒TOP5排行榜，并展示对应的事件数及终端数  |
| SIP检测到某主机访问僵尸网络恶意域名时，联动EDR定位到该主机上发起恶意域名访问的具体进程、及其进程链信息，并且SIP根据EDR返回的举证信息，联动EDR对恶意进程进行处置（需提供产品功能截图证明） |
| 支持将EDR采集终端资产信息（包括操作系统、硬件、软件、账户、监听端口、运行进程等）上报SIP，并由SIP统一组织主机资产的可视化呈现 |
| 基于对我院有效安全防护和防止勒索病毒的需求，支持与本次购买的下一代网络防火墙进行安全联动，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息（需要投标人对本功能项进行演示，提供演示视频。） |
| 支持管理员在我院现有的网络防火墙管理界面上实现一键隔离指令下发，对终端恶意文件进行隔离，防止病毒进一步扩散（需提供产品功能截图证明） |
| 支持与本院现有的网络防火墙进行情报共享，提供C&C通信检测，对僵尸网络实现联合举证溯源（需提供产品功能截图证明） |
| 支持与上网行为管理平台进行安全联动，支持管理员在上网行为管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息（需提供产品功能截图证明） |
| 支持管理员在上网行为管理平台界面下发一键隔离指令，对终端恶意文件进行隔离，防止病毒进一步扩散（需提供产品功能截图证明） |
| 支持管理员在本院上网行为管理平台界面下发推送指令，对指定网段的终端重定向推送客户端软件，支持自定义重定向的地址（需提供产品功能截图证明） |
| 支持将终端安全软件客户端检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到现有的安全态势感知平台，安全态势感知平台进行分析和展示 （需提供产品功能截图证明） |
| 支持与本院数据中心边界防火墙平台对接，支持在防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息（需提供产品功能截图证明） |
| 关键业务保障 | 为了便于部署关键业务系统，虚拟存储可支持Oracle RAC，支持共享盘，及共享块设备。 |
| 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响。 |
| 支持数据写入优化机制，将高速SSD作为写缓存，数据先写到SSD，再回写到机械硬盘，提升写IO性能。 |
| ★为保证医院核心HIS业务软件的可靠运行，要求云平台厂商具备与业内相关医疗软件厂家的兼容性认证，需要兼容的医疗软件厂家包括但不限于：联众、创业、九阵、海泰、篮网、卫宁等。（需提供产品兼容性认证证书） |

## 3.2服务器负载均衡

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 品牌 | 为保障本院集成平台的兼容性，与本项目超融合系统同一品牌。  |
| 硬件参数 | 规格≥2U，内存大小≥8G，硬盘容量≥240G SSD，冗余电源，接口≥6千兆电口+4千兆光口SFP+2个万兆光口SFP+。 |
| 整机性能 | 4层吞吐量（默认网口）≥15G，并发连接数≥1000万，4层新建连接数 CPS≥35万CPS，7层新建连接数 RPS≥35万CPS。 |
| 设备部署 | 支持串接部署方式和旁路部署方式，支持三角传输模式 |
| 多合一功能集成 | 提供针对多条出口线路的链路负载均衡功能，实现inbound和outbound流量的均衡调度，以及链路之间的冗余互备 |
| 提供针对多站点业务发布的全局负载均衡功能，通过智能DNS等机制实现内外网用户对多个数据中心的最优接入路径选择 |
| 负载均衡算法 | 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、最小流量、加权最小流量、按主机加权最小流量、带宽比例、哈希、主备、首个可用、优先级等算法 |
| 可编程流量控制 | ★通过某种编程语言（如lua）实现自定义的流量编排，对IP、TCP、UDP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作。（投标时提供设备操作界面截图材料) |
| 链路负载均衡 | 支持静态IP和PPPOE两种线路接入方式。（投标时提供设备操作界面截图材料） |
| ★支持基于URL的链路调度功能，内置不少于1000条的国外URL网址库，无需手动导入并支持自动更新，管理员可查看并进行编辑。可根据URL将访问国外网站的请求调度到指定线路。（投标时提供设备操作界面截图材料） |
| ★支持基于域名的流量调度，针对特定网站选择指定的链路转发。（投标时提供设备操作界面截图材料） |
| 服务负载均衡 | 支持源IP、Cookie（插入/被动/改写）、HTTP-Header、SSL Session ID等多种会话保持机制，支持跨虚拟服务的会话保持。（投标时提供设备操作界面截图材料） |
| ★支持银联8583等长连接负载，支持8583单工和双工的区分，对于非HTTP协议的长连接应用，可通过分析议特征来识别消息的开始和截止，以消息为对象进行七层负载均衡，而非传统基于连接的四层负载均衡。（投标时提供设备操作界面截图材料)  |
| ★支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规HTTP应用可配置基于反映URL失效的HTTP响应状态码的观测判断机制，对于复杂应用可配置基于RST关闭连接和零窗口等异常TCP传输行为的观测判断机制。（投标时提供设备操作界面截图材料） |
| 支持主动探测方式与被动观测方式结合使用的服务器健康检查手段，以便适应各种复杂应用交互流程，保障业务系统的高可用性。（投标时提供设备操作界面截图材料） |
| ★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；（投标时提供设备操作界面截图材料） |
| IPv6改造 | IPv6支持双栈模式，支持NAT46、NAT64、NAT66、FTP ALG、DNS64等协议转换 |
| IPv6改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题 |
| 业务交付优化（服务器负载） | 七层虚拟服务支持时间戳、TIME\_WAIT资源快速回收、节点失效关闭连接和重置无效连接功能 |
| ★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。（提供设备操作界面截图材料） |
| 运维管理 | 支持全中文管理界面和HTTPS方式登录、用户角色管理、多级授权管理。 |
| 支持SNMP v1/v2c/v3，标准MIB库和自定义库，可接受第三方网管平台如zabbix的管理（投标时提供设备操作界面截图材料） |

## 3.3 Pacs系统服务器

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 总体要求 | 国产品牌，自主研发，非OEM，适用于通用机房环境，支持标准机柜 |
| 机箱 | 标准2U服务器 |
| ★处理器要求 | 配置2颗CPU，规格不低于Intel® 3rd 6330(28C,205W,2.0GHz)处理器 |
| 内存要求 | 总体要求：最大支持32个内存插槽；支持高级内存纠错（ECC）、内存镜像（Ememory mirroring）、内存热备（rank sparing）等高级功能，最大支持4T内存容量，支持3200MT/s工作频率配置256GB内存；内存类型：支持RDIMM、LRDIMM、BPS内存; |
| 本地存储 | 前置：最大12块3.5英寸硬盘或25块2.5寸硬盘内置：最大4块3.5英寸硬盘及2块TF卡后置：最大4块3.5英寸硬盘+4\*2.5寸硬盘或者10\*2.5寸+2块SATA M.2/E1.s最大支持28个U.2 NVMe硬盘配置硬盘容量：4块480G SSD硬盘 |
| 标准接口 | 4个USB接口，2个VGA接口；1个串口，1个管理口 |
| RAID支持 | 配置RAID卡，缓存1GB以上，支持RAID-0、RAID-1、RAID-5， RAID-6 |
| 网络接口 | 配置2个千兆电口，2个万兆光口（含光模块）；支持OCP3.0网络模块，可不占用标准PCIE插槽，扩展配置高速以太网。 |
| HBA卡 | 双口16G bps HBA卡 |
| ★I/O扩展槽以及扩展模块配置 | 最大支持11个PCIE插槽 |
| 最大支持4个双宽GPU或者8个单宽GPU； 提供官网截图证明 |
| 散热 | 4个热插拔N+1冗余风扇；采用双转子大尺寸风扇，支持免工具热插拔维护。风扇转速自动调节，对节点透明；风流向前进后出；具备防回流设计 |
| 电源模块 | 两个冗余热插拔高效电源; 支持-48V / 336V直流电源 |
| 管理功能 | 板载BMC管理模块，支持带外和带内远程管理控制，如IPMI2.0、KVM Over IP、SOL、SNMP等，可实现与操作系统无关的远程对服务器的完全控制。管理软件支持同时部署多台主机或按照计划时间进行特定部署，可监控服务器CPU、内存等资源使用率，批量日志收集等。支持中文BIOS界面设置，支持TPM/TCM安全模块，支持带内和带外安全管理。 |
| ★系统安全保护 | 支持系统安全加固模块，支持主机操作系统安全加固功能模块扩展，从系统内核层对服务器进行安全加固规则配置。具有windows的兼容性认证证书。符合公安部等级保护三级技术要求。提升操作系统的安全等级，免除因操作系统漏洞带来的安全问题，操作系统可免疫已知、未知病毒及黑客的攻击。支持Windows、linux、AIX、Solaris等相关操作系统平台。（以上提供证明） |
| 安全认证 | 保证信息安全，并有效降低用户隐私及安全风险，要求制造商对信息安全、数据合规、隐私安全建立了安全控制体系。 |
| 静电防护标准 | 保证服务器生产、检测和仓储管理标准化，减少静电放电对设备的不良影响，提高产品质量和可靠性。 |

## 3.4 Pacs系统存储

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 控制器 | 多控制器架构，SAN+NAS架构采用SAN和NAS统一集成的控制器架构，统一管理；（具备FC/IP SAN和NAS融合组网能力）；控制器扩展能力≥16 |
| 本次配置控制器数量≥2；控制器冗余设计，支持在线更换控制器；在线升级存储系统，无须停机，具备控制器故障自动切换和自动重建功能，无单点故障影响数据的有效性； |
| 配置16Gb FC主机接口≥8个；10G iSCSI主机端口≥4个；1G iSCSI主机端口≥8个 |
| 支持三种2U12/2U25/3U48控制柜（或两种以上规格），支持2.5寸，3.5寸硬盘混插；提供官网截图本次配置 2U25机箱 |
| 双控配置4个12Gbps SAS3.0磁盘接口,双控可扩展到12个12Gbps SAS3.0磁盘接口，双控磁盘通道速率≥768Gb，集群最大支持48个磁盘接口。 |
| 支持缓存保护，并配置BBU电池保护模组，保证掉电时Cache数据可安全写入Flash或硬盘永久保存，实现无限时断电保护Cache数据的目的。 |
| 缓存 | 双控配置高速缓存≥128GB，集群最大可支持2T高速缓存（缓存不包含SSD磁盘、PCI-E SSD、闪存、压缩或重删缓存和NAS控制器缓存） |
| 硬盘 | 同时支持SSD、SAS、NL-SAS硬盘 |
| 所有磁盘可同时配置为RAID0/1/5/6/10/50/60，且可共存。支持两种RAID技术，且可以共存 |
| 配置4块1.92T SSD硬盘，21个1.2T 10k HDD硬盘 |
| 基础管理平台 | 图形界面管理软件，支持多种语言（至少包括简体中文和英文），支持多台设备集中管理，支持存储资源管理分析和资源使用历史记录分析，支持性能管理等功能，支持WEB管理，支持CLI管理。支持多种事件通知功能 |
| 高级软件特性 | 配置全容量许可精简功能，实现存储空间超分配，精简粒度32K、64K、128K、256K可调节，后续扩容无需额外购买许可，支持创建单卷≥256TB的容量 |
| 配置全容量许可的克隆功能，后续扩容无需额外购买许可。 |
| 配置全容量许可快照功能，有效预防各种软故障的发生，快照无需预留空间，后续扩容无需额外购买许可。 |
| 配置全容量许可卷备份功能，有效预防各种软故障的发生，无需预留空间，后续扩容无需额外购买许可。 |
| 配置存储QoS授权许可，支持单卷的IOPS、Bandwidth的限制设定， |
| 配置卷镜像功能，可实现存储内部，或者不同存储之间的数据同步功能，当其中一个卷离线时，可实现业务无中断，后续扩容无需额外购买许可。 |
| 支持SSD作为缓存进行业务加速特性，可支持配置最少1块SSD实现加速功能 |
| 支持全容量许可的存储自动分层功能，可实现四层数据分层，系统自动将动态热点数据提升至高速盘中，以解决动态数据热点的性能问题，后续扩容无需额外购买许可 |
| 全面的企业级容灾功能，包含同步、异步周期和异步复制三种模式，支持3DC远程复制组网模式 |
| Active-Active模式双活架构，主机端的LUN多路径为全Active状态，支持双活功能 |
| 支持存储虚拟化功能，可以整合异构厂商的存储阵列，通过虚拟化功能将存储资源统一管理和分配；接管异构存储厂商的空间后，可以把异构空间作为存储的RAID资源池，并且资源池可以划分多个卷对主机提供存储服务 |
| 配置NAS文件服务授权 |
| 兼容性 | Windows、Linux、VMware、UNIX (HP-UX、AIX、Solaris、K-UX等),支持中标麒麟系统  |
| 支持达梦数据库、神州通用数据库、人大金仓，并提供证明 |
| 支持阿里云、OpenStack Cinder对接能力 |
| ★能力要求 | SPC-1 实测IOPS≥270万（需提供SPC-1官网截图和SPC-1官网链接） |
| 厂商资质 | 保证信息安全，并有效降低用户隐私及安全风险，要求制造商对信息安全、数据合规、隐私安全建立了安全控制体系。 |
| 保证产品生产、检测和仓储管理标准化，减少静电放电对设备的不良影响，提高产品质量和可靠性。 |

## 3.5数据库一体机平台

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 硬件参数要求 | 超融合设备：3台，单台配置如下：CPU≥Gold 6248R 3.0 GHz（24C），CPU个数≥2，内存≥256GB，硬盘要求≥2\*240GB SSD，4\*3.2T NVME SSD，标配盘位数≥12，电源：冗余电源，接口≥6个千兆电口+4个万兆光口，自带万兆光模块。软件要求如下：提供1个授权销售key。包含服务器虚拟化、网络虚拟化、存储虚拟化、云计算管理平台软件授权、安全虚拟化授权各6套，数据库承载管理平台不少于1套，数据库容灾备份不少于30套授权许可。 |
| 其他品牌资质 | ★投标虚拟化产品要求提供第三方测试机构出具的虚拟化软件功能测试报告，为保证第三方测试机构的权威性，要求测试机构具有中国合格评定国家认可委员会（CNAS）实验室认可证书。 |
| 虚拟化功能参数 | 冗余性：冗余电源、风扇、控制器、缓存断电保护功能 |
| 虚拟化软件应基于KVM开发，可维护性好，部署时无需绑定安装OpenStack相关组件 |
| 虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，以保障系统平台的安全性 |
| 支持虚拟机的无代理备份，能提供至少100个虚拟机的高性能备份功能，无备份数据容量限制，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复 |
| 支持虚拟机卡死及蓝屏的检测功能并实现自动重启，无需人工干预，减少运维工作量（需提供产品功能截图证明并加盖公章） |
| 支持灵活的告警管理及阈值配置功能，提供告警开关 |
| 支持虚拟机分组视图的功能，管理员可根据部门或者业务类型等将虚拟机划分到不同的目录，进行统一管理 |
| ★支持漏洞及版本信息巡检，推送补丁及升级信息，并支持补丁管理、更新、回滚（需提供产品功能截图） |
| 提供热添加CPU、内存、磁盘、网卡的功能，无需中断或停机即可实现虚拟资源的在线添加 |
| 提供集群文件系统功能，通过集群文件系统为虚拟机提供存储资源，允许多个虚机镜像使用同一个虚拟存储卷，简化虚拟机的部署和管理 |
| 主机资源告警项支持主机CPU利用率、主机内存利用率，主机交换分区利用率，主机CPU温度异常，主机网口丢包率，并检测异常状态持续时间；支持主机网关不通，主机网口掉线，主机离线，数据通信口不通的监控告警，用户可自定义告警项并支持通过邮件和短信进行告警（需提供产品功能截图证明并加盖公章） |
| ★支持无代理跨物理主机的虚拟机USB映射，需要使用USB KEY时，无需再虚拟机上安装客户端插件，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的USB资源，对于业务的自适应能力、使用便捷性更佳（需提供产品功能截图证明并加盖公章） |
| 支持以EXCEL表格的方式导出虚拟机的配置信息，包括名称、IP、CPU内存磁盘配置、使用率信息 |
| 当虚拟机Windows、Linux操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性 |
| 支持虚拟机跨集群的虚拟机迁移，支持在不停机的状态下跨集群迁移 |
| 为尽可能保障数据中心断电场景下的业务，支持UPS联动，并在市电断电通过UPS临时供应电量，当UPS电量多低时，按照虚拟机优先级先将不重要的虚拟机进行软关机 |
| ★支持设置告警类型（紧急和普通）、告警内容（集群、主机、虚拟机、CPU、内存、磁盘），针对告警信息平台可自动给出告警处理建议，同时支持将告警信息以短信和邮件方式发送给管理员（需提供产品功能截图证明并加盖公章） |
| 每个虚拟机都可以安装独立的操作系统，为获得良好的兼容性操作系统支持需要包括Windows、 Linux，并且支持国产操作系统包括：红旗linux、中标麒麟、中标普华、深度linux等 |
| 支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源，确保业务持续高效运行 |
| 支持配置集群动态资源调度功能，系统支持自动评估物理主机的负载情况，当物理主机负载过高时，自动将该物理主机上的虚拟机迁移到其他负载较低的主机上，确保业务持续高效运行和集群主机负载均衡 |
| 支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源，确保业务持续高效运行 |
| ★支持UPS QoS（UPS联动），为尽可能保障数据中心断电场景下的业务，可在市电断电时通过UPS临时供应电量，当UPS电量过低时，按照虚拟机优先级先将不重要的虚拟机进行软关机（需提供产品功能截图） |
| 支持虚拟机的无代理备份，能提供至少100个虚拟机的高性能备份功能，无备份数据容量限制，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复 |
| 存储虚拟化 | ★支持存储分卷功能，以物理主机为单位划分为不同的存储卷，可将集群内全闪存的磁盘组成一个高性能存储池，满足高性能应用需求，将混闪磁盘组成一个大容量存储池，满足低性能大容量应用需求。所有类型不同性能磁盘均可支持分区，包含NL-SAS，SATA，SSD，SAS等。（需提供产品功能截图证明并加盖公章） |
| 支持磁盘亚健康监测，包括PCIE SSD寿命告警、硬盘卡、慢的检测和告警、IO错误告警、RAID卡错误告警等。 |
| 故障快速恢复：保障硬盘失效后的故障时间短，快速恢复数据，减少风险； |
| 物理硬件出现故障时业务能够实现自动漂移，保障业务系统快速恢复 |
| ★支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性（需提供产品功能截图证明并加盖公章） |
| 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响 |
| 支持多副本冗余功能，支持2个或以上副本，副本互斥地保存在集群的不同节点，当1个或多个主机或者磁盘故障，确保数据依旧正常访问。 |
| 支持数据写入优化机制，将高速SSD作为写缓存，数据先写到SSD，再回写到机械硬盘，提升写IO性能 |
| 在可视化的WEB管理平台上，可以查看虚拟分布式存储对应的容量大小、容量使用率、实时的IOPS读写次数、IOPS读写数据量等信息，方便为IT管理做为有效的决策依据。（需提供产品功能截图证明并加盖公章） |
| 当硬盘寿命到期、硬盘坏道数量过多，硬盘处于亚健康状态时，支持进入磁盘维护模式，在系统隔离硬盘之前，会对数据进行全面的巡检，确保硬盘隔离时业务不受影响。 |
| 为了更好地进行运维，准确识别出接下来会出现坏道的硬盘，支持智能坏道预测，实现故障前预测并处理，规避故障风险（需提供产品功能截图证明并加盖公章）  |
| ★为了便于部署关键业务系统，虚拟存储可支持Oracle RAC，支持共享盘，及共享块设备，支持向导式安装，降低部署复杂度（需提供产品功能截图） |
| 全自动化的分布式存储配置，和虚拟化平台紧密耦合，为虚拟机提供存储资源 |
| 采用分布式的软件定义存储架构，在通用x86服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点；通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out架构），扩容过程保证业务零中断 |
| 支持2个或以上多副本冗余功能，副本互斥地保存在集群的不同节点. 当1个或多个主机或者磁盘故障，确保数据依旧正常访问 |
| 支持对虚拟机业务按照小时/天/周自定义设置定时快照策略，以便业务发生故障时可以快速回滚覆盖原虚拟机或者通过对快照进行克隆的方式生成全新虚拟机，进而恢复至业务健康状态 |
| 支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能 |
| ★支持条带化功能，实现分布式raid0的性能提升效果，并且支持以虚拟磁盘为单位设置不同的条带数（需提供产品功能截图证明并加盖公章） |
| 支持多种克隆方式，实现虚拟机秒级启动，可根据需求选择克隆方式，包括节省空间的基于源虚拟机镜像文件生成链接克隆虚拟机；和保证业务高性能的基于源虚拟机镜像文件生成链接克隆虚拟机， 后进行源虚拟机数据的完整拷贝 |
| 支持多种存储配置；磁盘预分配根据业务需求分配固定的物理存储空间、磁盘精简分配根据应用实际写需要时才分配相应的物理存储空间，磁盘动态分配机制根据业务动态需求分配存储资源，实现预分配的高性能和提高磁盘利用率 |
| 为保证集群业务或者oracle rac数据库业务的快照一致性，以便故障时业务可通过快照恢复，支持对虚拟机配置一致性组，对整个一致性组进行快照 |
| 支持坏道扫描功能，由用户设置扫描的时间段定期对集群的硬盘进行扫描，及时发现潜藏的坏道 |
| 为了更好地进行运维，支持智能坏道预测，准确识别出接下来会出现坏道的硬盘，实现故障前预测并处理，规避故障风险 |
| ★支持针对卡慢盘、异常只读盘的自动检测、自动隔离及手动隔离，隔离分为临时拔盘、永久拔盘（注：永久拔盘后，需要手动替换磁盘，原有磁盘离线后无法上线），消除磁盘异常对业务的影响（需提供产品功能截图） |
| 支持磁盘亚健康监测，包括PCIE SSD寿命告警、硬盘卡、慢的检测和告警、IO错误告警、RAID卡错误告警等，支持邮件和短信告警 |
| 支持对虚拟机或虚拟磁盘设置不同的缓存QoS能力，区分出高性能虚拟机、普通性能虚拟机和低性能虚拟机 |
| 分布式存储能够提供超高性能，性能随着节点数增加线性增长，能够提供百万级IOPS和12GB/s以上的带宽能力 |
| 支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，且重建速度最快可达30min/TB以上，快速恢复副本的完整性和冗余度，确保用户数据的可靠性和安全性 |
| 支持存储业务网的自动负载均衡功能，自动分流存储业务流量，减轻单点压力 |
| 支持智能预测硬盘寿命，并预估硬盘剩余可使用时间，进行实时预警，提醒用户在寿命到期之前可实现在对业务无影响的情况下安全更换硬盘（需提供产品功能截图证明并加盖公章）  |
| 网络虚拟化 | 通过License激活的方式，实现网络虚拟化功能（虚拟应用负载均衡、虚拟路由器、虚拟应用防火墙、分布式虚拟交换机），支持Vxlan网络和现有的Vlan网络对接，实现虚拟化平台与原有网络的兼容性。 |
| 主动探测业务系统，实时监控业务可用性，监控策略包括SMTP、FTP、POP3、HTTP、自定义端口协议等，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障 |
| 本次配置虚拟路由器100台，虚拟路由器支持HA功能，当虚拟路由器运行的主机出现故障时，保障业务的高可靠性，可以实现故障自动恢复。 |
| 可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上 |
| 支持对Weblogic、sqlserver、oracle数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析 |
| 网络硬件检测（网络可通、网卡掉线、光模块、闪断、网卡） |
| 提供虚拟机报表功能，可以导出TOPN的虚拟机进行1年以内的性能分析与趋势分析报表，可以自定义报表模板 |
| 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、关闭、开启虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。（需提供产品功能截图证明并加盖公章） |
| 支持链路聚合，为网络中的每个虚拟机提供内置的负载均衡能力和网络故障切换，实现更高的硬件可用性和容错能力 |
| 可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上 |
| 支持创建分布式虚拟防火墙，基于虚拟机构建安全防火墙，当虚拟机在不同的物理节点之间迁移时，安全策略随之移动 |
| 提供虚拟路由器、虚拟交换机等设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，方便快速排查问题保障业务的高连续性，并且能够排查到acl策略配置错误等层面。  |
| 云管平台 | 提供统一的镜像管理功能，实现各个可用区上镜像的统一创建和管理，可实现一键快速生成云主机，要求可提供网络设备镜像，方便快速的部署虚拟化安全的组件 |
| 云资源的申请需要通过管理员审批方可使用，云操作系统支持多级审批流程，可以根据用户实际组织进行自定义 |
| 支持业务整体可靠性指标的集中展示，包括业务可靠性、平台可靠性和硬件可靠性，方便管理员能直观地掌握整个数据中心的可靠性状态。（需提供对应大屏展示功能截图并加盖公章） |
| 云平台采用冗余架构设计，避免出现单点故障  |
| 为有效保护客户投资，云安全服务平台需集成于虚拟化平台中，一体化方式交付，无需第三方平台承载，部署运维更便捷 |
| 平台支持模板化的组件部署模式，至少支持等保合规安全模板 |
| ★云计算管理平台，和底层资源池部分的（计算虚拟化、存储虚拟化、网络虚拟化）均为同一厂商品牌提供，并可以支持扩展同一品牌的网络功能虚拟化、虚拟应用防火墙、虚拟应用负载均衡等功能组件，以保障平台的扩展性和兼容性（需提供通过序列号方式扩展产品功能的截图） |
| 支持常见数据库、中间件、大数据平台的一键部署，包括但不限于RabbitMQ、Redis、MongoDB、Kafka、MySQL、CDH等应用的可视化快速部署，可对应用进行参数配置、应用监控、平台告警的全生命周期管理 |
| 支持以可视化的方式展示云平台可靠性，包括硬件可靠性、业务可靠性、平台可靠性三个层面，对CPU、存储、内存、多副本状态、数据重建状态等进行监控，对异常情况进行告警展示，方便管理员掌握云平台的整体情况 |
| 为简化用户运维管理，支持在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备 |
| 支持上传或利用现有云主机创建镜像，可对关联资源池、镜像进行管理、等操作，可通过镜像实现一键快速创建云主机及安全组件 |
| ★支持与安全产品联动，实现当发生僵尸网络、挖矿安全事故、勒索病毒时，实现自动隔离中毒云主机，并提供故障前一刻的业务安全状态供恢复，将安全事故损失最小化，也支持将病毒虚拟机进行关机或挂起，避免挖坑云主机消耗整个平台的性能。（需提供产品功能截图） |
| 平台具备独立的日志中心，支持关键安全组件的全量日志审计，支持syslog/WMI接收第三方日志，支持日志统一检索、备份、恢复等操作，支持磁盘按需扩展 |
| 支持创建云主机时设置使用时长，在云主机使用时长到期后可进行延期操作 |
| 安全虚拟化 | 支持安全事件展示，包括勒索病毒，暴力破解，后门等；支持安全事件报表分析；支持按优先级排序展示虚拟机安全状态，包括操作系统、内部应用、安全事件、是否开启防护等，支持搜索筛选；支持安全告警展示；支持安全事件处置记录展示；支持病毒扫描记录展示；支持查看虚拟机安全防护状态 |
| 支持虚拟化平台自动安装agent代理进行虚拟主机防护 |
| 可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率，并提供一键威胁处置  |
| ★支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离（需提供产品功能截图证明）  |
| ★提供向导化勒索病毒处理流程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（需提供产品功能截图证明） |
| ★支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截 |
| 支持防暴力破解，统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置，支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、最后攻击时间、发现方式、攻击内容、攻击历史  |
| 主机安全防护 | ★配置主机安全防护软件，配置100个虚拟机防护授权许可。主机安全防护软件需要与本超融合系统为同一品牌，提供主机安全防护软件的计算机软件著作权登记证书 |
| 采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能  |
| 支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量（需提供产品功能截图证明） |
| 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数 （需提供产品截图证明 ） |
| 支持按“最近7天”、“最近30天”、“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒TOP5排行榜，并展示对应的事件数及终端数  |
| SIP检测到某主机访问僵尸网络恶意域名时，联动EDR定位到该主机上发起恶意域名访问的具体进程、及其进程链信息，并且SIP根据EDR返回的举证信息，联动EDR对恶意进程进行处置（需提供产品功能截图证明） |
| 支持将EDR采集终端资产信息（包括操作系统、硬件、软件、账户、监听端口、运行进程等）上报SIP，并由SIP统一组织主机资产的可视化呈现 |
| ★基于对我院有效安全防护和防止勒索病毒的需求，支持与本次购买的下一代网络防火墙进行安全联动，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息（需提供产品功能截图证明） |
| ★支持管理员在我院现有的网络防火墙管理界面上实现一键隔离指令下发，对终端恶意文件进行隔离，防止病毒进一步扩散（需提供产品功能截图证明） |
| 支持与本院现有的网络防火墙进行情报共享，提供C&C通信检测，对僵尸网络实现联合举证溯源（需提供产品功能截图证明） |
| ★支持与同厂商的上网行为管理平台进行安全联动，支持管理员在上网行为管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息（需提供产品功能截图证明） |
| 支持管理员在同厂商的上网行为管理平台界面下发一键隔离指令，对终端恶意文件进行隔离，防止病毒进一步扩散（需提供产品功能截图证明） |
| 支持管理员在本次购买的上网行为管理平台界面下发推送指令，对指定网段的终端重定向推送客户端软件，支持自定义重定向的地址（需提供产品功能截图证明） |
| 支持将终端安全软件客户端检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到现有的安全态势感知平台，安全态势感知平台进行分析和展示 （需提供产品功能截图证明） |
| 支持与本次购买的数据中心边界防火墙平台对接，支持在防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息（需提供产品功能截图证明） |
| 数据库承载管理平台 | 为保障数据库稳定运行及数据库容灾效果，要求数据库承载管理平台与数据库一体机同一品牌，提供软件著作权登记证书 |
| 支持开源数据库MySQL的自动化部署，实现开箱即用的RDS能力 |
| 支持MySQL 5.7 版本，单机架构和一主一从架构 |
| 支持自定义编辑MySQL访问IP和端口（需提供产品功能截图证明） |
| 主从架构下，主数据库故障可以自动进行主从切换和故障自愈，实现自动化运维能力 |
| 单机和主从故障情况下，提供数据库故障自愈能力，将故障节点拉起；主从架构还可自动修复故障节点并加回集群中实现节点冗余度不变（需提供产品功能截图证明） |
| 支持从备份文件恢复某个时间点的数据，支持备份文件直接恢复为数据库。恢复完成验证可用性验证后可以替换原有业务作为生产业务（需提供产品功能截图证明） |
| 支持Oracle 11g的Oracle和RAC架构 |
| 支持Oracle单机和RAC的自动化部署，实现开箱即用的RDS能力 |
| 支持自定义编辑Oracle访问IP，包括RAC的SCAN IP，单机的VIP、Public IP（需提供产品功能截图证明） |
| 单机和RAC集群故障情况下，提供数据库故障自愈能力，将故障节点拉起；RAC可自动修复故障节点并加回集群中实现节点冗余度不变（需提供产品功能截图证明） |
| DMP经典网络模式下，支持针对Oracle单机、RAC向导式自动化创建DG备库来搭建数据库主备容灾系统 |
| DG支持配置最大性能模式、最大保护模式、最大可用模式，主备库同架构（单机->单机，RAC->RAC），支持跨资源池创建DG备库 |
| 支持页面一键进行主备切换，适用于容灾演练场景；支持一键式故障转移，应对真实的故障场景 |
| 支持数据库的拓扑监控，实时可视化查看数据库集群各个节点的健康情况（需提供产品功能截图证明） |
| 支持数据库一键诊断，可覆盖资源、会话、锁、性能分析，方便一键掌握数据库基本状况，发现异常问题 |
| 支持手动巡检与自动巡检，并生成巡检报告，巡检报告可提供健康评分（需提供产品功能截图证明） |
| 支持SQL Server单机和HA的自动化部署，实现开箱即用的RDS能力 |
| 主备架构下，数据库主备的运行位置支持互斥，默认分布在不同的物理主机上，以避免单主机故障导致的数据库主备故障 |
| 单机和主备故障情况下，提供数据库故障自愈能力，将故障节点拉起（需提供产品功能截图证明） |
| 支持Oracle11g数据库的数据迁移，包括单机与单机之间、单机与RAC之间、RAC与RAC之间的数据均可以执行迁移 |
| Oracle支持全量数据迁移，将源库的数据和表结构完整迁移至目标库，适用于整库或整表迁移场景 |
| 支持对迁移任务进行预检查，以便在执行迁移任务前对配置项进行确认、排错，提升迁移任务成功率。 |
| 为平台管理员、租户提供自服务门户，租户可通过自服务门户申请、使用数据库，平台管理员通过管理门户进行数据库统一管理运维 |
| 关键业务保障 | 为了便于部署关键业务系统，虚拟存储可支持Oracle RAC，支持共享盘，及共享块设备。 |
| 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响。 |
| 支持数据写入优化机制，将高速SSD作为写缓存，数据先写到SSD，再回写到机械硬盘，提升写IO性能。 |
| ★为保证医院核心业务软件的可靠运行，要求云平台厂商具备与业内相关医疗软件厂家的兼容性认证，需要兼容的医疗软件厂家包括但不限于：联众、创业、九阵、海泰、篮网、卫宁等。（需提供产品兼容性认证证书） |

## 3.6总分院一体化容灾系统节点（分院）

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 硬件服务器参数要求 | 超融合设备：3台，单台配置如下：CPU≥Gold 6226R 2.9 GHz，CPU个数≥2，内存≥512GB，硬盘要求≥2\*240GB SSD，8\*1.92T SSD，标配盘位数≥12，电源：冗余电源，接口≥6个千兆电口+2个万兆光口，自带万兆光模块。软件要求如下：提供1个授权销售key。包含服务器虚拟化、网络虚拟化、存储虚拟化、云计算管理平台软件授权、安全虚拟化授权各6套。 |
| 其他品牌资质 | ★投标虚拟化产品要求提供第三方测试机构出具的虚拟化软件功能测试报告，为保证第三方测试机构的权威性，要求测试机构具有中国合格评定国家认可委员会（CNAS）实验室认可证书。 |
| 虚拟化功能参数 | 冗余性：冗余电源、风扇、控制器、缓存断电保护功能 |
| 虚拟化软件应基于KVM开发，可维护性好，部署时无需绑定安装OpenStack相关组件 |
| 虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，以保障系统平台的安全性 |
| 支持虚拟机的无代理备份，能提供至少100个虚拟机的高性能备份功能，无备份数据容量限制，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复 |
| 支持虚拟机卡死及蓝屏的检测功能并实现自动重启，无需人工干预，减少运维工作量（需提供产品功能截图证明并加盖公章） |
| 支持灵活的告警管理及阈值配置功能，提供告警开关 |
| 支持虚拟机分组视图的功能，管理员可根据部门或者业务类型等将虚拟机划分到不同的目录，进行统一管理 |
| ★支持漏洞及版本信息巡检，推送补丁及升级信息，并支持补丁管理、更新、回滚（需提供产品功能截图） |
| 提供热添加CPU、内存、磁盘、网卡的功能，无需中断或停机即可实现虚拟资源的在线添加 |
| 提供集群文件系统功能，通过集群文件系统为虚拟机提供存储资源，允许多个虚机镜像使用同一个虚拟存储卷，简化虚拟机的部署和管理 |
| 主机资源告警项支持主机CPU利用率、主机内存利用率，主机交换分区利用率，主机CPU温度异常，主机网口丢包率，并检测异常状态持续时间；支持主机网关不通，主机网口掉线，主机离线，数据通信口不通的监控告警，用户可自定义告警项并支持通过邮件和短信进行告警（需提供产品功能截图证明并加盖公章） |
| ★支持无代理跨物理主机的虚拟机USB映射，需要使用USB KEY时，无需再虚拟机上安装客户端插件，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的USB资源，对于业务的自适应能力、使用便捷性更佳（需提供产品功能截图证明并加盖公章） |
| 支持以EXCEL表格的方式导出虚拟机的配置信息，包括名称、IP、CPU内存磁盘配置、使用率信息 |
| 当虚拟机Windows、Linux操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性 |
| 支持虚拟机跨集群的虚拟机迁移，支持在不停机的状态下跨集群迁移 |
| 为尽可能保障数据中心断电场景下的业务，支持UPS联动，并在市电断电通过UPS临时供应电量，当UPS电量多低时，按照虚拟机优先级先将不重要的虚拟机进行软关机 |
| 支持设置告警类型（紧急和普通）、告警内容（集群、主机、虚拟机、CPU、内存、磁盘），针对告警信息平台可自动给出告警处理建议，同时支持将告警信息以短信和邮件方式发送给管理员（需提供产品功能截图证明并加盖公章） |
| 每个虚拟机都可以安装独立的操作系统，为获得良好的兼容性操作系统支持需要包括Windows、 Linux，并且支持国产操作系统包括：红旗linux、中标麒麟、中标普华、深度linux等 |
| 支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源，确保业务持续高效运行 |
| 支持配置集群动态资源调度功能，系统支持自动评估物理主机的负载情况，当物理主机负载过高时，自动将该物理主机上的虚拟机迁移到其他负载较低的主机上，确保业务持续高效运行和集群主机负载均衡 |
| 支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源，确保业务持续高效运行 |
| ★支持UPS QoS（UPS联动），为尽可能保障数据中心断电场景下的业务，可在市电断电时通过UPS临时供应电量，当UPS电量过低时，按照虚拟机优先级先将不重要的虚拟机进行软关机（需提供产品功能截图） |
| 支持虚拟机的无代理备份，能提供至少100个虚拟机的高性能备份功能，无备份数据容量限制，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复 |
| 存储虚拟化 | ★支持存储分卷功能，以物理主机为单位划分为不同的存储卷，可将集群内全闪存的磁盘组成一个高性能存储池，满足高性能应用需求，将混闪磁盘组成一个大容量存储池，满足低性能大容量应用需求。所有类型不同性能磁盘均可支持分区，包含NL-SAS，SATA，SSD，SAS等。（需提供产品功能截图证明并加盖公章） |
| 支持磁盘亚健康监测，包括PCIE SSD寿命告警、硬盘卡、慢的检测和告警、IO错误告警、RAID卡错误告警等。 |
| 故障快速恢复：保障硬盘失效后的故障时间短，快速恢复数据，减少风险； |
| 物理硬件出现故障时业务能够实现自动漂移，保障业务系统快速恢复 |
| ★支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性（需提供产品功能截图证明并加盖公章） |
| 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响 |
| 支持多副本冗余功能，支持2个或以上副本，副本互斥地保存在集群的不同节点，当1个或多个主机或者磁盘故障，确保数据依旧正常访问。 |
| 支持数据写入优化机制，将高速SSD作为写缓存，数据先写到SSD，再回写到机械硬盘，提升写IO性能 |
| 在可视化的WEB管理平台上，可以查看虚拟分布式存储对应的容量大小、容量使用率、实时的IOPS读写次数、IOPS读写数据量等信息，方便为IT管理做为有效的决策依据。（需提供产品功能截图证明并加盖公章） |
| 当硬盘寿命到期、硬盘坏道数量过多，硬盘处于亚健康状态时，支持进入磁盘维护模式，在系统隔离硬盘之前，会对数据进行全面的巡检，确保硬盘隔离时业务不受影响。 |
| 为了更好地进行运维，准确识别出接下来会出现坏道的硬盘，支持智能坏道预测，实现故障前预测并处理，规避故障风险（需提供产品功能截图证明并加盖公章）  |
| ★为了便于部署关键业务系统，虚拟存储可支持Oracle RAC，支持共享盘，及共享块设备，支持向导式安装，降低部署复杂度（需提供产品功能截图） |
| 全自动化的分布式存储配置，和虚拟化平台紧密耦合，为虚拟机提供存储资源 |
| 采用分布式的软件定义存储架构，在通用x86服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点；通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out架构），扩容过程保证业务零中断 |
| 支持2个或以上多副本冗余功能，副本互斥地保存在集群的不同节点. 当1个或多个主机或者磁盘故障，确保数据依旧正常访问 |
| 支持对虚拟机业务按照小时/天/周自定义设置定时快照策略，以便业务发生故障时可以快速回滚覆盖原虚拟机或者通过对快照进行克隆的方式生成全新虚拟机，进而恢复至业务健康状态 |
| 支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能 |
| ★支持条带化功能，实现分布式raid0的性能提升效果，并且支持以虚拟磁盘为单位设置不同的条带数（需提供产品功能截图证明并加盖公章） |
| 支持多种克隆方式，实现虚拟机秒级启动，可根据需求选择克隆方式，包括节省空间的基于源虚拟机镜像文件生成链接克隆虚拟机；和保证业务高性能的基于源虚拟机镜像文件生成链接克隆虚拟机, 后进行源虚拟机数据的完整拷贝 |
| 支持多种存储配置；磁盘预分配根据业务需求分配固定的物理存储空间、磁盘精简分配根据应用实际写需要时才分配相应的物理存储空间，磁盘动态分配机制根据业务动态需求分配存储资源，实现预分配的高性能和提高磁盘利用率 |
| 为保证集群业务或者oracle rac数据库业务的快照一致性，以便故障时业务可通过快照恢复，支持对虚拟机配置一致性组，对整个一致性组进行快照 |
| 支持坏道扫描功能，由用户设置扫描的时间段定期对集群的硬盘进行扫描，及时发现潜藏的坏道 |
| 为了更好地进行运维，支持智能坏道预测，准确识别出接下来会出现坏道的硬盘，实现故障前预测并处理，规避故障风险 |
| ★支持针对卡慢盘、异常只读盘的自动检测、自动隔离及手动隔离，隔离分为临时拔盘、永久拔盘（注：永久拔盘后，需要手动替换磁盘，原有磁盘离线后无法上线），消除磁盘异常对业务的影响（需提供产品功能截图） |
| 支持磁盘亚健康监测，包括PCIE SSD寿命告警、硬盘卡、慢的检测和告警、IO错误告警、RAID卡错误告警等，支持邮件和短信告警 |
| 支持对虚拟机或虚拟磁盘设置不同的缓存QoS能力，区分出高性能虚拟机、普通性能虚拟机和低性能虚拟机 |
| 分布式存储能够提供超高性能，性能随着节点数增加线性增长，能够提供百万级IOPS和12GB/s以上的带宽能力 |
| 支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，且重建速度最快可达30min/TB以上，快速恢复副本的完整性和冗余度，确保用户数据的可靠性和安全性 |
| 支持存储业务网的自动负载均衡功能，自动分流存储业务流量，减轻单点压力 |
| 支持智能预测硬盘寿命，并预估硬盘剩余可使用时间，进行实时预警，提醒用户在寿命到期之前可实现在对业务无影响的情况下安全更换硬盘（需提供产品功能截图证明并加盖公章）  |
| 网络虚拟化 | 通过License激活的方式，实现网络虚拟化功能（虚拟应用负载均衡、虚拟路由器、虚拟应用防火墙、分布式虚拟交换机），支持Vxlan网络和现有的Vlan网络对接，实现虚拟化平台与原有网络的兼容性。 |
| 主动探测业务系统，实时监控业务可用性，监控策略包括SMTP、FTP、POP3、HTTP、自定义端口协议等，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障 |
| 本次配置虚拟路由器100台，虚拟路由器支持HA功能，当虚拟路由器运行的主机出现故障时，保障业务的高可靠性，可以实现故障自动恢复。 |
| 可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上 |
| 支持对Weblogic、sqlserver、oracle数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析 |
| 网络硬件检测（网络可通、网卡掉线、光模块、闪断、网卡） |
| 提供虚拟机报表功能，可以导出TOPN的虚拟机进行1年以内的性能分析与趋势分析报表，可以自定义报表模板 |
| 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、关闭、开启虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。（需提供产品功能截图证明并加盖公章） |
| 支持链路聚合，为网络中的每个虚拟机提供内置的负载均衡能力和网络故障切换，实现更高的硬件可用性和容错能力 |
| 可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上 |
| 支持创建分布式虚拟防火墙，基于虚拟机构建安全防火墙，当虚拟机在不同的物理节点之间迁移时，安全策略随之移动 |
| 提供虚拟路由器、虚拟交换机等设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，方便快速排查问题保障业务的高连续性，并且能够排查到acl策略配置错误等层面。  |
| 云管平台 | 提供统一的镜像管理功能，实现各个可用区上镜像的统一创建和管理，可实现一键快速生成云主机，要求可提供网络设备镜像，方便快速的部署虚拟化安全的组件 |
| 云资源的申请需要通过管理员审批方可使用，云操作系统支持多级审批流程，可以根据用户实际组织进行自定义 |
| 支持业务整体可靠性指标的集中展示，包括业务可靠性、平台可靠性和硬件可靠性，方便管理员能直观地掌握整个数据中心的可靠性状态。（需提供对应大屏展示功能截图并加盖公章） |
| 云平台采用冗余架构设计，避免出现单点故障  |
| 为有效保护客户投资，云安全服务平台需集成于虚拟化平台中，一体化方式交付，无需第三方平台承载，部署运维更便捷 |
| 平台支持模板化的组件部署模式，至少支持等保合规安全模板 |
| ★云计算管理平台，和底层资源池部分的（计算虚拟化、存储虚拟化、网络虚拟化）均为同一厂商品牌提供，并可以支持扩展同一品牌的网络功能虚拟化、虚拟应用防火墙、虚拟应用负载均衡等功能组件，以保障平台的扩展性和兼容性（需提供通过序列号方式扩展产品功能的截图） |
| 支持常见数据库、中间件、大数据平台的一键部署，包括但不限于RabbitMQ、Redis、MongoDB、Kafka、MySQL、CDH等应用的可视化快速部署，可对应用进行参数配置、应用监控、平台告警的全生命周期管理 |
| 支持以可视化的方式展示云平台可靠性，包括硬件可靠性、业务可靠性、平台可靠性三个层面，对CPU、存储、内存、多副本状态、数据重建状态等进行监控，对异常情况进行告警展示，方便管理员掌握云平台的整体情况 |
| 为简化用户运维管理，支持在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备 |
| 支持上传或利用现有云主机创建镜像，可对关联资源池、镜像进行管理、等操作，可通过镜像实现一键快速创建云主机及安全组件 |
| ★支持与安全产品联动，实现当发生僵尸网络、挖矿安全事故、勒索病毒时，实现自动隔离中毒云主机，并提供故障前一刻的业务安全状态供恢复，将安全事故损失最小化，也支持将病毒虚拟机进行关机或挂起，避免挖坑云主机消耗整个平台的性能。（需提供产品功能截图） |
| 平台具备独立的日志中心，支持关键安全组件的全量日志审计，支持syslog/WMI接收第三方日志，支持日志统一检索、备份、恢复等操作，支持磁盘按需扩展 |
| 支持创建云主机时设置使用时长，在云主机使用时长到期后可进行延期操作 |
| 安全虚拟化 | 支持安全事件展示，包括勒索病毒，暴力破解，后门等；支持安全事件报表分析；支持按优先级排序展示虚拟机安全状态，包括操作系统、内部应用、安全事件、是否开启防护等，支持搜索筛选；支持安全告警展示；支持安全事件处置记录展示；支持病毒扫描记录展示；支持查看虚拟机安全防护状态 |
| 支持虚拟化平台自动安装agent代理进行虚拟主机防护 |
| 可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率，并提供一键威胁处置  |
| ★支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离（需提供产品功能截图证明）  |
| ★提供向导化勒索病毒处理流程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（需提供产品功能截图证明） |
| ★支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截 |
| 支持防暴力破解，统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置，支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、最后攻击时间、发现方式、攻击内容、攻击历史  |
| 主机安全防护 | 采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能  |
| 支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量（需提供产品功能截图证明） |
| 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数 （需提供产品截图证明 ） |
| 支持按“最近7天”、“最近30天”、“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒TOP5排行榜，并展示对应的事件数及终端数  |
| SIP检测到某主机访问僵尸网络恶意域名时，联动EDR定位到该主机上发起恶意域名访问的具体进程、及其进程链信息，并且SIP根据EDR返回的举证信息，联动EDR对恶意进程进行处置（需提供产品功能截图证明） |
| 支持将EDR采集终端资产信息（包括操作系统、硬件、软件、账户、监听端口、运行进程等）上报SIP，并由SIP统一组织主机资产的可视化呈现 |
| ★基于对我院有效安全防护和防止勒索病毒的需求，支持与本次购买的下一代网络防火墙进行安全联动，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息（需提供产品功能截图证明） |
| ★支持管理员在我院现有的网络防火墙管理界面上实现一键隔离指令下发，对终端恶意文件进行隔离，防止病毒进一步扩散（需提供产品功能截图证明） |
| 支持与本院现有的网络防火墙进行情报共享，提供C&C通信检测，对僵尸网络实现联合举证溯源（需提供产品功能截图证明） |
| ★支持与同厂商的上网行为管理平台进行安全联动，支持管理员在上网行为管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息（需提供产品功能截图证明） |
| 支持管理员在同厂商的上网行为管理平台界面下发一键隔离指令，对终端恶意文件进行隔离，防止病毒进一步扩散（需提供产品功能截图证明） |
| 支持管理员在本次购买的上网行为管理平台界面下发推送指令，对指定网段的终端重定向推送客户端软件，支持自定义重定向的地址（需提供产品功能截图证明） |
| 支持将终端安全软件客户端检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到现有的安全态势感知平台，安全态势感知平台进行分析和展示 （需提供产品功能截图证明） |
| 支持与本次购买的数据中心边界防火墙平台对接，支持在防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息（需提供产品功能截图证明） |
| 容灾备份软件 | ★本次配置同品牌原生容灾软件，配置100个虚拟机容灾授权（提供相应的软件著作权登记证书） |
| 支持提供RPO可配置的虚拟机级容灾，RPO值范围从1秒到2周 |
| 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 |
| 容灾软件具备仿真容灾演练能力，在不影响业务的前提下，验证容灾系统的可靠性（需提供产品功能截图）  |
| 当主站点恢复正常后，容灾软件支持一键回迁功能，并可根据业务需求回迁全量数据或增量数据（需提供产品功能截图）  |
| 支持容灾状态可视化和状态监控，提供容灾大屏进行容灾计划的实时状态监控，并支持根据中断时长和重试次数设置链路告警策略，保障容灾计划的正常进行（需提供产品功能截图）  |
| 支持对异地容灾的备份文件设置保留策略，按照不同时间周期保留备份文件，满足容灾需求的同时最大化降低存储空间，当资源紧张情况下自动清理备份文件以减少资源开销（需提供产品功能截图）  |
| 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灾备数据中心，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 |
| 关键业务保障 | 为了便于部署关键业务系统，虚拟存储可支持Oracle RAC，支持共享盘，及共享块设备。 |
| 支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响。 |
| 支持数据写入优化机制，将高速SSD作为写缓存，数据先写到SSD，再回写到机械硬盘，提升写IO性能。 |
| ★为保证医院核心业务软件的可靠运行，要求云平台厂商具备与业内相关医疗软件厂家的兼容性认证，需要兼容的医疗软件厂家包括但不限于：联众、创业、九阵、海泰、篮网、卫宁等。（需提供产品兼容性认证证书） |

## 3.7总分院一体化容灾存储节点（分院）

|  |  |
| --- | --- |
| 类别 | 技术要求 |
| 基本要求 | 拥有自主知识产权，能够提供相关分布式存储授权软件的自主知识产权证书 |
| 采用全对称式分布式架构设计，无独立元数据节点。性能随节点数量的增加而近线性提升。提供多控制器负载均衡及故障自动切换功能。 |
| 要求提供SAN、NAS+Object统一存储系统，一套系统并发提供iSCSI、NFS、CIFS、S3、Swift存储服务，可实现三节点情况下同时提供块、文件、对象存储服务，资源可灵活分配，统一管理。（提供投标产品彩页） |
| 提供统一容量授权，容量授权不区分块、文件、对象存储服务。要求可灵活分配容量授权到不同存储需求。 |
| 要求存储系统可提供纯软件版本，纯软件版本兼容相关服务器厂商的X86服务器。 |
| 同时提供纠删码、副本做数据保护策略，保障数据冗余安全； |
| ★要求存储提供高可用能力，在三节点同时提供块/文件/对象三种存储服务时，可实现单节点损坏和单磁盘损坏存储系统依然可读写，且性能稳定。（要求提供第三方测试报告） |
| 支持在不停机情况下，向集群中添加存储节点，实现业务不中断情况下扩充容量和性能。 |
| 配置要求 | 存储节点，本次配置≥3个存储节点；每个存储节点配置至少1颗Silver 4210R 2.4GHz，内存≥64GB. |
| 系统支持千兆、10GE、25GE、100GE主机接口，本次要求每个存储节点配置不少于2个千兆口，2个10GE接口。 |
| 要求单台配置2块240GB企业级SSD，1块960GB企业级SSD，2块480GB企业级SSD，4块8T 企业级SATA磁盘。 |
| 提供分布式存储软件授权不少于96TB. |
| 支持SSD、SAS、NL-SAS、SATA类型硬盘混插； |
| 对象存储 | 支持Amazon S3标准接口，兼容S3生态体系； |
| 提供数据安全保障，支持对象数据网关加密，避免数据通过其他非法途径获取，造成严重损失。 |
| ★配置海量小文件高性能处理功能，支持百亿级海量小文件的高性能处理，可以实现100亿小文件高速写入，且性能衰减不超过5%。（提供具备CNAS(中国合格评定国家认可委员会)资质的三方权威评测机构签字盖章的测试报告） |
| 对象存储桶支持多版本，开启多版本后，桶中的对象都以多版本形式存储。同时，可自定策略删除多版本数据，从而清理过期数据，释放被占用空间。 |
| 对象存储支持SSL访问加密，通过购买受信任 CA 认证中心颁发的数字证书，然后应用在对象存储，可将 HTTP 访问转换成 HTTPS，提供认证加密功能。在客户端和服务器端之间建立加密通道，保证数据在传输过程中不被窃取或篡改。 |
| 配置对象存储负载均衡，在保证对象存储高可用的同时，实现负载均衡作用。避免热点节点或磁盘的高压力造成的物理损坏或性能堵塞。 |
| 配置bucket的生命周期配置功能，用于定期清理不需要的旧对象，从而处理垃圾数据，释放被占用的多余存储空间。 |
| 提供海量小文件快速修复能力，在三节点存储集群100亿小文件规模下，可实现单磁盘损坏，15分钟内修复完成，且存储集群在修复期间，性能衰减不超过5%。 |
| 配置对象存储Qos功能，可以设置不同用户访问某个bucket的带宽/请求数，从而防止边缘业务的过多资源占用。 |
| ★对象存储多中心同步动态感知，支持多中心动态感知功能，能够展示对象存储主站点的业务情况，和实时同步速率；（要求提供界面截图） |
| 配置多数据中心部署，通过设置策略可实现多中心的对象数据进行同步或异步复制，当某中心故障，其它数据中心可实现自动接管，保障业务的连续性。当故障中心修复可实现数据反同步，保障数据一致性。多中心可实现统一管理运维。（提供具备CNAS(中国合格评定国家认可委员会)资质的三方权威评测机构签字盖章的测试报告） |
| 支持对bucket的ACL配置，控制不同用户对同一bucket的访问权限（提供配置截图） |
| 文件存储 | 支持NFS V3.0和CIFS 1.0/2.0/3.0 标准接口 |
| 配置文件行为审计功能，用于记录客户如访问、创建、删除等常规文件操作行为； |
| ★配置目录级快照功能，可按时间点策略进行快照，支持快照数≥1024个。支持快照重命名功能，支持删除快照链上任意快照点，支持文件数据回滚。（要求提供界面截图） |
| 可实时查看访问CIFS共享目录的Session信息，并显示CIFS共享路径总的连接数； |
| 块存储 | ★支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，快速恢复数据的冗余度，确保用户数据的可靠性和安全性。（需提供产品功能截图） |
| 支持多副本冗余功能，支持2个或以上副本，副本互斥地保存在集群的不同节点，当1个或多个主机或者磁盘故障，确保数据依旧正常访问。 |
| 提供高性能块存储，可实现单节点（配置2块960GB SSD，两副本）提供至少10万IOPS。集群可实现线性增长，三节点满足30万以上IOPS处理能力。 |
| 支持自适应条带化功能，实现分布式raid0的性能提升效果，并且支持以逻辑卷或LUN为单位设置不同的条带数（需提供产品功能截图） |
| 高级功能 | 文件存储要求配置目录配额管理功能，支持容量和文件数配额。（要求提供界面截图） |
| ★支持一键检测功能，支持用户自行检测系统健康状态，检测包括CPU、内存、硬盘、网口等硬件故障、告警等问题，同时支持检测各类存储服务是否正常启动。针对问题能够提出解决推荐办法。（要求提供界面截图） |
| 智能缓存，通过基于sraft数据一致性协议实现分布式缓存，提供高性能的I/O读写优化。智能缓存拥有独立的可靠性机制，拥有3副本的容错能力。当缓存故障，依然保障数据不丢，业务不停。 |
| 智能分层，提供数据冷热智能分层，通过SSD缓存针对性提高读写性能。通过智能业务感知，分析判断数据冷热情况，从而实现热数据优先保存性能高的SSD中，从而实现提高存储性能。 |
| 故障自动恢复，在主机或者硬盘故障情况下，支持快速数据重建，重建速度1TB/30min，智能感知IO压力，保证运行业务性能； |
| 数据自动平衡，支持数据自动和手动进行热平衡，无需中断业务，自动感知业务IO，智能限速。支持设置平衡时间，利用空闲时间平衡数据。（要求提供界面截图） |
| 亚健康监测，支持对硬件健康及亚健康状态的检测及管理。通过扫描硬件状态，对故障点做预警分析，同时提出解决方案建议。减少设备故障对信息系统的影响。 |
| 机械盘加速，通过给机械盘配置缓存空间，提高数据写入磁盘的速度。 |
| 兼容性 | 应用集成插件，支持VMware等集群软件，支持虚拟存储API接口，使得虚拟机的部分操作能通过存储控制器来完成；支持VAAI； |
| 可视化 | 智能监控平台，能够清楚展示当前存储的关键硬件和逻辑资源，包含存储池、块存储、文件存储、对象存储、服务器硬件状态，并且能够在监控视图中根据当前状态给予客户提示，以达到快速清晰告警的目的。同时为了方便客户排错，支持点击各个资源和硬件等，能够展示当前选中单元的详细信息。（要求提供界面截图） |
| 配置界面上提供细化到每个节点的磁盘级监控，在管理界面上每个节点的磁盘与物理服务器真实盘位实现一一对应（要求提供界面截图） |
| ★存储拓扑，支持存储拓扑功能，展示块存储当前授权服务器和LUN之间的对应关系方便用户查看以及故障定位。（要求提供界面截图） |
| 数据安全 | 文件存储，访问审计，对用户访问操作的文件动作进行全量审计，并支持审计日志导出。 |
| 用户权限管理，支持NFS访问用户鉴权，共享目录访问权限校验，文件修改ACL策略权限校验。 |
| ★存储自带杀毒引擎功能，文件写入存储会进行杀毒，文件状态分为未知、安全、隔离、信任、被删除状态，防止病毒在存储进行扩散。**（需要投标人对本功能项进行演示，提供演示视频。）** |
| ★支持对象行为审计功能，用于记录客户如上传、下载等常规对象操作行为（提供产品功能截图） |

## B、第二部分

## 3.8准入设备

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 基础架构 | 拥有自主知识产权，基于linux开发的专用系统，标准机架式硬件产品，无需额外购买操作系统及数据库。 |
| 性能参数 | 1U机架结构；配置6个1000MBASE-T接口，每秒事务数（TPS)：≥2000（次/秒），最大吞吐量：≥1000Mbps，最大并发连接数：2000（条）；终端用户认证数量：1000点； |
| 管理平台要求 | 准入桌管一体化管理平台一体化客户端，只安装一个Agent即可实现准入桌管全部功能。（功能截图 ，加盖公章 ）客户端支持验证码防卸载（一对一）、万能验证码（一对多）、特权模式（策略全放开）。（功能截图 ，加盖公章 ） |
| 高可用 | 支持多种灵活的部署方式，无需改变网络结构，部署方式包括但不限于独立部署、热备部署、探针式部署、负载均衡部署、集群部署、扁平化部署、云化部署。 |
| ★支持智能逃生判断及管理恢复机制，在单位时间内终端异常离线达到指定逃生阀值则放开网络管控，当终端在线数达到阀值临界点时恢复网络管控；可灵活设置策略生效时间。（功能截图 ，加盖公章 ） |
| 提供专属逃生平台对系统服务状态进行实时评估，逃生平台策略被触发时可保障业务的稳定运行；策略包括但不限于系统服务异常等。 |
| 准入技术 | 支持策略路由、端口镜像、透明网桥、802.1X、ARP、DHCP、VLAN隔离、Portal等准入技术，支持准入技术自由组合使用，满足各种复杂网络环境。 |
| ★VLAN隔离技术须实现无客户端下的端口级准入效果，vlan隔离须采用不同正常vlan对应不同隔离vlan的方式，并可对通过小路由器、hub接入的设备实现颗粒度管控，不得采用全禁全放的风险行为。（功能截图 ，加盖公章 ） |
| 终端通过有线或无线申请接入，可无需用户操作，自动引导终端设备至认证入网页面。 |
| ★支持划定关键业务范围，针对终端用户发起的访问请求可强制要求二次认证校验。（提供产品功能截图 ） |
| 管理 | 管理页面布局及内容支持自定义，内容包括但不限于系统自身接口状态、流量等。 |
| 在多管理员状态下，支持设置私有、公有规范策略。私有规范只有创建账号有权限更改、删除，公有规范所有管理员均可更改或删除。（提供产品功能截图 ） |
| 提供移动端专属平台管理页面进行便捷管理，包括但不限于：设备快速定位、设备审核、实时报警监控、客户端卸载确认码生成等。（提供产品功能截图 ） |
| 客户端 | 支持安全客户端（Agent）、安全控件、无客户端等多种模式；提供Windows、linux、MAC OS、安卓、IOS专属客户端及APP。 |
| 提供中标麒麟(龙芯)、银河麒麟(飞腾)、统信UOS等国产操作系统专属客户端。 |
| 支持灵活的客户端卸载策略，包括但不限于万能卸载码，一对一卸载码，无需卸载码等多种模式。支持设置离线客户端策略，包括但不限于超过指定时间后客户端自动卸载，提醒用户确认是否卸载等。（提供产品功能截图 ） |
| ★客户端支持自定义菜单栏及终端用户故障诊断，诊断过程支持录屏，诊断结果支持一键压缩打包。（功能截图 ，加盖公章 ） |
| 边界管理 | ★支持自动生成全网拓扑图，5分钟自动更新一次网络拓扑信息并刷新。（功能截图 ，加盖公章 ） |
| 能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP表等信息；支持在界面上提供对该网络设备进行TELNET、SSH等管理；能够在网络拓扑图上由用户自定义显示的节点类型，方便用户通过不同方式查看拓扑连接。（功能截图 ，加盖公章 ） |
| 支持可网管型交换机面板图形化展现各接口状态（up、down、trunk、单/多MAC等），以及各接口下联的终端详细信息（IP、地址、MAC地址等），交换机型号库100+以上。（功能截图 ，加盖公章 ） |
| 支持自动识别、发现及阻断网络内私接的家用路由器、hub，提供网络定位功能（可直接定位接入的交换机端口 ）；可一键禁止全网的随身wifi（含软件版）使用。 |
| 身份认证 | 支持用户名密码、Ukey、指纹等认证方式，支持与AD域、LDAP、钉钉、Email联动。与钉钉等作为认证源时，终端认证自动跳转认证服务，无需打开相关app。 |
| ★支持设置来宾专属地址段；来宾入网提供二维码、来宾码、自助申请（管理员审批）多种方式；提供来宾入网审批气泡弹窗提醒功能，被访人点击即可审批。（功能截图 ，加盖公章 ） |
| 与AD域联动支持单点登录；支持管理员自定义域信息属性到认证设备，包括但不限于用户姓名、部门、联系电话等。 |
| 业务安全 | 支持关键业务端口映射，可设置映射的端口及选择映射的协议类型。（提供产品功能截图 ） |
| 安全基线检查（windows） | 支持IE控件、IE主页、操作系统版本、磁盘使用、计算机开关机、计算机名称、垃圾文件、服务端口、网络连接、系统时间、远程桌面、主机防火墙、p2p软件、软件黑白名单、黑白进程、系统服务、Guest来宾账户、密码策略、屏幕保护 、弱口令、共享检查。 |
| ★支持相关的杀毒软件版本、病毒库和运行情况的检查，包括但不限于微软MSE、火绒、安天、天融信、赛门铁克、瑞星、卡巴斯基、金山毒霸、江民、NOD32、360、天擎、亚信趋势、小红伞、可牛、Avast等，支持自动下发软件及运行修复功能。（功能截图 ，加盖公章 ） |
| 安检规范支持评分、设置修复期限，终端用户在允许期内即使不修复可正常使用网络。  |
| 支持自定义安全检查项，通过检测终端文件、指定文件版本、大小、MD5，注册表的项、注册表值，进程、服务状态进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。（提供产品功能截图 ） |
| 软件产品正版化检查，包括但不限于 windows、office、WPS产品的授权信息正版化检查。 |
| 系统补丁 | 准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分发表等功能。 |
| 准入设备能够对补丁进行分级，分为：严重、重要、中等的类别；能够在终端的浏览器页面显示入网终端的补丁检查情况；准入系统自身能够支持windows系列补丁库、补丁检查和补丁分发安装；支持windows10补丁检查及自动修复。 |
| 安全基线检查（linux/国产操作系统） | 支持操作系统版本、磁盘使用、计算机名称、网络监听端口、系统时间、主机防火墙、必须安装的软件、禁止安装软件、必须允许进程、禁止运行进程、软件白名单、系统服务、密码策略、弱口令检查。 |
| 安全基线检查（移动终端） | 移动终端可以支持通过将指纹和用户账户绑定的方法，实现用户按压指纹认证入网。（提供产品功能截图 ） |
| 支持禁用移动终端入网策略。 |
| 支持移动终端必须安装app、禁止安装app、必须运行进程 、禁止运行进程及杀毒软件检查。（提供产品功能截图 ） |
| 运维管理 | 软件、消息分发：支持基于部门、角色（分组）、设备或ip段进行软件、消息分发，分发周期支持立即、每天、每周、每月等周期设置。针对分发的源文件支持设置保留或不保留，分发后支持重启或关闭计算机。 |
| 远程协助：支持管理员或终端用户双向发起远程协助。 |
| IP资源管理：支持提供图形化的ip地址台账;支持一键绑定全网ip/mac；支持检查ip/组织架构绑定。 |
| 提供网络诊断工具，支持通过Web管理界面进行ping、抓包、traceroute、nslookup等。 |
| 提供IP地址分配矩阵图，可以通过组织架构为维度查看IP地址分配矩阵图；能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的IP使用情况。 |
| 报警信息 | 支持系统报警、网络报警、终端报警等报警类型，超过20种以上自定义报警类型。支持报警信息通过Syslog、邮件进行输出。 |
| 报表 | 支持提供每日/周/月入网报告及终端安全评估报告。 |

## 3.9虚拟化安全

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 授权要求 | 需要提供至少12个CPU安全虚拟化授权，不限制虚拟机数量，为了方便客户进行统一管理，需要兼容原有超融合集群实现无代理安全杀毒能力。 |
| 安全虚拟化 | 支持安全事件展示，包括勒索病毒，暴力破解，后门等；支持安全事件报表分析；支持按优先级排序展示虚拟机安全状态，包括操作系统、内部应用、安全事件、是否开启防护等，支持搜索筛选；支持安全告警展示；支持安全事件处置记录展示；支持病毒扫描记录展示；支持查看虚拟机安全防护状态 |
| 支持虚拟化平台自动安装agent代理进行虚拟主机防护 |
| 可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率，并提供一键威胁处置  |
| 支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离 |
| 提供向导化勒索病毒处理流程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御 |
| 支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截 |
| 支持防暴力破解，统计单个攻击源及分布式攻击源的暴力破解检测，支持按照RDP、SMB和SSH类型进行封堵并自定义爆破阈值，可对封停时间进行自设置，支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、最后攻击时间、发现方式、攻击内容、攻击历史  |

## 3.10防病毒设备

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 基础功能 | 提供不少于500个内网终端授权；抵御病毒、间谍软件、网络钓鱼和其它灰色软件的攻击。同时提供集中的管理、监控、更新和部署等功能，并具备主机防火墙、爆发阻止、Web站点信誉服务、预测机器学习、行为监控、勒索病毒防护等能力。 |
| 管理功能 | 产品采用B/S架构，支持通过HTTPS方式登录管理控制台，管理控制台访问需进行加密访问； |
| 产品管理端需要提供工具集，针对管理端、客户端提供用于自身配置的工具。同时WEB界面，需要提供有关如何使用工具的帮助信息； |
| 产品需要支持根据IP地址（包含IPv6）、操作系统、在线状态、处理器结构、病毒码版本、防火墙状态、爆发阻止状态等条件的组合搜索出符合条件的终端进行管理； |
| 产品支持必须自带数据库，安装后可以自行存储各类日志以及相关数据，同时也可以外接MSSQL数据库，保证数据存储的多样性； |
| 产品支持管理用户角色，支持用户权限的灵活设定； |
| 支持配置无法联系服务器的客户端自动发送波动信号至服务器端，并在配置的时间内仍无法联系，判定为脱机 |
| 为适应配置低的终端需求，不影响生产办公，终端在进行手动以及预设扫描时必须可以设置扫描时CPU占用比例，分高、中、低三个级别。低消耗下不得超过CPU使用率的20%； |
| 客户端支持系统 | Windows Embedded POSReady 7 Windows XP SP3 (32-bit)、SP2 (64-bit)、Embedded Standard SP1/SP2/SP3 Windows Vista SP2 Windows 7、SP1、Embedded SP1 (32位、64位) Windows 8、Embedded Windows 8.1、Embedded (32位、64位) Windows 10、IoT Embedded (32位、64位) Windows 11 (32位、64位)  |
| 安全防护 | 产品能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁； |
| 支持扫描并清除Office文档内的宏病毒； |
| 支持基于程序行为评估其可信度，并阻止未授权更改； |
| 产品需提供多种扫描引擎不少于五种，针对于机器学习必须使用独立扫描引擎，同时所有防毒引擎必须为自主知识产品非OEM产品； |
| 支持对压缩包文件进行扫描，并支持最大6层压缩，并对常用压缩格式文档中的病毒能有效的进行实时检测和清除。支持存档和压缩格式的扫描，包含rar、zip、cab、arj等压缩格式包内实时清除； |
| 对于文件扫描方式至少支持三种以上，包括所有文件统一措施、推荐扫描措施、以及针对不同类型病毒/恶意软件提供不同扫描措施，同时不同病毒/恶意软件类型不少于7种分类； |
| 扫描策略必须包含清除、隔离、删除处理措施，同时还应具备对病毒/恶意软件的不予处理（锁定）、监控、更名等措施，以保证对于文件多种处理的可选择性； |
| 提供基于程序行为的独立恶意行为监控引擎，基于进程的操作行为和序列组合来应对未知威胁，并提供配置界面截图； |
| 云安全检测支持行业属性配置，可基于行业提供更有针对性的检测服务； |
| 支持云安全扫描和传统病毒码扫描两种运行方式； |
| 支持将手动扫描添加到终端上的 Windows 快捷方式菜单； |
| 支持检测全局可疑站点（C&C)识别，监控可疑站点的连接，并提供记录或者阻止的处理措施； |
| 具有分组管理客户端的功能，可对不同的组实施不同的病毒防护策略； |
| 防火墙 | 产品需要支持主机入侵检测系统； |
| 防病毒软件必须具备个人防火墙功能,有效阻止各种恶意威胁； |
| 支持针对终端根据基于源IP（支持IPv6）、目的IP（支持IPv6）、源端口、目的端口、应用程序及注册表项，出站、入站等进行安全配置； |
| 移动设备防护 | 支持对USB存储设备、CD/DVD、网络驱动器的使用权限进行控制； |
| 支持阻止 USB 存储设备的自动运行功能； |
| 可对插入移动存储引导区或者移动设备的所有文件进行扫描设置； |
| web防护 | 支持拦截恶意URL功能，检测并阻止恶意的URL链接，并支持URL地址黑白名单功能； |
| 针对于web防护，必须可以区分内部客户端、外部客户端，对于不同的客户端可以实现不同的策略配置； |
| 具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新； |
| 客户端 | 支持多种安装方式，至少包括下载安装、MSI程序打包安装、共享安装、Web安装、脚本登录安装和域组策略安装，支持通过管理控制台方式进行远程安装，支持通过WEB方式进行远程安装； |
| 客户端应该具备组件更新功能，同时可以查看所有引擎、病毒码版本以及更新时间等信息； |
| 客户端提供本地语言自适应功能，可以根据客户端系统语言变更操作语言，至少支持中文、英文、日语、韩语等四种语言；可配置客户端语言应用本地语言和服务器端语言； |
| 提供首选IP功能，针对复杂网络环境，可以选择优先使用的注册到服务器的协议； |
| 爆发阻止 | 具备病毒爆发防御功能。当最新病毒爆发时，可在病毒代码未完成之前自动对企业网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击； |
| 漏洞弱点扫描 | 支持CVE漏洞弱点扫描功能，及时防护经由网页/电子邮件下载的文档漏洞利用(CVE)； |
| 勒索软件防护 | 防毒墙网络版客户端能够恢复由勒索软件威胁加密的文件，阻止与勒索软件关联的进程，并防止遭受危害的可执行文件感染您的网络； |
| 必须具备防勒索软件防护功能，管理界面提供配置项；并可配置在检测到勒索行为前备份文档； |
| 机器学习 | 具备机器学习能力，提供管理端及客户端的产品界面截屏； |
| 无文件攻击 | 具备无文件攻击检测能力，并在管理界面体现无文件攻击防护统计； |
| 更新升级 | 支持在线、离线两种更新方式； |
| 支持在客户端设置代理服务器； |
| 客户端更新实现并发更新数量的控制，同时可以按不同时间段进行更新并发限制； |
| 支持客户端更新代理，支持将任意客户端设置为更新代理，其他客户端从更新代理更新病毒码、策略，避免影响网络使用； |
| 可以设置边缘中继服务器，可利用中继服务器实现样本提交、日志提交、客户端状态更新等功能； |
| 支持组件更新还原功能，支持扫描引擎和病毒码回滚机制； |
| 日志 | 具有病毒日志查询与统计功能，可以随时对网络中病毒发生的情况进行查询统计； |
| 针对客户端防病毒感染情况进行监控、报警； |
| 消息通知 | 爆发通知：支持配置威胁类型，时间端，告警数发送爆发通知，支持的威胁类型包括（病毒/恶意软件，间谍/灰色软件，防火墙违规，共享文件会话，C&C会话） |
| 支持自定义客户端安全风险通知消息，支持威胁类型不少于8种 |
| 同时支持通过邮件，SNMP，NT事件日志进行病毒告警通知 |
| 可疑文件提交 | 具备将可疑文件提交沙盒设备的联动能力，可自动提交可疑恶意文件，并可接收； |
| 威胁情报下发 | 具备从统一管理控制台下发文件，IP，Domain等自定义情报，实现即时防护 |
| 补丁防护接口 | 产品需具备补丁防护接口，必要时可外接补丁防护产品，提供漏洞防护能力。同时补丁防护及补丁更新功能不能和杀毒软件一体化，避免和第三方桌面管理软件冲突。 |
| 插件管理功能 | 产品需支持以插件方式集成第三方产品或服务，实现平台化统一管理，并可提供集成接口和规范； |
| 产品需支持以插件的方式推送安装和卸载第三方组件客户端，到达灵活扩容的目的 |

## 3.11数据库审计

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 性能规格 | 性能要求 | 支持的数据库实例个数：12；★审计性能：峰值SQL处理能力≥20000条/秒；硬件最大吞吐量2000Mbps；双向审计数据库流量200Mbps；标配日志存储数20亿条；审计日志检索能力≥1500万条/秒。 |
| 硬件要求 | 2U机架式；内置交流双电源；产品采用专用工控机硬件架构，非普通PC服务器，MTBF(平均故障间隔时间)≥65000小时；处理器采用Intel高性能CPU，内存≥2\*8GB DDR4 2400Mhz，硬盘≥4TB（2T\*2），支持RAID1，最大支持扩展到4T\*4硬盘；网络端口：支持监听接口扩展，配备至少2个千兆电口管理口；支持千兆网络环境下的监听能力，标配至少4个千兆电口和4个千兆光口；支持最大扩展至8电8光或16电或16光共16个千兆以太网口。 |
| 功能项 | 部署方式 | ★可在云环境操作系统中安装软件代理，要求提供国家检测机构（公安部一所或国家保密科技测评中心）的检测报告； |
| 协议支持 | 支持MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、Cassandra、greenplum、LibrA、graphbase、cache、Redis、ArangoDB、Neo4j、OrientDB等非关系型数据库的审计；  |
| 审计功能 | ★审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集,提供功能截图，并提供国家检测机构（公安部或国家保密科技测评中心）检测报告 |
| 安全审计 | 产品具有内置规则，规则类型有sql注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警； |
| ★支持内置安全规则单独升级，需提供产品功能截图，并提供国家检测机构（公安部或国家保密科技测评中心）检测报告证明； |
| 查询分析 | 支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单； |
| 设置日志检索条件时，检索条件可根据历史信息自动弹出，检索条件支持源IP、目的IP、客户端工具、数据库名、数据库账号等，输入检索条件时支持智能联想；  |
| 支持告警分析功能，告警支持按照源IP和数据库账号对SQL模板维度进行排行，支持在页面一键去除规则、添加规则白名单； |
| 模型分析 | 可依据客户端工具名、数据库用户名、客户端IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器IP等配置行为模型，并可查看相应告警日志； |
| 系统管理 | 支持用户界面告警、邮件、短信、钉钉、SYSLOG、企业微信等方式告警；  |
| 支持系统资源使用率超阈值、Agent状态异常、长时间无审计日志时触发系统告警，且告警支持通过页面、SYSLOG、邮件、短信、钉钉、企业微信方式输出；  |
| Agent管理 | 支持在审计页面直接升级或回退已安装在数据库服务器上的Agent，且升级或回退不需要输入数据库服务器的账号、密码；  |
| ★可监控Agent的转发速率，以及Agent所在数据库服务器的CPU、内存利用率，并可设置CPU、内存利用率的上线阈值，超阈值时Agent将自动停止转发数据，需提供功能截图并盖公章，并提供国家检测机构（公安部或国家保密科技测评中心）检测报告； |
| API化 | 功能全面API化，支持第三方调用；  |
| 三层关联 | 可提供客户端访问Web服务器的URL和应用服务器访问数据库的SQL语句关联功能 |
| 易用性 | 支持分组管理，分组管理包含IP组、应用用户组、对象组、时间组、数据库账号组；  |
| 支持一键取证；  |
| 内置运维终端，可实现日志查看、设备状态检查、执行SQL语句、执行常用命令、特权运维等能力； |

## 3.12桌面管理

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 系统管理 | 控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能。提供≥200个windows服务器版本：终端杀毒+补丁管理许可,五年软件升级服务。 |
| 客户端：与安全控制中心通信，提供控制中心管理所需的相关数据信息；执行最终的木马病毒查杀、漏洞修复等安全操作。 |
| 麒麟/银河麒麟/普华/红旗桌面操作系统。（提供操作系统厂商提供的兼容证书） |
| 病毒、恶意代码、木马防护 | 要求产品具备本地引擎查杀能力 |
| 支持私有云查杀，预置至少2亿黑名单及2000万全面的白名单，终端威胁统一到控制中心查询黑白并进行查杀（提供截图） |
| 要求产品在断网状态下具备不依赖病毒库特征的情况下对未知病毒查杀的能力 |
| 要求产品具备主动防御技术 |
| 补丁分发与漏洞修复 | 产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能（提供截图） |
| 产品具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P2P补丁分发加速，有效节省外网带宽资源（提供截图） |
| 敲诈者病毒防御 | 对敲诈者病毒提供防护机制，同时可提供相关解密工具，解密工具为自主研发；（提供功能截图） |
| 针对近年的敲诈勒索病毒事件频发，产品厂商需具备针对敲诈勒索事件应急响应能力~~。~~ |
| 安全联动 | ★要求与总院外网终端管理系统相互联动，当发现网络威胁时，能够与总院外网终端管理系统及时同步威胁信息，快速处理。（提供功能截图加盖公章） |
| Linux、国产操作系统杀毒 | 支持Linux、国产操作系统杀毒（提供证明材料） |
| 其它 | 支持与本次所投防火墙联动，达到网关边界联动防御效果（提供截图证明） |
| 支持控制中心数据恢复与备份 |

## 3.13堡垒主机设备

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 产品资质要求 | 产品需符合GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》（idt ISP/IEC 15408:2008）,并获得由中国信息安全测评中心信息安全实验室颁发的《国家信息安全信息技术产品安全测评证书》，级别应为EAL3+，提供证书复印件 |
| 产品厂家需具备产品自主知识产权，禁止OEM贴牌投标 |
| 性能要求 | 授权资产：500个硬件性能：并发字符连接最大500个，并发图形连接最大100个 |
| 硬件要求 | 机箱高度：2U标配网口：2千兆电口管理口，千兆业务电口\*4，千兆业务光口\*4（含2个千兆SFP多模光模块）硬盘容量：2T\*2，RAID 1内存：8GUSB口：USB2.0口\*2串口：RJ45口\*1电源：1+1热插拔冗余电源 |
| 用户角色 | 支持用户多角色划分功能，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，对各类角色需要进行细粒度的权限管理。支持自定义用户权限。 |
| 用户管理和用户策略 | 支持用户的批量导入/导出；支持用户安全策略功能，如用户有效期、用户登录时间限制、用户登录IP范围等 |
| 部门层级管理 | 支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等 |
| 部门管理 | 每个部门的审计管理员仅仅可以管理本部门及下级部门的运维会话日志；每个部门的部门管理员可以管理本部门及下级部门的主机、授权关系、策略 |
| 部门数据管理 | 每个部门可针对导出的部门账号密码文件单独设置AB段安全码，解压时需要输入部门安全码，通过验证方可导出相关文件；管理员导出部门资产数据时，可设定是否对资产文件进行ZIP包加密。 |
| 身份认证方式 | 支持手机APP动态口令认证方式登录堡垒机，新用户首次登录后需强制绑定APP动态口令；支持AD、LDAP、RADIUS、吉大正元、北京CA认证系统联动登录堡垒机，支持自动同步AD/LDAP用户。 |
| 单点登录认证 | 支持标准化对接CAS、JWT单点登录认证，且支持配置是否自动创建堡垒机中不存在用户。 |
| 短信口令认证对接 | 支持与Get、Post、Soap发送方式的HTTP短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud联动。 |
| 双因子认证 | ★堡垒机须内嵌动态令牌和USBkey认证引擎，可使用动态令牌或USBkey进行双因子认证。（需提供相关授权和资质复印件） |
| 国密认证 | 支持基于国密算法的动态令牌进行双因子认证，提供《商用密码产品认证证书》 |
| 密码存储 | 支持采用国密加密算法进行核心敏感数据加密存储（需提供界面截图） |
| 多用户双因子认证 | 基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证。 |
| 单用户同时启用多种双因子认证方式 | 同一个用户支持同时启用多种身份认证方式，登录堡垒机时可任意选择，如A用户登录时，可选择本地密码+手机APP或本地密码+动态令牌等。 |
| 多种认证组合使用 | 支持域认证与双因子认证结合使用，如同时使用AD/LDAP用户名+AD/LDAP密码+手机APP动态口令登录堡垒机、同时使用AD/LDAP用户名+AD/LDAP密码+短信口令登录堡垒机。 |
| 用户密码及登录策略设置 | 可以设置用户密码的长度、复杂度、相关度，其中相关度可以设置密码与用户名的关系，可以选择是否检查历史密码。并可支持密码过期前告警；可设置用户密码错误达到一定次数后的锁定时长及登录失败次数的重置时间。 |
| 认证窗口全局设置 | 支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口。 |
| 自动改密要求 | 主机自动改密 | 支持定期自动修改Windows服务器、网络设备、linux/unix等目标设备密码功能，且自动改密不借助于Agent，无需开放445、135、139等高危端口。 |
| 数据库/web自动改密 | ★支持对数据库及Web应用的自动改密功能。（需提供相关截图证明） |
| 账号切换改密 | 支持Unix/Linux系统账号自动改密功能。并支持账号切换改密功能，当root不能直接远程登录时，依旧可以修改root密码。 |
| 改密脚本 | 可以通过编写改密脚本的方式进行改密操作 |
| 设备管理要求 | 支持的协议和应用 | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具 |
| IE/谷歌浏览器代填 | ★IE/Chrom代填应用发布：HTTP/HTTPS协议的web设备，且可以直接代填账号和密码（须提供国家机构证明） |
| 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（须提供国家机构证明） |
| 运维方式要求 | 运维管理 | 支持B/S架构进行堡垒机运维管理，至少支持使用IE、谷歌、火狐、Microsoft Edge等浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等本地运维客户端工具 |
| 专用客户端运维 | 支持Windows/Mac操作系统下C/S架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作。 |
| 运维客户端自带运维工具，可不依赖 xshell/Securecrt/mstsc等工具进行运维操作 |
| 客户端支持VPN登录功能 |
| 客户端工具登录 | 客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty/winscp/Xftp等客户端工具登录堡垒机访问图形、字符或SFTP、FTP设备 |
| 安全策略要求 | 运维规则策略 | 支持通过基于时间、IP/IP段、用户/用户组、主机组、主机账号、命令控制策略等组合访问控制策略，授权用户可访问的目标设备。 |
| 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。（须提供国家机构证明） |

## 3.14 VPN设备

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 性能参数 | 最大理论加密流量（Mbps）≥600，最大理论并发用户数≥800，最大理论https并发连接数（个）≥50000，理论https新建连接数（个/秒）≥120，零信任接入授权不少于100套。 |
| 硬件参数 | 规格≥1U，内存大小≥8G，硬盘容量≥128G SSD，电源：单电源，接口≥6千兆电口+2千兆光口SFP。 |
| 部署模式 | 为了满足灵活部署的要求，控制中心应支持单臂模式、路由模式部署 |
| 支持集群模式 | 为了满足高可靠性要求，控制中心应支持集群部署，集群功能不需要依赖外置设备，如负载均衡等 |
| 支持一体化部署模式 | 综合网关集成控制中心和安全代理网关，应支持一体化部署 |
| 支持免插件B/S-WEB资源纯浏览器访问 | 为了提升员工使用体验，便于用户无感接入，控制中心应支持跨平台免插件访问，支持多资源（http/https/websocket等）免客户端接入 |
| B/S应用依赖站点梳理 | 支持站点智能梳理1、支持使用自动改写采集的方式梳理依赖站点；2、支持依赖站点一键启用，自动采集便于业务快速上线，简化运维工作（要求提供配置截图证明） |
| 支持以通配符方式发布单位内部WEB和C/S业务（企业自有域名） | ★为减少配置难度，支持以通配符方式发布单位内部WEB系统，避免配置多次资源（如发布一条\*.sun.com资源即可访问oa.sun.com和crm.sun.com及其他域名资源)（要求提供配置截图证明） |
| WEB资源支持依赖站点 | 为简化授权和管理，应支持将WEB主站点的多个依赖站点资源，全部配置在一条资源中 |
| 支持PC终端以隧道模式接入访问C/S资源 | 支持终端以隧道模式接入访问内网C/S资源，包括Windows7（x86、x64）、Windows10（x86、x64、ARM）、MacOS10.12支持Ubuntu16.04、Ubuntu18.04、UOS v5.0.30(x86、飞腾)、银河麒麟V10（飞腾）及以上版本 |
| 客户端自带登录地址 | 为了尽可能简化员工登录操作难度，支持在客户端登录时内置登录地址。（要求提供配置截图证明） |
| 手机扫码登录PC | 支持手机APP登录后支持扫码上线PC端 |
| 手机零信任客户端安全设置 | 支持配置应用安全锁、同时开启指纹、手势解锁APP |
| 支持的认证方式 | ★为满足单位多样化安全便捷认证需求，控制中心在不需要额外搭建认证平台、认证组件的情况下便可支持以下认证方式：本地账号密码认证、LDAP/AD认证、OAuth2.0标准协议的票据认证、CAS标准协议的票据认证、证书认证、HTTP(S)短信认证、腾讯云短信网关、阿里云短信网关、标准Radius令牌认证、本地OTP动态令牌认证等认证方式，并可与企业微信、阿里钉钉结合实现扫码认证。（要求提供配置和实际效果演示截图证明） |
| 支持认证服务器对接 | ★支持第三方对接认证，支持对接OAuth2.0、CAS、LDAP、Radius、HTTPS、企业微信、钉钉等第三方认证服务器。（要求提供配置和实际效果演示截图证明） |
| 多因素认证 | 为了进一步保障用户身份安全，需支持多因素认证，比如用户名密码认证+短信认证 |
| 外部认证服务器登录用户支持设置默认权限 | 支持登录外部认证服务器（如oauth2、ad/ldap、cas）等，默认关联角色，简化权限授权 |
| 支持多认证服务器账号区分 | 支持在创建认证服务器时，为服务器指定认证域，(domain)，如sun.com，便于账号区分 |
| 支持用户访问时，以username@domain的方式进行精确账号指定，避免不同认证服务器中的重名账号的用户权限不清晰 |
| 单点登录 | 1、支持帐号密码代填的单点登录功能，可自动识别登录页面的用户名和密码输入框，根据设置的用户名密码规则自动填写WEB业务系统的帐号密码并登录；2、支持以零信任帐号密码或自定义帐号密码登录3、支持以零信任用户名、手机号、邮箱、邮箱前缀作为用户名进行帐号代填 |
| 本地用户管理 | 控制中心支持本地用户管理：1、支持新增/删除/修改本地用户2、支持新增/删除/修改本地用户组织架构3、支持配置本地用户基本信息，例如用户过期日期、手机号、启用/禁用状态登录4、支持批量编辑5、支持跨页多选，支持选中本页；6、支持保存并继续添加用户，此时会保存用户的一些基本授权来添加，减少运维成本 |
| 外部用户管理 | 控制中心应支持与外部用户管理服务器进行对接，包括LDAP用户目录、企业微信用户目录（要求提供配置截图证明） |
| 批量导入/导出用户 | 为减少用户创建难度，对于本地用户目录，支持批量导入/导出：1、支持按csv表格模板格式，批量导入用户2、支持批量导出csv格式的用户列表3、批量导入时，若用户所属组织架构不存在，支持批量新建 |
| 动态访问控制 | ★为满足组织灵活的管理要求，支持配置动态访问规则，可配置化的ACL规则引擎，可以灵活地将终端环境、用户身份、处置动作等进行配置，为单位不同业务不同部门提供灵活丰富的访问控制策略：1、动态访问控制策略可指定适用用户范围和排除用户，可指定适用应用；2、动态访问控制策略支持针对操作系统单独设定访问控制策略，操作系统需包括Windows、Mac OS、iOS/Android；3、动态访问控制策略支持“与”、“或”条件嵌套，可支持应用信息、端点信息、用户信息、内置变量进行条件设置；4、动态访问控制策略支持灵活的处置动作，包括阻止访问、注销登录、锁定账号，并可基于处置动作自定义提示语；5、当用户不满足访问控制条件时，可提供豁补救动作，补救动作包括：增强认证、安全警示等，且可设置灰度处置的时间范围（提供配置截图证明） |
| 动态准入 | 支持在登录上线后，持续、动态检测终端环境安全，不符合后注销用户或锁定用户，便于及时定位并响应终端威胁（要求提供配置和实际效果演示截图证明） |
| 联动要求 | ★须支持与总院现有防火墙、上网行为管理联动，实现外联接入安全审计联动。（要求提供证明文件加盖公章） |
| 基于应用信息的访问控制 | 支持不同的应用基于访问应用信息设定访问控制策略：1、访问应用的进程数字签名2、访问应用的进程名称3、客户端的公网源IP4、代理网关接入IP5、浏览器版本6、浏览器名称7、应用类型 |
| 终端环境动态安全检测 | 支持基于不同的应用，可针对终端环境检测设定访问控制策略，包括：1、aTrust客户端版本2、安装指定的软件3、杀毒软件是否为最新版本4、是否开启操作系统防火墙5、运行任意一款杀毒软件6、安装指定的杀毒软件7、运行进程8、是否存在指定文件9、Windows操作系统安装的补丁10、计算机操作系统版本11、计算机加入的域名称12、计算机本地IP列表13、计算机MAC地址列表14、计算机名称 |
| 屏幕安全（WEB水印） | 支持针对不同的B/S应用开启WEB水印水印内容包括：用户名+当前日期具有威慑作用，有效预防数据泄露（要求提供配置截图证明） |
| 可信应用 | 仅允许信任进程访问资源，有效防止木马入侵系统后攻击服务器 |
| 终端进程采集 | 1、支持对所有访问隧道应用的进程进行采集，采集信息包括：进程名、描述、系统平台、数字签名等基本信息2、支持对各采集进程的使用人数进行统计3、支持基于进程是否有合法数字签名、使用人数对进程的风险状态进行评估，以便于管理员基于风险状态判断进程是否可信 |
| 可信应用自定义 | 1、管理员可根据采集到的进程信息选择信任/不信任2、支持管理员自定义可信/不可信的进程 |
| 进程信息可视 | 支持对所有采集到的进程信息、管理员的处理进度进行统计。包括：1、全部进程，以及高风险/低风险/未知风险的进程数量2、管理员未处理的高风险/低风险/未知风险进程 |
| 基于可信应用的访问控制策略 | 支持将进程的可信状态作为访问控制评估条件，配置应用访问策略。限制仅可信的进程可访问指定的应用，或不可信的进程阻止访问。（提供配置截图证明） |
| 支持按角色授权 | 支持按用户、用户组、安全组进行角色授权，简化权限管理 |
| 支持组织架构的授权继承 | 1、支持下级组织结构继承上级用户组的角色和应用，简化权限管理2、支持用户选择是否继承上级用户组权限 |
| 支持授权可视化 | 支持可视每一用户或用户组的权限，可以看到该用户、该用户组关联的所有应用及应用分类，避免出现权限授权不可视、难管理的问题 |
| 权限梳理基本能力 | ★由于单位业务系统众多，员工权限交错复杂，需零信任平台提供权限梳理基本能力，帮助排除零信任建设障碍，且须支持应用采集、试运行、正式运行等多个阶段的梳理支持。（提供配置截图证明） |
| 应用采集及权限分配 | 1、采集阶段，可将用户与应用之间的关系可视，并提供权限确认机制验证权限有效性。基于身份化流量分析方式将权限可视，解决人工梳理导致的耗时长、难实现的问题；2、试运行阶段，能够不中断用户访问业务，提前试运行，并在该阶段对权限结构进行调优，以避免正式上线后，大面积影响用户访问业务。在此期间，用户均可以访问业务，未授权用户可以通过提交"访问理由"继续访问业务；3、正式运行阶段，进行智能权限梳理后，可将权限规范化，并正式上线。在此期间，只有有权限的用户才能访问业务系统。 |
| 支持权限申请和审批 | 支持员工权限的申请和审批，正式运行时，未获得授权的员工访问提供申请和管理员审批机制（支持管理员分级分权审批，符合业务安全要求），防止员工权限过大，同时简化权限运维工作 |
| SPA | 为了最大程度缩小网络、业务暴露面，零信任平台需提供SPA（单包授权机制）即可支持所有用户都必须安装安全专属客户端，经过SPA鉴权之后才能够访问认证登录界面，支持配置源IP地址白名单，白名单内的IP可正常访问（提供配置截图证明） |
| 虚拟专线 | 针对Windows用户，支持虚拟专线功能，当用户登录建立零信任登录零信任客户端之后，自动断开互联网连接，避免互联网威胁影响内网业务系统 |
| 流量镜像 | 支持将用户访问控制器的加密流量解密后镜像给外部系统，如态势感知等 |
| 设备证书管理 | 支持设备证书管理、域名证书管理，便于运维 |
| SNMP | 提供SNMP服务，可对接运维监控设备 |
| NTP时间同步 | 支持NTP时间同步 |
| 终端诊断工具 | 支持终端环境诊断排查，提供终端诊断工具，支持Windows、MAC系统，支持对当前终端的基本环境进行扫描和一键修复，便于员工自行排查修复终端问题，减少IT运维人员工作（要求提供配置截图证明） |
| 终端日志自助收集 | ★支持Windows客户端自助进行日志收集，方便运维排查（要求提供配置截图证明） |
| SSH自动关闭 | 支持自动式后台运维，支持选择开启和关闭SSH，同时支持SSH自动关闭，以免运维人员进行远程运维后，忘记关闭SSH，带来潜在风险 |
| 备份配置与恢复 | 1、支持当前设备配置自动同步、支持从备份配置中恢复2、支持导出当前设备配置3、支持恢复出厂设备配置4、支持系统时光机快照功能，万一设备升级出现故障，可手动恢复至升级前状态 |
| 防爆破 | 1、支持配置同名用户连续登录错误超过上限时锁定账号，并于指定时长后自动恢复2、支持配置同IP用户连续登录错误超过上限时锁定IP，并于指定时长后自动恢复 |
| 防机器人 | ★防机器人输入，提供强安全性的点击图像校验码机制，图形校验码支持中文和英文（要求提供配置截图证明） |
| 巡检工具 | 1、支持通过acheck客户端提交check包巡检设备安全状态和策略配置2、支持在客户端获取巡检报告，展示巡检结果 |
| HIDS文件监控 | 1、支持云脑下发指令在设备中进行全盘文件扫描和增量扫描2、支持云脑下发指令在设备中进行样本采集3、支持将文件扫描结果和样本采集结果上传到云脑4、支持根据定时任务进行全盘文件扫描和增量扫描5、支持根据文件md5对全盘扫描和增量扫描结果进行灰/黑文件分析 |
| 设备健康检查巡检 | 1、支持设备自身巡检安全状态和策略配置2、支持在设备上查看检查报告3、支持从设备上下载检查报告 |
| SP补丁在线升级 | 1、支持补丁包在云脑发布，客户端自动更新2、支持已打补丁的回滚3、支持控制台查看升级和回滚的日志 |
| OpenAPI | 1、支持对接多个设备进行openapi接口调用2、支持限制openapi调用ip范围 |
| 在线用户 | 1、支持查看当前在线用户总人数2、支持查看当前在线用户，包括用户名、组织架构、终端类型、浏览器类型、接入IP、最后接入时间、认证方式等等3、支持管理员对在线用户进行注销操作 |
| 用户状态 | 支持管理员在控制台查看“用户状态”，主要是异常状态，如爆破锁定、ACL锁定、异地登录等，支持管理员手动解锁用户。 |
| 设备状态 | 支持查看当前设备运行状态，包括CPU、内存、磁盘占比等等。 |
| 业务告警 | 1、支持告警信息设置，包含以下几个方面： CPU使用率超过80%、内存使用率超过80%、磁盘占用率超过80%、序列号即将到期（提前15天提醒）、在线用户数已达购买授权数2、支持配置邮箱服务器，告警事件支持邮件通知管理员 |
| 系统主题 | 支持替换主题包，对登录页、产品logo、应用中心背景图进行替换，替换范围：1、登录页背景图片替换；2、logo图片的替换；3、浏览器标签角标的替换；4、产品组织名称与登录公告的替换；5、主题样式修改6、隐藏隐私协议、隐藏下载客户端、隐藏温馨提示、修改温馨提示文案7、增加外部链接：例如增加用户手册外链、帮助中心外部链接等。 |
| 门户设置 | 管理员可自定义登录页面显示那些认证方式、认证方式的显示顺序。 |
| 控制台接入 | 1、支持TLS1.0 TLS1.1 TLS1.2 TLS1.3加密协议；2、支持多个https监听端口3、支持客户端接入地址的高级配置，做防host攻击 |

## 3.15上网行为管理设备

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 性能配置 | 产品为标准1U机架式设备，需满足多核X86架构。标配至少6个千兆电口，2个万兆光口SFP+，性能配置：最大并发连接数≥600000；用户规模≥6000人；网络层吞吐量（大包）≥10Gb；每秒新建连接数≥14000；应用层吞吐量≥1.5Gb；硬盘容量≥64G SSD+960G SSD。 |
| 部署方式 | 要求设备支持网关模式，支持NAT、路由转发、DHCP等功能；支持网桥模式，以透明方式串接在网络中；支持旁路模式，无需更改网络配置，实现上网行为审计；支持两台及两台以上设备同时做主机的部署模式； |
| IPv6支持 | ★支持部署在IPv6环境中，相应的所有功能（上网认证、应用控制、内容审计、报表等等）均都支持IPv6。（需提供产品功能截图证明并加盖公章） |
| 虚拟化模式 | 支持基于虚拟化平台的软件版本，支持的虚拟平台包括：VMware、深信服超融合等平台； |
| 链路负载 | ★为了提高出口多链路利用率，要求支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载。支持使用VPN做专线备份，支持链路故障检测；（需提供产品功能截图证明并加盖公章） |
| 接入认证 | ★支持多种接入认证；1）多种认证方式，支持触发式WEB认证，支持用户名密码认证、IP和mac认证、短信认证、微信认证、二维码认证、单点登录认证等多种认证方式；2）用户身份源：支持对接多种用户源，包含 内置账户、AD域用户、LDAP服务器用户验证、RADIUS服务器、数据库服务器、POP3服务器、第三方认证系统（cas）；3）支持基于802.1x的外部CA证书认证，同时支持在线证书状态查询（OCSP）;（以上均需提供产品证明截图并加盖公章） |
| 业务需要 | 为减少短信费用投入，要求设备支持微信身份验证，用户可以通过微信“扫一扫”、关注公众号等操作获取上网权限，后台能够记录下用户微信的ID，支持与第三方微信平台对接，无需修改第三方平台代码； |
| ★终端资产业务可视管理1）支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量；2）对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 3）支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；4）支持查看终端类型分布;（以上提供截图证明文件并加盖公章） |
| ★支持非法外联行为检查阻断，包括拨号、双网卡、有4G网卡、有无线网卡、连接非法wifi、使用非法网关、私连外网、自定义外联等行为，对不满足检查要求的终端强制断网，向管理员告警，并弹窗提示用户；（提供截图证明文件并加盖公章） |
| 为满足访客PC的简易接入授权，访客终端接入无线网络后，终端自动弹出二维码页面，审核人通过手机扫描访客终端二维码，添加备注信息，访客即可完成上网，同时设备记录访客备注信息、接入终端MAC以及审核人帐号。 |
| ★为满足公司内部实名认证，要求产品支持通过OAuth认证协议对接，支持阿里钉钉，企业微信第三方账号授权认证；（需提供产品功能截图证明并加盖公章） |
| ★为保证会议认证接入，支持提供二维码和会议号，用户扫码或输入会议号认证上网；支持通过验证手机号码实名认证;（需提供产品功能截图证明并加盖公章） |
| 为确保我单位不会通过SSL加密内容发生通过互联网出口泄密事件，要求设备必须能够识别并过滤SSL加密的钓鱼网站、金融购物网站；识别和审计加密的邮箱（如GMAIL）等； |
| ★针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测（需提供产品功能截图证明并加盖公章） |
| 终端安全检查 | ★无需安装客户端，通过流量状况检查10款以上相关杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复;（需提供产品功能截图证明并加盖公章） |
| 应用识别规则库 | 支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、相关论坛和微博发帖6大类；此外可根据我单位需求自定义标签，根据标签做应用控制。 |
| 应用控制 | 设备内置应用识别规则库，支持超过6700条应用规则数，支持超过2900种以上的应用，1000种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率； |
| 流控黑名单 | ★基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（需提供产品功能截图证明并加盖公章） |
| P2P智能流控 | 要求设备有效抑制如迅雷、ppstream等P2P应用带宽，通过抑制可看到出口上下行带宽的明显改善。 |
| IM审计 | 支持对QQ（客户端版本）、阿里旺旺、万德（Wind）、路透等应用的聊天，群聊天等内容的审计。 |
| 离线终端审计和管控 | 在非内网环境下实现客户端应用审计、U盘审计、IM审计，外发行为日志留存在终端本地，已配置的外设管控、外联管控、访问控制策略保持生效，终端接入内网后同步到设备日志中心。 |
| SSL加密内容审计和过滤 | 支持识别并过滤SSL加密的钓鱼网站、金融购物网站、非法网站等，同时支持SSL硬件加速卡解密，从而可提高SSL全流量解密性能； |
| 单用户行为分析 | 针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等） |
| 数据中心 | 要求设备必须支持将审计数据备份到外置数据中心，实现海量存储；必须支持通过USBKEY方式对数据中心管理员进行身份验证，确保我单位核心数据不会外泄 |
| 产品联动 | ★能够与总院防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；（需提供产品功能截图证明并加盖公章） |

## 3.16日志审计设备

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 产品资质要求 | 产品获得中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》，需符合GB/T 20945-2013 《信息安全技术 信息系统安全审计产品安全技术要求和测试评价方法》（增强级）； |
| 产品取得相关软件著作权登记证书 |
| 规格要求 | 标准2U硬件网口：10个工作管理口（1管理口+1HA口+4个千兆电口，4个千兆光口（配2个多模SFP光纤模块）），1个console口内存：16GB磁盘：2T\*2 raid1（支持raid1：只能是偶数、raid5：大于等于3块盘）双电源扩展项：内存：可扩展至32GB磁盘：单个磁盘可扩展至4T(4个盘位）网口：可扩展至34个（4电4光、8电、8光、2万兆光） |
| 性能要求 | 支持200个日志源；日志处理能力EPS：9000/秒（峰值：12000/秒） |
| 部署方式 | 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据； |
| 支持集中式管理和升级模式 |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需要代码开发； |
| 支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能，Kafka收发支持SSL加密。 |
| 日志收集 | 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集。 |
| 支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。 |
| 日志分析 | 可以通过自定义配置过滤掉用户不关心的日志； |
| 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展； |
| 内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景 |
| 对日志样例可进行划词辅助解析，一键生成正则表达式 |
| 支持解析规则性能以界面列表形式显示，可了解解析耗时、解析成功或失败次数等信息 |
| 支持基于跨设备的多事件关联分析； |
| ★三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件（须提供第三方检测报告） |
| 应用性能监控（APM） | 支持监控设备自身CPU、内存、磁盘等工作运行状况； |
| ★通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息（须提供第三方检测报告）； |
| 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理； |
| 提供一键式故障排除功能； |
| 提供自助式的升级接口，支持对产品升级、规则升级。 |
| 资产管理 | 注册用户资产时，提供自动发现识别能力； |
| ★资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息（须提供第三方检测报告）。 |

## 3.17态势感知设备

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 产品开发 | 产品取得相关软件著作权登记证书 |
| 性能要求 | 数据采集和处理性能≥15000EPS，每条数据大小>1KB；10亿数据关键字查询结果响应时间<2秒。 |
| 硬件要求 | CPU ≥24核 ，内存≥256GB，配置企业级存储磁盘总容量≥48TB；接口要求：至少具备4个千兆电口 |
| 数据接入 | 支持通过多种类型的安全、泛安全类数据接入采集，应包括但不限于设备日志数据、流量数据、弱点漏洞数据、系统性能数据、威胁情报数据、资产人员数据；支持通过流量采集设备采集接入全流量数据，包含流量中的请求包和返回包等信息，并可在数据检索中体现包信息；支持接入文本格式、CVS等格式的文件数据，可通过模板文件的填写导入实现资产数据的导入和管理；支持通过云端对接、本地导入或手动编辑的方式，接入威胁情报数据。 |
| 多级部署及管理 | ★本院主从中心多级部署，接入管理分院二级平台，对接入平台下发工单，主从平台联动处置，权限分立，本院单位具有查看全网风险权限、分院单位仅具有本单位相关问题查看处置权限等等全院区态势感知多维度、多方位全院区态势，从外部估计态势，内部攻击态势，业务系统攻击态势，资产失陷态势等维度对上下级的安全态势及进行全网风险风险监控实时通报预警风险通报预警，通过人工发布预警和剧本自动发布预警两种方式，对平台检测到的安全告警进行预警。经人工查验预警后，可发布通报，进行全院区风险排查。处置工单流程工单处置流转，通过平台的工单流转及处理状态实时追踪快速隔离并补救，减少跨院沟通协作的时间成本，将事件影响范围最快的降到最低。（需提供产品功能截图证明并加盖公章） |
| 安全分析能力 | 安全分析模型 | ★应内置包括规则模型、关联模型、统计模型、情报模型、AI模型等不少于5类安全分析模型，数据配置可选择不同作用域，如全局通用、单选机构，单选机构可选择单独的组织架构。（提供界面截图）安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击 链、可选字段、告警描述、处置建议等内容；★支持时间序列、UEBA、贝叶斯、随机森林等不少于三种长周期高级机器学习算法；（提供证明材料）支持对安全日志里200个以上字段进行任意形式的逻辑与或非形式组合建模，字段包括但不限于应用协议、目的IP、目的主机名、目的端口、目的用户名、数据流方向、情报IOC等，运算方式包括但不限于等于、不等于、大于、小于、大于等于、小于等于、属于、不属于、存在、不存在，并能根据组合方式自动生成运算表达式； |
| 威胁情报分析 | 碰撞情报IOC支持通过情报源、IOC类型、情报类型、置信度等多维度进行碰撞分析； 支持对接威胁情报中心，支持情报离线更新及在线更新，支持查看情报源中有效情报数、最近更新条数、最近更新时间、今日更新情报数、昨日命中情报数等；支持对接第三方威胁情报平台，支持配置情报碰撞接口及查询接口，支持查看请求接口数、今日情报请次数、昨日命中情报数，支持设置接口请求频率阈值，进行接口请求限制；  |
| 网络实体分析画像 | 实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持通过一键溯源进行威胁关系的自动拓展；（提供相关截图证明） |
| 场景化分析 | 支持需封禁的外部攻击者、外部攻击者成功入侵、CVE漏洞被利用成功的系统、感染勒索病毒的主机、正在挖矿的主机、威胁情报、存在Webshell后门的系统、收到钓鱼邮件的邮箱、正在暴力破解的攻击者、存在弱口令的系统等10种以上的内置安全分析场景，基于场景特性进行默认条件的数据聚合分析，支持至少3个任意字段的快速聚合分析，聚合后的所有数据均支持快速统计分析，展示统计排序信息，支持分析结果导出。 |
| 处置响应 | 设备联动 | 支持钉钉、阿里云、腾讯云等进行消息通知；支持与不同品牌的网关类安全产品进行联动防护，防护策略支持设置每次阻断不同时长生效时间，时间设置包括10分钟，30分钟，6小时，24小时，72小时，7天，15天，30天，3个月，永久阻断，支持将安全策略同步下发至多台联动设备；支持查看封禁设备数、封禁IP数、自动封禁IP数、本日解禁IP数、封禁订阅规则数、封禁SOAR剧本数，支持查看最近7天封禁IP趋势及防护设备封禁IP分布；支持封禁策略批量删除、解禁、导出；（须提供相关截图证明）支持对接同厂商EDR同步资产指纹信息及脆弱性信息，支持与EDR集成联动，一键查杀木马病毒； |
| 可视化安全分析 | 安全态势可视化 | 支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示，提供不少于10块大屏展示界面，支持大屏轮播，可自定义选择播放大屏及轮播时间间隔；★支持立体、平面、球面等多种维度的网络实体关系透视，点击每个实体可展示资产名称、风险评级、告警TOP3、最近异常发生时间等，点击实体间的访问连线可展示实体间访问方向、访问类型、累计流量、最近访问时间等（提供界面截图）； |
| 系统管理 | 组件管理 | 支持对接入探针进行统一管理，支持查看探针在线、离线、升级等状态，可对license已过期、即将过期探针进行预警，对内存长时间超出阈值、CPU长时间超出阈值探针进行预警；支持平台统一升级和配置探针，沙箱文件检测可配置安全文件大小、文件访问方向、检测配置、检测结果复用、真实格式识别、沙箱网络行为、沙箱操作系统配置等，流量探针可配置检测模式 |
| 综合流量探针 |
| 性能要求 | MTBF 大于65000小时吞吐率：网络层：2Gbps，应用层：1GbpsWEB检测：HTTP最大并发数8万/秒邮件检测：邮件处理数: 150万封/24小时文件检测：5万个/24小时支持管理节点10个 |
| 硬件要求 | 硬件外形：软硬一体化2U标准机架式设备； 电源：1+1冗余电源 CPU：4核8线程\*1 内存：32G 硬盘容量：2T\*2，带RAID1，可用磁盘空间不小于2T 接口数量：标配10个接口类型：千兆RJ45网口\*2(管理口\*2)、千兆RJ45网口\*4、千兆业务SFP光口\*4（标配千兆多模光模块\*2） |
| 综合能力 | 支持COAP、MQTT等物联网协议解析和审计支持GOOSE、MODBUS等工控协议解析和审计支持GTP、PFCP、NGAP等5G协议解析和审计支持识别QQ、WEB、LDAP、FTP、TELNET、邮件、SMB、RADMIN、ORACLE、MSSQL、SYBASE、MYSQL、DB2、PostgreSQL、REDIS、MQTT等登录行为；支持多层 VLAN、VXLAN、MPLS、GRE、VN-Tag、Capwap等网络流量的解析检测 |
| 审计协议 | 支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOWV9、TFTP等协议报文（HTTPS、SMTPS、POP3S、IMAPS加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号； |
| 风险告警抑制 | 支持告警抑制功能，在重复攻击手段下能够减少相同告警数量，提高用户分析效率，可自行设置告警抑制周期、告警上限、抑制阈值、持续时间、启用维度等 |
| 弱口令风险检测 | 支持对HTTP、IMAP、SMTP、POP3、Redis、Telnet、FTP、PostgreSQL、MQTT等协议的弱口令检测 |
| 攻击检测 | 支持30个以上的深度检测模块，对流量进行二次分析，提高攻击检测的准确性（提供功能截图证明） |
| 敏感信息分析 | 支持识别流量中的个人敏感信息，包括身份证、银行卡、手机号、港澳通行证等，并展示传输信息的协议、网站域名、URL、客户端IP、服务端IP，便于用户发现敏感信息的传输安全隐患和处置 |
| 流量异常监控 | 支持对流量中的数据包、会话连接、重传包、网络报文等状态进行检测，可对业务网络流量传输异常告警 |
| 自定义规则 | 支持根据规则类型、协议、源IP/端口、目的IP/端口、流量方向、流量状态、风险类别、风险等级、风险阶段、攻击者、攻击状态、阈值、Flowbits、规则内容等自定义审计规则。 |
| 动态沙箱检测 | ★采用多并发沙箱检测技术，集成相关的操作系统winXP、win7、win10、linux等多种检测环境，拥有多项自主研发技术。结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析（提供功能截图证明） |
| ★支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现（须提供相关截图及证明） |
| DNS协议分析 | 具备DNS重绑定攻击检测能力，分析域名与IP地址间的获取关系，并记录DNS解析返回的多个IP与时间 |
| NAT解析 | 支持导入和导出代理IP/IP段的过滤串配置 |
| 一键登录排错 | 支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、信息收集等功能。 |

## 3.18漏洞扫描设备

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 性能规格 | 软硬一体化2U标准机架式设备，1+1冗余电源，硬盘容量2TB\*1，内存32GB，支持4个扩展插槽，扩展类型支持4电4光、8电、8光、2万兆，1\*RJ45串口，2\*GE网口，2\*USB口，提供5年硬件维保服务及特征库升级，任务并发数≥15，单任务并发IP数≥90。 |
| 总体要求 | 支持用户自定义系统名称、版权信息和系统的Logo信息，而无需进行定制化，要求提供截图证明材料。 |
| 系统漏扫要求 | 厂商漏洞特征库大于200000条；提供详细的漏洞描述和对应的解决方案描述； |
| ★支持基于脚本的网站漏洞扫描方法，要求提供证明材料 |
| 支持取证式网站漏洞扫描方法，要求提供证明材料 |
| 支持对各种网络主机、操作系统、网络设备(如交换机、路由器、防火墙等)、常用软件以及应用系统的识别和漏洞扫描。 |
| 支持云平台扫描，漏洞覆盖OpenStack、Kvm、VMware、Xen等相关云计算平台。 |
| 支持对Apple软件和应用进行扫描，包括MacOS、Safari、itunes等。 |
| 支持扫描物联网设备的漏洞，至少支持国内摄像头品牌，包括海康威视、宇视、大华，打印机需支持惠普、三星，路由器需支持扫描TP-Link、Netgear、D-link等。 |
| 提供采用SMB、SSH、Telnet、RDP、SNMP等协议对Windows、Linux系统进行登录授权扫描。 |
| ★具备弱口令扫描功能，支持弱口令扫描协议数量≥22种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典，要求提供截图证明材料。 |
| 支持端口探测方式≥7种，如：TCPACK、TCPSYN、TCPConnect、TCPNull、TCPXmas、TCPWindow、TCPFin等。 |
| 网站漏扫要求 | 产品提供Web应用漏洞扫描功能，支持对Discuz、大汉CMS、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2等国内外常见第三方组件扫描。 |
| 支持常见Web漏洞类型的扫描，包括SQL注入、跨站脚本、命令执行、命令注入、代码注入、弱口令、目录遍历、URL跳转、文件包含、反序列化漏洞、文件上传、CSRF跨站请求伪造、信息泄露等。支持OWASPTOP10等安全漏洞。 |
| 存在误报漏洞可通过产品在扫描结果处支持以即时通讯的方式第一时间反馈给厂商协助修改，要求提供截图证明材料。 |
| ★支持识别国内外相关Web应用防火墙品牌，要求提供截图证明材料。 |
| 数据库扫描要求 | 支持Oracle、Mysql、SQLServer、DB2、informix、PostgreSQL、Sybase、达梦、人大金仓的授权数据库漏洞扫描。 |
| 支持配置授权扫描时能够远程对登录验证是否能成功登录目标数据库，防止因输错密码或网络限制未真正授权扫描。 |
| 数据库扫描的漏洞库数量大于3000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD等国际、国内漏洞库标准兼容。 |
| 数据库扫描支持的检测类型大于10种，至少包括弱口令、执行权限过大、访问控制漏洞、提权漏洞、缓冲区溢出漏洞、缺省配置、访问权限绕过、PL-SQL注入、危险程序、安全信息查看等。 |
| 基线核查要求 | 产品提供系统安全配置核查功能，能够对相关操作系统、中间件、数据库、虚拟化设备的安全配置项目进行检查。 |
| 支持相关操作系统的基线配置检查，包括但不限于windows、Linux、Suse、Hp-ux、Solaris、Aix、Debian。 |
| 支持的数据库基线配置检查包括但不限于Informix、DB2、MySQL、SQLServer、Sybase、Oracle。 |
| 支持的应用程序基线配置检查包括但不限于Exchange、Bind、Tongweb、Tomcat、WebSphere、Apache、Weblogic、HIS、IIS、Domino、Resin、Jboss、Nginx。 |
| 支持对云计算环境中相关产品或重要组件的配置核查，包括但不限于OpenStack、VMWareESX/ESXi、VMWarevCenter、Hyper-V、Xen、XenServer。 |
| 检查结果中至少包含如下检查信息：检查点名称、检查方法、标准值、实际值、检查结果、修复建议。 |
| 支持Telnet、SSH、SMB、RDP协议的安全基线配置检查方式。 |
| 用户管理 | ★支持对用户有效期进行详细设置，可以设置不限制，也可以设置每天的哪个时段、每周的周几至周几、每月几号至几号才能正常使用，要求提供截图证明材料。 |

## 3.19数据库内控管理设备

|  |  |
| --- | --- |
| 指标项 | 详细功能要求 |
| 规格 | 配置 | 至少支持10个数据库实例； |
| 硬件规格 | 至少2U机架式设备；双电源、6个电口（1个管理口+1个HA口+4个业务口）、2个扩展槽、32G内存，128G SSD，3T存储空间； |
| 基础功能 | 数据库支持 | 支持ORACLE、SQL SERVER、DB2、MySQL、PostgreSQL、ODPS、informix、达梦、impala、mongdb等相关数据库、国产化数据库、大数据平台、云数据库。 |
| 部署模式 | 支持反向代理、透明代理、透明代理NAT部署。 |
| 支持HA双机主备自动切换，支持策略同步、会话同步机制，保障主备间的一致性。 |
| 核心功能 | 数据智能发现 | ★具备敏感数据探测能力，自动发现SCHEMA、表中的敏感资产，系统内置的敏感数据类型至少包括（投标时提供功能截图）：个人敏感信息：包括中文姓名、身份证、银行卡、医师资格证书、医师执业证书、护照、军官证、中国护照、港澳通行证、永久居住证、大陆居民往来台湾通行证、韩文姓名、英文姓名、姓名拼音等个人信息；机构敏感信息：组织机构代码、组织机构名称、医疗机构登记号、营业执照、社会统一信用代码、税务登记证、开户许可证、证券名称、证券代码、基金名称、基金代码、英文公司名等与企业机构相关的信息；其它基础信息：电话、电子邮箱、地址、邮政编码、IP地址、日期、货币金额、json串、车牌号码等。 |
| 支持敏感发现结果列表展示，包括表名、列名、敏感类型、数据抽样示例等，支持对发现结果进行校正。 |
| 支持从表格、表格列、SCHEMA等维度归类敏感数据资产，形成敏感资产集合进行独立管理。（投标时提供功能截图） |
| 身份准入 | 支持身份的多因素认证，至少应支持应用程序名、IP地址、主机名、操作系统账户、数据库用户、数字证书、身份敏感标签、日期、时间、时间域、身份类别、有效时间、应用用户名、终端IP等因素的任意组合，系统根据多维身份管理策略，自动判别登录主体的合法性，如不符合设定的身份管理策略，登录失败。 |
| ★支持识别真实应用及SQL管理工具的MD5值，防止假冒应用及假冒SQL管理工具违规访问数据库。（提供功能截图证明） |
| ★支持为敏感数据管理人员身份分发唯一的数字证书，每张数字证书只能载入一个唯一的U盾，以实现在数据库用户密码被泄露的情形下，仍能阻止非法用户登陆目标数据库，解决仅依靠密码认证带来的安全不足问题。（投标时提供功能截图） |
| 支持通过不删除账户的方式，在系统中回收资产授权权限。 |
| 身份治理 | 对登陆访问事件信息中的主体信息与身份信息进行比对，对未命中的主体身份，快速发现进行治理 |
| 直连数据库 | 在反向代理模式下，通过在数据库服务器上安装安全代理插件，实现对于通过SQL管理工具或本地等直连数据库的违规连接行为进行准入控制，防止非法人员绕过安全系统，违规对数据库进行访问。（投标时提供功能截图） |
| 安全登陆 | ★支持数据库运维工具免密登陆功能，当数据库管理人员通过Toad或SQL DEVELOPER等工具登陆运维数据库时，通过数据库账号与数字证书的绑定，数据库管理员在运维PC工具中无需输入数据库用户名密码即可登陆已授权访问的数据库，避免运维数据库用户和密码泄漏，保障账号安全。（投标时提供功能截图） |
| ★通过账号托管功能，运维人员使用分配运维账号，运维用户与数据库用户及密码进行映射绑定，运维人员在不知道数据库真实密码的情况下，即可完成对数据库的运维和管理，全面保障数据库安全。（投标时提供功能截图） |
| 访问控制 | 针对敏感数据集合的访问，任何账户（包括DBA\SYSDBA\Schema User\any权限等用户）都需要通过授权才可以访问，对不具备访问权限的操作，明确阻断拒绝，并提示“安全权限不足错误”， 实现用户权限分离管理。 |
| ★支持拦截指定对象的ALTER TABLE、ALTER TABLESPACE、DROP DATABASE、DROP TABLE、DROP TABLESPACE、DROP USER、TRUNCATE等高危操作行为，支持数据库权限变更行为管控。 |
| 支持修改、删除等操作的行数控制，避免数据大量泄漏。 |
| 敏感数据脱敏 | 支持基于列的业务类型，设置脱敏策略，实现相同的业务类型脱敏 |
| 支持动态脱敏，实现脱敏的三层关联，针对不同用户返回对应的预授权结果，脱敏规则需要支持以下脱敏算法：（投标时提供功能截图）1、放行：对于已授权用户，返回真实数据；2、返回空：对含有敏感表格或敏感列的数据结果返回为空值；3、遮盖：全遮盖：默认以遮盖符‘\*’替换敏感列的值；4、部分遮盖：对敏感列的值进行分段，替换其中的一段或数段值；5、随机映射：对数值、字符或字符串进行随机映射处理。 |
| 误操作恢复 | ★至少支持oracle、SQL server、mysql数据库的误删除恢复，当使用DROP和truncate两种命令误删除敏感数据时，系统应及时记录操作的时间、数据库名称、操作类型、操作的对象类型、SCHEMA名称、对象名称、当前状态、使用的SQL语句等信息，并提供一键恢复的功能，辅助完成数据的快速恢复，以支持系统恢复正常。（投标时提供功能截图） |
| 工单管理 | 采用基于WEB界面的工单管理模式，而非授权码方式，通过工作流的方式对敏感表格和敏感SQL访问授权，形成逐级审批机制，只有当访问申请被工作流中的所有审核者审批通过时，才可在合理权限内访问数据库中的敏感资产，无需访问者进行二次输入，避免授权码泄漏带来的非法访问。（投标时提供功能截图） |
| 支持以图形化形式直观展现工单审批流程。 |
| 工单申请支持按不同的库，走不同的审批人方式 |
| 审计 | 支持SQL命令（包括查询、新增、修改、删除等行为）的细粒度审计和分析，并详细记录管理用户的行为信息，包括事件ID、连接ID、规则名称、数据库主机、目标数据库名称、数据库实例名、客户端IP/端口、主机名、数据库用户名、物理地址、交换机端口、应用名称、应用用户、企业用户、命令类型、资产名称、执行时间、影响表数、错误号、审计级别、响应行为、风险级别等。 |
| 数据库监控 | 支持统计数据库请求数、会话数、流量信息 |
| 报表管理 | 支持日报、月报、周报等生成，导出格式支持PDF/word。 |
| 系统管理 | 系统登录 | 支持与AD、LDAP系统联动登录系统。 |
| 平台安全 | 平台具有安全审计员、安全保密员、系统管理员三种角色，实现三权分立。 |
| 支持对平台用户的密码复杂度（数据、大小写字母、特殊字符、密码长度等）、有效期、复杂度、密码错误锁定策略等进行限制，有效期过后提供登录重置密码或禁止登陆需联系管理员处理2种处理方式，以确保平台自身账户的安全。 |
| 告警 | 支持以图形、列表等方式查看告警信息，以列表形式展现的告警信息应当包含告警时间、告警内容、告警等级、用户IP、数据库代理IP、事件等。 |
| 告警方式至少包括：邮件、页面、短信。 |
| 安全告警支持基于任意组合订阅的模式，实现个性化告警订阅管理。 |
| 日志外发 | 支持通过kafka的方式进行日志外发，支持审计、告警等日志外发。 |
| 资质证书 | 产品资质 | 具备ISCCC颁发的《中国国家信息安全产品认证证书》； |
| 具备国家保密科技测评中心颁发的《涉密信息系统产品检测证书》； |
| ★国产化兼容 | 与达梦数据库兼容（提供兼容性证书）；与巨杉数据库兼容（提供兼容性证书）；与南大通用数据库兼容（提供兼容性证书）；与神舟数据库兼容（提供兼容性证书）； |
| 服务能力 | 售后服务能力 | 项目经理、实施工程师须具备相关实施能力。 |

## 3.20信息交换设备

|  |  |
| --- | --- |
| 指标项 | 详细参数 |
| 系统架构 | 系统采用2+1架构设计，包括内端机、外端机和独立的硬件隔离信息交换区,内外网主机系统与交换模块之间采用高性能隔离板卡连接 |
| 隔离区包含基于ASIC设计的开关隔离芯片，不采用SCSI、网卡以及任何加/解密等方式，且不可编程 |
| 标准2U机架式设备 |
| 采用经过裁剪与安全加固的Linux操作系统 |
| 基础性能 | 吞吐率≥800Mbps |
| 最大并发连接数：≥20万 |
| 系统延时：<0.5ms |
| 用户数：无限制 |
| 工作模式 | 支持SAT映射、静态映射等部署模式 |
| 接口 | 接口：12千兆电口，4光口,2串口，4USB,液晶屏，双机热备;标配单电源，可选冗余电源。 |
| 具备网络接口桥接功能 |
| 外端主机不开放任何管理接口，所有配置通过内端主机完成，且配置保存在内端主机上 |
| 安全功能 | 具备访问控制功能，能针对接口、协议、源IP、目的IP、源端口、目的端口、时间、内容独立和组合进行控制 |
| 具备FTP命令过滤功能 |
| 具备FTP、HTTP等内容过滤 |
| 支持自定义对象类型设置，类型包括：主机、网络、端口、时间、内容等，并能与规则策略联动 |
| 支持VRRP协议 |
| 支持单、双向可选的访问控制策略配置管理 |
| 具备常用的系统工具，包括：ping、arp、route、free、ifconfig命令等 |
| 设备断开内外网络TCP/IP连接 |
| 应用功能 | 全面支持TCP/IP及以上协议，支持应用代理访问 |
| 支持FTP、SMB文件同步功能，支持私有协议文件同步客户端模式 |
| 文件同步支持文件名和文件内容关键字过滤、文件后缀黑白名单过滤、文件特征黑白名单过滤、文件大小过滤等 |
| 文件同步支持一对一、一对多、多对一 |
| ★具备自有非第三方的文件特征检查功能，能对EXE、DOC、DOCX、XLS、XLSX、TXT、BMP、MP3、S48、AVI-JPEG、WMV等文件格式进行检查（提供公安部计算机信息系统安全产品质量监督检验中心检验报告） |
| 能防止伪造后缀名或增加二进制执行代码的恶意文件传输（提供公安部计算机信息系统安全产品质量监督检验中心检验报告） |
| ★具备文件上传、下载和IC卡用户认证功能（提供公安部计算机信息系统安全产品质量监督检验中心检验报告） |
| ★具备按角色分配个人目录和共享目录访问操作权限（提供公安部计算机信息系统安全产品质量监督检验中心检验报告） |
| ★具备应用进程认证模块，能够根据设置的应用程序的白名单限制非法程序通过设备访问服务器（提供公安部计算机信息系统安全产品质量监督检验中心检验报告） |
| 支持断点续传功能 |
| 支持Oracle、SQLserver、mysql等相关数据访问和同步，支持同构和异构同步，支持数据库表及字段级同步 |
| 支持规则策略拖移，按照实际需求灵活调整策略顺序，无需重新编辑 |
| 具备端口镜像功能，实现交换机镜像口数据的交互 |
| 设备管理 | 采用B/S结构或串口管理, GUI图形管理界面，采用HTTPS协议连接管理设备 |
| 采用三权分立管理 |
| 支持监控内存使用率、CPU使用率、磁盘使用率、在线时长等信息 |
| 支持内端主机业务口与管理口合并或分离 |
| 系统升级，需要针对升级包做MD5校验 |
| 支持液晶屏显示设备运行状态 |
| 支持一键恢复默认值 |
| 支持设备配置备份和恢复 |
| 支持双机热备以及双机热备状态查询 |
| 日志审计 | 支持记录系统日志、业务日志、告警日志等相关日志，并通过时间、IP地址、动作等条件进行查询，支持日志导出 |
| 支持网络状态实时动态监控 |
| 支持通过SYSLOG、SNMP方式输出 |

## 3.21驻点工程师

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 驻点工程师要求 | 1、驻场期限：3年。2、提供一个驻点工程师负责浙西分院信息安全运维的工作，要求有三年以上的相关工作经验。3、每周驻场运维3天，工作范围包括：安全设备巡检，故障处理，应急响应。 |

## 3.22时间同步服务器

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 参数要求 | 1U标准机架式产品处理器：ARM处理器同步精度：卫星同步精度纳秒级；NTP同步精度毫秒级；存储：256M守时精度：≤28us跟踪通道数：32捕获通道数：128授时容量： 10000次/每秒（单端口）授时精度：≤5us授时频段：GPS: 1575.42±1.023MHz ，北斗: 1561.098±2.046MHz 接口：机箱前部：网络管理端口（RJ45）：管理口；NTP输入端口（RJ45）:NTP INP;PPS授时端口（SMA）：1PPS 10M授时端口（SMA）：10MHZ串行管理端口（RS232）：串口机箱后部；1路GPS/BD天线接口 （支持选配2路）4槽位输出位：NTP输出卡（RJ45）：NTP1~NTP4，支持端口、双卡绑定;光输出卡（ST）：1-4路RS422输出卡（凤凰端子）：1-5路，支持子钟管理指示灯：电源指示灯，标识PWR，绿：有外部电源输入，灭：无外部电源输入；卫星指示灯，标识GNSS，绿：卫星搜星正常，灭：卫星搜星异常； |

## C、第三部分

## 3.23终端

|  |  |  |
| --- | --- | --- |
| **序号** | **设备名称** | **基本参数** |
|  | 台式电脑 | 电脑参数：CPU：i3四核，主频：3.5GHz以上、 内存类型： 8G、显卡接口：HDMI+VGA、显示器类型：宽屏21寸以上、硬盘容量：混合（固态256G+1T机械硬盘），5年质保，提供windows专业版操作系统授权码。 |
|  | 办公软件 | Wps办公软件 三年许可 |
|  | 笔记本电脑 | CPU：i5四核，主频：3.4GHz以上、 内存类型： 8G、宽屏14寸以上、硬盘容量：SSD 512G以上，3年质保。 |
|  | 黑白激光打印机（单面） | 最大打印幅面A4，手动双面，分辨率1200dpi，打印速度18 ppm以上，1年质保。 |
|  | 黑白激光打印机（双面网络） | 最大打印幅面A4，自动双面，支持有线网络，分辨率1200dpi，正常模式(A4)：38ppm以上，1年质保。 |
|  | 彩色激光打印机 | 最大打印幅面 A4最高分辨率 600×600dpi以上黑白打印速度 21ppm以上彩色打印速度 21ppm以上处理器 800MHz以上内存 标配/最大：256MB DDR，256MB NAND闪存以上双面打印 自动网络功能 无线/有线网络打印无线功能 内置802.11b/g/n；通过WEP、WPA/WPA2或802.11x认证；AES加密或TKIP加密； Wi-Fi保护设置；无线直连，1年质保。 |
|  | 多功能一体机 | 最大打印幅面A4，自动双面，支持有线网络，分辨率1200dpi，正常模式(A4)：28ppm以上，支持打印/复印/扫描/传真，1年质保。 |
|  | 针式打印机 | 打印速度：超高速150汉子/秒以上，打印方式:点阵击打式，分辨率600dpi，最大打印幅面A4，3年质保。 |
|  | 热敏打印机（热敏处方） | 1、 打印方式直接行式热敏打印；2、打印速度≥330mm/s；3、接口:钱箱接口,USB（2.0全速）接口,以太网口，后期如要求可选扩并口、Wi-Fi、蓝牙4.0接口；4、黑标检测定位及标签检测功能,根据客户需求，提供二次开发技术支持；提供打印机缺纸、卡纸、联机故障、切刀故障、打印头故障返回指令代码；兼容DS双向通讯协议，带医院专用智能助手调节软件（用于修改打印机参数、升级版本、试双向通讯数据）；5、打印纸宽 82±0.5mm/57.5±0.5mm 纸张厚度0.056~0.1mm 纸卷直径最大外径ф83mm；最小内径ф13mm 打印头寿命：150km，切纸刀寿命：200万次，平均无故障工作时间：360，000小时， 机芯耐久性：15，000，000行；6、出纸方式：上出纸，分辨率：≥203DPI；7、标配自动切纸刀，切纸刀寿命：200万次，切纸方式：支持全切和半切；8、灰度级具备4级可调 智能省电/休眠功能；9、3C认证、CE、能源之星；10、提供3年原厂保修（含热敏头、切刀），厂家上门服务（费用包含在投标总价中），非第三方授权机构，送货时提供原厂针对此项目的质保授权书；投标产品具备自主知识产权的SOC控制芯片，能有效保障国家卫生信息安全，有效防止泄密；需现场提供样机验证及提供国家知识产权局证书证明 |
|  | 条码打印机（热敏标签） | 1. 腕带打印
2. 打印方式:热敏或热转印
3. 打印速度:102mm/s
4. 最大打印宽度:56mm
5. 最大打印长度:584mm
6. 条形码类型:一维:Code 39，Code 93，Codabar，Code 128（带 A/B/C 子集），Interleaved 2-of-5，UPC-A，UPC-E，UPC-A 和 UPC-E（带 2 位或 5 位扩展），EAN-13，EAN-8，EAN-8 和 EAN-13（带 2 位或 5 位扩展），Postnet，Japanese Postnet，Plessey，German Post Code，RSS-14，MSI-3，二维:
7. MaxiCode，MacroPDF417，QR Code（需要亚洲版本打印机），Data Matrix
8. 字体/字符集 标准字体：5种点阵，可扩展的8倍字体
9. 通信接口:USB，串行接口，并行接口，
10. 存储:内存128KB，闪存512KB
11. 介质传感器 反射式，传输式
12. ②标签打印
13. 打印方式:热敏或热转印
14. 打印速度:102mm/s
15. 最大打印宽度:104mm
16. 最大打印长度:991mm
17. 条形码类型:一维码：Code 11，Code 39，Code 93，Code 128，UPC-A，UPC-E，EAN-8，EAN-13，EAN-14，UPC-A，UPC-E，EAN 2 or 5 digit extensions，Plessey，POSTNET，Standard 2 of 5，Industrial 2 of 5，Interleaved 2 of 5，LOGMARS，MSI，Codabar，GS1 DataBar (formerly RSS)
18. 二维码：Aztec，Codablock，Code 49，Data Matrix，MacroPDF417，MaxiCode，MicroPDF417，PDF417，QR Code
19. 通信接口:USB接口，串行接口，并行接口，百兆网络接口（可选）
20. 存储 8MB
21. 介质传感器 反射式、穿透式，1年质保。
 |
|  | 立式扫码枪 | 扫描类型影像扫描 (832 x 504 像素)运动容差78 in/s扫描角度水平：大于46° 垂直：大于28°可识别的印刷对比度最低20%的反射差仰角，偏角70°, 75°解码能力自动识别所有标准1D, PDF, 2D, Postal and OCR码\*原始数据-根据配置不同解码能力有所差异图像传输速度USB2.0≥12兆位/秒，RS-232≥115kb/s图像传输时间USB应用100kb压缩JPEG格式图像传输≤0.15秒，1年质保。 |
|  | 手持扫码枪 | 扫描模式影像式扫描 (838 x 640 像素)抗抖动性最佳焦点处扫描13 mil UPC条码可达到610厘米/秒（240英寸/秒）扫描角度高密度HD：水平41.4°; 垂直：32.2°标准距离SR：水平: 42.4°; 垂直：33°1900/1902:长距离ER：水平l: 31.6°; 垂直：24.4°可识别反射对比度最低20％的反射差斜度，偏度45°, 65°解码能力可读取标准一维、堆叠、二维条码和邮政码以及特定的OCR字符，1年质保。 |
|  | 医生PAD | 处理器架构 ARM架构最高频率 ≥2.8GHz处理器核心 ≥八核心系统内存 ≥4GB存储容量 ≥64GB存储扩展 支持Micro SD（TF）卡，最大支持512GB显卡芯片 ≥Mali G76 720MHz显示屏屏幕尺寸 10.8英寸屏幕分辨率 2560x1600屏幕描述 IPS屏，280 PPI，电容十点触控功能应用WiFi功能 支持802.11a/b/g/n/ac无线协议，双频（2.4GHz+5GHz）蓝牙功能 支持，蓝牙5.0模块，1年质保。 |
|  | 护理PDA | 1、处理器 高通八核处理器，CPU主频≥1.8GHz2、操作系统 Android7.0及以上，定制移动医疗操作系统软件，须提供软件著作权证书3、RAM ≥2GB4、ROM ≥16GB，支持用户存储扩展最大到128GB5、显示屏幕 ≥5.2英寸FHD显示屏，电容式触摸,支持戴手套/带水触摸≥1920(W)×1080(L)全高清6、重量 ≤230g7、设备尺寸 ≤158mm\*78mm\*13mm（提供产品彩页）8、电源 ≥4500mAh锂离子充电电池；电池可拆卸更换，须提供锂电池UN38.3测试报告和锂电池空运证书9、5年质保。 |
|  | 护理移动推车 | CPU芯片：Intel 酷睿i5主板：HM76OS系统：WIN10USB端口 ：USB2.0\*2，USB3.0\*1内存：双通道DDR3 =4GB硬盘：SSD固态硬盘=120GB无线网络：802.11 ac/a/b/g/n内置5Db 天线\*2设计 处理器显卡：IntelHD Graphics 频率200MHz电池电芯：磷酸铁锂电池容量：24V12Ah（288Wh）5寸医疗级双边脚轮，2个万向轮带刹车、2个万向不带刹车，铝合金、不锈钢等优质防锈金属材料，面板采用高光、高亮的ABS抑菌材料，1年质保。 |
|  | 床边结算推车 | 床前结算工作站核心部件包括：计算机、电池、电源控制系统、推车、摄像头。1、计算机参数：CPU芯片：Intel 酷睿i5 ，内存：8GB DDR4，硬盘：PCle NVMe Class35固态硬盘 256GB、无线网络：802.11 ac/a/b/g/n内置5Db 天线\*2设计 2、电池参数：电池原材料：磷酸铁锂，循环次数：可充放电2000次、1000cycles DOD 80%，充电时间：充电时间≤8小时，★电池容量：1152Wh3、推车参数（1）按钮显示面板：电池电源按钮、电量显示指示（2）★外形尺寸：:970（高）\*650（宽）\*550（深） 单位：mm（3）工作台面尺寸：650（宽）\*550（深） 单位：mm（4）推车整机重量：83KG（W/O显示器、计算机、电源）（5）整机材质：全车优质合金防锈金属材料 （6）导轨：进口带阻尼静音导轨（7）抽屉、延伸板：抽屉、延伸板可按医院要求定制4、显示器参数（1）尺寸：大于等于19.5"LED5、1年质保。 |
|  | 摄像头 | 3D体感摄像头，1年质保。 |
|  | 碎纸机 | 碎纸方式 碎状碎纸能力≥15张/次碎纸速度≤3.5米/分碎纸宽度≥220mm，1年质保。 |
|  | 复印机 | 颜色类型:黑白涵盖功能:复印/打印/扫描纠错速度类型:中速最大原稿尺寸:A3处理器:≥1.33GHz（双核）内存容量:≥4GB硬盘容量:≥320GB供纸容量:标准：1200页，最大：3200页介质重量:60-256g/㎡双面器:标配网络功能:支持有线网络打印接口类型:高速USB2.010Base-T/100Base-TX/1000Base-T（RJ-45网络接口）选配：IEEE802.11b/g/n（无线局域网）最高月印量 10万页复印功能复印方式:间接静电成像复印速度:25cpm复印分辨率:600×600dpi，2400×600dpi（平滑处理）复印尺寸:A3-A5R输稿器：25-200%灰度等级 256级复印其它性能 电子分页，自动双面，封面插页/封面复印，复印到封二，校验复印，周边消除功能(开盖复印功能)，边缘/中央消除，校验复印，图像移位，修剪/遮蔽，作业合成，纸型选择，模板，注释，装订，X/Y轴变倍，2合1/4合1/8合1，作业存储，文档存储，自动旋转复印，标签复印，交错分页/杂志分页，背景调整/锐度调整等，1年质保。 |
|  | 读卡器（实体插卡） | 可支持操作接触式 IC 卡、非接触式 IC 卡和磁条卡的多合一读写器，采用 32位高速 CPU 和大容量存储器，具有强大的数据处理能力和存储能力。设备取电和通讯统一通过 RS232 口或 USB 口，USB 采用无驱技术，支持 2 个接触式大卡座，主卡座用于普通常规的使用方式，辅卡座用于插入管理员卡来起到认证和管理的作用，主卡座采用下降式插拔方式，1年质保。 |
|  | 电子卡读卡器 | 识读参数识读模式 CMOS分辨率 752x480识读码制 二维码 PDF417，QR Code，Data Matrix，汉信码等一维码 Code 128，EAN-13，EAN-8，Code39 等识读精度 ≥ 3mil识读景深 40mm~300mm打印对比度 ≥ 30%条码旋转灵敏度 360°@ 0°Pitch and 0°Skew条码倾斜灵敏度 60° @ 0°Roll and 0°Pitch条码偏转灵敏度 60°@ 0°Roll and 0°Skew环境光照度 0 ~ 100,000 LUX，1年质保。 |
|  | 自助挂号机 | 主机：Intel I3 CPU及以上/Intel工控主板/内存不低于4G/固态硬盘容量不小于120G/长城350W电源/集成网卡、显卡/接口部份：串口：6个；USB口：8个；网络100/1000M口：1个操作系统：正版WIN7操作系统。各地区医保中心专用的读卡器，可读医院就诊卡、市民卡读卡，USB（HID无驱）通讯，可配置1个大卡座、4个SAM安全模块17寸（4：3）电容式（10点）触摸屏, 防尘、防漂移,免维护,单点触摸≥7000万次；感应时间：<6ms 透光率：>98%；分辨率：4096\*409617寸液晶屏，显示比例:4:3标准屏; 最大分辩率1280\*1024，1年服务。 |
|  | 自助检验单打印机 | 1、显示模块尺寸：19”（4:3）LED屏（横式）；最大分辨率：1280x1024；亮度：250°亮度以上；对比度：1000:1；（透射）；响应时间：6.3ms；输入/接口方式： VGA、HDMI；观看视角（水平/垂直）：80°/80°/80°/80°（上/下/左/右）； 2、触摸模块电容触摸屏；支持10个精确触摸点并支持多指手势；真多点，无鬼点，无漂移；操作灵敏，通过手指或其他实体触摸全面实现鼠标功能；透光性90%；触摸点数：10；触摸次数 60,000,000 次/cm²；分辨率：4096\*4096；触摸协议 HID, TUIO, Flash；最小触摸直径：5mm；触摸所需力度无需挤压，仅需接触屏幕表面 3、主机部分嵌入式工控主机CPU I5，内存配置: 4G；固态硬盘:128G，声卡、网卡、显卡集成）4、黑白激光打印机产品类型:黑白激光打印机，最大打印幅面 A4，内存标配：32MB，黑白打印速度 38ppm，首页打印时间6.9秒 产品特性:自动双面打印，打印方式：激光电子成像，双面打印：自动5、二维码扫描模块识读参数：识读模式 CMOS分辨率 752x480识读码制：二维码 PDF417，QR Code，Data Matrix，汉信码等；一维码 Code 128，EAN-13，EAN-8，Code39等识读精度 ≥ 3mil；识读景深 40mm~300mm；打印对比度 ≥ 30%条码旋转灵敏度 360°@ 0°Pitch and 0°Skew条码倾斜灵敏度 60° @ 0°Roll and 0°Pitch条码偏转灵敏度 60°@ 0°Roll and 0°Skew环境光照度 0 ~ 100,000 LUX6、外形：钢制金属烤漆机柜（可定制颜色）；材质：坚硬厚实，不易变形；表层处理：防锈、防腐、耐磨，不易沾污损坏，亚光漆；内部结构：模块定位，布线规范整齐；外部结构：各部件模块与机柜结合紧密，布局合理，工艺精细。装有立体音响、机柜材料为1.5mm锌板、1.5mm冷钢板，内置音响，外接网络接口、USB接口等。整机充分考虑设备散热问题，提供无噪音的散热解决方案；安全性要求：充分考虑到设备使用环境的特殊性，在安全性及防尘、防盗方面处理的解决方案，1年服务。 |
|  | 自助发票打印机 | 1.全加强钢架立式机柜；机内模块全部采用拖拉式导轨维护；全开门设计，方便维护机身整体防暴设计；2.金属机身；钢板选用优质冷轧钢板；厚度≥2mm；机身坚固耐用，机身表面采用耐磨防腐喷粉工艺。3.一体工控主机 1.CPU I3或以上，32寸触摸屏；4.内存： 4G或以上；5.接口：6个COM，6个USB；6.网口：1个RTL8111H千兆网络接口；7.音频接口：一组音频输入/输出接口；8.操作系统：Windows 7；9.全金属工控主机机箱；10.输入电压：220VAC±10%，50Hz/60Hz；11.5-12V电源接口。12.摄像头 可扩展双目摄像头，支持人脸识别。13.票据打印机 热转印碳带打印机，可支持110MM宽卷式医疗票据。14.凭证小票打印机 可扩展80mm热敏切刀打印机。15.彩色A4打印机 A4幅面彩色打印机，纸盒容量500页或以上；16.二维码扫码模组 霍尼韦尔二维码模组。17.市民卡、健康卡阅读器 卡触点可使用次数>20万次；支持ISO7816标准卡尺寸，同时可附加4个符合GSM 11.11的SIM的卡尺寸SAM卡座；卡电流70MA；USB接口；通讯速率 T=0:9600-38400bps T=1:9600-115200bps；状态显示4指示灯；LCD 128\*64；工作温度：-10℃-50℃，相对湿度：5%-93%（非冷凝）；操作系统支持WINXP、7、8、Linux、Android、IOS；外观尺寸180mm\*80mm\*54mm；符合卫健委标准；18.输入 电源：198V～242V，1.5A，整机功率≤400W，1年服务。 |

**四、商务及技术要求**

**4.1商务条款**

1、实施要求

1）：投标人有完整的备品备件库。投标时需提供相关设备清单及序列号，中标后以便用户现场确认，项目实施期间，需根据用户要求提供核心产品的现场备件服务。因本次涉及整个医院核心数据中心建设，为保证数据中心的稳定运行，中标后5个工作日内（合同签订前）前至项目建设试运行结束，要求提供与医院现有核心虚拟化平台等同的设备作为保障数据中心业务割接使用的备机置于用户现场。预计现场保障时间为1个月左右，租用费用计入总报价。

2、售后服务

1）：整体系统验收合格后质保5年（除产品明确要求外），与单个产品质保要求冲突时，以单个产品要求为准。

2）：在系统的服务期内，投标人应确保系统的正常使用。在接到用户服务要求后应立即做出回应，并在承诺的服务时间内实施服务。

3）：维保期内出现问题，7×24小时服务，1小时内响应，4小时内到达现场，如出现重大问题，必须2小时内到过现场，快速判断及排除故障，如2小时内不能解决问题，应提供替代设备应急。

**第四部分** **评标办法**

**评标办法前附表**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评标标准 | 权重 | 投标文件中评标标准相应的商务技术资料目录 \* |
| 1 | 投标人资信：投标人具有ISO27001信息安全管理体系认证证书得1分，其他不得分。提供证书扫描件，否则不得分。投标人具有ISO45001职业健康安全管理体系认证证书得1分，其他不得分。提供证书扫描件，否则不得分。 | 2 |  |
| 2 | 提供投标人类似项目成功案例，每个业绩得1分，最多得2分（提供合同扫描件） | 2 |  |
| 3 | 根据采购内容及要求“招标设备参数要求”的响应情况（包括所投标产品的详细配置、主要技术参数、随机软件等）未满足招标文件标注“▲”的实质性要求（条款、参数）的，该供应商的投标文件将被视为无效。标注 “★”的重要技术指标（条款、参数）有偏离的，负偏离（功能、性能和技术指标低于招标内容及需求）项每项扣1.5分；扣完为止。未标注“★”的一般技术指标（条款、参数）有偏离的，负偏离（功能、性能和技术指标低于招标内容及需求）项每项扣1分；扣完为止。 | 20 |  |
| 4 | 根据投标人对采购人现状的理解与分析，对采购人系统运行的硬件平台、系统环境以及系统平台安全方案。方案详细合理可行的得4分，基本合理可行的得3分，方案内容存在缺陷的得2分，方案混乱、不可行的得1分，不提供不得分。 | 4 |  |
| 5 | 投标方案总体设计和产品选型等，是否详细阐述实现思路和关键技术，包含了完整的软硬件系统建议方案。方案详细合理可行的得4分，基本合理可行的得3分，方案内容存在缺陷的得2分，方案混乱、不可行的得1分，不提供不得分。 | 4 |  |
| 6 | 投标人组织实施方案的情况，包括系统集成、产品供货、验货、安装调试、试运行、测试、调优、系统管理、系统运行维护培训、网络培训等内容，以及组织机构、工作时间进度表、工作程序和步骤、管理和协调方法、关键步骤的思路和要点等。全部满足得2分；欠佳或缺陷的每项（次）扣0.5分；缺项或不合理的每项（次）扣1分，本项分值扣完为止；未提供不得分。 | 2 |  |
| 7 | 演示：为满足我院特性化需求，要求本项目部分设备需提供部分功能演示，以验证产品厂家是否可以满足我院的需求，演示功能项要求如下：1、超融合系统（1）支持存储分卷功能，以物理主机为单位划分为不同的存储卷，可将集群内全闪存的磁盘组成一个高性能存储池，满足高性能应用需求，将混闪磁盘组成一个大容量存储池，满足低性能大容量应用需求。所有类型不同性能磁盘均可支持分区，包含NL-SAS，SATA，SSD，SAS等。全部满足得2分，否则不得分。（需要投标人对本功能项进行演示，提供演示视频。）（2）支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离。全部满足得3分，否则不得分。（需要投标人对本功能项进行演示，提供演示视频。）（3）基于对我院有效安全防护和防止勒索病毒的需求，支持与本次购买的下一代网络防火墙进行安全联动，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息。全部满足得2分，否则不得分。（需要投标人对本功能项进行演示，提供演示视频。）2、本院容灾节点（1）存储自带杀毒引擎功能，文件写入存储会进行杀毒，文件状态分为未知、安全、隔离、信任、被删除状态，防止病毒在存储进行扩散。全部满足得3分，否则不得分。（需要投标人对本功能项进行演示，提供演示视频。）以上演示内容及讲解过程录制视频，总共演示时间不超过5分钟，以.mp4格式，存储于U盘或光盘。演示U盘或光盘以EMS或顺丰邮寄形式在响应文件提交截止时间前递交，演示U盘应当密封包装并在包装上标注演示U盘、项目名称、标项、供应商名称并加盖公章。未按文件要求提供演示U盘造成评审专家无法正常评审的风险由供应商自行承担。（演示U盘或光盘请单独封装），能够清晰展示演示项目内容即可。 | 10 |  |
| 8 | 1、投标人提供的售后服务方案及服务承诺的可行性、完整性，免费质保年限、售后服务响应时间、到达现场时间、修复速度、备件库的面积及备件库的管理情况，是否满足或优于采购人要求，服务承诺落实的保障措施，质保期内外的后续技术支持和维护能力情况等。完全满足得2分；有缺失得1分；未提供不得分。2、结合采购人设备清单及目前实际情况，投标人需提供以下实施方案：①数据库灾备实施方案②虚拟化平台迁移方案；从数据库灾备、虚拟化平台迁移方案的安全性、稳定性、完整性出发，提供整个数据库灾备、虚拟化平台迁移的具体方案，回退机制等。每满足一项得1分，最高得2分。3、信息安全管理能力：投标人具有信息安全风险评估类系统软件的得2分，提供软件截图及软件著作权登记证书扫描件件 | 6 |  |
| 9 | 投标人项目负责人要求：项目负责人同时具有系统集成项目管理工程师证书、安全服务工程师证书、CISP注册信息安全管理人员证书得6分，否则得0分； | 6 |  |
| 10 | 投标人服务团队人员要求：拟投入本项目的项目团队（除项目负责人）整体能力情况（各人员工作履历、职称、学历、技术能力等情况介绍）及人员配置合理性（提供以下人员的社保证明，否则不得分）：1、项目团队（除项目负责人）中具有工信部认证的操作系统高级应用工程师认证的，每个得1分，最高得2分，提供证明材料，否则不得分。2、项目团队（除项目负责人）中具有系统集成项目管理工程师证书的，每个得1分，最高得2分，提供证明材料，否则不得分。3、项目团队（除项目负责人）中具有中国网络安全审查技术与认证中心（CCRC）CISAW认证的，得2分，提供证明材料，否则不得分。）4、项目团队（除项目负责人）中具有信息系统项目管理师（高级）得2分，提供证明材料，否则不得分。5、项目团队（除项目负责人）中具有信息安全工程师CISP认证的，得2分，提供证明材料，否则不得分。 | 10 |  |
| 11 | 验收方案：方案详细合理可行的得2分，方案内容存在缺陷的得1分，不提供不得分。 | 2 |  |
| 12 | 培训方案：方案详细合理可行的得2分，方案内容存在缺陷的得1分，不提供不得分。 | 2 |  |
| 13 | 有效投标报价的最低价作为评标基准价，其最低报价为满分；按［投标报价得分=（评标基准价/投标报价）\*30］的计算公式计算。评标过程中，不得去掉报价中的最高报价和最低报价。因落实政府采购政策需要进行价格调整的，以调整后的价格计算评标基准价和投标报价。 | 30 |  |

 \***备注：**投标人编制投标文件（商务技术文件部分）时，建议按此目录（序号和内容）提供评标标准相应的商务技术资料。

**一、评标方法**

**1.本项目采用综合评分法。**综合评分法，是指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

**二、评标标准**

**2.** **评标标准：**见评标办法前附表。

**三、评标程序**

**3.1符合性审查。**评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。不满足招标文件的实质性要求的，投标无效。

**3.2 比较与评价。**评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

**3.3汇总商务技术得分。**评标委员会各成员应当独立对每个投标人的商务和技术文件进行评价，并汇总商务技术得分情况。评标委员会成员总评分偏离平均分30%以上的，以及个人主观打分偏离所有评标委员会成员主观打分平均值30%以上的，由评标委员会启动评分畸高、畸低行为认定程序，评标委员会组长应提醒相关评审人员进行复核或书面说明理由，评审人员拒绝说明的，由现场监督员据实记录；评审人员的评审、修改记录应保留原件，随项目其他资料一并存档。

**3.4报价评审。**

3.4.1投标文件报价出现前后不一致的，按照下列规定修正：

3.4.1.1投标文件中开标一览表(报价表)内容与投标文件中相应内容不一致的，以开标一览表(报价表)为准;

3.4.1.2大写金额和小写金额不一致的，以大写金额为准;

3.4.1.3单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价;

3.4.1.4总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

3.4.1.5同时出现两种以上不一致的，按照3.4.1规定的顺序修正。修正后的报价按照财政部第87号令 《政府采购货物和服务招标投标管理办法》第五十一条第二款的规定经投标人确认后产生约束力。

3.4.2投标文件出现不是唯一的、有选择性投标报价的，投标无效。

3.4.3投标报价超过招标文件中规定的预算金额或者最高限价的，投标无效。

3.4.4评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在合理的时间内提供书面说明，必要时提交相关证明材料;投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

3.4.5对于未预留份额专门面向中小企业的政府采购货物或服务项目，以及预留份额政府采购货物或服务项目中的非预留部分标项，对小型和微型企业的投标报价给予20%的扣除，用扣除后的价格参与评审。接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的政府采购货物或服务项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体或者大中型企业的报价给予6%的扣除，用扣除后的价格参加评审。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

**3.5排序与推荐。**采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

多家投标人提供相同品牌产品（单一产品采购项目中的该产品或者非单一产品采购项目的核心产品）且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

**3.6编写评标报告。**评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告。评标委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。

**四、评标中的其他事项**

**4.1投标人澄清、说明或者补正。**对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容需要投标人作出必要的澄清、说明或者补正的，评标委员会和投标人通过电子交易平台交换数据电文，投标人提交使用电子签名的相关数据电文或通过平台上传加盖公章的扫描件。给予投标人提交澄清、说明或补正的时间不得少于半小时，投标人已经明确表示澄清说明或补正完毕的除外。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

**4.2投标无效。**有下列情形之一的，投标无效：

4.2.1投标人不具备招标文件中规定的资格要求的（投标人未提供有效的资格文件的，视为投标人不具备招标文件中规定的资格要求）；

4.2.2投标文件未按照招标文件要求签署、盖章的；

4.2.3采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人未按招标文件要求提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的；

4.2.4投标文件含有采购人不能接受的附加条件的；

4.2.5投标文件中承诺的投标有效期少于招标文件中载明的投标有效期的；

 4.2.6投标文件出现不是唯一的、有选择性投标报价的;

4.2.7投标报价超过招标文件中规定的预算金额或者最高限价的;

4.2.8报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，未能按要求提供书面说明或者提交相关证明材料，不能证明其报价合理性的;

4.2.9投标人对根据修正原则修正后的报价不确认的；

4.2.10投标人提供虚假材料投标的；

 4.2.11投标人有恶意串通、妨碍其他投标人的竞争行为、损害采购人或者其他投标人的合法权益情形的；

4.2.12投标人仅提交备份投标文件，未在电子交易平台传输递交投标文件的，投标无效；

4.2.13 投标文件不满足招标文件的其它实质性要求的；

4.2.14法律、法规、规章（适用本市的）及省级以上规范性文件（适用本市的）规定的其他无效情形。

**5.废标。**根据《中华人民共和国政府采购法》第三十六条之规定，在采购中，出现下列情形之一的，应予废标：

5.1符合专业条件的供应商或者对招标文件作实质响应的供应商不足3家的；

5.2出现影响采购公正的违法、违规行为的；

5.3投标人的报价均超过了采购预算，采购人不能支付的；

5.4因重大变故，采购任务取消的。

废标后，采购机构应当将废标理由通知所有投标人。

**6.修改招标文件，重新组织采购活动。**评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的，将停止评标工作，并与采购人、采购机构沟通并作书面记录。采购人、采购机构确认后，将修改招标文件，重新组织采购活动。

**7.重新开展采购。**有政府采购法第七十一条、第七十二条规定的违法行为之一，影响或者可能影响中标结果的，依照下列规定处理：

7.1未确定中标供应商的，终止本次政府采购活动，重新开展政府采购活动。

7.2已确定中标供应商但尚未签订政府采购合同的，中标结果无效，从合格的中标候选人中另行确定中标供应商；没有合格的中标候选人的，重新开展政府采购活动。

7.3政府采购合同已签订但尚未履行的，撤销合同，从合格的中标候选人中另行确定中标供应商；没有合格的中标候选人的，重新开展政府采购活动。

7.4政府采购合同已经履行，给采购人、供应商造成损失的，由责任人承担赔偿责任。

7.5政府采购当事人有其他违反政府采购法或者政府采购法实施条例等法律法规规定的行为，经改正后仍然影响或者可能影响中标结果或者依法被认定为中标无效的，依照7.1-7.4规定处理。

**第五部分 拟签订的合同文本**

项目名称：

甲方：

乙方：

签订地：

签订日期： 年 月 日

 年 月 日， （采购人） 以 （政府采购方式） 对 （同前页项目名称） 项目进行了采购。经 （相关评定主体名称） 评定， （中标供应商名称）为该项目中标供应商。现于中标通知书发出之日起三十日内，按照采购文件确定的事项签订本合同。

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规之规定，按照平等、自愿、公平、诚实信用和绿色的原则，经 （采购人） (以下简称：甲方)和 （中标供应商名称） (以下简称：乙方)协商一致，约定以下合同条款，以兹共同遵守、全面履行。

**1.1 合同组成部分**

下列文件为本合同的组成部分，并构成一个整体，需综合解释、相互补充。如果下列文件内容出现不一致的情形，那么在保证按照采购文件确定的事项的前提下，组成本合同的多个文件的优先适用顺序如下：

1.1.1 本合同及其补充合同、变更协议；

1.1.2 中标通知书；

1.1.3 投标文件（含澄清或者说明文件）；

1.1.4 招标文件（含澄清或者修改文件）；

1.1.5 其他相关采购文件。

**1.2 货物**

1.2.1 货物名称： ；

1.2.2 货物数量： ；

1.2.3 货物质量：　　　　　　　　　 　 。

**1.3 价款**

本合同总价为：￥ 元（大写： 元人民币）。

分项价格：

|  |  |  |
| --- | --- | --- |
| 序号 | 分项名称 | 分项价格 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 总价 |  |

**1.4 付款方式、时间和条件**

1.4.1甲方应严格履行合同，及时组织验收，验收合格后及时将合同款支付完毕。对于满足合同约定支付条件的，甲方自收到发票后5个工作日内将资金支付到合同约定的乙方账户，有条件的甲方可以即时支付。甲方不得以机构变动、人员更替、政策调整、单位放假等为由延迟付款。

1.4.2合同预付款比例为合同金额的40％；项目分年安排预算的，每年预付款比例为项目年度计划支付资金额的40％；采购项目实施以人工投入为主的，预付款比例为合同金额的20%。对供应商为大型企业的项目或者以人工投入为主且实行按月定期结算支付款项的项目，预付款可低于上述比例或者不约定预付款。在签订合同时，乙方明确表示无需预付款或者主动要求降低预付款比例的，甲方可不适用前述规定。甲方根据项目特点、供应商诚信等因素，可以要求乙方提交银行、保险公司等金融机构出具的预付款保函或其他担保措施。政府采购预付款应在合同生效以及具备实施条件后7个工作日内支付。政府采购工程以及与工程建设有关的货物、服务，采用招标方式采购的，预付款从其相关规定。乙方可登录政采云前台大厅选择金融服务 - 【保函保险服务】出具预付款保函，具体步骤：选择产品—填写供应商信息—选择中标项目—确认信息—等待保险/保函受理—确认保单—支付保费—成功出单。政采云金融专线400-903-9583。

1.4.3资金支付的方式、时间和条件详见***合同专用条款***。

1.4.4乙方可以登录：http://czj.hangzhou.gov.cn/zfcg（杭州市政府采购网），在线发起付款申请和提交发票，并可以在线查询支付信息。具体操作指南可以查询该网站文件《杭州市财政局关于进一步加强政府采购信息公开优化营商环境的通知》（杭财采监〔2021〕17号）。

**1.5 货物交付期限、地点和方式**

1.5.1 交付期限：详见***合同专用条款***；

1.5.2 交付地点：***合同专用条款***；

1.5.3 交付方式：***合同专用条款***。

**1.6 违约责任**

1.6.1 除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式交付货物，那么甲方可要求乙方支付违约金，违约金按每迟延交付货物一日的应交付而未交付货物价格的 0.05 %计算，最高限额为本合同总价的 20 %；迟延交付货物的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同；

1.6.2 除不可抗力外，如果甲方没有按照本合同约定的付款方式付款，那么乙方可要求甲方支付违约金，违约金按每迟延付款一日的应付而未付款的 0.05 %计算，最高限额为本合同总价的 20 %；迟延付款的违约金计算数额达到前述最高限额之日起，乙方有权在要求甲方支付违约金的同时，书面通知甲方解除本合同；

1.6.3 除不可抗力外，任何一方未能履行本合同约定的其他主要义务，经催告后在合理期限内仍未履行的，或者任何一方有其他违约行为致使不能实现合同目的的，或者任何一方有腐败行为（即：提供或给予或接受或索取任何财物或其他好处或者采取其他不正当手段影响对方当事人在合同签订、履行过程中的行为）或者欺诈行为（即：以谎报事实或者隐瞒真相的方法来影响对方当事人在合同签订、履行过程中的行为）的，对方当事人可以书面通知违约方解除本合同；

1.6.4 任何一方按照前述约定要求违约方支付违约金的同时，仍有权要求违约方继续履行合同、采取补救措施，并有权按照己方实际损失情况要求违约方赔偿损失；任何一方按照前述约定要求解除本合同的同时，仍有权要求违约方支付违约金和按照己方实际损失情况要求违约方赔偿损失；且守约方行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式；

1.6.5 除前述约定外，除不可抗力外，任何一方未能履行本合同约定的义务，对方当事人均有权要求继续履行、采取补救措施或者赔偿损失等，且对方当事人行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式；

1.6.6 如果出现政府采购监督管理部门在处理投诉事项期间，书面通知甲方暂停采购活动的情形，或者询问或质疑事项可能影响中标结果的，导致甲方中止履行合同的情形，均不视为甲方违约。

1.6.7违约责任***合同专用条款***另有约定的，从其约定。

**1.7 合同争议的解决**

 本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；不愿和解、调解或者和解、调解不成的，可以选择以下第 ***合同专用条款*** 条款规定的方式解决：

1.7.1 将争议提交***合同专用条款***仲裁委员会依申请仲裁时其现行有效的仲裁规则裁决；

1.7.2 向***合同专用条款***人民法院起诉。

**1.8 合同生效**

本合同自双方当事人盖章或者签字时生效。

**甲方**：  **乙方**：

统一社会信用代码： 统一社会信用代码或身份证号码：

住所： 住所：

法定代表人或 法定代表人

授权代表（签字）： 或授权代表（签字）:

联系人： 联系人：

约定送达地址： 约定送达地址：

邮政编码： 邮政编码：

电话: 电话:

传真: 传真:

电子邮箱： 电子邮箱：

开户银行： 开户银行：

开户名称： 开户名称：

开户账号： 开户账号：

**第二部分 合同一般条款**

**2.1 定义**

本合同中的下列词语应按以下内容进行解释：

2.1.1 “合同”系指采购人和中标供应商签订的载明双方当事人所达成的协议，并包括所有的附件、附录和构成合同的其他文件。

2.1.2 “合同价”系指根据合同约定，中标供应商在完全履行合同义务后，采购人应支付给中标供应商的价格。

2.1.3 “货物”系指中标供应商根据合同约定应向采购人交付的一切各种形态和种类的物品，包括原材料、燃料、设备、机械、仪表、备件、计算机软件、产品等，并包括工具、手册等其他相关资料。

2.1.4 “甲方”系指与中标供应商签署合同的采购人；采购人委托采购代理机构代表其与乙方签订合同的，采购人的授权委托书作为合同附件。

2.1.5 “乙方”系指根据合同约定交付货物的中标供应商；两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购的，联合体各方均应为乙方或者与乙方相同地位的合同当事人，并就合同约定的事项对甲方承担连带责任。

2.1.6 “现场”系指合同约定货物将要运至或者安装的地点。

**2.2 技术规范**

货物所应遵守的技术规范应与采购文件规定的技术规范和技术规范附件(如果有的话)及其技术规范偏差表(如果被甲方接受的话)相一致；如果采购文件中没有技术规范的相应说明，那么应以国家有关部门最新颁布的相应标准和规范为准。

**2.3 知识产权**

2.3.1 乙方应保证甲方在使用该货物或其任何一部分时不受任何第三方提出的侵犯其著作权、商标权、专利权等知识产权方面的起诉；如果任何第三方提出侵权指控，那么乙方须与该第三方交涉并承担由此发生的一切责任、费用和赔偿；

2.3.2具有知识产权的计算机软件等货物的知识产权归属，详见***合同专用条款***。

**2.4 包装和装运**

2.4.1除***合同专用条款***另有约定外,乙方交付的全部货物,均应采用本行业通用的方式进行包装，没有通用方式的，应当采取足以保护货物的包装方式，且该包装应符合国家有关包装的法律、法规的规定。如有必要，包装应适用于远距离运输、防潮、防震、防锈和防粗暴装卸，确保货物安全无损地运抵现场。由于包装不善所引起的货物锈蚀、损坏和损失等一切风险均由乙方承担。

2.4.2乙方提供产品及相关快递服务的具体包装要求应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》，并作为履约验收的内容，必要时甲方可以要求乙方在履约验收环节出具检测报告。

2.4.2 装运货物的要求和通知，详见***合同专用条款***。

**2.5 履约检查和问题反馈**

2.5.1甲方有权在其认为必要时，对乙方是否能够按照合同约定交付货物进行履约检查，以确保乙方所交付的货物能够依约满足甲方之项目需求，但不得因履约检查妨碍乙方的正常工作，乙方应予积极配合；

2.5.2 合同履行期间，甲方有权将履行过程中出现的问题反馈给乙方，双方当事人应以书面形式约定需要完善和改进的内容。

**2.6 技术资料和保密义务**

2.6.1 乙方有权依据合同约定和项目需要，向甲方了解有关情况，调阅有关资料等，甲方应予积极配合；

2.6.2 乙方有义务妥善保管和保护由甲方提供的前款信息和资料等；

2.6.3 除非依照法律规定或者对方当事人的书面同意，任何一方均应保证不向任何第三方提供或披露有关合同的或者履行合同过程中知悉的对方当事人任何未公开的信息和资料，包括但不限于技术情报、技术资料、商业秘密和商业信息等，并采取一切合理和必要措施和方式防止任何第三方接触到对方当事人的上述保密信息和资料。

**2.7 质量保证**

2.7.1 乙方应建立和完善履行合同的内部质量保证体系，并提供相关内部规章制度给甲方，以便甲方进行监督检查；

2.7.2 乙方应保证履行合同的人员数量和素质、软件和硬件设备的配置、场地、环境和设施等满足全面履行合同的要求，并应接受甲方的监督检查。

**2.8 货物的风险负担**

货物或者在途货物或者交付给第一承运人后的货物毁损、灭失的风险负担详见***合同专用条款***。

**2.9 延迟交货**

在合同履行过程中，如果乙方遇到不能按时交付货物的情况，应及时以书面形式将不能按时交付货物的理由、预期延误时间通知甲方；甲方收到乙方通知后，认为其理由正当的，可以书面形式酌情同意乙方可以延长交货的具体时间。

**2.10 合同变更**

合同继续履行将损害国家利益和社会公共利益的，双方当事人应当以书面形式变更合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，各自承担相应的责任。

**2.11 合同转让和分包**

2.11.1合同的权利义务依法不得转让，但经甲方同意，乙方可以依法采取分包方式履行合同，即：依法可以将合同项下的部分非主体、非关键性工作分包给他人完成，接受分包的人应当具备相应的资格条件，并不得再次分包，且乙方应就分包项目向甲方负责，并与分包供应商就分包项目向甲方承担连带责任。

2.11.2乙方采取分包方式履行合同的，甲方可直接向分包供应商支付款项。

**2.12 不可抗力**

2.12.1如果任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间；

2.12.2 因不可抗力致使不能实现合同目的的，当事人可以解除合同；

2.12.3 因不可抗力致使合同有变更必要的，双方当事人应在***合同专用条款***约定时间内以书面形式变更合同；

2.12.4受不可抗力影响的一方在不可抗力发生后，应在***合同专用条款***约定时间内以书面形式通知对方当事人，并在***合同专用条款***约定时间内，将有关部门出具的证明文件送达对方当事人。

**2.13 税费**

与合同有关的一切税费，均按照中华人民共和国法律的相关规定。

**2.14乙方破产**

如果乙方破产导致合同无法履行时，甲方可以书面形式通知乙方终止合同且不给予乙方任何补偿和赔偿，但合同的终止不损害或不影响甲方已经采取或将要采取的任何要求乙方支付违约金、赔偿损失等的行动或补救措施的权利。

**2.15 合同中止、终止**

2.15.1 双方当事人不得擅自中止或者终止合同；

2.15.2合同继续履行将损害国家利益和社会公共利益的，双方当事人应当中止或者终止合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，各自承担相应的责任。

**2.16检验和验收**

2.16.1货物交付前，乙方应对货物的质量、数量等方面进行详细、全面的检验，并向甲方出具证明货物符合合同约定的文件；货物交付时，乙方在***合同专用条款***约定时间内组织验收，并可依法邀请相关方参加，验收应出具验收书。

2.16.2合同期满或者履行完毕后，甲方有权组织（包括依法邀请国家认可的质量检测机构参加）对乙方履约的验收，即：按照合同约定的技术、服务、安全标准，组织对每一项技术、服务、安全标准的履约情况的验收，并出具验收书。

2.16.3 检验和验收标准、程序等具体内容以及前述验收书的效力详见***合同专用条款****。*

**2.17 通知和送达**

2.17.1任何一方因履行合同而以合同第一部分尾部所列明的传真或电子邮件 发出的所有通知、文件、材料，均视为已向对方当事人送达；任何一方变更上述送达方式或者地址的，应于3个工作日内书面通知对方当事人，在对方当事人收到有关变更通知之前，变更前的约定送达方式或者地址仍视为有效。

2.17.2以当面交付方式送达的，交付之时视为送达；以电子邮件方式送达的，发出电子邮件之时视为送达；以传真方式送达的，发出传真之时视为送达；以邮寄方式送达的，邮件挂号寄出或者交邮之日之次日视为送达。

**2.18 计量单位**

除技术规范中另有规定外,合同的计量单位均使用国家法定计量单位。

**2.19 合同使用的文字和适用的法律**

2.19.1 合同使用汉语书就、变更和解释；

2.19.2 合同适用中华人民共和国法律。

**2.20 履约保证金**

2.20.1 采购文件要求乙方提交履约保证金的，乙方应按***合同专用条款***约定的方式，以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式，提交不超过合同金额1%的履约保证金；鼓励和支持乙方以银行、保险公司出具的保函形式提供履约保证，乙方以银行、保险公司出具保函形式提交履约保证金的，甲方不得拒收。

2.20.2 甲方在项目验收结束后及时退还履约保证金。甲方在项目通过验收之日起 5 个工作日内，按***合同专用条款***约定的方式将履约保证金退还乙方，逾期退还的，乙方可要求甲方支付违约金，违约金按每迟延退还一日的应退还而未退还金额的 0.05 %计算，最高限额为本合同履约保证金的 20 %；

2.20.3 如果乙方不履行合同，履约保证金不予退还；如果乙方未能按合同约定全面履行义务，那么甲方有权从履约保证金中取得补偿或赔偿，同时不影响甲方要求乙方承担合同约定的超过履约保证金的违约责任的权利。

2.20.4 甲方根据杭州市政府采购网公布的供应商履约评价情况减免履约保证金。乙方履约验收评价总分为100分的，甲方免收履约保证金；确需收取履约保证金的，履约保证金缴纳最高比例不得超过合同金额的1.0%。

2.20.5甲方在乙方履行完合同约定义务事项后及时退还，延迟退还的，应当按照合同约定和法律规定承担相应的赔偿责任。

2.21对于因甲方原因导致变更、中止或者终止政府采购合同的，甲方应当依照合同约定对供应商受到的损失予以赔偿或者补偿。

**2.22合同份数**

合同份数按***合同专用条款***规定，每份均具有同等法律效力。

**第三部分 合同专用条款**

本部分是对前两部分的补充和修改，如果前两部分和本部分的约定不一致，应以本部分的约定为准。本部分的条款号应与前两部分的条款号保持对应；与前两部分无对应关系的内容可另行编制条款号。

|  |  |
| --- | --- |
| **条款号** | **约定内容** |
| 1.4.4 | 资金支付的方式、时间和条件：**一、中标人为中小企业的，付款方式为：**（1）合同签订并具备实施条件后7个工作日内，甲方向乙方支付2022年度预算金额的40%作为预付款；2022年12月10日前，甲方向乙方支付2022年度预算金额的60%。（若2022年度累计支付款金额达到合同总金额，则最多支付至合同总金额）（2）2023年度预算下达并具备实施条件后5个工作日内，甲方向乙方支付2023年度预算金额的40%作为预付款；项目具备实施条件6个月内，完成系统建设并试运行正常、初步验收合格，甲方向乙方支付2023年度预算金额的60%。（若2022、2023年度累计支付款金额达到合同总金额，则最多支付至合同总金额）（3）2024年度预算下达并具备实施条件后5个工作日内，甲方向乙方支付剩余合同款项的40%作为预付款；正式运行正常6个月后，甲方向乙方支付剩余合同款项的60%。（若2022、2023、2024年度累计支付款总金额达到合同总金额，则至多支付至合同总金额）**二、中标人为大型企业的，付款方式为：**（1）合同签订并具备实施条件后7个工作日内，甲方向乙方支付2022年度预算金额的100%。（若2022年度预算金额达到合同总金额，则最多支付至合同总金额）（2）2023年度预算下达，项目具备实施条件6个月内，完成系统建设并试运行正常、初步验收合格，甲方向乙方支付2023年度预算金额的100%。（若2022、2023年度累计支付款金额达到合同总金额，则最多支付至合同总金额）（3）2024年度预算下达且正式运行正常6个月后，甲方向乙方支付剩余合同款项的100%。**注：本项目预算为780.51万元，其中各年度暂定预算金额为：2022年度为234万元，2023年度为468万元，2024年度为78.51万元（具体以各年度财政实际下达预算为准）。** |
| 1.5.1  | 交付期限：2023年12月前完成建设，投入正常运行，运行6个月后系统无问题，进行项目验收。 |
| 1.5.2 | 交付地点：甲方指定地点 |
| 1.5.3  | 交付方式：详见采购需求 |
| 1.6.7 | 违约责任约定：（1）甲方应当履行合同约定的义务，如有违反，须承担相应的违约责任。（2）乙方必须在整个项目安装调试全部完成后，会同甲方及有关部门共同按有关规范验收，如因项目实施质量问题，不能按期验收或验收不合格，乙方应负责返工所造成的经济损失。由此而造成推迟交付的时间按超期天数计算，每超过一天乙方按本项目总价款的1‰赔偿甲方的经济损失。如因甲方原因造成不能按期完工，工期相应顺延。（3）如在合同规定的工期内，达不到项目规定的技术指标，乙方应当承担违约责任。承担方式和违约金额如下：超期30天内，每天扣合同金额的0.5‰；累计超期30天，甲方有权终止执行合同，并没收履约保证金，同时乙方须无条件退还甲方所有已支付的款项，所退款项每超过一天，乙方按须本项目总价款的1‰赔偿甲方的经济损失。（4）如因乙方原因达不到合格等级的，则必须无条件返工至合格，并全额没收履约保证金。（5）未经甲方同意，乙方不得在任何时期擅自更换投标文件中规定的项目负责人和技术负责人，同时必须确保项目技术人员的数量和水平与投标文件一致，否则甲方有权放弃或终止合同，并没收投标保证金或履约保证金。（6）因乙方原因造成甲方其他系统不能正常运行，酿成重大事故（正常工作日系统中断一天或一天以上）的，将承担全部法律责任，并赔偿经济损失，赔偿金额为项目总价的50%。（7）履行本合同的过程中，确因在现有水平和条件下难以克服的技术困难，导致部分或全部失败所造成的损失，风险责任由乙方全部承担。（8）因不可抗力导致合同不能全部或部分履行，甲、乙双方协商解决。 |
| 1.7 | 本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；不愿和解、调解或者和解、调解不成的，可以选择以下第 1.7.2条款 条款规定的方式解决： |
| 1.7.1 | 将争议提交杭州市仲裁委员会依申请仲裁时其现行有效的仲裁规则裁决； |
| 1.7.2 | 向杭州市人民法院起诉。 |
| 2.3.2 | 不适用 |
| 2.4.1 | 无 |
| 2.4.2 | 按照国家标准和相关规定。 |
| 2.8  | 乙方承担。 |
| 2.12.3 | 因不可抗力致使合同有变更必要的，双方当事人应在30日 内以书面形式变更合同 |
| 2.12.4 | 受不可抗力影响的一方在不可抗力发生后，应在 30日 内以书面形式通知对方当事人，并在 30日 内，将有关部门出具的证明文件送达对方当事人。 |
| 2.16.1 | 1年 |
| 2.16.3 | 检验和验收标准、程序等具体内容以及前述验收书的效力：乙方应提供设备的有效检验文件，经用户认可后，与产品性能指标、合同内容一起作为产品验收标准。用户对产品验收合格后，双方共同签署验收合格证书并加盖公章。验收中发现产品达不到验收标准或合同规定的性能指标，中标人必须更换产品，并且赔偿由此给用户造成的损失。验收费用根据“杭州市政府采购履约验收暂行办法”第二十条规定，首次验收过程中产生的，由甲方承担；属于首次验收不合格，重新验收过程中产生的由乙方承担。 |
| 2.20.1 | 采购文件要求乙方提交履约保证金的，乙方以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式，提交不超过合同金额1%的履约保证金；鼓励和支持乙方以银行、保险公司出具的保函形式提供履约保证。 |
| 2.20.2  | 履约保证金在服务期内不予退还。乙方在前述约定期间届满前能履行完合同约定义务事项的，甲方在前述约定期间届满之日起 5 个工作日内，按约定的方式将履约保证金退还乙方，逾期退还的，乙方可要求甲方支付违约金，违约金按每迟延退还一日的应退还而未退还金额的 0.05 %计算，最高限额为本合同履约保证金的 20 %；  |
| 2.22  | 合同份数一式四份，每份均具有同等法律效力。 |

**第六部分 应提交的有关格式范例**

**资格文件部分**

**目录**

（1）符合参加政府采购活动应当具备的一般条件的承诺函……………（页码）

（2）落实政府采购政策需满足的资格要求………………………………（页码）

（3）本项目的特定资格要求………………………………………………（页码）

**一、 符合参加政府采购活动应当具备的一般条件的承诺函**

（采购人）、（采购代理机构）：

我方参与（项目名称）【招标编号：（采购编号）】政府采购活动，郑重承诺：

（一）具备《中华人民共和国政府采购法》第二十二条第一款规定的条件：

1、具有独立承担民事责任的能力；

2、具有良好的商业信誉和健全的财务会计制度；

3、具有履行合同所必需的设备和专业技术能力；

4、有依法缴纳税收和社会保障资金的良好记录；

5、参加政府采购活动前三年内，在经营活动中没有重大违法记录；

6、具有法律、行政法规规定的其他条件。

（二）未被信用中国（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

（三）不存在以下情况：

1、单位负责人为同一人或者存在直接控股、管理关系的不同供应商参加同一合同项下的政府采购活动的；

2、为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后再参加该采购项目的其他采购活动的。

投标人名称(电子签名)：

 日期： 年 月 日

**二、落实政府采购政策需满足的资格要求**

（根据招标公告落实政府采购政策需满足的资格要求选择提供相应的材料；未要求的，无需提供）

**A**.专门面向中小企业，货物全部由符合政策要求的中小企业（或小微企业）制造或者服务全部由符合政策要求的中小企业（或小微企业）承接的，提供相应的中小企业声明函（附件5）。

**B.**要求以联合体形式参加的，提供联合协议和中小企业声明函（附件5），联合协议中中小企业合同金额应当达到招标公告载明的比例；如果供应商本身提供所有标的均由中小企业制造或承接的，视同符合了资格条件，无需再与其他中小企业组成联合体参加政府采购活动，无需提供联合协议。

 **联合协议**

（联合体所有成员名称）自愿组成一个联合体，以一个投标人的身份参加（项目名称）【招标编号：（采购编号）】投标。

一、各方一致决定，（某联合体成员名称）为联合体牵头人，代表所有联合体成员负责投标和合同实施阶段的主办、协调工作。

二、所有联合体成员各方签署授权书，授权书载明的授权代表根据招标文件规定及投标内容而对采购人、采购机构所作的任何合法承诺，包括书面澄清及相应等均对联合投标各方产生约束力。

三、本次联合投标中，分工如下：（联合体其中一方成员名称）承担的工作和义务为： ；（联合体其中一方成员名称）承担的工作和义务为： ；……。

四、中小企业合同金额达到 %，小微企业合同金额达到 %。

五、如果中标，联合体各成员方共同与采购人签订合同，并就采购合同约定的事项对采购人承担连带责任。

六、有关本次联合投标的其他事宜：

1、联合体各方不再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

2、联合体中有同类资质的各方按照联合体分工承担相同工作的，按照资质等级较低的供应商确定资质等级。

3、本协议提交采购人、采购机构后，联合体各方不得以任何形式对上述内容进行修改或撤销。

联合体成员名称(电子签名/公章)：

联合体成员名称(电子签名/公章)：

……

 日期： 年 月 日

**C、**要求合同分包的，提供分包意向协议和中小企业声明函（附件5），分包意向协议中中小企业合同金额应当达到招标公告载明的比例；如果供应商本身提供所有标的均由中小企业制造或承接，视同符合了资格条件，无需再向中小企业分包，无需提供分包意向协议。

**分包意向协议**

（**中标后以分包方式履行合同的，提供分包意向协议；采购人不同意分包或者投标人中标后不以分包方式履行合同的，则不需要提供。**）

（投标人名称）若成为（项目名称）【招标编号：（采购编号）】的中标供应商，将依法采取分包方式履行合同。（投标人名称）与（所有分包供应商名称）达成分包意向协议。

一、分包标的及数量

（投标人名称）将 XX工作内容 分包给（某分包供应商名称），（某分包供应商名称），具备承担XX工作内容相应资质条件且不得再次分包；

……

二、分包工作履行期限、地点、方式

三、质量

四、价款或者报酬

五、违约责任

六、争议解决的办法

七、其他

中小企业合同金额达到 %，小微企业合同金额达到 % 。 投标人名称(电子签名)：

分包供应商名称：

……

 日期： 年 月 日

**三、本项目的特定资格要求**

（根据招标公告本项目的特定资格要求提供相应的材料；未要求的，无需提供）

**商务技术文件部分**

**目录**

（1）投标函…………………………………………………………………………………（页码）（2）授权委托书或法定代表人（单位负责人、自然人本人）身份证明………（页码）

（3）联合协议………………………………………………………………………………（页码）

（4）分包意向协议…………………………………………………………………………（页码）

（5）符合性审查资料………………………………………………………………………（页码）

（6）评标标准相应的商务技术资料……………………………………………………（页码）（7）投标标的清单……………………………………………………………………（页码）（8）商务技术偏离表………………………………………………………………………（页码）

（9）政府采购供应商廉洁自律承诺书…………………………………………………（页码）

**一、投标函**

（采购人）、（采购代理机构）：

我方参加你方组织的（项目名称）【招标编号：（采购编号）】招标的有关活动，并对此项目进行投标。为此：

1、我方承诺投标有效期从提交投标文件的截止之日起 天（不少于90天），本投标文件在投标有效期满之前均具有约束力。

2、我方的投标文件包括以下内容：

2.1资格文件：

2.1.1承诺函；

2.1.2落实政府采购政策需满足的资格要求（如果有）；

2.1.3本项目的特定资格要求（如果有）。

2.2 商务技术文件：

2.2.1投标函；

2.2.2授权委托书或法定代表人（单位负责人）身份证明；

2.2.3联合协议（如果有）；

2.2.4分包意向协议（如果有）；

2.2.5符合性审查资料；

2.2.6评标标准相应的商务技术资料；

2.2.7投标标的清单；

2.2.8商务技术偏离表；

2.2.9政府采购供应商廉洁自律承诺书；

2.3报价文件

2.3.1开标一览表（报价表）；

2.3.2中小企业声明函（如果有）。

3、我方承诺除商务技术偏离表列出的偏离外，我方响应招标文件的全部要求。

4、如我方中标，我方承诺：

4.1在收到中标通知书后，在中标通知书规定的期限内与你方签订合同；

4.2在签订合同时不向你方提出附加条件；

4.3按照招标文件要求提交履约保证金；

4.4在合同约定的期限内完成合同规定的全部义务。

5、其他补充说明: 。

投标人名称（电子签名）：

 日期： 年 月 日

注：按本格式和要求提供。

**二、授权委托书或法定代表人（单位负责人、自然人本人）身份证明**

**授权委托书（适用于非联合体投标）**

（采购人）、（采购代理机构）：

现委托 （姓名）为我方代理人（身份证号码： ，手机： ），以我方名义处理（项目名称）【招标编号：（采购编号）】政府采购投标的一切事项，其法律后果由我方承担。

 委托期限：自 年 月 日起至 年 月 日止。

 特此告知。

 投标人名称(电子签名)：

 签发日期： 年 月 日

 **授权委托书（适用于联合体投标）**

（采购人）、（采购代理机构）：

现委托 （姓名）为我方代理人（身份证号码： ，手机： ），以我方名义处理（项目名称）【招标编号：（采购编号）】政府采购投标的一切事项，其法律后果由我方承担。

 委托期限：自 年 月 日起至 年 月 日止。

 特此告知。

联合体成员名称(电子签名/公章)：

联合体成员名称(电子签名/公章)：

……

 日期： 年 月 日

**法定代表人、单位负责人或自然人本人的身份证明（适用于法定代表人、单位负责人或者自然人本人代表投标人参加投标）**

身份证件扫描件：

|  |
| --- |
| 正面： 反面： |

 投标人名称(电子签名)：

 日期： 年 月 日

**三、联合协议**

**（以联合体形式投标的，提供联合协议；本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供）**

（联合体所有成员名称）自愿组成一个联合体，以一个投标人的身份参加（项目名称）【招标编号：（采购编号）】投标。

一、各方一致决定，（某联合体成员名称）为联合体牵头人，代表所有联合体成员负责投标和合同实施阶段的主办、协调工作。

二、所有联合体成员各方签署授权书，授权书载明的授权代表根据招标文件规定及投标内容而对采购人、采购机构所作的任何合法承诺，包括书面澄清及相应等均对联合投标各方产生约束力。

三、本次联合投标中，分工如下：（联合体其中一方成员名称）承担的工作和义务为： ；……。

四、（联合体其中一方成员名称）提供的全部货物由小微企业制造，其合同份额占到合同总金额 %以上；……。**（未预留份额专门面向中小企业采购的的采购项目，以及预留份额中的非预留部分采购包，接受联合体投标的，联合体其中一方提供的货物全部由小微企业制造，且其合同份额占到合同总金额 30%以上，对联合体报价给予6%的扣除）**

五、如果中标，联合体各成员方共同与采购人签订合同，并就采购合同约定的事项对采购人承担连带责任。

六、有关本次联合投标的其他事宜：

1、联合体各方不再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

2、联合体中有同类资质的各方按照联合体分工承担相同工作的，按照资质等级较低的供应商确定资质等级。

3、本协议提交采购人、采购机构后，联合体各方不得以任何形式对上述内容进行修改或撤销。

联合体成员名称(电子签名/公章)：

 日期： 年 月 日

注：按本格式和要求提供。

**四、分包意向协议**

（**中标后以分包方式履行合同的，提供分包意向协议；采购人不同意分包或者投标人中标后不以分包方式履行合同的，则不需要提供。**）

（投标人名称）若成为（项目名称）【招标编号：（采购编号）】的中标供应商，将依法采取分包方式履行合同。（投标人名称）与（所有分包供应商名称）达成分包意向协议。

一、分包标的及数量

（投标人名称）将 XX工作内容 分包给（某分包供应商名称），（某分包供应商名称），具备承担XX工作内容相应资质条件且不得再次分包；

……

二、分包工作履行期限、地点、方式

三、质量

四、价款或者报酬

五、违约责任

六、争议解决的办法

七、其他

（分包供应商名称）提供的货物全部由小微企业制造，其合同份额占到合同总金额 %以上。**（未预留份额专门面向中小企业采购的的采购项目，以及预留份额中的非预留部分采购包，允许分包的，分包供应商提供的货物全部由小微企业制造，且其合同份额占到合同总金额 30%以上的，对大中型企业的报价给予6%的扣除）**

 投标人名称(电子签名)：

分包供应商名称：

 日期： 年 月 日

注：按本格式和要求提供。

**五、符合性审查资料**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **实质性要求** | **需要提供的符合性审查资料** | **投标文件中的****页码位置** |
| 1 | 投标文件按照招标文件要求签署、盖章。 | 需要使用电子签名或者签字盖章的投标文件的组成部分 | 见投标文件第 页 |
| 2 | 采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人按招标文件要求提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书。 | 节能产品认证证书（本项目拟采购的产品不属于政府强制采购的节能产品品目清单范围的，无需提供） | 见投标文件第 页 |
| 3 | 投标文件中承诺的投标有效期不少于招标文件中载明的投标有效期。 | 投标函 | 见投标文件第 页 |
| 4 | 投标文件满足招标文件的其它实质性要求。 | 招标文件其它实质性要求相应的材料（“▲” 系指实质性要求条款，招标文件无其它实质性要求的，无需提供） | 见投标文件第 页 |

注：按本格式和要求提供。

**六、评标标准相应的商务技术资料**

**（按招标文件第四部分评标办法前附表中“投标文件中评标标准相应的商务技术资料目录”提供资料。）**

**七、投标标的清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **品牌（如果有）** | **型号（如果有）** | **规格配置详细说明** | **数量** | **备注** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |

注：按本格式和要求提供。

**八、商务技术偏离表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **招标文件章节及具体内容** | **投标文件章节及具体内容** | **偏离说明** |
| 1 |  |  |  |
| 2 |  |  |  |
| …… |  |  |  |

投标人保证：除商务技术偏离表列出的偏离外，投标人响应招标文件的全部要求

注：按本格式和要求提供。

**九、政府采购供应商廉洁自律承诺书**

（采购人）、（采购代理机构）：

我单位响应你单位项目招标要求参加投标。在这次投标过程中和中标后，我们将严格遵守国家法律法规要求，并郑重承诺：

一、不向项目有关人员及部门赠送礼金礼物、有价证券、回扣以及中介费、介绍费、咨询费等好处费；

二、不为项目有关人员及部门报销应由你方单位或个人支付的费用；

三、不向项目有关人员及部门提供有可能影响公正的宴请和健身娱乐等活动；

四、不为项目有关人员及部门出国（境）、旅游等提供方便；

五、不为项目有关人员个人装修住房、婚丧嫁娶、配偶子女工作安排等提供

好处；

六、严格遵守《中华人民共和国政府采购法》《中华人民共和国招标投标

法》《中华人民共和国民法典》等法律法规，诚实守信，合法经营，坚决抵制各种违法违纪行为。

如违反上述承诺，你单位有权立即取消我单位投标、中标或在建项目的建设资格，有权拒绝我单位在一定时期内进入你单位进行项目建设或其他经营活动，并通报市财政局。由此引起的相应损失均由我单位承担。

投标人名称（电子签名）：

日期： 年 月 日

注：按本格式和要求提供。

**报价文件部分**

**目录**

（1）开标一览表（报价表）………………………………………………………（页码）

（2）中小企业声明函………………………………………………………………（页码）

一、开标一览表（报价表）

（采购人）、（采购代理机构）：

按你方招标文件要求，我们，本投标文件签字方，谨此向你方发出要约如下：如你方接受本投标，我方承诺按照如下开标一览表（报价表）的价格完成（项目名称）【招标编号：（采购编号）】的实施。

**开标一览表（报价表）(单位均为人民币元)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **品牌（如果有）** | **规格型号（或具体服务）** | **数量** | **单价** | **总价** | **服务要求（年限）** |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **投标报价（小写）** |  |
| **投标报价（大写）** |  |

**注：**

1、投标人需按本表格式填写，不得自行更改。

2、有关本项目实施所涉及的一切费用均计入报价。**采购人将以合同形式有偿取得货物或服务，不接受投标人给予的赠品、回扣或者与采购无关的其他商品、服务**，**不得出现“0元”“免费赠送”等形式的无偿报价，否则视为投标文件含有采购人不能接受的附加条件的，投标无效；采购内容未包含在《开标一览表（报价表）》名称栏中，投标人不能作出合理解释的，视为投标文件含有采购人不能接受的附加条件的，投标无效。**

3、以上表格要求细分项目及报价，在“规格型号（或具体服务）”一栏中，货物类项目填写规格型号，服务类项目填写具体服务。

4、特别提示：采购机构将对项目名称和项目编号，中标供应商名称、地址和中标金额，主要中标标的的名称、规格型号、数量、单价、服务要求等予以公示。

5、符合招标文件中列明的可享受中小企业扶持政策的投标人，请填写中小企业声明函。注：投标人提供的中小企业声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

二、中小企业声明函

**[招标公告落实政府采购政策需满足的资格要求为“无”即本项目或标项未预留份额专门面向中小企业时，符合《政府采购促进中小企业发展管理办法》规定的小微企业拟享受价格扣除政策的，需提供中小企业声明函（附件5）。]**

**政府采购支持中小企业信用融资相关事项通知**

为贯彻落实中央、省、市关于支持民营经济健康发展有关精神，发挥政府采购在促进中小企业发展中的政策引导作用，缓解中小企业融资难、融资贵问题，杭州市财政局、

中国银保监会浙江监管局、杭州市地方金融监督管理局、杭州市经济和信息化局制定《杭州市政府采购支持中小企业信用融资管理办法》。相关事项通知如下：

**一、适用对象**

凡已在浙江政府采购网上注册入库，并取得杭州市政府采购合同的中小企业供应商（以下简称“供应商”），均可申请政府采购信用融资。

**二、相关信息获取方式**

市财政局在杭州市政府采购网上建设信用融资模块，并与“浙里办”浙江政务服务平台对接，推进政府采购中标成交信息、合同信息等信息资源共享，鼓励各银行采用线上融资模式，将银行业务系统与信用融资模块对接，实现供应商“一次也不跑”，同时提供相关的服务支持，做好协调工作。

**三、　政府采购信用融资操作流程：**

（一）线上融资模式：

　　1.供应商根据合作银行提供的方案，自行选择金融产品，并办理开户等手续；

　　2.供应商中标后，可通过杭州市政府采购网或“浙里办”测算授信额度；

　　3.采购合同签订后，供应商在杭州市政府采购网或“浙里办”向合作银行发出融资申请；

　　4.审批通过后，在线办理放贷手续。

　　（二）线下融资模式：

　　1.供应商根据合作银行提供的方案，自行选择金融产品，向合作银行提出信用资格预审，并办理开户等手续；

　　2.采购合同签订后，供应商在杭州市政府采购网或“浙里办”向合作银行发出融资申请；

　　3.合作银行在信用融资模块受理申请后，供应商提供审批材料。合作银行应对申请信用融资的供应商及备案的政府采购合同信息进行核对和审查；

　　4.审批通过后，合作银行应按照合作备忘录中约定的审批放款期限和优惠利率及时予以放款。

（三）杭州e融平台申请融资

供应商通过杭州e融平台政采贷专区，自行选择金融产品，按规定手续办理贷款流程。

**四、注意事项**

1、对拟用于信用融资的政府采购合同，供应商在签订合同时应当在合同中注明融资银行名称及账号，作为在该银行的唯一收款账号。

2、供应商弄虚作假或以伪造政府采购合同等方式违规获取政府采购信用融资，或不及时还款，或出现其他违反本办法规定情形的，按融资合同约定承担违约责任；涉嫌犯罪的，移送司法机关处理。

附件

**附件1：**

**残疾人福利性单位声明函**

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加\_\_\_\_\_\_单位的\_\_\_\_\_\_项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

 投标人名称（电子签名）：

 日 期：

**附件2：质疑函范本及制作说明**

**质疑函范本**

一、质疑供应商基本信息

质疑供应商：

地址： 邮编：

联系人： 联系电话：

授权代表：

联系电话：

地址： 邮编：

二、质疑项目基本情况

质疑项目的名称：

质疑项目的编号： 包号：

采购人名称：

采购文件获取日期：

三、质疑事项具体内容

质疑事项1：

事实依据：

法律依据：

质疑事项2

……

四、与质疑事项相关的质疑请求

请求：

签字(签章)： 公章：

日期：

**质疑函制作说明：**

1.供应商提出质疑时，应提交质疑函和必要的证明材料。

2.质疑供应商若委托代理人进行质疑的，质疑函应按要求列明“授权代表”的有关内容，并在附件中提交由质疑供应商签署的授权委托书。授权委托书应载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.质疑供应商若对项目的某一分包进行质疑，质疑函中应列明具体分包号。

4.质疑函的质疑事项应具体、明确，并有必要的事实依据和法律依据。

5.质疑函的质疑请求应与质疑事项相关。

6.质疑供应商为自然人的，质疑函应由本人签字；质疑供应商为法人或者其他组织的，质疑函应由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

**附件3：投诉书范本及制作说明**

**投诉书范本**

一、投诉相关主体基本情况

投诉人：

地 址： 邮编：

法定代表人/主要负责人：

联系电话：

授权代表： 联系电话：

地 址： 邮编：

被投诉人1：

地 址： 邮编：

联系人： 联系电话：

被投诉人2

……

相关供应商：

地 址： 邮编：

联系人： 联系电话：

二、投诉项目基本情况

采购项目名称：

采购项目编号： 包号：

采购人名称：

代理机构名称：

采购文件公告:是/否 公告期限：

采购结果公告:是/否 公告期限：

三、质疑基本情况

投诉人于 年 月 日,向 提出质疑，质疑事项为：

采购人/代理机构于 年 月 日,就质疑事项作出了答复/没有在法定期限内作出答复。

四、投诉事项具体内容

投诉事项 1：

事实依据：

法律依据：

投诉事项2

……

五、与投诉事项相关的投诉请求

请求：

签字(签章)： 公章：

日期：

**投诉书制作说明：**

1.投诉人提起投诉时，应当提交投诉书和必要的证明材料，并按照被投诉人和与投诉事项有关的供应商数量提供投诉书副本。

2.投诉人若委托代理人进行投诉的，投诉书应按照要求列明“授权代表”的有关内容，并在附件中提交由投诉人签署的授权委托书。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.投诉人若对项目的某一分包进行投诉，投诉书应列明具体分包号。

4.投诉书应简要列明质疑事项，质疑函、质疑答复等作为附件材料提供。

5.投诉书的投诉事项应具体、明确，并有必要的事实依据和法律依据。

6.投诉书的投诉请求应与投诉事项相关。

7.投诉人为自然人的，投诉书应当由本人签字；投诉人为法人或者其他组织的，投诉书应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

**附件4：业务专用章使用说明函**

（采购人）、（采购代理机构）

我方 (投标人全称)是中华人民共和国依法登记注册的合法企业，在参加你方组织的（项目名称）项目【招标编号：（采购编号）】投标活动中作如下说明：我方所使用的“XX专用章”与法定名称章具有同等的法律效力，对使用“XX专用章”的行为予以完全承认，并愿意承担相应责任。

特此说明。

投标单位（法定名称章）：

 日期： 年 月 日

**附：**

投标单位法定名称章（印模） 投标单位“XX专用章”（印模）

**附件5：中小企业声明函**

**中小企业声明函（货物）**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46 号）的规定，本公司（联合体）参加 杭州市第七人民医院 的 杭州市第七人民医院浙西院区信息化基础设备建设项目 采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. 超融合系统 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

2. 服务器负载均衡 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

3. Pacs系统服务器 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

4. Pacs系统存储 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

5. 数据库一体机平台 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

6. 总分院一体化容灾系统节点（分院） ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

7. 总分院一体化容灾存储节点（分院） ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

8. 准入设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

9. 虚拟化安全 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

10. 防病毒设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

11. 数据库审计 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

12. 桌面管理 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

13. 堡垒主机设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

14. VPN设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

15. 上网行为管理设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

16. 日志审计设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

17. 态势感知设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

18. 漏洞扫描设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

19. 数据库内控管理设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

20. 信息交换设备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

21. 驻点工程师 ，属于 软件和信息技术服务业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

22. 台式电脑 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

23. 笔记本电脑 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

24. 黑白激光打印机（单面） ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

25. 黑白激光打印机（双面网络） ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

26. 彩色激光打印机 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

27. 多功能一体机 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

28. 针式打印机 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

29. 热敏打印机（热敏处方） ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

30. 条码打印机（热敏标签） ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

31. 立式扫码枪备 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

32. 手持扫码枪 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

33. 医生PAD ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

34. 护理PDA ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

35. 护理移动推车 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

36. 床边结算推车 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

37. 摄像头 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

38. 碎纸机 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

39. 复印机 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

40. 读卡器（实体插卡） ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

41. 电子卡读卡器 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

42. 自助挂号机 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

43. 自助检验单打印机 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

44. 自助发票打印机 ，属于 工业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

45. 省专线市医保线路 ，属于 信息传输业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

46. 视联网线路 ，属于 信息传输业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

47. 卫生专网线路 ，属于 信息传输业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

48. 互联网宽带线路 ，属于 信息传输业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

49. 公众互联网宽带线路 ，属于 信息传输业 行业 ；制造商为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 （中型企业、小型企业、微型企业） ；

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

投标人名称(电子签名)：

 日期： 年 月 日

从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

注：1、填写要求：①“标的名称”、“采购文件中明确的所属行业”依据招标文件第二部分投标人须知前附表中“采购标的对应的中小企业划分标准所属行业”填写，不得缺漏；②从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报；③中型企业、小型企业、微型企业等3种企业类型，结合以上数据，依据《中小企业划型标准规定》（工信部联企业〔2011〕300号）确定；④投标人提供的《中小企业声明函》与实际情况不符的或者未按以上要求填写的，中小企业声明函无效，不享受中小企业扶持政策。声明内容不实的，属于提供虚假材料谋取中标、成交的，依法承担法律责任。

2、符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供《残疾人福利性单位声明函》（附件1）的残疾人福利性单位视同小型、微型企业；根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，投标人提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业证明文件的，视同为小型和微型企业。