湖州市中医院

湖州市中医院新院迁建数据中心建设项目

（财政审批编号:HZCG[2023]680号）

公开招标文件

（全流程电子）

项目编号：ZJKX-湖2024006

项目名称：湖州市中医院新院迁建数据中心建设项目

招 标 人：湖州市中医院 （盖章）

代理机构：科信联合工程咨询有限公司 （盖章）

2024年2月

目　　录

第一章 公开招标招标公告

根据《中华人民共和国政府采购法》《政府采购货物和服务招标投标管理办法》及相关法律、法规等规定，经湖州市财政局政府采购监管处(财政审批编号：HZCG[2023]680 号)批准，**科信联合工程咨询有限公司**受**湖州市中医院**委托，现就**湖州市中医院新院迁建数据中心建设项目**进行公开招标采购，欢迎中华人民共和国境内的合格投标人前来参加投标。

一、项目编号：ZJKX-湖 2024006

二、采购组织类型：分散采购委托代理

三、采购方式：公开招标

四、招标项目概况（内容、数量、简要技术要求等）：

序号	项目内容	采购预算	最高限价	数量	简要技术要求
1	湖州市中医院新院迁建数据中心建设项目	1498 万元	1100 万元	1 项	详见招标需求

五、投标人资格要求：

1、符合《中华人民共和国政府采购法》第二十二条规定和浙财采监【2013】24 号《关于规范政府采购投标人资格设定及资格审查的通知》第六条规定,且未被“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、本项目不接受联合体投标。

六、招标文件的获取：

1、获取招标文件时间：/至投标截止时间(潜在投标人获取招标文件前应当在电子交易平台上注册账号并登录，截止时间后不再接受潜在投标人获取招标文件)。

2、本项目招标文件实行网上获取，不再接受投标人现场报名。投标人登录浙江政府采购网（http://zfcg.czt.zj.gov.cn/)进入政采云系统“项目采购”模块“获取招标文件”菜单，进行网上获取招标文件。（“政采云”注册账号、密码登录系统后获取招标文件）。

3、免费注册网址：浙江政府采购网（投标人注册页面）:https://middle.zcygov.cn/settle-front/#/registry“政采云”，咨询电话：95763。已经注册成功的投标人无需重复注册

七、投标文件的递交及相关事宜

1、投标文件递交的截止时间（投标截止时间，下同）为 2024 年 3 月 11 日 14:00 时（北京时间）。

2、投标文件递交方式：

(1)电子投标文件：按政采云平台项目采购-电子交易操作指南及本招标文件要求递交。投标人应于 2024 年 3 月 11 日 14:00 时(北京时间)前将加密的电子版投标文件上传到政采云系统中（不准时上传视为不参加）。

（2）数据电子备份投标文件：以 U 盘形式提供的数据电子备份投标文件（生成格式为.bfbs）格式及内容须与政采云平台项目采购-电子交易操作指南中制作、加密并递交的电子投标文件格式及内容一致。**递交方式：**数据电子备份投标文件应通过邮寄快递方式送达，邮寄地址为：科信联合工程咨询有限公司湖州分公司[湖州市清远路 699 号福美达科技大厦 4 楼]，联系电话：0572-2566197。邮寄截止时间：投标人应于 2024 年 3 月 11 日 12:00 时前准时送达，逾期不予受理。截止开标时间前，招标代理机构统一负责接收。投标人须留足投标文件邮寄时间,确保数据电子备份投标文件于规定的时间前送达指定地点，未按时送达的，均按未提供处理。

注：（1）投标人应权衡利弊考虑是否提供数据电子备份投标文件，招标人及招标代理机构不做强制性要求，若因下一条款（第 3 条）原因须启用数据电子备份投标文件时，而投标人未提供的，视为放弃投标资格，作未递交投标文件处理；（2）投标人提供数据电子备份投标文件的，若需要启用数据电子备份投标文件时，由招标人或招标代理机构启封并进行解密；（3）若投标人未提供数据电子备份投标文件的，招标公告及招标文件中关于数据电子备份投标文件的要求及内容不再适用。

3、CA 锁解密时间为开标当日投标截止时间后 30 分钟内。投标截止时间止未完成上传的电子投标文件作未递交投标文件处理；未按招标文件要求密封、包装的数据电子备份投标文件将拒绝接收。整个开标过程中若因投标人问题造成电子投标文件无法正常解密的，均认定为未提交电子投标文件。若因网络或者其他非投标人问题造成电子投标文件无法正常解密的，启用数据电子备份投标文件，因投标人自身原因造成数据电子备份投标文件无法打开的，作未递交投标文件处理。若正常解密成功，则数据电子备份投标文件不予开启。

4、投标人须在线获取 CA 数字证书（完成 CA 数字证书办理预计一周左右，建议各投标人自行把握时间）,办理流程详见 https://service.zcygov.cn/，并登录“浙江政府采购

网”（https://zfcg.czt.zj.gov.cn/),进入“下载专区”下载“电子交易客户端”，制作投标文件。

5、投标人将加密的电子版投标文件于投标截止时间前上传到政采云系统中。

6、具体的投标文件加密上传等操作详见政采云平台操作指南。(https://service.zcygov.cn）。

八、投标地址：

1、本项目通过“政府采购云平台（www.zcygov.cn）”实行在线投标响应（电子投标）。

2、投标人应当在投标截止时间前，将生成的文件格式“.jmbs”的“电子加密投标文件”上传递交至“政府采购云平台”实行在线投标响应。投标截止时间以后上传递交的投标文件将被“政府采购云平台”拒收，作未递交投标文件处理。

九、开标时间：2024 年 3 月 11 日 14:00 时整

十、开标地址：湖州市公共资源交易中心 2 号楼二楼开标室（湖州市仁皇山片区金盖山路 66 号，届时详见二楼休息区电子显示屏），投标人应在投标截止时间前登入“政府采购云平台（www.zcygov.cn）”在线参与开标，并完成 CA 锁在线解密投标文件等相关工作。

十一、其他事项：

1、本项目为电子招投标项目，实行网上招投标，应按照本招标文件及政采云平台的要求编制、加密并要求投标人通过政采云系统在线投标响应，投标截止时间前须完成电子投标文件的上传，同时投标人须使用在线投标响应文件时所用的 CA 锁，投标人在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政采云平台技术支持热线咨询，联系方式：95763。

2、本项目公告期限为自本公告发布之日起 5 个工作日。投标人如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，以书面形式向招标人、招标代理机构提出质疑，根据《中华人民共和国财政部令第 94 号-政府采购质疑和投诉办法》第十条第二款规定，投标人在法定质疑期内须一次性提出针对同一采购程序环节的质疑，否则招标代理机构有权拒绝第一次质疑以外其他所有质疑。答疑内容是招标文件的组成部分，并将在网上发布补充（答疑、澄清）文件，潜在投标人应自行关注网站公告，招标人不再一一通知，潜在投标人因自身贻误行为导致投标失效的，责任自负。质疑投标人对招标人、招标代理机构的答复不满意或者招标人、招标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。

3、潜在投标人已依法获取**（依法获取指：投标人按本项目招标公告要求在政采云系统上获取并报名成功）**其可质疑的招标文件，可以对该文件提出质疑。未按照规定方式依法获取招标文件的，不得对招标文件提起质疑投诉。

4、答疑内容是招标文件的组成部分，并将在网上发布补充（答疑、澄清）文件，潜在投标人应自行关注网站公告，招标人不再一一通知，潜在投标人因自身贻误行为导致投标失效的，责任自负。

5、参与政府招标项目的注册投标人，需登录浙江政府采购云平台（http://www.zcygov.cn）进行网上报名，尚未注册的投标人应当先在浙江政府采购云平台上申请注册，注册终审通过后再进行网上报名。

6、为有效破解当前中小微企业面临的“融资难、融资贵”困局，充分发挥好政府采购扶持小微企业发展的政策功能，本项目中标人可凭中标通知书等材料至“绿贷通平台”网页（www.lvdt.huzldt.com）或“政采贷”平台网页（www.zcygov.cn）申请相关融资产品。具体操作方式可在“绿贷通”或“政采贷”平台网站查询，也可向“绿贷通”或“政采贷”平台电话咨询（“绿贷通”联系电话：0572-2392590、“政采贷”联系电话：0572-2151055、18698580797）。

7、本项目是否专门面向中小企业采购：否。

8、本项目公告发布网站：浙江政府采购网：http://zfcg.czt.zj.gov.cn/ 、湖州市公共资源交易信息网：http://ggzyjy.huzhou.gov.cn/

十二 、告知事项：

1、评审中需要投标人对投标文件作出澄清、说明或者补正的，评审小组可要求投标人在合理期限内（不少于半小时）通过电子邮件、传真等书面形式或政采云系统作出。

2、所有进入湖州市公共资源交易中心的相关人员应自觉遵守规定，请自觉做好个人防护工作，听从交易中心工作人员引导，主动配合做好体各项防控措施。

十三、联系方式：

1、招标代理机构名称：科信联合工程咨询有限公司

联　　系　　人：王女士　　联系电话：0572-2566197

质疑函接收人：孙女士　　联系电话：0572-2566059

地址：湖州市清远路 699 号福美达科技大厦 4 楼

2、招标人名称：湖州市中医院

联　系　人：杜女士　　联系电话：0572-2770829

质疑函接收人：马先生　　联系电话：0572-2770823

3、同级政府采购监督管理部门

名　　称：湖州市财政局政府采购监管处

联　系　人：程先生

监督投诉电话：0572-2150216

湖州市中医院

科信联合工程咨询有限公司

2024 年 2 月 18 日

第二章 招标需求

一、项目名称：湖州市中医院新院迁建数据中心建设项目

二、项目编号：ZJKX-湖 2024006

三、项目预算：1498 万元

四、项目需求清单和规格型号、技术参数、附件清单等：

1、需求清单

序号	产品	数量	单位
一、硬件（分项最高限价：446 万元）			
1	服务器 1	8	台
2	服务器 2	10	台
3	互联交换机	4	台
4	数据中心汇聚交换机	4	台
5	存储	1	台
6	CDSS 服务器	1	台
7	验章服务器	1	台
8	光纤交换机	4	台
9	云桌面服务器扩容	3	台
10	云桌面终端扩容（含 100 个授权）	200	台
11	运维大屏	3	台
二、软件（分项最高限价：268 万元）			
1	分布式存储软件	1	套
2	虚拟化软件	1	套
3	超融合软件	1	套
4	虚拟化容灾备份系统	1	套
5	数据库容灾系统	1	套
6	IT 综合运维监管平台	1	套
7	IT 综合运维服务平台	1	套
8	数据支撑平台	1	套

9	业务性能保障与优化系统	1	套
10	桌面管理软件	1	套
11	文件安全交互系统	1	套
三、安全（分项最高限价：202 万元）			
1	专网防火墙	4	台
2	外网防火墙	1	台
3	数据中心防火墙	2	台
4	WEB 应用防火墙	1	台
5	数据库审计	1	台
6	内网准入控制	1	套
7	外网准入控制	1	套
8	威胁探针	2	台
9	零信任	1	套
10	终端杀毒软件	1	套
11	服务器防护软件扩容	1	套
12	数据加密	1	套
四、服务（分项最高限价：184 万元）			
1	光纤专线租赁	4	条
2	等保测评服务	1	项
3	安全服务	1	项
4	运维服务	1	项
5	设备部署及系统集成服务	1	项
6	搬迁服务	1	项
7	利旧设备改造	1	项

2、硬件

2.1 服务器1

技术指标	参数要求
品牌	技术成熟的服务器品牌
外观	≥2U机架式服务器，标配原厂导轨
▲配置要求	1.CPU≥2颗Intel 6348 (2.6GHz/28-core)至强系列处理器 2.内存≥1024GB DDR4-3200内存，Advanced ECC、内存在线热备，具备内存主动式检测，最大支持32根DDR4内存，最高速率3200MT/s，支持RDIMM或LRDIMM 3.硬盘≥12*1.92T NVME SSD 硬盘，≥2*480GB SSD (RAID1)用于系统盘，具备Raid重建不可拔出硬盘提示指示灯。配置≥12个热插拔硬盘槽位，可扩展至20个热插拔硬盘槽位。
阵列控制器	≥1个标配SAS Raid阵列卡（不占用PCIE扩展槽），支持Raid0/1/10/5/6，≥4GB缓存，支持缓存数据保护
PCI插槽	最多提供≥8个标准PCIE4.0插槽可用，同时提供阵列卡和网卡扩展
★网卡	配置≥6个10Gb 光纤以太网接口（含原厂光模块），≥4个千兆以太网口，≥2*双口32G HBA卡
GPU	支持8个单宽/3个双宽
接口	≥5个USB3.0接口；
冗余电源	2个≥1300w铂金版热插拔冗余电源，支持96%能效比的钛金版电源选件
冗余风扇	热插拔冗余风扇
工作温度	符合ASHARE A4标准，5-45° C标准工作温度
嵌入式管理	★配置≥1Gb独立的远程管理控制端口，配置前面板独立的USB管理端口。配置虚拟KVM功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。**（提供**

	官网截图证明）
	免费提供升级工具，无需安装代理即可可统一升级同一网络中服务器的固件及驱动程序。
服务器管理系统	服务器管理平台，从服务器管理角度出发，管理服务器内部组件，包含CPU、内存、硬盘、电源、各类插卡等，支持创建、删除存储卷，显示卷的空间使用率、支持对存储的监控，查看使用情况，以及IO。实时IOPS、卷属性，支持将卷挂载在某个主机上。支持对软件定义存储，以及独立存储等存储的管理。支持创建，删除主机，主机集，支持将存储卷和主机的关联
★数据保护	配置数据保护功能，采用无代理的方案，为持续保护业务及数据的安全与平台的深度兼容性，最小恢复单位为一个写I/O操作，可从任意时间点中选择，使应用程序能够基于以前的事务快速地从任一时间点恢复。支持本地复制功能。对于捕获的写I/O，既支持同步复制到本地站点，也支持异步复制到远程站点，提供对同一数据卷的并行本地和远程保护;可以恢复到任意时间点的数据，保证数据安全性
其它安全选项	提供UEFI安全启动; 可配置机箱入侵侦测，在外部打开机箱时提供报警功能。
节能政策	提供中国质量认证中心颁发的节能产品认证证书**（提供有效证书复印件）**
质保服务	提供原厂五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.2 服务器 2

技术指标	参数要求
品牌	技术成熟的服务器品牌
外观	≥2U机架式服务器，标配原厂导轨
▲配置要求	1.CPU≥2颗Intel 6348 (2.6GHz/28核)至强系列处理器 2.内存≥1024GB DDR4-3200内存，Advanced ECC、内存在线热备，具

	备内存主动式检测，最大支持32根DDR4内存，最高速率3200MT/s，支持RDIMM或LRDIMM 3.硬盘≥2*480GB SSD硬盘，≥2*3.84TB SSD缓存盘，≥8*12TB SAS HDD硬盘，托架具备Raid重建不可拔出硬盘提示指示灯。配置≥12个热插拔硬盘槽位，可扩展至20个热插拔硬盘槽位。
阵列控制器	≥1 个标配 SAS Raid 阵列卡（不占用 PCIE 扩展槽），支持 Raid0/1/10/5/6，≥4GB 缓存，支持缓存数据保护
PCI 插槽	最多提供≥8个标准PCIE4.0插槽可用，同时提供阵列卡和网卡扩展
★网卡	配置≥6 个 10Gb 光纤以太网接口（含原厂光模块），≥4 个千兆以太网口，≥2*双口 32G HBA 卡
GPU	支持8个单宽/3个双宽
接口	≥5个USB3.0接口；
冗余电源	2个≥1300w铂金版热插拔冗余电源，支持96%能效比的钛金版电源选件
冗余风扇	热插拔冗余风扇
工作温度	符合 ASHARE A4 标准，5-45° C 标准工作温度
嵌入式管理	★配置≥1Gb独立的远程管理控制端口，配置前面板独立的USB管理端口。配置虚拟KVM功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。**（提供官网截图证明）**
	免费提供升级工具，无需安装代理即可可统一升级同一网络中服务器的固件及驱动程序。
服务器管理系统	服务器管理平台，从服务器管理角度出发，管理服务器内部组件，包含CPU、内存、硬盘、电源、各类插卡等，支持创建、删除存储卷，显示卷的空间使用率、支持对存储的监控，查看使用情况，以及IO。实时IOPS、卷属性，支持将卷挂载在某个主机上。支持对软件定义存

	储，以及独立存储等存储的管理。支持创建，删除主机，主机集，支持将存储卷和主机的关联
★数据保护	配置数据保护功能，采用无代理的方案，为持续保护业务及数据的安全与平台的深度兼容性，最小恢复单位为一个写I/O操作，可从任意时间点中选择，使应用程序能够基于以前的事务快速地从任一时间点恢复。支持本地复制功能。对于捕获的写I/O，既支持同步复制到本地站点，也支持异步复制到远程站点，提供对同一数据卷的并行本地和远程保护;可以恢复到任意时间点的数据，保证数据安全性
其它安全选项	提供UEFI安全启动； 可配置机箱入侵侦测，在外部打开机箱时提供报警功能。
节能政策	提供中国质量认证中心颁发的节能产品认证证书**（提供有效证书复印件）**
质保服务	提供原厂五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.3 互联交换机

技术指标	参数要求
交换容量	≥2.56Tbps，若有不同指标，以官网公布最小值为准；
转发性能	≥1080Mpps，若有不同指标，以官网公布最小值为准；
★安全插卡	要求支持安全插卡，满足后续对安全控制、管理的要求
电源	模块化双电源
风扇	模块化双风扇，前/后通风，风道可调
★接口形态	固定接口48个10G/1G BASE-X SFP+端口，2个40G QSFP+端口，配置2端口40G QSFP+端口，配置24个万兆单模光模块、2条3m万兆互联堆叠线缆，配置≥2个扩展插槽
ERPS	要求支持ERPS功能，并且收敛时间小于50ms，提供第三方测试报告
CPU 保护	实现CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作

网络质量分析	支持智能网络质量分析（iNQA）技术，可快速测量网络性能的检测机制，直接对业务报文进行测量，测量数据可以真实反映网络质量状况，实时感知丢包时间、丢包位置、丢包数量。
业务插卡类型	支持端口扩展板卡
	支持哑终端扫描器插卡
	支持网管插卡
融合 AC	主机融合AC功能，无需配置AC插卡即可以实现对AP的管理，实现有线网络和无线网络一体化
SAVI	设备支持SAVI功能
云管理	要求设备能够被公有云平台管理，能通过蓝牙方式登录公有云平台
Vxlan	支持VxLAN二层互通
	支持VxLAN集中式网关互通功能
	支持EVPN分布式网关二三层互通功能
堆叠	最大堆叠台数≥9台
	支持跨设备链路聚合，单一IP管理，分布式弹性路由
	支持通过标准以太端口进行堆叠（万兆或40G均支持）
	支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预
	支持远程堆叠
Macsec	支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。无需软件授权，要求**提供官网截图证明**
SDN/ OPENFLOW	支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换，需提供官网网站命令手册佐证支持多控制器（EQUAL模式、主备模式）
管理和维护	支持SNMP V1/V2/V3、RMON、SSHV2
	支持OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准
节能政策	设备入选工信部绿色制造名单**（提供工信部官网截图证明）**
	提供中国质量认证中心颁发的节能产品认证证书**（提供有效证书复印**

	件）
质保服务	提供原厂商五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.4 数据中心汇聚交换机

技术指标	参数要求
交换容量	≥2.56Tbps，若有不同指标，以官网公布最小值为准；
转发性能	≥1080Mpps，若有不同指标，以官网公布最小值为准；
★安全插卡	要求支持安全插卡，满足后续对安全控制、管理的要求
电源	模块化双电源
风扇	模块化双风扇，前/后通风，风道可调
★接口形态	固定接口48个10G/1G BASE-X SFP+端口，2个40G QSFP+端口，配置2端口40G QSFP+端口，配置24个万兆单模光模块、2条3m万兆互联堆叠线缆，配置≥2个扩展插槽
ERPS	要求支持ERPS功能，并且收敛时间小于50ms，提供第三方测试报告
CPU 保护	实现CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作
网络质量分析	支持智能网络质量分析（iNQA）技术，可快速测量网络性能的检测机制，直接对业务报文进行测量，测量数据可以真实反映网络质量状况，实时感知丢包时间、丢包位置、丢包数量。
业务插卡类型	支持端口扩展板卡
	支持哑终端扫描器插卡
	支持网管插卡
融合 AC	主机融合AC功能，无需配置AC插卡即可以实现对AP的管理，实现有线网络和无线网络一体化
SAVI	设备支持SAVI功能
云管理	要求设备能够被公有云平台管理，能通过蓝牙方式登录公有云平台
Vxlan	支持VxLAN二层互通

	支持VxLAN集中式网关互通功能
	支持EVPN分布式网关二三层互通功能
堆叠	最大堆叠台数≥9台
	支持跨设备链路聚合，单一IP管理，分布式弹性路由
	支持通过标准以太端口进行堆叠（万兆或40G均支持）
	支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预
	支持远程堆叠
Macsec	支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。无需软件授权，要求**提供官网截图证明**
SDN/ OPENFLOW	支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换，需提供官网网站命令手册佐证支持多控制器（EQUAL模式、主备模式）
管理和维护	支持SNMP V1/V2/V3、RMON、SSHV2
	支持OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准
节能	设备入选工信部绿色制造名单**（提供工信部官网截图证明）**
	提供中国质量认证中心颁发的节能产品认证证书**（提供证书复印件）**
质保服务	提供原厂商五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.5 存储

技术指标	参数要求
▲品牌	技术成熟的存储品牌，投标品牌（非 OEM 原厂）入选 Gartner 主存储魔力四象限领导者象限。**(提供 2023 年 Gartner 魔力四象限截图)**
★体系架构	SAN 和 NAS 一体化，配置 NAS 协议（包括 NFS、CIFS 以及 NDMP），支持 SAN 和 NAS 共资源池，无需独立分配。支持 S3 协议的对象存储。
	存储系统采用对称 AA 架构，LUN 无控制器归属，在多控配置下，能够负载到所有控制器，CPU 利用率差异小于 5%。实现控制器间的负载均

	衡，消除控制器的性能瓶颈，提高系统高可用性；单控制器故障对 LUN 或文件系统访问无影响，业务无感知。**提供第三方测试报告。**
NVMe 协议	前端采用基于 FC 或者 RDMA 的 NVMe 协议，后端支持基于 RDMA 或者 PCIE 的 NVMe 协议，支持端到端 NVMe 架构，减少 IO 路径上的 CPU 开销，进一步提升 IO 性能。**提供官网截图证明。**
时延	稳定时延≤1ms，稳定低时延，确保对于时延要求苛刻的业务能够正常运行；提升提升主机 IO 并发量，应对业务峰值流量冲击。
Raid 支持	支持三盘校验，同一 RAID 组内任意三块数据磁盘(不含热备盘)失效时，数据不丢失。**提供官网截图证明。**
控制器扩展	配置 2 个存储控制器，单台存储可以扩展到 8 个控制器引擎，可以跨控制器实现资源访问，LUN 无控制器归属，多控配置下能够负载到所有控制器。提供相关证明材料。
▲容量要求	1.配置≥8*1.92T NVME SSD 硬盘，≥10*10T NL SAS 硬盘，可用容量≥80TB 2.一级缓存容量配置≥512GB，且任意控制器一级缓存容量≥256GB（不含任何性能加速模块、FlashCache、PAM 卡，SSD Cache、SCM 等）
★端口	配置 10GbE（光口）端口≥8、32Gb FC 端口≥8
空间	采用 2U 盘控一体架构，节省空间，2U 控制框可以支持 36 个盘
端口类型	支持 32Gb FC/16Gb FC/100Gb/25Gb /10Gb /1Gb iSCSI 等主机接口
磁盘扩展性	最大支持磁盘插槽个数≥1200
软件升级	存储系统支持无中断系统软件在线升级和回退。在版本升级和回退的过程中无需重启控制器，主机与存储之间的链路无中断，客户端无感知，升级时长小于 10 分钟。
★QoS	存储配置服务质量控制功能，支持按照 LUN、LUN 组以及主机的方式进行流量控制。提供上限控制和下限保障两种 QoS 策略，支持 Burst 突发流量控制。**（提供相关证明材料）**

快照	存储系统支持保护周期高密快照功能 1.整系统支持 1000000 个快照 2.系统提供每 3 秒做一次快照备份 3.提供无损快照功能，快照创建与删除，系统性能变化幅度小于 5%。 4、支持安全快照功能，支持对快照设置保护周期，在保护周期内快照无法删除，无法篡改快照中的数据。
克隆	存储系统配置克隆功能，并且克隆的从 LUN 创建后无需等待数据同步完成即可映射给主机 I/O 访问，且不影响源 LUN 的业务。
复制	存储支持同步远程复制，支持复制 LUN 在线扩容，容量修改在单端完成，对端容量信息同步修改，对同步复制的状态无任何影响，主机无感知。支持同步复制和异步复制在线相互转换。
租户	存储系统配置 SAN 的多租户功能，多租户功能能够提供存储资源、网络和业务的隔离，客户端通过租户数据逻辑端口只能访问该租户内的共享，并且支持租户自管理。
校验特性	存储支持端到端 DIF 校验特性，对静默数据的修复可以检测和修复。
运维管理	通过性能监控界面可以实时统计指定对象（控制器的缓存、处理器、前端端口，以及 LUN 和卷组等）的性能指标（例如：占用率、IOPS、时延、带宽），并能单独统计读、写 IOPS、时延和带宽指标，且性能监控数据的采样间隔小于等于 5 秒，支持半年以上历史数据的查看和统计。
★SSD 寿命监控	提供 SSD 寿命监控技术，并在系统中显示每一块 SSD 硬盘的磨损度以及预估剩余寿命。**（提供截图证明材料）**
管理软件	有功能全面，图形化的管理软件，包括：盘阵，卷管理软件。配置存储的图形化管理配置和监控软件。
集中管理	支持用一套软件面向管理运维全场景的融合管理，包括资源发放，智能运维以及副本管理，问题检测&定界定位，数据中心洞察等功能，支持快照、克隆、复制、双活等配置策略的统一管理，支持对存储、交换机、主机以及存储池、LUN、文件系统等资源对象，导出性能容

	量等报表和大屏展示。
存储多路径	存储系统支持厂商自研的多路径软件，支持链路的负载均衡，支持路径故障自动切换与回切，支持链路检测和隔离，支持主机链路告警在存储界面统一管理。
功能测试验证	合同签订后七天内提供测试设备对产品功能和性能测试，若无法在规定时间内提供测试设备或测试结果与招标内容不符，影响医院互联互通等级评定和应用软件上线，取消中标资格，中标人承担所有责任。
节能政策	提供中国质量认证中心颁发的节能产品认证证书**（提供有效证书复印件）**
质保服务	提供原厂商五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物。投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.6 CDSS 服务器

技术指标	参数要求
品牌	技术成熟的服务器品牌
外观	≥2U机架式服务器，标配原厂导轨
★配置要求	1.处理器：CPU≥2颗Intel 6326 (2.9GHz/16核)至强系列处理器 2.内存≥64GB DDR4-3200内存，Advanced ECC、内存在线热备，具备内存主动式检测，最大支持32根DDR4内存，最高速率3200MT/s，支持RDIMM或LRDIMM 3.硬盘≥2*480GB SSD硬盘，≥2*1.2T SAS硬盘，具备Raid重建不可拔出硬盘提示指示灯。 4.本次采购Redhat企业版一套
阵列控制器	≥1 个标配 SAS Raid 阵列卡（不占用 PCIE 扩展槽），支持 Raid0/1/10/5/6，≥4GB 缓存，支持缓存数据保护
PCI 插槽	最多提供≥6个标准PCIE4.0插槽可用，同时提供阵列卡和网卡扩展
★网卡	配置≥4 个 10Gb 光纤以太网接口（含原厂模块）
GPU	另配：≥2 个 NVIDIA A40 48G 显存 GPU

接口	≥5个USB3.0接口；
冗余电源	2个≥1300w铂金版热插拔冗余电源，支持96%能效比的钛金版电源选件
冗余风扇	热插拔冗余风扇
工作温度	符合 ASHARE A4 标准，5-45° C 标准工作温度
嵌入式管理	★配置≥1Gb独立的远程管理控制端口，配置前面板独立的USB管理端口。配置虚拟KVM功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。**（提供官网截图证明）**
	免费提供升级工具，无需安装代理即可可统一升级同一网络中服务器的固件及驱动程序。
服务器管理系统	支持创建、删除存储卷，显示卷的空间使用率、支持对存储的监控，查看使用情况，以及IO。实时IOPS、卷属性，支持将卷挂载在某个主机上。支持对软件定义存储，以及独立存储等存储的管理。支持创建，删除主机，主机集，支持将存储卷和主机的关联
★数据保护	配置数据保护功能，采用无代理的方案，为持续保护业务及数据的安全与平台的深度兼容性，最小恢复单位为一个写I/O操作，可从任意时间点中选择，使应用程序能够基于以前的事务快速地从任一时间点恢复。支持本地复制功能。对于捕获的写I/O，既支持同步复制到本地站点，也支持异步复制到远程站点，提供对同一数据卷的并行本地和远程保护;可以恢复到任意时间点的数据，保证数据安全性
其它安全选项	提供UEFI安全启动； 可配置机箱入侵侦测，在外部打开机箱时提供报警功能。
节能政策	提供中国质量认证中心颁发的节能产品认证证书**（提供有效证书复印件）**
质保服务	提供原厂商五年技术支持和原厂保修服务，为了货物是原厂家最新生

	产合法渠道货物，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.7 验章服务器

技术指标	参数要求
功能指标	多密码应用服务支持：设备支持通过密码服务节点来添加多个服务，密码服务节点可独立分配给不同的用户使用
	设备支持“多因子”身份鉴别与访问控制。认证因子至少包含PIN码和智能密码钥匙
	设备支持多版本备份恢复，支持补丁包升级；
	设备支持HA双机热备和多机负载均衡，可多机扩展并行工作
	设备支持通过SNMP协议监控设备状态，支持keystore的配置功能，支持syslog配置。
	设备满足《财政信息系统基于国密算法安全应用接口标准》，与财政现有数字签名服务器器之间实现互签互验，提供财政标准符合性验证截图和数字签名服务器使用场景测试结果截图。
服务器配置指标	2U机架式机箱/550W（1+1）冗余电源/英特尔E3-1220V5 四核/2*RJ-45千兆网口,1*RJ-45管理端口/DDR4-8G内存/2块 1T SATA 企业级硬盘/centos 操作系统
★性能参数指标	SM2生密钥：10000 SM2签名/验签（tps）：20000/10000 SM2加密/解密（tps）:2000/4000 RSA生密钥（1024）：290 RSA1024签名/验签（tps）：11000/140000 RSA生密钥（2048）：60 RSA2048签名/验签（tps）：3100/93000 SM1：9Gbps SM4：8Gbps AES：14Gbps

	DES：1.5Gbps 3DES：620Mbps SM1杂凑算法：6Gbps SHA256杂凑算法：5Gbps SM3杂凑算法：5Gbps
★配置	实际配置：CPU：Intel E3-1220V5 4核；内存：512GB；硬盘：配置2*1T SATA硬盘；2块万兆网卡
质保服务	提供原厂商五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.8 光纤交换机

技术指标	指标参数
类型	FC协议交换机，支持SNMPv3，SMI-S，TACACS+,AAA，SFTP
★配置功能	配置VSAN技术和VoQ技术功能许可 配置ISL Trunking、Extended Fabric、Fabric Vision软件功能
系统架构	机架式安装，无拥塞架构设计，所有FC端口全线速
★端口速率	同时支持FC 128Gb/s，32Gb/s，16Gb/s， 8Gb/s和4Gb/s速率
端口类型	同时支持F/E/M/EX等端口类型
互联扩展	可支持多台交换机级联和Fabric扩展
链路捆绑	支持基于数据帧级的“即插即用”的链路捆绑功能，单个链路聚合带宽最大256G
系统延时	平均延迟≤2.1微秒
监控管理	支持SNMPv1/v3的集中监控管理
安全性	支持数据的压缩及加密、基于数据帧级别的前向纠错和交换机接入认证功能
诊断	提供基于D_Port的端口自诊断功能，包括电/光环回、链路流量、延时和距离
管理功能	具备免费的HTTP方式的交换机管理并支持端口性能监控，参数修改等

	功能
冗余性要求	风扇电源等部件均可热插拔并支持在线升级微码
配置	48口交换机，本次激活24个FC端口，配置24个32G FC多模光模块，另配2个单模模块，满配相关线缆
质保服务	提供原厂商五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.9 云桌面服务器扩容

技术指标	参数要求
品牌	技术成熟的服务器品牌
外观	≥2U机架式服务器，标配原厂导轨
★配置要求	1.CPU≥2颗Intel 6326 (2.9GHz/16核)至强系列处理器 2.内存≥1024GB DDR4-3200内存，Advanced ECC、内存在线热备，具备内存主动式检测，最大支持32根DDR4内存，最高速率3200MT/s，支持RDIMM或LRDIMM 3.配置≥2*480GB SSD系统盘，≥5*1.92TB SSD 硬盘，≥1*960GB SSD缓存盘，具备Raid重建不可拔出硬盘提示指示灯。
阵列控制器	≥1 个标配 SAS Raid 阵列卡（不占用 PCIE 扩展槽），支持 Raid0/1/10/5/6，≥4GB 缓存，支持缓存数据保护
PCI 插槽	最多提供≥8个标准PCIE4.0插槽可用，同时提供阵列卡和网卡扩展
★网卡	配置≥6 个 10Gb 光纤以太网接口（含原厂光模块），≥4 个千兆以太网口
GPU	支持8个单宽/3个双宽
接口	≥5个USB3.0接口；
冗余电源	2 个≥1300w 铂金版热插拔冗余电源，支持 96%能效比的钛金版电源选件
冗余风扇	热插拔冗余风扇
工作温度	符合 ASHARE A4 标准，5-45° C 标准工作温度

嵌入式管理	★配置≥1Gb独立的远程管理控制端口，配置前面板独立的USB管理端口。配置虚拟KVM功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶。**（提供官网截图证明）**
	免费提供升级工具，无需安装代理即可可统一升级同一网络中服务器的固件及驱动程序。
服务器管理系统	支持创建、删除存储卷，显示卷的空间使用率、支持对存储的监控，查看使用情况，以及IO。实时IOPS、卷属性，支持将卷挂载在某个主机上。支持对软件定义存储，以及独立存储等存储的管理。支持创建，删除主机，主机集，支持将存储卷和主机的关联
★数据保护	配置数据保护功能，采用无代理的方案，为持续保护业务及数据的安全与平台的深度兼容性，最小恢复单位为一个写I/O操作，可从任意时间点中选择，使应用程序能够基于以前的事务快速地从任一时间点恢复。支持本地复制功能。对于捕获的写I/O，既支持同步复制到本地站点，也支持异步复制到远程站点，提供对同一数据卷的并行本地和远程保护;可以恢复到任意时间点的数据，保证数据安全性
其它安全选项	提供UEFI安全启动; 可配置机箱入侵侦测，在外部打开机箱时提供报警功能。
节能政策	提供中国质量认证中心颁发的节能产品认证证书**（提供有效证书复印件）**
质保服务	提供原厂商五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.10 云桌面终端扩容

技术指标		参数要求
★终	硬件配置	X86 架构 CPU：核心数≥双核 主频≥2.0GHz 内存≥4G 硬盘≥32G

端配置	接口要求	为满足多屏办公及外设兼容使用，USB 3.2Gen2 Type-C≥1 个，DP≥1 个 ，HDMI≥2 个；提供 USB 口≥8 个，前置 USB 口≥4 个，USB 键盘；USB 鼠标；底座；含显示器。
终端管理	终端纳管	可以通过手动搜索 IP 或者设置 ip 地址段自动搜索终端加入管理；
	资产统计	★为提高桌面整机的管理，需支持统一纳管，并支持针对远程批量下发的软件/补丁自动升级，减少维护；为减少统计工作，需支持针对桌面桌面整机设备快速进行资产统计，提供对纳管桌面整机的软硬件资产（包括对应用软件、操作系统、硬件资产等）的图表化展示和导出**（提供资产统计功能截图）**
		为了解桌面整机使用情况和健康状态，需提供可视化资源监控平台，展示纳管桌面整机的整体数量、在线数量、系统安装数量 TOP、告警等统计信息**（需要提供统一资源监控平台截图）**
	权限管理	为提供严格的权限管理，需将权限细分为多个等级。支持用户按需新建子级管理员，按权限查看对应终端，方便管理。该管理员只能看到本子集的终端信息和下属的终端信息，权限划分明确，降低终端运维成本。
	终端运维	为保证终端记录的可追溯性，需提供终端每天上下线的日志记录，并支持记录按时间导出，上下线的日志记录也按权限划分。
	日志收集	为方便数据的展示，需提供终端上下线日志的图表展示。可按日期区间选择对应的上下线日志，并支持选择权限下所有终端上下线日志展示，或者下属任一或多个地市的终端上下线日志展示。
	终端维护	为方便终端维修记录的统计，需提供维修记录模块。提供 CPU，内存，硬盘，主板四大类的维修情况，并支持新增自定义的维修类型。页面支持展示各种维修类型的终端数以及终端数占比。
		为方便维修状态的查询，需提供维修记录的状态区分。支持展示处理中，维修完成，不维修三种状态。管理员可根据实际终端维修情况手动修改状态，提高终端维修模块的管理便携性。
	电源管理	支持远程关闭、唤醒、重启终端；

		支持终端和桌面开关机一体化功能：终端开机自动登录桌面；在桌面内部关机，终端也能一并关机；
	终端外设管控	为提高外设应用的安全性，支持外设接入桌面的策略配置，支持配置以下类型的外设：USB、打印机、摄像头、串并口、扫描仪、视频、磁盘和剪切板等；
		策略应用到组织结构、用户组和用户，支持例外配置；策略支持修改、删除和优先级的调整；
		USB 支持配置设备的黑白名单模式，并支持设备 ID 配置；
		磁盘支持配置自动重定向和只读属性、剪切板支持分别控制终端和桌面的单向剪切板；
		以上功能需提供经 CNAS 或 CMA 认可的权威实验室出具的测试报告复印件并加盖原厂投标专用章或公章作为证明
	管理软件许可	★需要提供与本次终端采购数量相同的管理软件永久授权许可
外设支持	外设映射	终端支持的操作系统类型：Windows7、Windows10、Linux 等。
		支持的外设类型：1、USB 存储设备；2、打印机；3、串并口设备；4、USB 摄像头（支持同时接入多个）；5、USB 扫描仪
		“共享桌面”模式下，USB 设备实现“用户隔离”，不同用户映射不同的终端外设；
▲授权		本次新增配置 100 个云桌面授权，兼容现有云桌面系统
质保服务		提供原厂商五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

2.11 运维大屏

技术指标	参数要求
配置要求	屏幕尺寸≥65 寸液晶电视机，存储容量≥2GB+32GB，分辨率≥3840*2160，刷屏率≥120HZ
质保服务	提供五年技术支持和保修服务，投标时提供服务承诺函。

3.软件

3.1 分布式存储软件

技术指标	参数要求
总体要求	知名品牌，禁止借用第三方软件的整合，以保证软件产品质量、可靠性、合法性。
	▲本次采购超融合分布式存储软件高级版共 16CPU 永久授权
	本次采购企业使用级别的超融合分布式存储软件，新增加的存储虚拟化软件需要能够与原有硬件平台的虚拟 CPU、虚拟内存等资源池进行无缝融合，统一管理，不需要停机或者数据迁移。
基本要求	分布式存储(Server SAN)，支持多个独立的服务器本地存储组成一个可以共享的逻辑存储资源池。基于横向扩展架构，易于管理。支持混合架构（SSD/HDD 混合）和全闪存架构（全 SSD）。
	采用嵌入虚拟化层（hypervisor）内核的体系结构，无需单独安装，缩短 I/O 数据路径降低延时，减少对服务器的 CPU 和内存资源占用。**（提供官网截图证明）**
性能	支持存储性能 QOS 控制，以虚拟机为颗粒度限制和监控每个虚拟机使用的 IOPS，可防止某个虚拟机独占大量存储 IOPS，消除邻位干扰问题。
	采用 SSD 作为高速读/写缓存，支持针对每个虚拟机进行读缓存预留，且可以动态调整，确保重要应用的读性能;支持 ULLtra DIMM SSD 和 NVMe SSD，用作读写缓存
可用性	支持跨数据中心的容灾复制技术和跨数据中心的存储双活技术，跨数据中心双活部署时，可以保证单一数据中心存储系统故障自动切换，另一数据中心自动接管，并恢复对外提供服务，无需人工干预，保障业务连续性
	针对每个虚拟机可设置多个副本镜像（最大 4 副本）来确保在发生磁盘、主机、网络或机架故障时绝不丢失数据，保证业务连续性。
存储效率	★配置重复数据删除和数据压缩功能，优化数据占用空间，实现最经

	济高效的全闪存性能。**（提供官网截图证明）**
	★配置纠删码（类似 RAID 5\6）功能，针对每个虚拟机可实现跨节点的冗余保护，增加存储的可用容量，提高全闪存存储空间利用率。**（提供官网截图证明）**
兼容性	支持现有市场上的主流 x86 服务器、I/O 控制器、磁盘等等，包括但不限于 Cisco、DELL、Fujitsu、Hitachi、HP、Huawei、Inspur、Intel、Lenovo、SuperMicro 等
	支持运行 Oracle、SQL 等主流数据应用，并提供 Oracle RAC 和 SQL Server Always On 数据高可用集群技术官方部署手册
扩展性	单个存储集群支持不少于 64 个节点（服务器）
	最大可支持虚拟机（VM）数不少于 6400 个
	支持无存储的计算节点加入到集群享受共享存储的服务
运维管理	★在同一个图形界面里管理服务器和存储资源，并监控详细的性能与容量。配置部署无需命令行操作，只需在图形化管理界面上点击即可完成。**（提供官网截图证明）**
	提供基于存储策略的管理机制，根据业务应用的需求，以单个虚拟机为颗粒度在线的动态调整应用正在使用的存储资源(包括为每个虚拟机独立设置磁盘条带数、读缓存大小、数据冗余策略、软件校验保护、存储空间预留等)，而无需进行 LUN 或 RAID 配置。**（1.需提供官网截图证明。2.提供该功能的真实操作界面截图）**
质保服务	提供一年原厂软件质保服务；在线支持服务、800 电话支持服务，投标时提供服务承诺函，中标后明确软件设备数量和服务年限，提供软件原厂商授权服务函，并关联最终用户名为湖州市中医院，可以官网或 800 电话验证。

3.2 虚拟化软件

技术指标	参数要求
总体要求	业界知名的虚拟化品牌，市场占有率高，以保障良好的性能、可靠性、安全性及技术支持服务。禁止借用第三方软件的整合,以保证软件产

	品质量、可靠性、合法性。
	▲本次采购虚拟化软件企业增强版共 16CPU 永久授权
	需要能够与原有硬件平台的 CPU、内存等计算资源和存储资源池进行无缝融合，不需要停机或者数据迁移。可以使用同一个管理界面原生的管理现有和新增的虚拟化资源环境。
基本要求	为保证虚拟化平台性能，产品需采用裸金属架构，即无需绑定操作系统即可搭建虚拟化平台，部署后所占用的存储空间在 200MB 以下
	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，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性。
	虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 IP 地址、MAC 地址等。
	能够提供性能监控功能，可以对资源中的 CPU、网络、磁盘使用率等指标进行实时统计，并能反映目前物理机、虚拟机的资源瓶颈。
兼容性要求	支持现有市场上的主流 x86 服务器,认证服务器必须包括 Intel 或 AMD 最新处理器，**（提供官网支持说明或实际产品界面截图）**
	兼容现有市场上主流的存储阵列产品，具有双方认可的官方存储阵列兼容性列表，存储阵列类型包括 SAN、NAS 和 iSCSI 等。
	支持与多个第三方杀毒软件集成，无需在虚拟机内安装杀毒代理（客户端）即可保护虚拟机，实现虚拟化环境下无代理的安全防范。
	兼容 NVIDIA K1\K2、M60 图形加速卡，支持 NVIDIA GRID vGPU 硬件虚拟化技术，NVIDIA 硬件加速图形处理为虚拟机提供出色的 2D 和 3D 图形处理能力。
高可用要求	提供 HA 功能，当集群中的主机硬件或虚拟化软件、客户机操作系统发生故障时，该主机上的虚拟机可以在集群之内的主机上自动重启。
	提供零停机容错保护机制，保证关键应用的连续性，且被保护的应用虚拟机所在服务器发生故障时，业务访问不中断，应用持续可用，确保零停机、零数据丢失。且被保护的虚拟机配置不少于 8 个虚拟 CPU。

	（提供官网支持说明或实际产品界面截图）
	支持虚拟机的在线迁移功能，无论有无共享存储，都可以在不中断用户使用和不丢失服务的情况下在服务器之间实时迁移虚拟机，保障业务连续性。
	监控服务器运行状况信息，并在问题发生之前，自动将虚拟机从性能降低的主机迁移出来
	支持跨数据中心在线迁移功能，即在两个完全独立的数据中心，独立的服务器集群之间，远距离将虚拟机从一个数据中心在线迁移至另一个数据中心，迁移过程业务无中断。
存储管理要求	提供虚拟机存储的动态负载平衡功能，通过存储特征来确定虚拟机数据在创建和使用时的最佳驻留位置，可根据存储卷性能及容量情况进行无中断自动迁移，消除存储隐患。支持跨不同存储类型以及不同厂商存储产品之间进行存储在线迁移。
	提供具有存储识别功能的 API，使第三方存储厂商可以将存储软件与虚拟化平台更好的整合，使虚拟化平台能够识别特定磁盘阵列的功能特性以及状态信息，虚拟机也可以被外部存储阵列识别**（提供官网支持说明或实际产品界面截图）**
	支持跨多个 LUN 的共享数据文件系统，可以聚合至少 32 个异构逻辑卷（LUN），支持在线实时添加 LUN 以实现集群卷容量动态增长，可支持至少 64TB 容量集群卷。虚拟机文件系统也支持主流存储厂商的存储自动分层功能。
	实现以虚拟机为颗粒度，对存储资源和功能的使用进行更加精细的控制(例如：快照、远程复制、重复数据消除等功能的开启和应用，读/写 IOPS 的控制，是以虚拟机为单位)，并在需要时进行动态实时调整。
服务质量管理	支持存储和网络的 I/O 控制功能，通过对持续监控工作负载，一旦发现拥塞，会自动根据业务需求，以虚拟机为单位进行带宽限制，以保证关键虚拟机的带宽。

扩展性要求	每个集群至少支持 64 个主机；每台虚拟化主机至少支持 768 颗逻辑 CPU、16TB 内存、单个存储卷 64TB；每个虚拟机至少支持 256 个 vCPU、6128GB 内存、62TB 虚拟磁盘容量。提供热添加 CPU，磁盘和内存的功能，实现无需中断或停机即可向虚拟机添加 CPU，磁盘和内存。
运维管理	支持单点登录，用户只需登录一次，无需进一步的身份验证即可访问控制台并对集群进行监控与管理。支持 AD 域整合，域用户可以访问控制台，由 AD 来处理用户身份验证。
	提供统一的图形界面管理软件，可以在一个地点完成所有虚拟机的日常管理工作，包括控制管理、CPU 内存管理、用户管理、存储管理、网络管理、日志收集、性能分析、故障诊断、权限管理、在线维护等工作。同时能够直接配置、管理存储阵列，具有对存储阵列的多路径管理功能。支持 QoS 能力，支持基于应用程序的服务级别自动管理功能。虚拟化管理控制台支持在 Linux 和 Windows 两种环境部署
	控制台自身具备备份和还原机制，可以对数据进行备份和还原。
质保服务	提供一年原厂软件质保服务；在线支持服务、800 电话支持服务，投标时提供服务承诺函，中标后明确软件设备数量和服务年限，提供软件原厂商授权服务函，并关联最终用户名为湖州市中医院，可以官网或 800 电话验证。

3.3 超融合软件

技术指标		参数要求
超融合软件总体要求	架构要求	采用符合超融合特性的分布式架构。将所有节点的存储空间无缝融合为单一的存储池，并支持单一存储池内横向扩展。
		节点间无主次之分，每个节点可同时提供计算、存储、管理服务。
	▲软件授权	超融合软件须为永久授权，非订阅模式，本次提供≥8 颗 CPU 超融合授权，超融合授权包括计算虚拟化、分布式存储和虚拟网络功能。
	产品资质	非 OEM，拥有完全的自主知识产权及软件著作权，提供至少 6 项超融合虚拟化以及软件定义分布式存储相关的软件著作权或相关专利，有相关材料证明有分布式存储核心系统的开发、维护能力。

	国产服务器支持	需兼容支持主流的国产 CPU 架构服务器，支持鲲鹏、海光等 CPU 架构。
	集群硬件兼容性	超融合软件支持主流服务器硬件厂商如：戴尔、联想、HPE、浪潮、华为、新华三等，保证用户后续硬件品牌选择的灵活性。
	集群硬件异构	为保障后续可持续扩容，须支持不同品牌、不同部件（CPU、内存、硬盘）部署在同一个集群，保证不同时期采购的服务器硬件能够兼容在同一集群正常运行。提供管理界面截图证明。
	★虚拟化平台支持	超融合可支持 VMware vSphere、KVM 等主流虚拟化平台作为 Hypervisor 使用（非通过云管平台纳管虚拟化的方式），保障用户原有虚拟化平台的使用习惯，**（提供官网链接截图和产品功能截图证明）**
虚拟化平台	HA 高可用	内置虚拟化平台支持 HA 功能，当单一节点主机或网络故障时，自动触发 HA，该节点上的虚拟机自动迁移至其他节点并启动运行。
	虚拟机热迁移	支持将主机上的虚拟机热迁移至集群内其他主机上，迁移过程中业务不中断。
	虚拟机克隆	虚拟机支持快速克隆和完整克隆两种方式满足不同业务需求，快速克隆时间不会因为磁盘大小而改变，且都能在一分钟之内完成。同时支持批量克隆，实现运维效率提高
	虚拟机快照	可以对虚拟机执行快照操作，保留快照节点的虚拟机状态。快照数量无限制，最少可以支持 30 个虚拟机快照，并且快照之间无依赖关系；
		支持通过虚拟机快照重建虚拟机
	虚拟机定时快照	支持虚拟机快照策略，可针对虚拟机配置定时快照策略，在不增加额外授权前提下进行数据保护，可按月\周\天\小时\分钟等周期设置定时快照，定时快照可设置最短 20 分钟。
	虚拟机模版	可创建虚拟机模版，并支持通过虚拟机模版批量创建虚拟机，提升运维效率
		为方便快速创建和交付虚拟机给申请人使用，模板创建虚拟机过程中，管理界面支持自定义虚拟机内部的客户机操作系统的主机名、默认用户密码、SSH 公钥、IP、静态路由、DNS 等参数，无需手工进入

		虚拟机内部进行修改。
	标签管理	支持用户对虚机设置标签，方便按照不同的属性进行资源归类，进行快速的资源查询，资源分析等功能。
	CPU 兼容性	支持 CPU 物理透传,支持对集群和虚拟机设置 CPU 兼容性,支持 CPU 模型兼容性≥5 种。
	智能放置与放置组	支持设置主机资源和与虚拟机资源的亲和和反亲和性，可灵活设置虚拟机与主机的放置关联关系，以满足应用高可用、许可限制、业务关联依赖等需求。
虚拟网络	分布式虚拟交换机	支持创建分布式交换机，统一配置集群间不同物理机节点的网卡设备，并支持网卡故障切换以及负载均衡功能。
	VLAN 支持	支持虚拟网络 VLAN
	网络拓扑展示	支持以拓扑图方式展示虚拟机与分布式交换机及网络链路之间的关系。
分布式存储	实现技术	为保障研发快速相应，避免因开源社区 bug 导致的数据安全问题，要求分布式存储软完全用自主研发，不得采用开源产品（例如 GlusterFS、Ceph 等）进行二次开发，提供第三方的代码开源率检查报告，核心分布式存储的组件代码自主率必须>90%。 **（提供相关证明文件）**
	★IO 数据本地化	为提升数据读写性能,VM 虚拟盘在磁盘分配时将一个完整的副本分配在本地，写 I/O 保障有一份在本地进行，所有读 I/O 仅访问本地，避免跨节点的网络访问照成性能损失。
	数据保护机制	支持 2 副本、3 副本数据保护策略
	★故障自愈	硬盘或节点故障后，系统可利用已有空间自动重新分布数据以恢复系统到正常状态，恢复的数据量不大于故障节点已写入数据。数据恢复不使用独立的热备盘。单节点故障时不会影响整个存储空间的使用且数据不会发生错误或丢失。整个数据恢复过程无需人工干预，全部自动完成。

		存储池不采用磁盘组的技术，当 SSD 或 HDD 故障情况下，影响范围仅限于故障的 SSD 或 HDD，不影响其它磁盘掉线和数据恢复，磁盘故障不影响存储的数据访问，
	灵活存储策略	支持同一集群内,不同虚拟机可以灵活选择 2 副本或 3 副本保护机制，满足不同业务对可靠性要求，提升存储资源分配的灵活性。
	横向扩展	支持以 1 个节点为单位进行扩容，自动发现新增节点/节点，在不中断业务的情况下将新节点自动或手动加入现有集群中，实现集群计算和存储资源的无缝扩展，单一集群及存储资源池内可支持扩展节点数≥250
	智能数据分层	节点内所有 HDD 共享 SSD 缓存，系统自动将经常访问的随机数据缓存到 SSD 磁盘上，而将不常用的数据放在 SATA/SAS/SSD 数据磁盘上，无需手工干预。
	机架级别高可用	为避免因单一机架掉电照成的数据丢失，支持数据副本基于服务器机架智能分布，可自动将副本放置到不同机架上，保障即使单一机架多台节点故障不会照成数据损失。
	数据块校验	支持数据校验功能，校验数据随数据写入并在读出时校验，防止由于意外掉电或者射线干扰造成比特翻转而引发的数据丢失风险。
	存储协议	提供标准的 NFS 或 iSCSI 存储访问协议。可将超融合集群的存储资源作为共享存储挂载给外部的物理机或者虚拟机使用。
	资源占用	每节点存储软件 CPU 资源占用≤4 个物理核（或 8vCUP），内存资源占用≤20G，资源消耗不随着节点内磁盘数量的增加而增加。
	数据恢复/迁移智能调节	动态感知上层业务压力，在不影响用户的业务 IO 前提下，智能调整集群的数据恢复/迁移速率。高负载时自动降低数据恢复速率，避免数据恢复对上层业务 IO 产生影响，在低负载情况下提升数据恢复。**（提供产品功能界面截图证明）**
	IO 限速	可以在控制台通过设置 IOPS 以及带宽对虚拟机 IO 进行限速，保证集群内的存储资源得到良好的资源分配和控制
运维	安装部署	安装简单方便，图形化安装。

监控	多集群集中式管理	内置统一管理组件，实现跨集群管理。可以在同一界面中对分布在不同位置的多个集群进行统一管理，同时通过一个界面统一管理到计算、存储、虚拟化资源。
	自定义监控视图	支持自定义监控视图，能够针对集群、主机、虚拟机等监控对象，以及 CPU、内存的使用情况等监控指标创建监控视图，满足不同运维团队的监控需要。同时支持监控数据导出。
	保留监控数据	支持监控数据保存周期超过 3 个月。
	服务器硬件监控	监控物理服务器的运行状态，包括 cpu 温度、风扇以及机器故障等。
	虚拟机资源优化	可以自定义监控僵尸虚拟机、长期关机虚拟机、资源分配不合理的虚拟机等，有效地对虚拟机资源进行诊断和优化。
	智能报警	能够主动地对事件进行提醒、通知支持 Email 和 SNMP 协议报警通知。报警包括硬件故障警告及资源使用过高警告和软件异常通知。
	开放接口	能够提供 REST API 接口方便进行定制开发以及与第三方厂商产品进行结合；
	资产管理	支持在管理界面中一键收集超融合集群的所有资产信息，包含 ISO 映像、数据中心、集群、虚拟机、主机、物理硬盘、报警信息、虚拟网络、任务等资产信息，方便管理员进行统计分析。
	★一键升级	支持一键滚动升级功能， 在不需要关闭业务系统的情况下，可以实现平台软件的在线升级（不限大小版本）。
服务	售后服务	提供一年原厂软件质保服务；投标时提供服务承诺函，合同签订后提供原厂盖公章的售后服务承诺函，售后服务承诺函必须明确软件设备数量和服务年限，并关联最终用户名湖州市中医院。
	巡检服务	提供每年不少于 4 次的巡检服务，及时获取集群的运行及健康状态。需原厂服务工程师提供服务，并在每次巡检完成后提供巡检报告。

3.4 虚拟化容灾备份系统

技术指标	参数要求

体系结构	软件实现系统功能，备份空间由硬件提供，可以实现数据保护、数据恢复、数据迁移、数据发现以及数据调用等多种数据管理功能。即一个管理平台能实现：应用数据管理、企业级备份及灾难恢复、存储快照及复制管理、终端数据安全及保护、云盘共享、虚拟机及混合云数据管理、大数据管理、数据归档及信息治理，
平台构成方式	采用“软件定义”的方式，利用通用的服务器构成数据管理平台，利用通用的存储设备（磁盘、磁带、云存储）构成数据存储仓库。
开放性	平台利用第三方接口，调用备份、归档、复制、快照以及REST命令等多种API接口，来获取、收集数据，并将数据保存在数据存储仓库中。
扩展性	平台具有超强的横向扩展能力，单一平台就能管理PB级的数据，管理2万个以上客户端，管理多个私有云和公有云，管理上百个分支机构。
操作系统平台兼容性	数据管理软件客户端支持各种主流操作Unix、Linux、Windows、MAC OS系统
数据库及应用兼容性	数据管理软件支持多平台下的主流数据库和应用的在线备份，包括：Active Directory、SQL Server、Exchange、SharePoint，Oracle、Oracle RAC、Sybase、DB2、DB2 MultiNode、 Informix、MySQL,、IBM Lotus Domino、 PostgreSQL、Documentum、SAP on Oracle/DB2/MaxDB、SAP HANA、MongoDB、Cachｅ、3DFS
★NAS 兼容性	支持多种NAS设备的保护，通过NDMP协议实现全备份及增量备份，同时支持NAS的3-Way保护，本次需配置NetApp NAS备份模块
虚拟机、云平台以及大数据平台兼容性	支持VMware、、Huawei Fusion Compute、OpenStack、Docker、Amazon EC2/RDS、Microsoft Azure等主流虚拟化平台。 支持Amazon S3、Azure Blob Storage、Google Mail、Google Drive、OneDrive for Business、Salesforce、Azure SQL、O365、Alicoud等主流云平台。
备份介质支持	支持磁盘备份介质、NAS、VTL和磁带备份介质，支持LTO4、LTO5、LTO6、LTO7、LTO8驱动器。支持磁带出库管理，并支持磁带对磁带拷贝。 支持多台介质服务器之间可利用SAN/iSCSI传送备份数据，这样在做

	LAN-Free备份时可以共享同一个磁盘LUN或介质驱动器。 支持AliCloud、Amazon S3及兼容云存储厂商、AT&T Synaptic Storage、Caringo CAStor、DDN WOS、Dell DX Object Storage Platform、EMC Atmos、EVault LTS2、Google、Hitachi Content Platform、HGST、Huawei OceanStor 9000 Storage System、Microsoft Azure Storage、OpenStack® Object Storage、Oracle Storage Cloud Service、Rackspace Cloud Files、Verizon等,
图形化管理	数据管理软件支持对Oracle、MS SQ、Sybase，MySQL，MS Exchange，SharePoint及Lotus Domino的全中文图形化的备份恢复操作，以简化备份恢复管理，优先考虑无需写任何脚本。
★数据库及应用的备份恢复	1.对所保护的对象支持在线数据备份，能确保操作系统、应用系统的数据完整性一致性 2.能对文件系统及应用进行数据块级别增量备份及合成全备份，极大提高海量小文件及应用的备份性能。支持的系统： Windows、UNIX/Linux、MySQL、PostgreSQL、Exchange、SQL Server 3.把数据库归档日志即时复制到目标数据库，并立即把复制日志应用到目标数据库，确保数据库即时同步。要求支持的数据库： Oracle、Oracle RAC、PostgreSQL 4.对关键应用数据库的Log备份至关重要，Log自动备份极大提高了数据健壮性，防止Log丢失，也可以防范Log空间不足引起的数据库停机。支持的数据库：SQL Server、Oracle、Oracle RAC、SAP for Oracle、Notes Database 5.把数据库归档日志即时复制到目标数据库，并立即把复制日志应用到目标数据库，确保数据库即时同步。支持的数据库：Oracle、Oracle RAC、PostgreSQL SQL Server、Oracle、Oracle RAC、SAP for Oracle、Notes Database 6.无需写任何脚本，利用图形界面提供单表恢复功能，极大简化数据库恢复操作。支持的数据库：Oracle、Oracle RAC、MySQL、PostgreSQL、

	SQL Server、DB2、Informix 7.当操作系统磁盘被破坏时，能进行裸机恢复，完整恢复操作系统及应用程序。当操作系统状态或文件被破坏时，可直接恢复系统状态或文件。
★虚拟机备份支持	1.虚拟机备份模块（VSA）安装在备份代理服务器中，而不是安装在需要备份的虚拟机中，对多个虚拟机进行在线备份。能实现对变化的数据块进行增量备份，并能进行合成全备份，极大方便部署并提高虚拟机备份性能；能支持Amazon、Citrix Xen、Microsoft Azure、Microsoft Hyper-V、Nutanix、 Acropolis、OpenStack、Oracle VM、Red Hat Virtualization、VMware
	2、对虚拟机增量数据块进行即时复制保护，满足用户灾难备份的ROP/RTO要求，能复制到同平台的虚拟机，也可以复制到AWS、ARM、Azure云平台。 能支持： VMware、Hyper-V、AWS
	3、支持物理机完整恢复到虚拟机环境中，还支持虚拟机跨平台完整恢复到另一虚拟机环境中或公有云环境中。 需要支持的跨平台迁移转换：物理机到VMware、Hyper-V VMware到Hyper-V、OpenStack、AWS、Azure Hyper-V到VMware、AWS、Azure
	4、不需要恢复虚拟机备份数据，直接浏览并恢复虚拟机中文件，极大提高恢复速度并简化恢复操作。支持虚拟化： VMware、Hyper-V、Citrix Xen、Red Hat Virtualization、Amazon、Azure、Nutanix Acropolis、OracleVM、OpenStack
	5、不需要恢复虚拟机备份数据，直接运行备份虚拟机，并可选择同时进行后台恢复，不仅提高了RTO，也极大简化了恢复测试。 支持的虚拟化平台： VMware、Hyper-V
	6、不需要恢复虚拟机备份数据，直接运行备份虚拟机，并可选择同时进行后台恢复，不仅提高了RTO，也极大简化了恢复测试。

持续复制功能	支持文件系统及相关应用连续数据复制保护，并能创建应用一致点快照，数据丢失少并确保应用一致性，满足用户灾难备份的ROP/RTO要求，支持一对多，多对一模式。支持的平台及应用： Windows、AIX、HP-UX、Linux、Solaris、Exchange、SQL Server、AD、Oracle
数据归档/迁移功能	1、对不常使用的文件自动归档到二级存储并保留归档存根，需要访问时，归档数据自动回迁，这样可减少对在线存储的占用，也减少数据备份数据和备份窗口的目的。要求支持的文件系统： Windows、Unix、Linux及NAS 2、支持虚拟机归档，可自动对不经常使用的虚拟机做自动关机，并将整个虚拟机自动迁移到二级存储，需要访问时可实现虚拟机自动回调，以降低主存储成本及释放虚拟服务器资源。要求支持虚拟机平台：VMware、Hyper-V、OpenStack
重复数据删除技术支持	内含数据块级别去重功能，支持源端去重、目标端去重、全局去重，重复数据复制功能。采用SHA-512去重算法，理论上没有重码，并可调整去重因子大小，以提高不同应用的去重比。支持磁盘、磁带、云存储去重。去重数据恢复不依赖去重数据库，数据更安全。利用去重数据进行合成全备份，使全备份速度极大提高，而且不占用生产设备资源。仅复制去重后的新增数据块，利用该功能可以极大提高灾难备份的效率，节省网络带宽资源。
多备份域集中管理	多个备份域可以进行集中管控，备份数据可跨域传输，跨域恢复，多备份域可共享云存储，极大简化云灾备中心部署和管理。
用户权限管理	数据管理软件内置完善的用户和用户组管理功能，对不同业务系统分组管理，且能对单个用户组的操作权限作细致划分，如：备份、恢复、介质管理、报告等，并可对用户的操作进行追踪审计，以满足企业级客户多部门分组管理需求；
跨域防火墙	支持多种防火墙：单向/双向端口隧道直连（仅需一个端口）、端口转发网关、DMZ、HTTP代理（包括WIFI连接）、上述各种方式组合的防火墙。

预检测功能	能定时或在备份前对备份系统的每个环节进行检测，提供预检报告，及早发现各种软件、硬件、网络及系统问题，以便保证备份系统稳定工作。
断点续传功能	支持断点续传功能，可以在图形界面上对文件系统和数据库进行中断、继续复制备份操作，复制备份从断点继续，而不是从头开始
支持自服务恢复操作	数据的拥有者能对自己拥有的数据进行恢复操作，不需要麻烦备份管理员，从而极大减轻备份管理员的工作压力。可支持自服务恢复的数据类型： 文件、邮件、虚拟机、Oracle、SQL Server、SAP HANA
支持自动恢复演练	通过制定恢复演练策略，自动完整恢复演练测试，可恢复到灾备中心的物理机、虚拟机，或者私有云及公有云中。
报警功能	数据管理软件能收集各种报警信息，并以短信、电子邮件等方式发送给管理员，支持与主流事件报警平台集成，以实现统一事件告警和审计。
报表功能	数据管理软件集成了中文界面的Web图形化报表系统，无需提供第三方软件，支持完善的运维报表，统计分析备份系统的健康状态，数据分布，数据增长，方便运维管理及系统优化
★配置要求	配置备份空间≥500T，配置容灾虚拟机数量≥500个，能实现应急情况下实时接管核心业务的运行
访问控制	因政策法规要求，备份软件需具备接入堡垒机的功能，运维人员访问备份软件服务器必须经过堡垒机设备才能登陆
功能测试验证	合同签订后七天内，提供测试系统对产品功能和性能测试，若无法在规定时间内提供测试设备或测试结果与招标内容不符，影响医院互联互通等级评定和应用软件上线，取消中标资格，中标人承担所有责任；
服务要求	提供原厂商五年技术支持服务和保修服务，灾备系统查询分析服务；原厂实施服务，每年四次现场巡检，免费升级服务；投标时提供服务承诺函，中标后提供原厂商技术服务承诺函。

3.5 数据库容灾系统

技术指标	参数要求

基本功能要求	实现核心业务系统数据实时同步灾备要求；
	★软件授权许可：同时合法支持≥5套数据库授权许可
	要求软件支持Oracle、Sybase、SQL、MySQL、DB2、Cache等主流数据库的交易复制，且灾备数据库始终处于Open状态，实现业务系统读写分离，灾备系统查询分析等服务，
	要求软件支持任意数据库版本，硬件平台异构实时灾备
兼容性要求	支持主流操作系统：Linux、HP-UNIX、Sun Solaris、IBM AIX、Windows、中标麒麟；并支持操作系统异构；
	支持Oracle/Sybase/SQLServer/MYSQL/DB2/Gbase8a/ Gbase8M/Hadoop/Hbase/华为MPP/Hbase/Hive/Cache/GP/阿里云RDS（Mysql、PostgreSQL、PPAS、PolarDB）等主流数据库的不同版本；
	在数据迁移初始化同步过程中，业务不能停止；在异构平台或跨数据库版本之间的数据初始化过程中不需要人工干预
数据库容灾要求	支持一对一，双向，一对多，多对一，和级联复制
	支持数据转换、数据拆分及分发；
	支持从多个数据库中同一类型表的记录整合到一个表中去；
	支持数据转换，包括列映射、增/删除列、列转换；
	支持DML操作复制、支持SEQUENCE、函数、存储过程、视图、同义词、索引、应用包、用户等数据库对象进行复制
	支持没有PK/UK字段的表的复制、并无需打开或修改数据库参数，可定义并过滤不需要复制的事务；
	支持按照schema方式设置复制关系，无需单表设置复制关系，支持不同源和目标端在不同的schema名情况下的复制；
	支持中文汉字内码，符合双字6节编码；支持DXF数据格式的装载；支持Rowid mapping的方式实现数据快速定位；
故障应对能力	在遇到系统错误引起的复制中断时，例如硬件故障、数据库故障、网络中断或延迟，分级存储机制能完好的保存已经合成的交易信息，避免数据丢失，直到系统故障解决，恢复从队列传输的中断点开始；

	系统需提供数据比对功能，如果发现不一致情况后能够提供便利的单表以及单用户的数据修复工作，要求操作简单，修复速度快，且修复过程中不影响业务正常运行； 生产灾备切换后，支持快速的增量回切、全量回切功能；
DDL 支持要求	支持从数据库日志中分析所有DDL操作，不影响整个同步过程。
智能要求	在源端数据库数据结构发生变化(如修改表结构，增加表等)后，复制软件可自动将新增结构变化同步到目标端。
归档功能	按照客户要求将使用频度低的数据一次性(从数据库文件读取)或者连续归档(分析数据库日志)到目标数据库中，并在源端进行数据清理，从而减少源库数据量，提升系统效率，分担系统压力。
质保服务	提供原厂商五年技术支持服务和保修服务，灾备系统查询分析服务；原厂实施服务，每年四次现场巡检，免费升级服务；投标时提供服务承诺函，中标后提供原厂商技术服务承诺函

3.6 IT 综合运维监管平台

技术指标		参数要求
系统	管理范围	支持节点数≥2000；监控设备类型为交换机、服务器、操作系统、数据库、网络安全设备、应用监控等。部分设备监控细则项要求可定制化开发
	管理界面	全中文界面，采用HTML5技术，要求B/S模式的管理，界面友好，支持基于Web的图形用户界面（GUI），能够以简单、直观的方式显示信息，简化配置；
	操作系统	软件基于自主开发系统或是采用CentOS操作系统（64位）；
	用户	支持多用户基于角色的用户管理，可以按权限进行管理。
开发	定制开发	本次项目要求厂商对系统进行定制性需要开发，开发内容包括但不限制于1、多大屏类型的大屏展示页面2、对设备的定制性开发扩展监控3、各应用系统的监控 4、资产管理的定制开发等内容。定制需求周期为三年。
		要求与其他各第三方系统进行整合对接定制开发

		支持研发现场系统优化服务；
		支持IT运维流程设计服务；
		支持ITIL与OA业务系统对接；
	大屏展示系统	大屏展示，通过可视化图表实时展示系统运行状况，大屏要求对接视频监控画面，动力环境系统运行状况，安全告警状况等多视图多屏页面 。支持不同管理视图和实时拓扑图在大屏幕上切换；要求大屏展示界面美观，并可根据用户需求来开发定制大屏界面，大屏展示系统能抽取其他业务系统数据，进行数据可视化展示及告警
业务服务	业务服务管理组件	与“IT综合运维服务平台”统一品牌，底层数据联通，进行相关业务模块的关联性分析，支持通过端到端的方式对业务系统进行实时监测；
		支持业务系统异常波动告警；支持通过大屏实时展示业务系统运行状态；
		可根据客户需求，定制业务系统展示模块；
准入	准入管理	要求投标方提供的软件具备网络接入控制功能，无需第三方软件及硬件，就可以及时发现非法占用IP资源，内部设备非法跨网段接入，以及外部设备非法接入内部网络，并进一步定位到设备端口，实现实时干扰，保障全网的IP管理秩序和网络接入安全。
堡垒系统组件	堡垒系统组件	具备网络设备web terminal远程登录功能，支持TELNET，ssh ,RDP，web等登录方式。实现WEB端与本地管理完全一样的操作和功能
		具备设备密码的管理功能。
		支持集中管理所有用户操作记录；
呼叫中心	Web 呼叫中心	具备web 呼叫中心功能，可进行在线的咨询及远程服务
ITIL服务管理组件	ITIL服务管理组件	用户可以通过服务台实现客户流程事件的入口，和相应事件状态的管理；
		支持知识库管理，知识库搜索引擎，管理客户的知识库信息，可定制化；

		支持事件KPI，可生成相应事件的统计报告；
		支持自定义流程，可根据客户的组织架构定义个性化流程；
		支持自定义表单，可个性化生成流程业务表单；
		支持大屏展示，展示待办、已办数、待办流程展示、工作量的统计。待办流程可查看流程详情与流程图信息；
监控管理	监控方式	支持SNMP、WMI、SSH、TELNET、SHELL、IPMI、HTTP、Agent、Rsyslog、TCPDUMP、JDBC、JMX和仿真等方式进行数据采集
	网络设备监控	支持主流厂商交换机、路由器、网络安全设备；可添加定制所有支持SNMP协议的网络设备；要求监控细项可定制化开发
	网络设备监控	必须能够持续监测网络设备状态。以不同的颜色从拓扑图上区分出网络设备的状态（包括连续运行时间、CPU负载、Mem利用率等），并显示出各链路的实时数据流量；在拓扑图上直接显示各设备间每条线路实时数据流量（包括帧流量、广播流量、数据丢包情况和出错包情况等）提供对交换机的信息查询功能，包括接口所连接的设备名及IP地址、系统信息、接口流量分布情况、设备路由表、ARP缓存等信息。以上数据均可按数据表或图形时间曲线展开数据分析，在数据表方式中，每一列数据均可按用户要求进行升序、降序，便于寻找峰值数据、最小数据，也可即时提供网络设备的基本信息；能够直接开启和关闭端口。能够以列表方式显示设备中所有端口的流量分布情况（包括出入端口的流量、数据帧流量、广播包流量、丢包情况和错误包情况）。对网络中异常情况能够进行告警并且记入日志；系统支持基于周期轮询的系统性能指标的统计，历史的性能指标数据能够保存一年以上。管理系统也能够支持对设备运行性能实时查看，能够以秒为颗粒度实时的对特定性能指标绘制曲线图。

	服务器及应用监控	主机：以多种形式实时展示主机服务器的软硬件配置信息、运行状态，如CPU、内存、磁盘运行等情况；提供文件管理指标、进程运行指标，以及检查日志和网络连接等。数据库：能够监控到数据库的各类关键参数指标，这些指标包括：基本信息、告警信息、锁信息、错误信息、配置信息、空间信息、活动信息、进程信息、文件信息、会话信息、缓存信息、日志信息、性能信息、存储信息、管理器信息、库表信息等。中间件：基于监视所记录的各种中间件的状态数据，可帮助业务人员分析服务响应速度变化的技术原因和规律，在业务受到影响前，主动发现潜在问题。提供对中间件各类关键参数指标的监控，这些指标包括：基本信息，数据库连接池信息、会话信息、任务信息、JTA、JVM、Servlet、EJB、JDBC、运行队列、内存信息、线程信息等等。应用：支持对多种web应用的实时监控，对端口状态、响应时间、连接信息等提供关键参数管理
	历史曲线	支持所有监控参数的历史数据查询；
		支持所有监控参数数据的1年内的数据查询；
		支持用户自定义时间段的历史数据查询；
监控视图	监控雷达	支持雷达扫描器；雷达扫描可以直观显示所监控的节点及正常与否；
		提供监控告警类型显示以及声音告警提示；
	节点视图	提供监控节点的设备类型、系统类型、运行服务状态的直观试图；
		提过节点运行正常率的最差TOP10排名；
		提过节点CPU、Memory、Disk的使用率的排名；
	机柜视图	对机房内的机柜使用情况进行统一的管理，系统能够很方便的对机柜内的设备摆放情况进行编辑、调整。并能实时显示设备当前的运行状态，在需要时，可以很方便的打开机柜内设备的真实面板图进行操作。**（提供功能截图证明）**
	网络接口视图	提供设备网络接口的状态、流量、收发错包/丢包直观显示；**（提供功能截图证明）**
	系统对接	可以底层代码级对接“虚拟化容灾备份系统和数据库容灾系统“，抓

		去相应数据，监控管理数据备份任务的执行情况，及时对各类备份容灾任务进行异常情况报警。
日志管理	支持设备	支持网络设备（交换机、路由器），安全设备（防火墙）系统日志管理；
		支持Windows全系列主机和Linux/Unix全系列主机日志的管理；
	日志规则库	内置大于1000条以上日志规则库
	日志显示	采用瀑布式日志显示，根据时间排列
	管理功能	支持自定义日志自动移除功能；
		支持自定义日志告警规则；
		支持日志实时告警功能；
		所采集日志可以按主机、时间、告警级别自动备份；
	统计图表	可按任意指定时间、指定设备、指定事件/告警类型等条件组合查询日志；
		提供日志告警级别的统计比例饼形图；
		提供日志告警主机的TopN图表；
		可按指定条件生成主机事件、日期、告警级别、告警事件来源、告警事件类型的统计图表；
资产管理	合同管理	支持合同管理；
		支持设备与合同的关联；
	维保折旧	支持设备的维保管理，具有维保到期提醒功能；
		支持资产折旧管理；
	二维码管理	支持设备二维码标签管理；
		通过智能手机扫描二维码可以查看设备的信息及状态，可以进行设备信息配置以及进行资产盘点；
	机房资产	支持机房机架物理拓扑显示，用户可以直观地看到每个机架上的每台设备的运行状态；可以看到设备的真实面板图；支持通过鼠标拖动进行机柜内设备布局信息的调整。
	查询及图表	可按设备类型、品牌型号、存放位置、业务归属、管理归属、维保状

		态等信息进行查询；
		支持生成设备的使用状态、品牌分类、维保状态、业务归属、采购日期等图表；
运维辅助	IP地址管理	提过IP地址资源分配管理；提供IP地址使用历史回溯功能；可以对IP地址分配、使用数据生成Excel或PDF格式的统计报表；
	全网设备定位	支持全网统一IP/MAC/设备端口对照一览表，支持跨网段、跨地域的IP地址管理，自动、动态、完整提供全网所有活动用户的网络连接位置信息，可根据IP地址-机器名-MAC-物理端口唯一对应关系，支持IP全网动态定位，迅速定位其所连接到的交换机端口，便于故障定位和问题查找。
	故障管理	支持对于运维中的故障问题记录、分类、统计功能；
		支持自定义故障级别；
		支持自定义故障分类；
		可以按时间周期、故障级别、故障类型提供故障记录的图表分析；
		提供故障记录的生成PDF格式文档，并下载；
	运维文档管理	能够实现对运维文档的WEB管理；
		可以在线编辑、上传、下载运维技术文档；
		支持常用文档格式（WORD、EXCEL、PDF、JPG等）；
	运维通讯录	支持运维应急通信录功能；
		通信录按公司划分；
拓扑管理	拓扑功能	支持多层次网络拓扑结构图；
		支持拖拽进行设备拓扑布局；
		支持托拽直接完成设备链路连接；
		直观显示网络链接流量数值或占用情况，并以不同颜色进行显示；
		直观显示设备监控及性能监控状态，并以不同颜色进行显示；
		显示设备互联端口以及流量来源端口；**（提供功能截图证明）**
	拓扑配置	用户可以自定义、编辑、修改业务拓扑图，业务拓扑的元素包括主机、网络设备、安全设备、数据库、中间件、各种类型的服务和应用；

	拓扑融合	通过点击拓扑中的设备，可直接进入对应设备流量汇总列表页面；
		通过点击拓扑中的链路，可选择进入对应链路最近四小时、最近一周、最近一月的流量报表页面；
告警管理	监控告警	支持监控主机/设备的在线监控告警；
		支持各项性能监控数据的阀值监控告警；
		支持日志告警；
	告警方式	支持自定义告警分组；
		支持EMAIL、微信、声音、短信告警方式；
	告警记录	记录全部的告警事件；
		可以提供告警的发生时间、恢复时间信息；
		提供运维人员对于告警的确认以及处理记录功能；
报告报表	报告报表	支持自动定义生成报告报表功能；
		可针对节点生成全数据统计报告；
		可生成节点运行可用性、节点资源利用率的统计报告；
		可生成资产数据统计报告；
		可生成告警报告文档；
		提供报告下载功能；
服务	升级服务	提供五年免费升级，并提供终身免费日常维护指导；
测试	功能测试	合同签订后七天内，提供测试产品对功能和性能测试，若无法在规定时间内提供测试设备或测试结果与招标内容不符，影响医院互联互通等级评定和应用软件上线，取消中标资格，中标人承担所有责任；
其他	服务	提供原厂商五年技术支持服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

3.7 IT 综合运维服务平台

技术指标	参数要求
系统整体要求	管理系统平台要求基于B/S架构，采用JAVA+HTML5开发，客户端支持IE9以上版本及其他Chrome、火狐等主流浏览器
	必须遵循“ITIL最佳实践”框架，可实现基于IT信息部门的信息化，

		包括工单管理、合同管理、项目管理、资产管理、巡检管理、耗材管理、知识库管理等ITIL核心流程。支持移动端微信号。促进提升信息科的工作效率及服务质量。
系统功能	角色与权限	提供普通用户、管理员、工程师、供应商、监理等多种角色。
		提供权限域功能，控制不同类型用户的权限范围，包含合同管理、项目管理、工单管理、巡检管理、资产管理、知识库管理等数据
	富文本编辑框	提供富文本编辑框常用功能，包括全屏放大、表格、格式调整、链接、特殊符号、锚点等功能。提供编辑框内图片复制粘贴功能，可以从粘贴板直接粘贴，支持BMP、JPG、PNP等常见图片格式，且可以定义图片大小。提供编辑框内word文档快速导入功能，支持03、07等常见版本，且保持文档格式正常。
	文档在线预览	提供附件内容在线预览，支持包括各版本Office文档、PDF及图片等附件格式，支持PowerPoint文档在线播放，在线预览需保持排版、格式正常，同时提供打印功能。
		支持只读浏览word、excel、ppt、pdf文档，可禁止修改、复制粘贴、下载等操作。
	文档在线编辑	提供office文档在线编辑功能，包括各版本word、PPT、Excel
		支持修改痕迹保留，模板套用，多人同时编辑控制，word文档拆分合并，word文档内容差异对比等功能。
		可自定义office工具条，对话框及右键菜单；可以禁止复制、下载、打印、复制、另存等功能；
	系统提醒	系统提供站内消息、微信公众后、企业微信号等多种提醒方式，提醒事项包括：工单指派，工单转派，巡检任务，合同计划，项目审批，项目变更，项目验收等
	系统对接要求	支持医疗行业HL7标准协议；Windows AD，LDAP协议；
		系统接口开放，功能扩展要求支持与现有的资产管理系统、运维监控系统、OA系统等软件进行数据对接，实现流程衔接和数据同步；
		提供标准的API接口。

	数据备份	可以底层代码级对接“虚拟化容灾备份系统和数据库容灾系统“，抓去相应数据，管理和展示数据备份任务的执行情况，提供对系统数据和附件相应备份。
首页功能	大数据展示	终端大屏展示，提供图形动态化方式实时展示信息科室人员工作统计、工单事件、来电统计及时效等信息；数据定时自动刷新；提供功能界面展示，项目看板功能支持项目的实时展示，包括且不限于项目整体数量、进行中的项目数量、任务完成情况等数据；工单看板功能支持工单的实时展示，包括且不限于工单数量、工单类型、工单状态等信息，可查看工单处理进度明细； 与“IT综合监管服务平台”统一品牌，底层数据联通，进行相关业务模块的关联性分析，支持通过端到端的方式对业务系统进行实时监测；
	报表统计	合同报表，对已签订合同生成报表统计，可通过时间段、合同类别、合同状态等维度进行数据统计分析，同时可统计合同对应的供应商，合同金额和付款金额情况。
		项目统计，系统内项目生成报表统计，提供以时间段、项目类别、项目状态、项目阶段等进行项目的数据统计分析，同时可统计项目对应供应商。
		工单统计，系统内工单生成报表统计，提供以时间段、工单类别、工单状态、工单趋势等多个维度，包括：报修来电量、建单量、未接通来电量、工程师接单量、接单时效。。
		巡检统计，提供巡检任务的数据报表，内容包括且不限于巡检总任务量、完成任务量、异常对象排行、工程师巡检排行等；
		资产统计，提供以资产状态、供应商、关联合同、地理位置等多种方式的资产视图展现；
		耗材统计，支持实时监控耗材使用情况的数据统计分析功能；
	全局检索	实现全局快速查询功能，查询内容包括且不限于合同编号、合同名称、项目名称、资产设备名称、设备型号、设备序列号、供应商单位名称

		等；
		数据关联与查询，通过查询单个对象，可检索到所有关联信息；例如通过查询合同编号，可查询到与此合同相关的设备清单，巡检任务，项目进度，供应商单位等信息；
		实现对结构化数据及非结构化数据的全文关键字检索。
合同管理功能	合同整体要求	经过结构化录入形成基础服务数据，合同条款内容实现自动化提醒和执行，为项目管理和日常维护提供数据支撑，实现合同系统化管理，提升查询与统计效率。
		提供合同附件的管理，包括合同电子档案、收（开）发票等内容；支持合同附件或增补内容管理。
	合同付款	新增合同提供付款方式录入，根据状态进度生成付款计划。付款申请可上传附件。支持付款统计。
	合同提醒	提供对合同付款提醒、合同到期提醒、巡检任务提醒等内容。可自定义提醒周期。
	合同检索	提供按照合同名称关键字、合同编号、供应商单位、合同状态、合同签订时间等进行快速查询；
项目管理功能	项目管理整体要求	提供对项目全生命周期的监控和管理，包括且不限于：通过关键性里程碑管理项目的总体进度和阶段性成果，同时可拆解建立任务计划对子任务进度进行实施监控、提供设备到货跟踪、提供项目交付物文档的管理、项目实施日志录入、提供验收报告和项目遗留问题等管理；
	项目申报	提供项目背景介绍、项目达成目标、预算投入情况等便于院内申报审批。申报成功可进入立项启动
	项目提醒功能	提供项目提醒功能，包括且不限于项目实施阶段性成果、验收及变更等内容，对项目每个节点可控
	任务计划管理	提供建立自定义里程碑及任务计划，支持对任务计划设定模板，包括且不限于项目调研、项目实施、安装部署、项目评审、项目验收等任务；
	交付物管理	提供项目交付物管理，可将项目实施过程的文档收集管理，如项目计

		划书、设备交付清单表、环境调研报告、变更申请表、初验报告、终验报告等；
	关联查询与检索	功能扩展要求支持提供通过多个条件查询项目，并可通过项目查询到关联的合同、资产设备清单、供应商单位等；查询条件包括且不限于项目编号、项目名称关键字、供应商单位等；
工单管理功能	工单整体要求	系统要求提供PC端、移动电话、移动端等多种工单发起方式，实现工单全流程闭环管理，包括创建、指派、实施、转接、评价、归档等流程；可在移动端完成工单的持续管理。提供对工单数据进行图表展示。
	工单报修渠道	提供PC端、移动电话、微信公众号及企业微信等多渠道报修方式；
	来电识别	提供报修来电自动识别科室、用户，快速创建工单自动关联科室和电话，并可以根据来电号码关联历史工单。
	电话录音	来电通话可自动录音，音频文件在系统做保存可下载；
	系统派单规则	提供自定义人工手动派单；系统接单后可进行再次转派；派单时可查看工程师状态和工单量。
		功能扩展要求支持系统智能派单，可根据事件类别、资产设备类型、报修科室自动派发；
	终端功能支持	提供来电弹屏功能，系统能自动获取来电人信息等内容；
		提供终端语音识别录入，可将语音在线转换文字内容。
	工单消息推送	提供通过移动端、PC端等接收工单指派和完成的消息；
	知识库对接	提供工单处理结果到知识库的直接快速转入；
	超时催单提醒	功能扩展要求支持工单定义超时时间，超时未接单、未完成自动向首次接单人员发出提醒。
巡检管理功能	巡检整体要求	对供应商单位交付设备及项目进行巡检管理，规范供应商在项目验收后的巡检工作流程。提供科室内对各系统进行巡检的管理功能，提供完整的巡检过程管理和结果统计，
	巡检类型	提供针对供应商单位的合同巡检，及信息科室的内部日常巡检；

	巡检指标	提供针对不同对象，自定义巡检内容；
	巡检提醒	巡检任务提供站内消息、移动端等多种方式的到期自动提醒功能；
资产设备管理功能	资产管理整体要求	提供对入库、出库、变更、借用、领用、折旧、报废等资产的全流程生命周期管理；通过完善资产IP、版本号等，帮助信息科进行软硬件资产的精细化管理，实时掌握资产状态。可生成条码管理，并通过资产可查询关联的合同、项目、供应商等信息。
	序列号管理	提供资产主件及配件的序列号精细化管理；
	条码管理	提供通过主件及配件的SN号生成其唯一条码/二维码；
		功能扩展要求支持通过移动端识别资产条码，查询资产基本信息、质保状态、维修记录、生命周期、巡检任务和记录等；
	自动获取质保	提供资产与合同项目的数据关联，合同及项目验收交付设备可自动转入资产系统，同时根据验收时间自动计算质保。**（提供功能截图证明）**
	自定义类型	提供资产的自定义分类，支持至少三级内容。
	资产盘点	功能扩展要求支持对接现有无线定位引擎及地图引擎，结合蓝牙或RFID，提供资产定位；
供应商管理功能	供应商整体要求	通过供应商管理，实现对单个供应商关联的合同、项目、资产设备、巡检任务等合作记录快速查询；系统可开放给供应商进行项目实施录入、巡检结果录入，工单维修等工作，简化甲方工作量，同时可通过系统规范供应商工作流程，数据支撑管理
	数据关联	功能扩展要求支持系统内提供对单个供应商查找与之关联的合同、项目、资产、巡检等数据。
	供应商配置	提供对供应商合作级别、业务范围标签等自定义配置；
知识库	知识库整体要求	将信息科常见问题的解决方案，日常维护手册，产品配置手册作统一系统化管理，知识库要求关联工单模块，通过工单和资产类型快速查询知识库。形成有效知识体系，提升问题解决效率实现经验分享。
	自定义分类	提供知识库的自定义分类和标签管理；
	知识库建立	提供从工单处理到知识库的快速录入，及日常新增；**（提供功能截图证明）**

	数据安全	提供关键性知识库文档的权限加密功能；
	在线预览编辑	提供知识库附件的在线预览与编辑操作，包括word、PPT、Excel等；无需下载即可在线完成知识库维护更新。支持对操作修改痕迹的保留。
	知识库检索	提供知识库的正文关键字检索；
系统辅助	排班管理	功能扩展要求提供对信息科室人员的日常工作排班功能；
		功能扩展要求提供对信息科室人员的日报、周报、月报等管理功能；
	会议管理	提供信息科日常会议的安排及记录功能；
	文档管理	功能扩展要求提供针对信息科室的日常工作文档管理平台；
功能测试		合同签订七天内，提供测试产品对功能和性能测试，若无法在规定时间内提供测试设备或测试结果与招标内容不符，影响医院互联互通等级评定和应用软件上线，取消中标资格，中标人承担所有责任；
质保服务		提供原厂商五年技术支持服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

3.8 数据支撑平台

技术指标	参数要求
核心功能	辅助大数据应用的源端数据接入、转换、传输及管理平台，支持多平台、异构，集数据质控、差异补偿及自动化预警于一体的稳定可控国产化数据支撑平台。
整体要求	自主研发软件，非 OEM 产品，有软件著作权。**（要求提供软件著作权复印件）**
多层级	支持多层级配置，可多层级数据上传；下级单位往上传输数据过程，可防止数据篡改。
自动检测	支持对于同步作业的运行环境进行检查，检查项包括：数据源连接、网络延时、源库字符集、数据源抽取权限、日志校验、附加日志校验等，当不通过时，需提供处理建议 表结构发生变化时自动同步，保证源端与数仓的表结构完全一致
表格配置	支持对于同步的表格进行映射配置

	支持表、列重命名，时间戳自定义命名等规则 以适配多源集中到单一目标的表格重复问题
跨用户授权	支持对业务的访问权限控制，禁止直接访问业务库，只针对所需要同步表进行查询授权，在保证正常同步的基础上保证数据安全性
数据脱敏	针对姓名,手机号码,身份证号码等具有敏感性的数据可进行数据脱敏，可针对表和表中字段进行规则配置，实现隐私数据的可靠保护
增量指标	要求使用数据库自带 CDC 捕捉机制记录数据的操作类型和先后顺序,根据主键和操作类型进行数据增量同步,在主键发生变动时保证增量数据的一致性
一致性	支持对于源删除数据在目标进行逻辑删除 支持源数据主键发生变动时保证增量数据的同步 支持目标数据库在逻辑删除时自动保存删除数据到日志表
实时性	实时同步延迟时间不超过 15 秒
容错性	当下级单位往上层传输数据的过程中，因网络故障中断情况下，恢复后可自动恢复传输，并保证数据一致性。
性能要求	对生产业务系统的性能损耗影响平均不得超过生产业务服务器总体的性能的 5%
质控管理	要求可以设置质控的字段，质控方式等质控策略，并根据所设置的质控策略，对所同步的数据和源数据进行 HASH 比对，并对质控结果进行钉钉提醒 要求支持全量和增量质控执行等多种质控策略 要求质控策略可设置不同的自动执行周期 要求质控支持正向和反向质控并设置不同的质控条件
质控执行	要求支持定时自动执行数据质控 要求定时执行支持调度粒度包括月、周、天、时、分、秒 要求有页面可以手动进行质控并可以查看质控结果
补偿机制	要求对质控结果数据不完全匹配的，可以在页面上进行补偿 补偿只针对于不完全匹配的数据，禁止全量补偿

异常自处理	要求同步过程中针对同步失败数据进行自动补偿处理,保证数据的一致性
预警	要求提供增量同步异常，表结构变化，质控结果，软件运行状况等预警提醒，提醒方式采用钉钉，支持多层级预警
时间戳	要求落地中心数据库的数据必须有落地时间戳
监控	时间监控数据同步系统的运行情况,系统出现异常在一分钟内进行钉钉提醒
同步日志	要求记录每张表每次同步的时间，同步耗时，同步数量，同步是否成功等信息 支持记录同步过程中插入目标失败的错误记录，并在页面中进行展现，包括失败记录相应的 DML 语句 要求支持页面查看
作业调度	支持用户根据实际使用情况对于增量同步作业进行自定义调度 支持调度粒度包括月、周、天、时、分、秒 支持同一作业拥有多个调度粒度 支持定义表的调度粒度
同步模板	实现一次配置 N 次复用的功能，针对厂商、系统、版本的不同设置不同的模板
数据库支持	支持对 Oracle、SQLServer、MySQL、Postgresql、Greenplum 等数据库，支持异构数据源之间的数据同步，并自动进行数据类型的转化，且允许用户进行手动调整
部署要求	要求软件安装过程中，无需改造生产主机上的文件系统，无需更改系统卷配置 支持针对部署在小型机，X86 物理服务器，虚拟及和云主机上 支持部署在 Windows 和 Linux 等操作系统下 支持多节点同步，如主主、主备、一对多、级联等同步模式 软件部署完后，无需重启或中断业务即可生效
功能测试	合同签订七天内，提供测试产品对功能和性能测试，若无法在规定时间

	内提供测试设备或测试结果与招标内容不符，影响医院互联互通等级评定和应用软件上线，取消中标资格，中标人承担所有责任；
质保服务	提供原厂商五年技术支持服务，中标后提供原厂商授权书和服务承诺函。

3.9 业务性能保障与优化系统

技术指标		参数要求
系统总体要求		不安装 agent、不安装插件，不改变用户网络环境的基础上，对用户环境 5 个及以上的业务系统，实现全局感知（用户体验感知、业务服务感知），异常定位（业务报错、业务卡顿等异常的原因定位），性能瓶颈分析等功能，并按需实现业务系统相关的核心资源监控功能。
★硬件配置		1.硬件设备： 2U 机架式服务器， CPU：12 核，24 线程；内存：64GB；容量：企业级 SSD，960GB。 支持千兆/万兆网络环境，单台网络流量处理能力 1Gbps。 2.网络接口：镜像监听口：2 个千兆口/万兆口；管理口：1 个
部署方式		为不影响应用系统的运行和性能，系统部署不对现有网络结构进行调整，采用网络旁路监听技术、日志采集技术实现数据采集。不得在用户环境中安装任何客户端程序，不得安装插件。
主要功能	全局感知	提供已监控业务系统的全局感知能力，包括业务终端的用户使用体验感知（包括终端组体验感知、区域服务体验感知）、业务服务状态感知、网络状态感知（网络性能感知、链路感知）、计算资源感知、业务服务接口状态感知等。
	异常定位	★提供异常定位功能，支持按业务路径上的业务终端、网络、主机、服务端（应用、数据库）、外联依赖等进行异常诊断定位，支持按时间、按系统、组件、节点进行定位异常源头和异常内容。帮助管理者明确异常原因，快速处理异常**（提供功能截图证明）**
	瓶颈发现	提供性能瓶颈发现功能，跟踪记录业务服务的性能，提供可供改进的资源类瓶颈、性能类瓶颈。能按业务系统提供低效语句、报错语句、

		数据库锁等影响业务服务性能类瓶颈进行导出，支持按时间下载导出
	运行保障	提供核心资源监控、网络态势、业务服务感知等运行可视化大屏告警能力，提供管理需要的事件告警能力，并支持按多指标的逻辑告警能力。
业务系统监测	全路径延时占比分析	系统监控的核心业务系统，需提供终端到服务端的业务路径各组件延时占比分析，在选定时间点支持显示终端延时、中间件延迟、数据库延时情况。
	业务访问分析	系统提供业务访问行为分析能力，支持通过对业务系统的网络层协议解析、应用层协议解析，提供终端访问服务端的访问行为分析功能。并能根据业务系统提供任意时间的数据归类分析，必须包括报错 URL、报错 SQL、慢 URL、慢 SQL、锁阻塞、高 IO、大查询等数据查询能力，并提供历史数据分析功能。
	终端组性能分析	监控业务服务的各个终端组或机构是否存在业务报错、业务卡顿等问题，当报错数量、耗时等超出预期时，需要提供告警（告警可以按多种数据维度进行用户自定义），以便快速处理异常。
	业务服务状态分析	支持业务服务、业务服务接口、微服务的自定义配置能力，并提供业务服务状态的统计分析功能，业务服务状态需要包括报错比例、失败比例、卡慢比例。
业务组件监测	业务终端监测	★支持业务终端在数据库中的执行语句发现功能,语句需要包括 IO 次数、CPU 耗时、是否被阻塞等信息**（要求提供功能截图证明）**
		支持业务终端访问数据库的登录会话信息发现能力，会话信息包括客户端主机名、客户端程序名、登录账号等信息。
		支持业务终端与服务端的会话信息监测功能，提供会话连接请求、连接响应、连接建立的耗时，以及会话中业务语句操作内容的查看功能。
	网络数据监测	★提供网络数据分析功能，提供网络性能（网络延时、丢包重传）、带宽（网络流量、连接数）、应用（WEB、数据库）、用户（在线服务、在线终端）等指标分析能力。**（提供功能截图证明）**
		提供网络数据按时段的数据标签分类查询功能，提供丢包重传、连接

		复位、网络扫描、广播风暴等网络数据异常监控功能。
		提供网络扫描发现功能，内容包括扫描方地址、目标地址数、扫描次数和扫描失败率。存在网络扫描时，需要提供扫描方的 IP 及目标方的 IP 与端口，并提供下载查看功能。
	业务接口监测	提供基于业务服务接口定义功能，能对业务服务接口的性能进行监控，包括接口的调用情况，包括报错状态、卡慢状态、失败状态等。接口性能异常时，实时告警。
功能测试		合同签订七天内，提供测试产品对功能和性能测试，若无法在规定时间内提供测试设备或测试结果与招标内容不符，影响医院互联互通等级评定和应用软件上线，取消中标资格，中标人承担所有责任；
质保服务		提供原厂商五年技术支持服务，中标后提供原厂商授权书和服务承诺函。

3.10 桌面管理软件

技术指标	参数要求
▲终端安全管理系统功能	可以为管理员提供丰富的终端安全管理功能，包括日志审计、移动存储管理、外设管理、补丁管理、运维管理、水印管理系统盘还原等核心管理功能；提供≥1200 个终端管理授权。
系统构架	为了能够体现更好的远程运维需求，系统设计为 C/S 构架，管理员需通过 EXE 控制台程序对于终端进行管理。
远程屏幕协助	管理员可以快速接管（在 1 秒钟内接管终端电脑屏幕）远程监看或者（控制效果流畅 ）客户端的计算机。当对终端计算机进行远程控制时，客户互传终端计算机中的文件，针对终端为双屏的电脑，管理员可以点击主/副屏切换进行控制，客户端本地也可以邀请管理员远程操作自己的电脑。
★远程协助安卓设备	管理员可以对于医院的安卓系统的 PDA 和诊间屏进行远程屏幕控制，管理员可以在一秒内接管移动设备的屏幕，控制速度快，无卡顿。**(提供功能截图证明)**

桌面助手	管理员开启桌面助手策略，终端计算机桌面底层一直展示半透明窗口，管理员可以配置窗口上多个快捷方式的网址和打开浏览器名称，用户点击每个快捷方式会打开相应系统。管理员可以以九宫格的形式设置桌面助手的固定展示位置。**(提供功能截图证明)**
桌面 IP 展示	支持桌面展示机器名称、IP、MAC、日期、工作组以及自定义内容。显示的文字字体、大小、颜色均可设置，管理员可以通过九宫格的方式设置显示位置。
内网聊天	终端用户可以登录自带的聊天模块功能，可以选择医院的其他用户发送、接收即时消息，支持文件发送和接收，可以查看历史消息。
多屏墙	管理员可以实时查看多个计算机的电脑屏幕,最大支持64屏同时监看;可灵活设置监控屏数和自动循环播放的时间。
★系统盘自动还原	对于终端计算机提供系统盘还原功能，每次计算机重启，对于系统盘的写入信息，全部丢弃，系统盘恢复原状。**(提供功能截图证明)**
U 盘管理	可以设置禁止使用 U 盘，可以为 U 盘设置只读，只写权限。U 盘插入报警。对于鼠标键盘等 USB 非存储设备不禁用。支持制作注册 U 盘，制作后的例外 U 盘，可以在单位内部按权使用。客户端本地也可向管理员申请例外 U 盘，管理人员可以收到申请消息，并进行审批。
资产管理	管理者可以查询硬件资产统计报表，自动收集硬件资产的变更情况。包括 CPU、内存、硬盘、打印设备、串口设备等。可以对于硬件资产信息进行自定义操作，包括设置维保日期，责任人，机器品牌，配备时间，配备方式。管理者可以查询软件统计报表，自动收集软件的变更情况。可以统计安全软件名称、安装日期、版本号、发布者。
屏幕保护	可以远程批量统一分发客户端桌面屏保；管理员可以在系统中上传制作好的屏幕保护文件，以及无操作多长时间后启动屏保。
桌面背景	可以远程批量统一分发客户端桌面背景。
杀毒软件检测	管理员可以按计算机模式查看所有客户端的杀毒软件状况，包括是否安装杀毒软件、杀毒软件状态、杀毒软件版本号等。
Windows 服务	查看客户端的 windows 服务状况，可以设置 WINDOWS 服务端状态，如

	禁用、启用服务等。可以禁止、禁用、启用服务。
windows 补丁管理	系统可以搜集当前终端计算机的系统漏洞,以折线图的形式展现最近 7 天全网终端的漏洞数和趋势；以这线图的形式展示最近 7 天全网终端修复漏洞数；系统可以展示全部补丁信息，管理员可以根据补丁编号、补丁名称、补丁支持的操作系统进行搜索，选择需要的补丁；管理员可以查看每个补丁，在那些计算机上安装了；管理员可以查看所有补丁安装的信息，包括安装成功、安装失败、忽略信息。管理员可以设置补丁的分发速度和分发时间。管理员可以设置补丁的分发部门和分发终端。
自动同步时间	客户端自动同步服务器时间。
功能测试	合同签订七天内，提供测试产品对功能和性能测试，若无法在规定时间内提供测试设备或测试结果与招标内容不符，影响医院互联互通等级评定和应用软件上线，取消中标资格，中标人承担所有责任；
质保服务	提供原厂商五年技术支持服务，中标后提供原厂商授权书和服务承诺函。

3.11 文件安全交互系统

技术指标	参数要求
系统构架	系统需为 B/S 架构，为满足等级保护的相关要求，要求系统需为内、外网各一台设备，内、外网设备之间可以通过网闸实现文件双向交换。**（提供功能截图证明）**
硬件配置	两台 2U/8 盘位服务器，单台配置： CPU：E5/8 核/16 线程，内存：16G，硬盘：16TB 硬盘，需自带软件防火墙。不限制用户数，不限制并发数。
同步方式	系统需支持自动同步与手动同步俩种同步方式。自动同步：用户上传文件后，自动同步到对向；手动同步:用户上传文件后，选择文件手动操作同步到对向。
文件杀毒	系统内置杀毒引擎，并支持第三方杀毒引擎；在文件从一端传输到另一端时，系统能对文件进行病毒和木马检测，识别可能导致系统风险的恶意文件，一旦发现可疑文件，可自动阻止文件交换步骤。

★移动端支持	文件具备 APP 客户端，用户可以通过手机登录公网 IP 从而连接外网设备；支持用户将第三方软件中的文件通过 APP 申请，校验后传输至内网；支持安卓、IOS 系统；支持钉钉、企业微信、微信小程序端应用。**（提供功能截图证明）**
Windows 客户端	Windows 客户端具备文件的上传与下载功能，同时可以对于下载的文件进行控制，禁止拷贝到 U 盘，可以只允许将下载的文件拷贝到授权 U 盘，系统自带授权 U 盘制作工具。**（提供功能截图证明）**
个人空间	具备个人空间，用户可以对于文档进行备注说明，进行个人的文档存储。系统可以显示这个文档被下载的次数。
公共空间	管理员可以建立多个目录，给不同部门设置不同权限，包括查阅、管理、上传、下载等权限，也可以设置指定的用户的例外权限。
★在线编辑	系统支持用户可以对存储的文档，包括 WORD、EXCEL、PPT 等文件进行在线编辑操作，同时支持多人协同编辑。**（提供功能截图证明）**
版本管理	所有文件在线修改具备版本备份功能，用户可以选择历史版本进行版本恢复。
★互联网安全接入	系统自带虚拟隧道安全访问功能，用户在互联网直接访问系统时，系统的端口为隐藏的，用户无法访问系统。用户需要专用的身份验证客户端进行身份验证，验证成功后系统才会对这个终端开放访问端口，用户才可以访问系统登录页面。
快捷登录	系统支持用户将账号与微信绑定，实现通过微信扫码登录系统。
数据防泄漏	系统内置对于身份证号、银行卡号等多种检测规则，用户传输文件时，系统会对文件内容进行检测，含有敏感信息的文件将被限制外传。
资质要求	软件产品登记证书、公安部颁发的网络安全产品认证证书
功能测试	合同签订七天内，提供测试产品对功能和性能测试，若无法在规定时间内提供测试设备或测试结果与招标内容不符，影响医院互联互通等级评定和应用软件上线，取消中标资格，中标人承担所有责任；
质保服务	提供原厂商五年技术支持服务，中标后提供原厂商授权书和服务承诺函。

4.安全

4.1 专网防火墙

技术指标	参数要求
★基本要求	设备≥1U，≥8 个千兆电口，≥8 个千兆光口，≥8 个万兆光口，1 个 CON 口，≥2 个 USB 口，≥1 个管理口，≥1 个 HA 口，≥1 扩展模块槽位，≥4T SSD 硬盘，双电源。
	网络吞吐量≥20Gbps，IPS 吞吐量≥10Gbps，AV 吞吐量≥5Gbps，IPsec VPN 吞吐量≥6Gbps，并发连接数≥480 万，每秒新建连接数≥14 万，IPSec 隧道数≥10000，SSL VPN 并发在线用户数≥8000。（提供第三方专业测试报告）
	配置 5 年 IPS 入侵防御、AV 病毒过滤、TI 威胁情报、APP 应用识别、8 个 SSL VPN 许可、5 个虚拟防火墙许可、云安全运维/订阅许可。
	提供 5 年硬件保修、特征库和软件升级服务。
路由功能	支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议。
NAT	要求所投产品支持 NATv6、NAT444、NAT64、DS-Lite、Full-Cone-NAT 等地质转换技术，并可对 SNAT\DNAT 进行命中分析，帮助用户识别长期未命中的 NAT 规则。
	支持 NAT 扩展技术，突破传统单个公网 IP 地址 64512 个端口的瓶颈达到更大值。
IPV6	支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议。
	支持 NAT66，NAT64 隧道。
策略管理	支持基于国家/地区维度进行流量控制等安全策略，支持垃圾策略清理，支持聚合策略以及策略导出。
	支持自学习生成策略功能，聚合流量并生成细化的策略规则，辅助用户更快速、更准确和更完整的配置安全策略。
负载均衡	支持智能链路负载均衡技术，可动态探测链路响应速度并选择最优链路进行转发。
	支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS

	请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。
VPN	要求所投产品支持 IPSec VPN\SSL VPN\L2TP VPN 等 VPN 技术，且 SSL VPN 具备 USB-KEY 认证的能力。
	支持对登录 SSL VPN 的用户端系统进行端点安全检查，至少包括文件路径、运行进程、安装服务、运行服务、防火墙设置等方面。
IOT 安全	支持识别视频监控专网中的 IPC（网络摄像机）和 NVR（网络硬盘录像机）等网络视频监控设备，对识别出的设备进行实时监控，然后根据配置对出现非法行为的网络视频监控设备进行阻断等操作。
SD-WAN	能够支持全生命周期的 SD-WAN 整体解决方案，包括：自动化部署、链路双活、链路质量检测、隧道安全、控制器高可靠等功能。
云安全运维	★支持通过云端 SaaS 管理平台为用户提供便捷、高质量以及低成本的增值安全服务，支持手机 APP 对设备进行监控：通过手机可以第一时间获知设备的基础信息，安全风险实时告警，帮助快速定位问题、安全可视化实时呈现。提供 App 下载 URL。该 APP 不能是 VPN 客户端软件。该 APP 不限制使用用户数（提供配置截图证明）
管理功能	支持 2 个系统软件并存，并可在 WEB 界面上直接配置启动顺序，支持不少于 8 个配置文件并存，并支持回滚。
	产品必须支持全功能 CLI（SSH、TELNET、CONSOLE 等方式）命令配置，以方便快速进行脚本操作和故障调试，且 CLI 配置必须支持中文输入，支持通过 CLI 配置接口、路由、安全策略等功能模块。
入侵防御	基于状态、精准的高性能攻击检测和防御，支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御。
	具备 16000 种以上攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征 ID 等方式的查询。（提供配置截图证明）
病毒过滤	支持基于流模式的病毒过滤，可对 SMB\IMAP 等协议传输的病毒以及不少于 5 层压缩病毒文件进行检出，要求本地病毒特征库规模≥330 万，

	支持手动添加、删除病毒特征。
URL 过滤	支持 30 种以上域名分类库，控制不良网站访问，支持查询 URL 归属的 URL 分类库。
流量管理	支持流量管理，支持两层八级管道嵌套，能够同时做到两个维度的流量控制，能够根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、Vlan 等信息划分管道。
云沙箱平台对接	支持扩展云端沙箱技术，可将可疑文件提交云端沙箱进行安全模拟运行，并根据运行结果与防火墙实现联动。
僵尸网络防护	支持扩展僵尸网络防御服务，支持扫描 TCP/HTTP/DNS 协议流量并进行 C&C 检测。
威胁情报	支持与云端威胁情报中心联动，支持威胁情报与防火墙威胁事件、威胁日志检测结果加强与取证，用户可通过手动触发与自动触发将日志元素上送威胁情报平台进行上下文查询。
★防雷击	产品通过第三方专业检测中心浪涌（冲击）抗扰度（4KV）测试项目，提供第三方专业检测中心委托测试报告
虚拟系统	支持虚拟系统功能，本次提供 5 个虚拟防火墙系统授权，每个虚拟系统可自定义 CPU 资源、会话数、策略数、安全域数、源 NAT 数、目的 NAT 数、IPSEC VPN 隧道数、会话限制规则数、IPS 功能、URL 功能、关键字类别、威胁日志等。
IP 信誉库	要求所投产品具备 IP 信誉库的能力，可对对僵尸肉鸡、垃圾邮件发送者、Tor 节点、失陷主机、暴力破解等风险 IP 的流量进行识别和过滤，并进行丢弃、阻断以及记录日志等功能。
	要求所投产品的 IP 信誉库可联动云平台定期更新，且云平台和所投产品为同一厂商。
资质要求	为保障产品质量及市场可信度，要求产品连续 5 年入围 Gartner 企业级防火墙魔力象限（**提供有效证明材料**）
质保服务	提供原厂商五年技术支持服务和保修服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

4.2 外网防火墙

技术指标	参数要求
▲基本要求	设备≥1U，≥8 个千兆电口，≥4 个万兆光口（含光模块），1 个 CON 口，≥2 个 USB 口，≥1 个管理口，≥1T SSD 硬盘，双电源。
	网络吞吐量≥20Gbps，IPS 吞吐量≥6Gbps，AV 吞吐量≥4Gbps，IPsec VPN 吞吐量≥700M，并发连接数≥250 万，每秒新建连接数≥13 万，IPSec 隧道数≥1000。
	配置 5 年 IPS 入侵防御、AV 病毒过滤、云威胁情报订阅许可授权。
	提供 5 年硬件保修、特征库和软件升级服务。
网络适应性	产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。
	产品支持虚拟防火墙功能，支持虚拟防火墙的创建和删除，具备独立的接口、会话管理、应用控制策略、NAT 等资源。
	产品支持链路连通性检查功能，支持基于 3 种以上协议对链路连通性进行探测，探测协议至少包括 DNS 解析、ARP 探测、PING 和 BFD 等方式。
	产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等。
用户识别与认证	产品支持 3 种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证。
应用控制	★产品支持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。**（需提供产品功能截图证明）**
访问控制	产品支持基于网络区域、网络对象、MAC 地址、服务、应用等维度进行访问控制策略设置。
	产品支持 ftp 协议命令控制功能，至少包含 delete、rmdir、mkdir、rename、mget、dir、mput、get、put 等，保护对外服务不被恶意篡改。

安全防护	产品支持异常数据包攻击防御,防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型。
	产品支持对压缩病毒文件进行检测和拦截,压缩层数支持15层及以上。
	★勒索病毒在医疗行业高发，是我单位重点防护内容之一，为保障产品勒索病毒的防护能力和防护效果，产品应对支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略，为保障功能的可靠性，**需提供产品相关功能截图，并提供第三方专业机构出具的关于“勒索病毒”的相关证书证明功能有效性。**
	产品内置超过4500种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。
	产品支持X-Forworded-For字段检测，并对非法源IP进行日志记录和联动封锁。
	产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。
	产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。
	产品内置不低于10800种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。
	产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。
	★为保障产品本身运维安全性，避免账号暴力破解、弱口令等安全问题发生，产品需支持用户账号安全保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。**需提供产品相关功能截图，并提供第三方专业机构出具的关于“账号保护”的相关证书证明功能有效性。**

安全策略管理	产品支持安全策略有效性分析功能，能够分析出策略冲突、策略冗余、权限放通过大、无效策略等，给运维人员提供优化建议。
	产品支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率。
高可用性	产品支持 A|A、A|S 两种双机模式部署。
产品运维管理	产品支持 Web 管理、串口管理、SSH 管理等多种不同方式。
	产品支持多种安全日志存储方式，至少包括防火墙本机、日志服务器等不同方式；产品支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间。
	产品支持管理员双因子认证，可以通过用户密码和 Key 等不同方式登陆产品管理界面。
资质要求	为保障产品质量及市场可信度，要求产品连续 5 年入围 Gartner 企业级防火墙魔力象限**（提供有效证明材料）**
售后服务	提供原厂商五年技术支持服务和保修服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

4.3 数据中心防火墙

技术指标	参数要求
★基本要求	设备≥1U，≥8 个千兆光口，≥8 个千兆电口，≥8 个万兆光口，≥2 个 40GE(QSFP+)接口，≥1 个 CON 口，≥2 个 USB 口，≥1 个 HA 口，≥1 个管理口，≥4T SSD 硬盘，双电源。
	网络吞吐量≥40Gbps，IPS 吞吐量≥20Gbps，AV 吞吐量≥12Gbps，IPsec VPN 吞吐量≥12Gbps，TCP 并发连接数≥1000 万，TCP 每秒新建连接数≥31 万，IPSec 隧道数≥20000，SSL VPN 并发在线用户数≥10000。**（提供第三方专业测试报告）**
	配置 5 年 IPS 入侵防御、AV 病毒过滤、TI 威胁情报、APP 应用识别、8 个 SSL VPN 许可、10 个虚拟防火墙许可、LB 服务器负载均衡、云安全运维/订阅许可。
	提供 5 年硬件保修、特征库和软件升级服务。

路由功能	支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议。
NAT	要求所投产品支持 NATv6、NAT444、NAT64、DS-Lite、Full-Cone-NAT 等地质转换技术，并可对 SNAT\DNAT 进行命中分析，帮助用户识别长期未命中的 NAT 规则。
	支持 NAT 扩展技术，突破传统单个公网 IP 地址 64512 个端口的瓶颈达到更大值。
IPV6	支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议。
	支持 NAT66，NAT64 隧道。
策略管理	支持基于国家/地区维度进行流量控制等安全策略，支持垃圾策略清理，支持聚合策略以及策略导出。
	支持自学习生成策略功能，聚合流量并生成细化的策略规则，辅助用户更快速、更准确和更完整的配置安全策略。
负载均衡	支持智能链路负载均衡技术，可动态探测链路响应速度并选择最优链路进行转发。
	为保障服务器资源均衡，所投产品支持服务器负载均衡，可对服务器会话状态进行监控，支持服务器健康检查和服务器会话保护，支持会话保持，支持加权哈希、加权轮询、加权最小连接数等算法。（提供界面配置截图证明）
VPN	要求所投产品支持 IPSec VPN\SSL VPN\L2TP VPN 等 VPN 技术，且 SSL VPN 具备 USB-KEY 认证的能力。
	支持对登录 SSL VPN 的用户端系统进行端点安全检查，至少包括文件路径、运行进程、安装服务、运行服务、防火墙设置等方面。
IOT 安全	支持识别视频监控专网中的 IPC（网络摄像机）和 NVR（网络硬盘录像机）等网络视频监控设备，对识别出的设备进行实时监控，然后根据配置对出现非法行为的网络视频监控设备进行阻断等操作。
SD-WAN	能够支持全生命周期的 SD-WAN 整体解决方案，包括：自动化部署、链路双活、链路质量检测、隧道安全、控制器高可靠等功能。
云安全运维	★支持通过云端 SaaS 管理平台为用户提供便捷、高质量以及低成本的

	增值安全服务，支持手机 APP 对设备进行监控：通过手机可以第一时间获知设备的基础信息，安全风险实时告警，帮助快速定位问题、安全可视化实时呈现。提供 App 下载 URL。该 APP 不能是 VPN 客户端软件。该 APP 不限制使用用户数（提供配置截图证明）
管理功能	支持 2 个系统软件并存，并可在 WEB 界面上直接配置启动顺序，支持不少于 8 个配置文件并存，并支持回滚。
	产品必须支持全功能 CLI（SSH、TELNET、CONSOLE 等方式）命令配置，以方便快速进行脚本操作和故障调试，且 CLI 配置必须支持中文输入，支持通过 CLI 配置接口、路由、安全策略等功能模块。
入侵防御	基于状态、精准的高性能攻击检测和防御，支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御。
	具备 16000 种以上攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征 ID 等方式的查询。（提供配置截图证明）
病毒过滤	支持基于流模式的病毒过滤，可对 SMB\IMAP 等协议传输的病毒以及不少于 5 层压缩病毒文件进行检出，要求本地病毒特征库规模≥330 万，支持手动添加、删除病毒特征。
URL 过滤	支持 30 种以上域名分类库，控制不良网站访问，支持查询 URL 归属的 URL 分类库。
流量管理	支持流量管理，支持两层八级管道嵌套，能够同时做到两个维度的流量控制，能够根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、Vlan 等信息划分管道。
云沙箱平台对接	支持扩展云端沙箱技术，可将可疑文件提交云端沙箱进行安全模拟运行，并根据运行结果与防火墙实现联动。
僵尸网络防护	支持扩展僵尸网络防御服务，支持扫描 TCP/HTTP/DNS 协议流量并进行 C&C 检测。
威胁情报	支持与云端威胁情报中心联动，支持威胁情报与防火墙威胁事件、威胁日志检测结果加强与取证，用户可通过手动触发与自动触发将日志

	元素上送威胁情报平台进行上下文查询。
★防雷击	产品通过国家无线电监测中心检测中心浪涌（冲击）抗扰度（4KV）测试项目，**提供国家无线电监测中心检测中心委托测试报告**
虚拟系统	支持虚拟系统功能，本次提供 10 个虚拟防火墙系统授权，每个虚拟系统可自定义 CPU 资源、会话数、策略数、安全域数、源 NAT 数、目的 NAT 数、IPSEC VPN 隧道数、会话限制规则数、IPS 功能、URL 功能、关键字类别、威胁日志等。
IP 信誉库	要求所投产品具备 IP 信誉库的能力，可对对僵尸肉鸡、垃圾邮件发送者、Tor 节点、失陷主机、暴力破解等风险 IP 的流量进行识别和过滤，并进行丢弃、阻断以及记录日志等功能。
	要求所投产品的 IP 信誉库可联动云平台定期更新，且云平台和所投产品为同一厂商。
资质要求	为保障产品质量及市场可信度，要求产品连续 5 年入围 Gartner 企业级防火墙魔力象限（**提供有效证明材料**）
质保服务	提供原厂商五年技术支持服务和保修服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

4.4 WEB 应用防火墙

技术指标	参数要求
★基本要求	专业 Web 应用防火墙设备，非防火墙带 web 防护功能或授权许可的硬件设备。
	配置 1 个 RJ-45 Console 口,1 个 10/100M 管理接口、1 个 10/100/1000M HA 口，≥8 个千兆电接口，≥8 个千兆光口，≥2 个万兆光口，≥1 个网络接口扩展槽位（可扩展 40G 接口），双电源。
	网络吞吐率≥25Gbps，HTTP 吞吐量≥12Gbps，最大并发 HTTP 连接数≥1000 万，每秒新建 HTTP 事务数≥15 万。
	提供 5 年硬件保修、特征库和软件升级服务。
接入模式	支持智能部署，上线 WAF 设备能够自动感知 Web 网站 IP 和端口；
	支持策略路由、透明模式、代理模式、旁路部署和单臂部署；

	支持 NAT 环境下的用户识别能力；
	支持大屏展示能力，满足客户对 WAF 产品大屏展示要求；
	支持对 WEB 相关应用协议进行自定义，支持详细协议分析变量；
WEB 攻击防护	支持基于区域的访问控制，可按区域进行地址访问限制，防止区域性攻击对业务系统造成影响；
	★具备语义防护、AI 智能防护、算法防护功能，**（提供人工智能安全分析平台软件著作权登记证书）**
	具备 CSRF 防护及自学习功能，能够有效防止 CSRF 攻击及通过自学习可减少 CSRF 配置
	具有对外提供 API 接口能力，可通过 API 接口给设备下发策略；
	支持攻击日志可高亮显示，有利于用户比较直观看到攻击脚本；
	具备双引擎防护功能，支持 API 防护，可支持 API 协议合规、API 访问速率限制等；
	支持 Web 应用安全 XSS 攻击、Webshell、敏感信息泄露、弱口令等；
	★具有蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断（提供 TTL、CNAS、MA、ilac-MRA 检测盖章报告证明）；提供第三方专业机构出具的滤除网络攻击流量的方法的技术证明文件）
	★具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截，**（提供第三方专业机构针对 DNS 服务的防御方法的技术证明文件）**
	支持网站锁功能，对网站进行锁定，可按日期、周期进行锁定设置；
	支持网站一键关停功能，网站异常后可通过一键关停，将网站转为维护状态；
	支持源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对 Web 网站造成影响；
	具备客户端访问控制功能，预防恶意客户端进行访问频率的多层次恶意访问；

	支持恶意地址主动屏蔽，提前免疫包括病毒网站或者攻击源地址的攻击
安全联动	支持和全流量分析取证产品进行联动，根据填写的时间偏移，可获取到相关时间段内的流量，有利于获取攻击事件进行进一步分析；
	支持和外联策略联动，满足用户对 Web 应用安全防护和外联策略联动需求，提供截图证明；
	支持和检测产品联动，满足用户对网络流量镜像给网络安全检测设备需求；
产品资质	具有《信息技术产品安全测评证书 EAL3+》**（提供相关证明文件）**
质保服务	提供原厂商五年技术支持和保修服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

4.5 数据库审计

技术指标	参数要求
★配置要求	2U 机架式结构，双电源，≥6 个千兆电接口，≥4 个千兆光口，≥2 个万兆光口，≥1 个接口扩展槽，≥1 个管理口，≥1 个 HA 口，1 个 RJ45 串口，内存≥32G，硬盘≥12T(4*4T raid5)。性能吞吐量≥4G，审计处理能力≥50000 条 SQL/s，日处理事件数≥3 亿，配置≥10 个被审计 DB 服务授权。
平台专业性要求	采用具有自主知识产权的 VSP 通用安全平台，具备高效、智能、安全、健壮、易扩展等特点；
	采用多核并行安全架构,具有自主研发的多核多线程 ASIC 并行操作系统软件著作权；
部署方式	采用旁路部署方式对原有网络不造成影响，安全审计产品的故障不影响被审计系统的正常运行；无需在被审计系统上安装任何代理。
安全审计	支持对 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、MongoDB、redis、Hbase、hive、ES 数据库进行审计、支持高斯（Gauss）、人大金仓 KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase)等国产数据库审计

	★支持对 Oracle 数据库状态的自动监控，可监控会话数、连接进程、CPU 和内存占用率等信息，**（提供第三方专业机构出具的硬件状态监测方法的技术证明文件）**
	支持双向审计，支持对 Select 操作返回行数和返回内容的审计；
	支持访问数据库的源主机名、源主机用户、SQL 操作响应时间、数据库操作成功、失败的审计；
	支持数据库中存储过程自动学习，可学习存储过程中涉及的操作并与审计事件中的存储过程名进行关联,方便确认存储过程是否存在风险；
协议审计	支持审计 HTTP 和 HTTPS 协议的 URL、访问模式、cookie、页面内容、Post 内容；
文件内容审计	可审计记录 FTP、邮件、HTTP、HTTPS、SCP、SFTP 等方式传输的文件（包括文本、Word、Excel 等格式），并且可对审计到的文件进行查询和下载；
智能发现与敏感数据分类分级	支持用户环境中的数据库和资源账号、表名的自动发现，方便用户使用；
	支持用户数据库中敏感信息的自动发现，可定位敏感数据存储的服务器、库名、表名、列名，并形成针对敏感信息的审计规则；
	支持对敏感信息敏感级别进行定义，各级别可对应不同风险值，方便对敏感数据泄露进行风险进行评估；
	敏感信息发现支持探测器和正则表达式两种方式，探测器至少包含：姓名、地名、银行卡、身份证、IP 地址、密码等多种探测器；
审计策略支持	用户可自定义审计策略，审计策略支持时间、源 IP、目的 IP、协议、端口、登陆账号、命令数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件(非正则表达式方式)，并且表字段可匹配与或关系
	支持频次统计，某一操作在周期时间内达到设定的次数阀值后可以进行单独记录和展示，周期事件和次数可按需配置；
	审计策略支持字段名称和字段值作为分项响应条件（非正则表达式方

	式）
日志查询统计	支持按时间、级别、源\目的 IP、源\目的 MAC、协议名、源\目的端口为条件进行查询
	★支持敏感数据访问独立大屏展示，可直观展示各类各级别敏感数据占比、敏感数据访问量与分布、敏感数据访问用户 TOP5、敏感数据访问源 IPTOP5、敏感数据增删改插操作分析等内容，**（提供功能截图证明）**
	支持场景异常行为分析，可展现账号多 IP 登录、同账号上下班操作统计、访问时长审计、疑似暴力破解、疑似撞库攻击、数据库异常信息、异常账号访问检测等；
	支持疑似暴力破解、疑似撞库攻击、场景的操作异常分析；行为周期与阀值可按需定义；
	查询需返回全部符合查询条件的事件，不可限制最大返回数量，防止因返回结果不全导致异常信息遗漏；
	可支持根据 sql 语句关键字进行查询，查询事件为 sql 语句中包含该关键字的所有符合条件的操作记录；
自身管理	支持一键自检功能，可以检查系统当前运行状态，检查内容包括：系统信息、进程信息、数据库信息、授权信息、用户信息等 17 项内容，协助管理员迅速定位系统异常，减少日常维护工作量；
	支持动态口令卡认证，账号具备独立动态口令卡，提升管理员账号安全级别，降低账号泄露风险；
联动功能	支持与 Web 应用防火墙（WAF）的联动，可对 WAF 上报的应用系统攻击实现场景还原展示；
	支持与 APT 检测产品的联动，对于网络传输的文件不仅可以审计，还支持恶意代码检测，报告可疑的攻击文件；
响应方式	★支持按照风险级别进行告警，告警方式支持界面告警、Syslog 告警、SNMP trap 告警、短信告警、邮件告警，（提供第三方专业机构出具的基于消息队列的报警信号处理方法的技术证明文件）

第三方接口	支持 NTP 时间同步；
	支持 SNMP 方式，提供系统运行状态给第三方网管系统
	支持 Syslog、SNMP 方式向外发送审计日志
质保服务	提供原厂商五年技术支持和保修服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

4.6 内网准入控制

技术指标	参数要求
基础架构	基于 linux 开发的专用系统，标准机架式硬件产品，所有功能基于一台设备即可实现，无需额外购买服务器、操作系统及数据库等中间件，具有独立自主知识产权。**（要求提供相关证明材料）**
★性能参数	1U 机架结构；配置冗余电源；配置 6 个 1000MBASE-T 接口，配置 2 个万兆网口；每秒事务数（TPS）≥6000（次/秒），最大吞吐量≥2.3Gbps，最大并发连接数≥5000（条）；终端用户认证数量≥1000 点
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。
	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。**（要求提供功能截图证明）**

管理	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。
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。**（提供功能截图证明）**
	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。
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。
	★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。**（提供功能截图证明）**
	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。
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。
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。
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。
	支持主流的杀毒软件版本、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。
	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。
	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。
	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。

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。
质保服务	提供原厂商五年技术支持和保修服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

4.7 外网准入控制

技术指标	参数要求
基础架构	基于 linux 开发的专用系统，标准机架式硬件产品，所有功能基于一台设备即可实现，无需额外购买服务器、操作系统及数据库等中间件，具有独立自主知识产权。**（要求提供相关证明材料）**。
★性能参数	1U 机架结构；配置单电源；配置 6 个 1000MBASE -T 接口；每秒事务数（TPS)≥1500（次/秒），最大吞吐量≥1Gbps，最大并发连接数≥1500（条）；终端用户认证数量≥200 点；
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。
	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。**（要求提供功能截图证明）**
管理	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。
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。**（提供功能截图证明）**
	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。
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。
	★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。**（提供功能截图证明）**
	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。
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。
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。
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。
	支持主流的杀毒软件版本、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。
	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。
	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。
	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。
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。
质保服务	提供原厂商五年技术支持和保修服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

4.8 威胁探针

技术指标	参数要求
性能要求	MTBF ＞65000 小时；吞吐率≥网络层 2Gbps
硬件配置	★软硬一体化 2U 标准机架式设备：CPU≥4 核 8 线程*1；内存≥32GB；硬盘≥2T*2 RAID1；1+1 冗余电源（300W）；网络接口：标配 10 个，管理口 2 千兆电，业务口 4 千兆电，4 千兆光；
	▲要求适配现有态势感知平台或提供新平台满足态势感知平台功能
综合能力	支持双向流量审计，可对请求和响应内容进行审计
	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。

	风险查询支持一键切换运营模式和专业模式，满足不同场景的研判需求。 运营模式可自由选择常用条件，如事件类型、风险级别、攻击状态、规则 ID、回放包 ID、报文、CVE/CNNVD 编号等；专业模式支持多语法组合查询，包含但不限于 AND、OR、NOTIN、IN、==、!=，专业模式包含数据窃取、恶意文件投递、内部横向扩散等 7 种常用查询模版外，支持通过历史筛选条件新增自定义模版，方便后续查询使用
Web 攻击检测	支持 Websocket 通信的 HTTP、HTTPS（需要导入服务器私钥证书）协议解析，检测 WEB 攻击
	★包含 30 种以上的深度检测模块，可支持 shiro 反序列化、蚁剑、哥斯拉、冰蝎 3.0、冰蝎 4.0 等检测能力，且能识别如 shootback、TunnaProxy、dnscat2、reGeorg、reDuh、CobaltStrike 等隧道通信工具**（提供功能截图证明）**
	★支持 WEBSHELL 检测，可检测访问 webshell 的行为，包含具体对应的 URL、返回码、返回数据包内容等，可显示一句话类 webshell 后门是否植入成功**（提供功能截图证明）**
管理功能	支持对流量中的 IP 地址、端口等进行统计，快速识别未登记资产。可基于特定应用或服务对内部资产进行梳理（系统类型、IP、域名、端口等），查看资产端口暴露情况，特别是以非标端口提供的服务情况；可深入识别运行在资产上的设备类型、应用、服务信息详细情况（类型、版本、服务名称等） 支持资产风险及健康度评估，支持对资产活跃程度分类，支持对资产分组，可配置资产 IP 所属的组织和网段，以展示资产层级关系。可自定义配置资产分组属性，包括但不限于资产等级、所属地理位置、内外网属性、单位地址、责任人等。
日志报表	告警可详细展示风险级别、发生时间、告警名称、客户端 IP、服务器 IP、ATT&CK 矩阵、报文内容（URL、请求头、请求参数、请求内容）
	支持告警管理功能，可通过告警来源、IP 分类等维度统计误报和漏报

	告警数据
	支持 KAFKA、syslog、ftp、sftp 等数据外送方式。 KAFKA、syslog、sftp 和 ftp 外送方式支持配置多个服务器，分别发送不同业务数据
	支持对 KAFKA、syslog 发送的风险信息进行 AES、SM4 加密传输 KAFKA 服务器配置支持 SASL 认证和 Kerberos 认证；KAFKA 数据传输支持明文或 SSL 加密。
	审计数据保留策略应至少满足天数和百分比两个控制参数，支持 web 界面可配置，且恢复数据不影响正常的审计功能。对审计日志可自动备份并加密，无法通过撞库、混淆还原等方式解密，必须导入设备才能进行恢复查看，并可自动释放磁盘空间。 ★设备产生的数据重要程度至少分为 3 级，可自定义配置不同级别数据的清理比重**（提供功能截图证明）**
质保服务	提供原厂商五年技术支持和保修服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

4.9 零信任

技术指标	参数要求
★设备规格	性能参数：最大理论加密流量（Mbps）≥350Mbps，最大理论并发用户数（个）≥600。 硬件参数：规格≥1U，内存大小≥16G，硬盘容量≥128G SSD，电源：单电源，接口不少于 6 千兆电口+2 千兆光口 SFP。 本次提供不少于 300 套零信任接入授权。
网络部署	为了满足灵活部署的要求，综合网关应支持 IPV4/IPV6 双栈网络 IP 配置，可自主选择配置 LAN 口或 WAN 口。为了保护设备的安全，可支持默认限制所有 IP 通过 WAN 口访问系统，支持通过配置 IP 白名单的方式来放通 WAN 口接入的特殊需求。
★集群模式下授权漂移	为了保障系统的稳定性，集群节点故障后剩余节点仍能接管所有业务，本地集群需支持授权漂移机制：集群中的单节点故障后，集群的总授

	权数跟故障前保持一致。**（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明）**
应用打开方式	应支持配置应用资源指定的打开方式，如浏览器等；为了适应某些业务系统对浏览器的兼容性，还应支持配置应用打开的指定浏览器类型。
隧道模式的审计与安全能力增强	在业务应用兼容性良好的情况下，支持以隧道模式发布 http/https 协议的资源，以增加在隧道模式下发布的资源的 URL 级别审计能力，同时支持为隧道资源添加 WEB 水印以及单点登录功能。
WEB 资源支持依赖站点	对于一些主要在主站点中点击使用的子站点 WEB 业务系统，且子站点跟主站点业务系统权限一致的场景，为简化管理员配置，零信任系统应支持开启依赖站点功能。为方便业务快速上线，还应支持自动采集站点功能对依赖站点进行梳理。
私有 DNS 解析	支持以私有 DNS 发布企业资源，无需额外购买 DNS 服务即可使用域名访问内网资源，支持管理员自主配置是否允许从具体网络区域（局域网/互联网）接入时使用此私有 DNS 解析地址。
客户端国产终端兼容性	为了保障用户在国产化终端上的正常业务访问，零信任客户端应兼容主流国产硬件 CPU 的国产操作系统终端，需提供国产操作系统与零信任厂商的兼容性证明，包括但不限于麒麟 V10×龙芯、麒麟 V10×龙芯 LoongArch、麒麟 V10×飞腾、麒麟 V10×鲲鹏、麒麟 V10×兆芯、麒麟 V10×海光、麒麟 V10×海思麒麟；统信 V20×龙芯（3A3000、3A4000）、统信 V20×龙芯（3A5000）、统信 V20×飞腾、统信 V20×鲲鹏、统信 V20×海光、统信 V20×兆芯等。
CDN 接入能力	★支持配置企业的 CDN 作为零信任客户端下载地址，以降低设备本身的非业务访问带宽压力。**（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明）**
终端管理	1、为方便管理用户的终端，并对其进行分类管理，支持为终端设置资产类型，如企业终端、个人终端、企业纳管个人终端等类型。2、为方便统一管理用户的终端，支持为接入系统的终端设置标签，支持通过终端标签来配置特殊的上线准入策略及应用访问策略。终端标签应至

	少内置内网终端、外网终端、开发终端、办公网终端等标签，且支持管理员自定义新增标签。3、支持以表格的形式批量导入导出终端列表，可查看接入系统的终端详细类型，包括但不限于：终端名称、品牌、操作系统、资产类型、终端标签、硬件特征码、MAC 地址、授权类型、最后登录用户、最后接入方式、最后接入 IP、最后接入网络区域、最后活跃时间、首次接入时间、闲置时长、在线状态等。
支持的认证方式	为满足单位多样化安全便捷认证需求，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、Radius 账号认证、HTTPS 帐号认证、证书主认证、证书辅认证、短信主认证、短信辅认证、标准 Radius 令牌认证、第三方令牌认证、TOTP 动态令牌认证等认证方式，并可与企业微信、阿里钉钉、飞书结合实现扫码认证，支持飞书用户或个人微信企业号通过 H5 接入。
自适应认证	为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、闲置帐号登录、弱密码登录、异常时间登录、非常用地点登录等。
单点登录	1、支持帐号密码代填的单点登录功能，支持智能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；支持精准识别的代填模式，以业务登录界面的帐号输入框、密码输入框、登录按钮等作为匹配项，自定义精确匹配零信任用户名、密码、组织架构名、手机号、邮箱、邮箱前缀等值，也可以设置由终端用户自定义输入或管理员设定固定值登录。 2、在业务系统已经有第三方统一身份认证系统的场景下，零信任系统支持通过票据共享的方式跟统一身份认证系统进行单点登录对接，以间接实现业务系统的单点登录对接。为了适应多种身份认证系统获取票据的方式，票据共享应至少支持反向 OAuth 对接及票据注入等模式。 3、在对接企业微信、钉钉等主流超级 APP 时，零信任系统支持直接单

	点登录发布在企业微信或钉钉工作台的H5微应用，不改变用户原有访问习惯。
弱密码库自定义	支持管理员自行配置单位的弱密码库，可配置不少于10W行的弱密码。
动态业务访问控制	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支持按需授权，支持用户或用户组直接关联到应用，避免需要为部门中的个别特殊人员或用户组建立大量角色，简化权限管理，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或多系统设定访问控制策略，操作系统需包括Windows、macOS、linux/麒麟/统信、iOS/Android；3、动态访问控制策略支持“与”、“或”条件嵌套，并可通过单一条件或条件组的方式灵活组合嵌套，可支持的条件变量应包括但不限于：应用类型、浏览器版本、客户端源IP、网关接入IP、应用访问的进程名称、终端名称、MAC地址、终端本地IP列表、操作系统版本、终端资产类型、终端标签类型、存在指定文件、操作系统安装的补丁、运行进程、运行指定杀毒软件、运行任一杀毒软件、零信任客户端版本、安装指定软件、开启系统防火墙、用户接入城市、用户登录国家、用户登录时间、应用进程的信任状态、弱密码、授信终端、授信域环境等；4、可联动本次采购的终端安全管理的检测评分作为策略条件；5、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；6、当检测到不符合安全条件时，支持设置如短信增强认证、告警等灵活的补救动作，实现灰度处置，且能配置处置有效时长，平衡员工访问体验和安全保障。
第三方安全能力集成能力	支持提供开放的API，管理员可以在控制台创建API KEY，供第三方安全设备或单位自有安全分析平台对接，便于形成统一的安全体系。
可信应用防护策略	1、支持自动生成基于可信应用的动态访问策略模板，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。2、管理员可基于自动生成的防护策略模板增加组合条件，灵活使用可信应用的分析能力。3、可信应用防护策略可配置多条。
服务隐身	★1、为了最大程度缩小网络、业务暴露面，零信任平台需提供单包授权能力（SPA），支持 UDP+TCP 组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口，不会出现敲门放大漏洞。2、PC 端和移动端均支持通过安全码激活客户端为授权客户端，从而可进行 SPA 敲门和连接，安全码支持共享码和一人一码两种模式，支持短信分发安全码，保障业务的安全性。3、一人一码模式下，当实际登录用户跟分发 SPA 安全码绑定的用户不一致时，零信任系统可以阻止用户登录上线并产生安全告警，帮助管理员溯源，进一步提升系统安全性。**（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明）**
支持全面的日志记录	1、支持用户登录日志（登录、注销，含 MAC 地址、终端类型、浏览器类型等）2、支持管理员操作日志（含管理员、接入 IP、时间、管理行为、对象）3、支持用户安全日志提取，审计中心应将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位。用户安全日志包括但不限于：帐号安全（应包含帐号首次登录、异常时间登录、非常用地点登录、弱密码登录、爆破登录、闲置帐号登录、帐号在新终端登录等）、中间人攻击、SPA 安全（应包含 SPA 端口扫描、SPA 爆破攻击、SPA 敲门伪造、SPA 重放攻击、SPA 安全码泄漏等）、cookie 劫持等。4、支持将设备安全事件单独记录在设备安全日志中，事件类型包括但不限于：接口扫描、接口 webshall 攻击、接口参数爆破、接口越权调用等设备 API 防护日志。
设备稳定性检查	包括但不限于：1、应支持系统黑匣子及核心进程的状态检测。2、应支持 CPU 负载、内存负载、磁盘空间、网卡健康、硬盘健康、网卡日志、BIOS 固件等硬件相关状态的检测。3、应支持软件版本及补丁修复状态等检测。

国家商用密码	支持中国商用密码标准，支持加密算法 SM2、SM3、SM4。
	★1、支持使用商密密码卡进行加密 2、支持在控制台对密码卡进行管理（包括：激活、取消激活、密钥备份/恢复、管理 KEY 口令）**（需提供产品功能截图证明）**
开放能力	1、为方便整合业务系统的工作流程，应支持通过 OPEN API 的方式将零信任系统的能力开放给第三方业务系统进行调用配置，如满足员工需要业务系统访问权限时可以直接通过OA办公系统的工单审批流程来申请的需求。支持通过限制访问 OPEN API 的 IP 接入地址、API 密钥加密等方式来保障 OPEN API 的调用安全。2、为满足业务客户端个性化接入的需求，应支持通过 SDK 集成的方式将零信任系统的 PC 端客户端与移动端客户端接入能力集成到第三方业务系统中，从而不体现零信任厂商的信息。
产品资质	提供国家密码管理局商用密码检测中心出具的含有“访问控制系统”字样，符合 GM/T 0024 标准或 GM/T 0025 标准要求，以及符合 GM/T 0028《密码模块安全技术要求》第二级的《商用密码产品认证证书》
质保服务	提供原厂商五年技术支持和保修服务，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

4.10 终端杀毒软件

技术指标	参数要求
★基本要求	本项目要求提供≥1200 个办公 PC 终端授权许可，含 5 年功能、病毒特征库、补丁规则库更新服务。 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。
安全防护	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；
	支持对压缩文件扫描，并可设定最大的压缩层数为 6；提供压缩文件扫描功能，可以对超过固定大小文件不予扫描，以减少扫描时间；

	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；
	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；
	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；
web 防护	★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**（提供功能截图证明）**
客户端	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
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；
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）
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；
web 防护	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

产品资质	产品必须具有公安部颁发的《计算机信息系统安全专用产品销售许可证》网络版防病毒产品（一级品）证书；
质保服务	提供原厂五年质保服务，投标时提供服务承诺函，中标后提供原厂商针对本项目的授权函及质保承诺函；供货三天内提供原厂商针对湖州市中医院的授权记录查询结果。

4.11 服务器安全防护扩容

技术指标	参数要求
安装部署要求	★对现有服务器防护平台进行升级，可统一纳管现有服务器安全防护，扩容满足支持≧56 CPU 服务器防护授权；同时满足服务器增减配置虚拟补丁无需重启，支持防病毒、防火墙、虚拟补丁、入侵防御等防护功能
	无代理模式支持 VMware vSphere，华为 Fusion Compute， 新华三 CAS 等云平台；
	★无代理部署支持宿主机及虚拟机的防护**（提供功能截图证明）**
	系统控制台支持横向扩容，支持多节点集群化部署，保证系统高可用性。控制台离线，客户端仍可进行安全防护。控制台支持级联部署。
主机管理要求	支持与 VMware vCenter， 新华三 CAS、华为 FusionCompute 等云平台对接，同步虚拟机相关信息。
	支持 Linux、windows 客户端在同一页面进行集中管理
	应提供自动分组功能，可配置分组策略，策略包括不限于主机名、操作系统、IP 地址、安全策略、物理机/虚拟机/Docker 主机分类等。
主机防病毒功能	支持本地扫描和云扫描，支持实时扫描（文件落地即扫描）、预设扫描、手动扫描和快速扫描；如发现特殊情况 （如业务高峰期），可支持终止操作。
	支持扫描办公文件、压缩文件、Office 宏病毒、文本文件等各种类型文件，支持配置扫描类型、文件大小、压缩层级、数量等参数
	★支持通过行为监控的方式，如检测可疑活动和未经授权的更改，防止勒索软件感染，并提供针对勒索软件事件专有历史纪录和勒索软件

	统计的监控组件（**提供功能截图证明**）
	支持挖矿行为监控及告警
	提供多种病毒的处理措施：包括不限于清除、删除、拒绝访问、隔离、不处理等，并针对不同的恶意软件类型，定制处理措施。
	支持病毒库在线更新及离线式更新
	具备 web 信誉库，通过 Web 信誉支持阻止主机访问恶意站点，支持恶意站点自定义。
主机防火墙	支持网络访问控制功能，自定义防火墙策略，支持 IP、MAC 地址、端口，支持协议：TCP、 UDP、 ICMP、ICMPv6 、IGMP、IDP 等，支持 IPv4、IPv6、ARP、RARP 等
	防火墙策略应该支持独立执行，不影响操作系统的防火墙及 IP-Table 相关配置
	支持 NSX 安全标签，一旦检测到恶意威胁，可将 NSX 安全标记应用于受保护的 VM，NSX 安全标记可与 NSX Service Composer 一起使用，以自动执行某些任务，例如隔离受感染的 VM。
入侵防御及漏洞防护	支持网络入侵攻击的防护，包含支持防护 SQL 注入,Cookie 注入，命令注入,跨站脚本(XSS),跨站请求伪造(CSRF),WebShell 攻击防护等，
	内置入侵防御的规则库，支持关联 ATT&CK 框架的技术 ID，便于了解网络入侵技战术点。
	★支持 0Day 漏洞暴露后，快速定制入侵防御规则，包括不限于签名、特征码、XML 等方式，进行 0day 的快速防护，同时可支持配置优先级、检测或阻止模式、严重性等（**提供功能截图证明**）
	虚拟补丁规则不少于 6000 条，支持虚拟补丁规则自定义，服务器增减配置虚拟补丁无需重启；
系统管理	支持不同租户分权分域，包括计算机、终端、事件、安全策略、管理、日志文件相互隔离
	支持虚拟化环境的 VMotion，Storage VMotion 以及 HA，能够自动感知

	和保护虚拟环境的变更和迁移。
	管理员可以通过控制台获取 debug 日志，包括系统信息，运行状态，驱动日志等状态信息导出
	对系统账号安全进行管理，包括不限于登录失败数、并发会话数、密码过期时长、密码复杂度、信任证书、密钥对等。
产品要求	★产品必须和 VMware Operation Manager 集成**（提供证明文件）**
质保服务	中标后提供原厂商针对本项目的授权函以及五年原厂质保承诺函；供货三天内提供原厂商针对湖州市中医院的授权记录查询结果。

4.12 数据加密

技术指标	参数要求
★基本要求	软硬一体化设备，≥2U，≥4 千兆电口，≥4 千兆光口，≥2 万兆光口，≥1 个扩展槽位，≥1 个 CON 口，≥2 个 USB 口，≥2 个管理口，≥4T+128G SSD 硬盘，≥内存 32G，双电源。
	配置≥10 个数据库授权数许可
	每台加密设备内置一块加密卡，提供加密卡商用密码产品认证资质证书。
部署方式	★旁路部署，路由可达即可，支持 HA 双机热备模式，防止主机故障、网络故障、程序故障引起的业务异常。同时容灾手段能快速启用、自动切换，且切换期间能保证数据一致性，业务不受损失。**（提供配置截图证明）**
数据库兼容性	应支持 Oracle、MySQL、PostgreSQL、GaussDB、KingbaseES、KADB、达梦。
加密算法兼容性	支持 AES 国际密码算法，SM4 国家商用密码高强标准加密算法，两种算法均采用 GCM 模式，同时也支持 SM2、SM3 非对称算法。
存储加密能力	实现对数据库中的敏感数据加密存储，防止明文存储引起的数据泄密
	支持所有数据库字段类型，支持随机数加密技术，相同的明文数据加密后密文数据不同。
	以表为单位进行数据加密，加密表的数据在数据库中以密文格式存储。

	支持配置选择一表一密钥，一表一算法的加密策略
	支持所有数据库字段类型，支持随机数加密技术，相同的明文数据加密后密文数据不同。
	提供基于 WEB 方式的数据加解密配置，支持数据库中数据加密存储进行完整性校验，支持加密操作回滚的保障机制。
数据加解密权限控制	提供独立于数据库管理系统自身的权限控制体系，所有账户（包括数据库管理系统特权账户）访问密文数据前均应通过数据库加密产品管理员的授权，防止数据库用户的权限提升引起的数据泄密；
	支持对数据库用户授权，实现授权用户能够访问明文，非授权用户只能够访问密文。支持通过安全策略限制 DBA、开发人员、第三方外包服务人员等高权限用户访问敏感数据。
	支持基于应用系统指纹、应用系统用户的访问权限控制，仅允许合法的应用或用户对密文进行访问。防止授权数据库用户口令泄露后，绕开业务系统，直接访问密文数据。
	支持基于数据库账号，select、insert、update、delete 操作类型的访问拦截阻断能力。
	★支持对加密数据的访问可基于表、列、客户端工具、来源 IP、时间范围等组合条件的授权控制能力。**（提供配置截图证明）**
业务透明性	支持 SQL、PL/SQL、JDBC、ODBC 的透明性，即数据库加密和访问控制功能对数据库客户端、业务系统完全透明，不需要对现有业务系统进行任何改造。
	支持对 Oracle SQL Develop、Navicat 等数据库运维工具的透明性，不影响管理员使用数据库提供的工具实现备份恢复和数据库维护。
密钥管理	密钥管理提供密钥全生命周期的管理，确保密钥以安全的方式完成该系列操作，防止密钥被泄露。密钥管理采用了三级密钥保护机制，即密钥加密密钥 KEK、主密钥 AMK 和数据加密密钥 DEK。
	支持密钥的规格，对称密钥 8000 个。
	支持数据加密密钥与数据密文分离管理，密钥储存在数据库之外，独

	立管理，提供对密钥的备份恢复机制。
加密卡状态监控	支持实时监控加密插件网络连接状态，统计在线时长状态。
	采用 Kerberos 协议来实现插件与加密系统之间的身份互认证，保障系统模块间的通信安全。支持实时监测加密卡工作状态，发生异常时及时告警。
自身安全性	支持系统加密，解密，授权操作，管理账号登入登出等审计日志信息。
	实现系统管理员、安全管理员和审计管理员的三权分立。其中安全管理员通过 WEB 管理配置日常的加密数据配置、数据库用户的密文权限控制、密钥管理等安全维护和管理操作。
可靠性	支持使用离线密文恢复工具将密文恢复成明文，防止不可预测原因导致系统宕机后数据库数据不可解密。
功能测试	合同签订后七天内提供测试设备对产品功能和性能测试，若无法在规定时间内提供测试设备或测试结果与招标内容不符，影响医院互联互通等级评定和应用软件上线，取消中标资格，中标人承担所有责任。
质保服务	提供原厂五年技术支持和原厂保修服务，为了货物是原厂家最新生产合法渠道货物，投标时提供服务承诺函，中标后须提供原厂盖章授权函。

5.服务

5.1 光纤专线租赁

技术指标	参数要求
光纤专线	2 个运营商；提供 2 年专线租赁服务；支持提供负载均衡
	单条配置：100M 互联网光纤专线，上下行速率 100M，含 IP 地址 4 个。光缆采用室外敷设型单模光纤，支持 1310nm、1490nm 和 1550nm 波长

5.2 等保测评服务

技术指标	服务要求
等级保护测评	根据国家信息安全等级保护相关标准，投标人对湖州市中医院的信息系统完成等级保护测评工作。要求对相关信息系统进行摸底、分析和

	梳理，提出测评方案，逐一对信息系统进行安全等级保护测评。信息安全等级保护测评的内容包括但不限于以下内容： 1、安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个方面的安全测评。 2、安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全控制测评。 完成测评工作后，投标人提出整改意见并配合湖州市中医院进行整改，最后出具符合公安机关要求的信息系统安全保护等级测评报告，协助湖州市中医院完成信息安全等级保护测评结果备案工作。
	提供三年等保测评服务（含关键基础设施及面向患者服务系统 2 个模块）

5.3 安全服务

技术指标		服务要求
提供蜜罐主动防御系统	蜜罐主动防御系统	★本次项目服务期内，服务提供商需提供统一安全运营平台，含蜜罐主动防御等功能；蜜罐可全网部署，要求系统功能授权无限，支持 7*24 小时安全托管服务。提供服务工具品牌“蜜罐部署和管理系统”软著证明。
	无侵入式全网病毒监测服务	投标人提供服务工具应能通过 trunk 方式将诱捕能力发布到全内网各 vlan 网段，实现在全内网中部署大量高交互病毒监测诱饵，无侵入式部署不影响用户业务运行，同时极大提高黑客攻击病毒监测诱饵的概率。 探针支持 trunk 接入客户网络，可通过 trunk 方式将诱捕能力发布到全内网各 vlan 网段，实现在全内网中部署大量高交互病毒监测诱饵，同时支持软件和硬件版本的流量牵引探针。 支持高交互病毒监测诱饵，并可同时启用：“samba、ftp、ssh、rdp、telnet、mssql、mysql、mongoDB、postgresql、tomcat、weblogic、jenkins、redis、hadoop、memcache、solr、activeMQ、struts2、wordpress、nginx、jboss、joomla、smtp”等，以上服务须为真实应

		用服务，能够正常交互，欺骗攻击者，提供产品功能界面截图。
	蜜罐仿真、攻击吸引	服务工具支持通过反向代理的方式，接入用户自身搭建的应用系统，从而实现完全仿真真实业务系统，生成完全仿真蜜罐； 支持智能克隆仿真功能，可以模拟真实业务系统进行前后端的数据交互，包括但不限于以下动态交互类型：“搜索查询、登陆验证、账号注册”等，要求拟态仿真蜜罐系统为纯静态系统； 可利用仿真邮件服务进行钓鱼邮件模拟演练，可在平台中统计打开钓鱼邮件的账号、点击连接的账号、提交敏感数据的账号等数据，统计维度包括账号名称、访问 ip、提交敏感数据内容、访问时间等； 可将访问真实业务系统的流量引流到仿真蜜罐，使攻击无法命中真实业务系统，真正有效消耗攻击资源，并直接保护真实资产。 可在 web 管理界面上自定义生成 github 互联网诱饵，可自定义添加蜜罐 IP 地址、github 项目说明、项目提交人信息、邮箱信息等内容，以便黑客可以从互联网上搜索到自定义信息内容，从而转向攻击蜜罐。
	威胁感知	服务工具参考 MITRE ATT&CK，采用多种取证技术手段，还原黑客攻击入侵蜜罐的过程，形成黑客攻击链，攻击链检测包含：“针对蜜罐的探测扫描、渗透攻击、攻陷蜜罐、在蜜罐上安装后门远控程序、利用蜜罐进行跳板攻击”等入侵过程。 支持还原攻击者的网络数据包，包括 icmp、tcp、udp 等协议的攻击包，可查看攻击者发起的具体攻击请求数据，比如 SQL 注入、XSS 攻击的 http 请求头部信息。 支持时间轴告警分析：可根据基于告警时间/攻击类型/地理位置等对攻击行为进行筛查，其中攻击类型可分类为：“可疑访问、尝试登陆、端口扫描、攻击尝试、强力攻击、异常进程、暴力破解、登陆成功、

		命令执行、可疑文件、恶意文件、跳板攻击”等类型，对于攻击事件分析起关键作用。
	攻击溯源	服务工具支持记录攻击者的“黑客社交画像”信息，包括社交账号、手机号、昵称、用户 ID、头像等信息，支持多种黑客社交画像，至少包括：百度、网易、当当等 6 种不同类型的社交账号。 可基于显卡成像参数、CPU 等硬件信息，计算攻击者唯一身份指纹,就算攻击者换了 IP 也可以通过该指纹确定攻击者。 设备指纹溯源至少包括：操作系统信息、浏览器指纹、浏览器类型、mac 地址、设备厂商、屏幕分辨率、浏览器历史记录、计算机名。
	攻击反制	可警告攻击者，比如灌输国家网络安全法、告知已获得相关溯源信息，发挥蜜罐威慑作用，使攻击者放弃后续的攻击行为；可灵活指定对某个攻击源 IP 地址发起威慑反制； 可使攻击者在连接数据库类模拟应用时，识别攻击者身份信息。包括但不限于:计算机名称、使用浏览器版本、浏览器历史记录、浏览器上记录的访问账号等； 可使攻击者下载某个文件时，替换成木马文件，诱骗攻击者下载安装； 可在 web 管理界面上灵活指定对某个攻击源 IP 地址发起木马远控反制； 支持一键扫描攻击源 IP 地址，探测攻击者主机的开放端口信息、弱口令、漏洞等。
	交付物	按季度提供包含但不限于《安全托管服务报告》
资产梳理服务	安全服务工具	★本次项目服务期内，服务提供商需提供统一安全运营平台，含内外网资产管理等功能；通过本地化部署，结合人工服务，实现主机及互联网资产闭环管理。**提供服务工具品牌“资产安全管理系统软件”软著证明。**
	主机资产梳理	对湖州市中医院主机资产进行自动化梳理服务，包括“操作系统版本、端口开放情况、协议情况、服务版本、应用程序版本、存活 IP、设备厂商、中间件、服务版本”等资产指纹特征。**提供服务工具品牌“资**

		产探测扫描软件”软著证明。
	网站资产梳理	服务工具支持自动识别网站资产信息，识别到的网站资产包括如下详细属性信息：“中间件信息、web 框架信息、CMS&OA、程序语言”等指纹信息； 能够抓取识别网站后台、ICP 备案编号、网站标题、网站返回码等；
	资产趋势分析	可按最近一周、最近一个月、最近一个季度分析新增或下线的主机资产、网站资产，掌握资产变化趋势。
	二级域名扫描	★投标人自带服务工具，支持二级域名扫描功能，输入一级域名进行一键扫描，通过搜索互联网数据，自动获取到该域名的二级域名、网站标题、解析 IP 地址。**（提供服务工具功能界面截图）**
	网站资产相关度分析	通过爬取企业单位已知的网站页面，分析网页中是否包含企业单位相关的网站链接，从而发现未知网站；可配置“网段、域名”等命中规则，自动判断是否属于企业单位的网址。
	下线资产监测服务	可及时发现未存活 IP、未存活端口以及访问延迟的网站，可查看未存活 IP 列表、未存活端口列表，可对未存活的资产进行移除操作。
	IP 反查域名监测	输入 IP 或者网段，通过搜索互联网数据，自动获取到 IP 对应的域名、url 链接、网站标题、返回状态码。
	资产认领	★资产责任人可认领 IP、网站资产，可显示资产认领状态，未认领的资产无法进行编辑。**（提供服务工具功能界面截图）**
	服务期限	服务期 5 年，每年不少于 4 次，每次提交《资产梳理报告》
漏洞扫描服务	安全服务工具	★本次项目服务期内，服务提供商需提供统一安全运营平台，含漏洞管理、基线及配置核查等功能；通过本地化部署，结合人工服务，实现漏洞及安全基线的闭环管理。**提供服务工具品牌“系统漏洞扫描软件”软著证明；**
	完善的漏洞库	服务工具的漏洞库漏洞信息大于 220000+条，与 CVE、CNNVD 等主流标准兼容，提供详细的漏洞描述和对应的解决方案描述。支持通过多种维度对漏洞进行检索，包括：CVE ID、CNNVD ID、漏洞名称、漏洞风险等级等维度。可基于资产的版本信息，全面、快速进行漏洞版本比

		对，兼容 CVE 、CNNVD 等漏洞库。
	可入侵漏洞监测	集成 2700+POC 对内网资产进行自动漏洞验证与渗透，发现可导致数据泄露、系统入侵 、越权等可入侵漏洞，先于黑客发现此类漏洞，主动发现。
	弱口令监测	支持各类应用资产的弱口令扫描，可扫描的应用包括“SSH、SMB、RDP、Telnet、Ftp、pop3、VNC、SNMP、Vmauthd、Postgres、MsSQL、MySQL、Oracle”支持自定义字典，支持设置弱口令扫描白名单，可以指定某个 ip 某个应用不执行弱口令扫描。
	漏洞管理服务	支持漏洞跟踪管理，能够自动对漏洞状态进行处置，自动识别“新增、已修复、未修复”的漏洞，同时支持人工方式进行漏洞状态处置，以及编写漏洞备注。**（提供服务工具功能界面截图）**
	服务期限	服务期 5 年，包含每年不少于 4 次，每次提交《主机漏洞扫描报告》
基线核查服务	安全服务工具	★本次项目服务期内，服务提供商需提供统一安全运营平台，含基线核查等功能；可本地化部署，结合人工服务，提供安全基线核查服务。**提供服务工具品牌“基线配置核查软件”软著。**
	配置核查能力	支持 20 种以上常见设备和应用的配置检查，包括操作系统、应用中间件、数据库。
	配置核查支持类型	能够自动化实现对包括操作系统、应用中间件、数据库等在内的 20 种以上常见设备和应用的配置检查。包括但不限于操作系统，支持 Windows 2003、2008、2012、2016、2019、7、8、10、11；支持 linux（Centos、Redhat、suse 等）；应用服务，支持 Linux、Windows 下的 Apache、Weblogic、TOMCAT、Websphere、Nginx，以及 IIS 6、7、8；数据库，支持 Linux、Windows 下 Oracle8i、9i、10、11g、Mysql。
	服务期限	服务期 5 年，每年不少于 4 次，每次提交《基线核查安全评估报告》
安全加固协助服务	服务内容	安全管理视图：结合安全感知日志和威胁情报进行深度分析，研判网络中存在的威胁和攻击行为，明确对业务的影响和危害 1）外部威胁评估：综合分析数据，发现攻击威胁、持续性攻击和高级黑客等安全事件；

		2）精准入侵检查：webshell 检查、恶意文件查杀、web 日志分析、系统状态分析，发现已经被入侵或感染的主机； 3）位置威胁发现：及时对未公开威胁进行评估、针对高危威胁风险进行通告。未知威胁快速规避措施：通过安全策略的运营（例：自定义策略临时防护）临时应对、规避最新爆发的风险。安全功能迭代升级（例：更新规则库、升级安全组件）将防护能力整合到安全设备。 安全加固整改：根据事件发生的根因、影响范围，针对性给出安全加固建议，并针对安全问题负责整改工作，彻底解决问题。
	服务期限	服务期 5 年，每年不少于 4 次，每次提交《安全加固协助报告》
安全预警通告服务	服务内容	投标人应实时跟踪网络安全热点事件和漏洞，并始终站在湖州市中医院的视角实时监测、周期性度量行业风险隐患，协助采购方掌握自有 IT 资产的安全漏洞状态，及时跟踪修补 IT 资产漏洞，提高脆弱性管理能力。致力于第一时间实事求是地发送对湖州市中医院真正构成威胁的安全风险通告和行之有效的解决方案。 1.安全通告对象范围如下： （1） 常见厂商的软、硬件网络设备：思科、华为等路由、交换设备； （2）常见厂商的操作系统：微软、惠普、苹果、IBM 等操作系统； （3） 常见厂商的数据库软件：微软 MSSQL、甲骨文 Oracle 等； （4） 常见厂商的 Web 软件：BEA Weblogic、IBM Websphere、Apache、JBoss、Tomcat 等。 2.安全通告提供最新安全漏洞、威胁（0day、系统漏洞、网络攻击）的解决办法、安全问题描述和相应的处理意见，及时提供符合湖州市中医院实际需求的安全信息。
	服务期限	服务期 5 年，服务期内以电子邮件的方式每月发送“安全通告”或不定期发送“紧急安全通告”到采购方指定的电子邮箱，每半年提交《网络与信息安全通告报告》
安全监测	安全服务工具	本次项目服务期内，服务提供商需提供统一安全运营平台，含互联网攻击面监测、主机威胁监、主机漏洞攻击屏蔽、web 漏洞监测、敏感信

处置服务		息监测、敏感内容审查等功能；可本地化部署，结合人工服务，实现互联网及主机安全监测及处置。**提供服务工具品牌“网络安全管控平台”软著证明**
	主动威胁监测服务	在用户的服务器、业务系统上安装安全监控软件，主动监测恶意文件（webshell、病毒木马）、挖矿病毒等，发现可疑的入侵事件,能够将监测到的风险信息在服务工具上实时展示。
	互联网攻击面监测服务	通过扫描，探测互联网上潜在的未知资产，不必要开放的资产，并自动验证互联网资产是否存在可利用漏洞、弱口令，提供暴露面收敛等相关整改建议，监测数据通过本地平台统一展现和管理。包括但不限于： （1）互联网资产详情：从基本信息到应用组件、应用指纹、开放端口等 （2）风险暴露面排查：远程访问端口、VPN 入口、后台入口、弱口令、可入侵漏洞等 （3）生成暴露面监测报告：提供暴露面收敛整改建议，定期更新和审核。
	恶意文件检测服务	真对 Webshell 网马、病毒木马、攻击脚本、宏病毒文件等进行检测
	挖矿病毒检测服务	支持检测挖矿病毒，识别挖矿程序文件、挖矿进程名称、进程号、运行参数、CPU 运行异常状态、网络连接状态、病毒程序打开的文件
	网站篡改检测服务	可检测网站文件的篡改行为，包括：“创建、写入、修改权限、重命名、删除”等篡改行为。
	漏洞攻击屏蔽服务	服务商提供专业资产安全运营服务平台工具帮助客户屏蔽各类漏洞扫描攻击。精准检测恶意攻击源、扫描源，并可基于告警风险值、或者定向源进行屏蔽，使漏洞扫描器、恶意攻击源无法扫描到主机存在的漏洞，包括可利用漏洞、版本漏洞。
	失陷主机微隔离服	不需要联动第三方设备、不需要在主机上安装 agent 脚本，就能对失陷主机进行网络隔离，隔离后失陷主机无法访问同网段以及其它网段

	务	IP，防止失陷主机继续对东西向主机进行病毒传播、横向攻击等行为。
	web 漏洞监测	支持网站漏洞评估能力，提供多种 Web 应用漏洞的安全检测，如“SQL 注入、跨站脚本、文件包含、CSRF、目录遍历”等网站脆弱性漏洞。
	网站应用监测	支持监测网站的可用性、域名劫持等事件
	黑链/篡改事件监测	高频率监测站点是否存在被黑客植入黑链、篡改的事件，系统需要保留植入黑链、篡改的快照页面，监测频率低至 5 分钟/次
	全站敏感词事件监测	用户可对不同网站自定义不同的敏感词库，并对企业、单位的网站进行全站页面爬取，发现敏感词字眼。
	敏感文件事件泄露监测	可监测发布到网上的 pdf、word、excel 文件中是否包含“身份证号、邮箱、手机号码、用户名/密码”等敏感信息，可在系统上查看泄露的信息以及敏感文件下载链接。
	敏感内容审查服务	可上传文件(pdf、word、excel)、或者粘贴内容进行敏感词审查，内置敏感词库 10 万+，支持人工再确认审查结果。
	安全事件处置	对安全事件进行处置，清除恶意文件、快速恢复业务； （1）策略管理：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新。策略冲突、策略有效性调优服务。 （2）事件分析与处置：对用户上报的安全事件进行及时响应。实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助客户快速恢复业务，消除或减轻影响。
事	事件溯源分析	深入分析安全事件的成因，发现存在的薄弱点，溯源攻击路径； （1）入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。 （2）入侵威胁清除：排查攻击路径，恶意文件清除。

		（3）入侵原因分析：还原攻击路径，分析入侵事件原因。
	服务期限	服务期5年，包含服务期内新增加的安全系统，提交《安全监测处置报告》
护网/重大活动保障服务	服务内容	人员驻场：依据医院活动要求提供技术支持及驻场时间支持，如需包含法定节假日。 设备租借：在相关活动中所需的安全设备服务商负责提供免费租借，设备范围限于相关安全系统。 活动安排：服务供应商应负责相关活动的统筹安排，包含规划、调整、测试、校验活动成果，并负责处理遗留问题。
	服务期限	服务期5年，每年不少于60人/天驻场重保，提交《重保支持报告》
攻防演练服务	服务内容	1.在服务期内根据湖州市中医院信息系统的实际情况，制定符合需求的攻防演练方案，并组织实施攻防演练，发现系统漏洞，并提供修复建议，汇总攻防演练过程中发现的所有漏洞，形成详细的报告，并提出相应的修复建议。 2.应搭建应急演练模拟环境、提供攻防演练方案及演练脚本。 3.出现安全事件时，必须及时进行响应，技术人员必须30分钟内到达现场，对入侵事件进行分析，查找原因；抑制入侵事件的进一步发展，将事故的损害降低到最小化；排除安全隐患，消除安全威胁，协助恢复系统正常运作；
	服务期限	服务期5年，每年1次，提交《攻防演练报告》《信息系统应急演练报告》《应急响应报告》
信息安全风险评估服务	评估服务要求	对湖州市中医院重要信息系统进行安全风险评估，根据业务系统现状，结合医疗行业未来发展方向，依据国家政策法规、技术标准要求以及安全技术攻防经验，识别现有技术措施的不足之处以及可能存在的风险点，并提出针对性安全建设规划。评估内容包括网络层、主机层、应用层、代码层。 1.网络层安全评估 网络层安全评估主要是对信息系统的部署安全性进行评估，评估内容

		包括但不限于：架构可靠性、边界安全、信息系统供应链安全等。 2.系统层安全评估 系统层安全评估主要是对信息系统中承载业务的应用主机服务器的操作系统进行安全性评估，评估内容包括但不限于：系统架构、身份认证、访问控制、系统漏洞、安全配置等。 3.应用层安全评估 应用层安全评估主要是对信息系统的接口、组件、数据库、WEB 应用进行安全性评估，评估内容包括但不限于：1）接口、组件、数据库的弱口令漏洞、数据字典漏洞、用户权限漏洞、进程权限漏洞等。2）Web 应用的 SQL 注入、跨站脚本（XSS）、失效的身份认证和会话管理、不安全的直接对象引用、跨站请求伪造（CSRF）、安全配置错误、不安全的加密存储、没有限制 URL 访问、传输层保护不足、未验证的重定向和转发等。3）涉及应用层业务逻辑安全方面的内容，包括但不限于：非授权访问、越权访问、命令执行、验证码暴力破解等。
	服务期限	服务期 5 年，每年 2 次，提交《风险评估报告》
密评测评服务		根据国家标准文件《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）对商用密码应用安全的检测要求，不同安全保护等级的信息系统中密码技术应用要求，本密评改造等保定级均为三级， 提供密评测评服务 1 次。

5.4 运维服务

技术指标		服务要求
基础运维服务	服务器运维服务	1.定期对服务器运行状态进行检查和分析，完成巡检报告；对服务器故障提供现场、远程支持，修复故障，提供故障报告； 2.日常维护：硬件设备巡检（设备电源状态，风扇状态；备机设备可用性；服务器 CPU 使用率，内存使用率，连通性状况）； 3.服务器日志检查，日志清理；故障处理：硬件故障排查、分析；故障排除、恢复；设备硬件报修及跟踪处理；提供医院现有服务器安装部署、服务器集群等架构和资源使用现状情况。

	存储运维服务	1.对磁盘阵列、光纤交换机等设备定期进行运行状态检查和分析，完成巡检报告，提供现场和远程支持，提供故障报告； 2.日常维护：设备巡检（设备运行状态、硬盘状态、热备盘接管状态、电源模块、存储连通状态）； 3.故障处理：故障排查、分析；故障排除、恢复；确认排除、恢复的结果；设备硬件报修及跟踪处理； 4.数据迁移：存储规划调整、数据迁移。
	虚拟化运维服务	1.对超融合、虚拟化平台软件运行状态进行检查和分析，完成巡检报告；对平台软件故障提供现场和远程支持；根据业务发展趋势，评估当前性能并给出优化建议； 2.日常运维：虚拟机配置、资源调整； 3.系统巡检：平台软件运行状态进行检查和分析（包括机柜图、备份、集群的虚拟机数量、主机内存使用率、存储使用率、虚拟机前后端性能），根据系统运行情况给出相关建议； 4.故障处理：虚拟机系统故障和问题进行分析和排除；虚拟机网络故障和问题进行分析和排除；系统底层问题排查处理； 5.升级：如有安全需要，做虚拟机版本升级； 6.数据迁移：基于虚拟系统数据迁移；虚拟资源调整涉及的数据迁移。
	虚拟化网络安全服务	1.安全策略部署：部署实施虚拟化网络安全策略服务，控制和保护要数据中心内的东西向流量，防止勒索病毒、木马及黑客后门程序横向爆发； 2.主机安全升级：如有数据中心虚拟化平台升级需要或系统安全需要，根据医院要求做相应的硬件固件版本更新，协助医院对数据中心主机系统完成相应的操作系统版本更新。
	数据容灾备份服务	1.备份策略规划：为医院核心业务系统制订数据容灾备份管理策略，部署实施系统数据备份工作； 2.备份策略运维监控：定期对数据备份情况进行检查确认，确保所有备份任务正常运行，对发现未正常完成的任务应及时排查解决，定期

		确认备份完整可用； 3.服务范围：数据库服务范围主要涉及：EMR 异地容灾数据库、 HIS 异地容灾数据库、 PACS 异地容灾数据库、 LIS 异地容灾数据库、CDR 异地容灾数据库、异地容灾数据库以及相应备份数据；虚拟化系统服务范围主要涉及：数据恢复演练：根据医院现有的备份系统，每季度至少抽取 2 台虚拟机进行恢复测试验证。
	安全设备巡检服务	1、安全设备运巡检：对指定安全设备进行安全巡查，包括物理层面、策略层面、维护层面以及安全操作层面； 2、安全设备策略加固：包括网络架构安全、安全设备策略、可用性检查、数据流向分析等。
其他运维要求	★人员配置	1.投标人需要为招标人提供本地化服务和技术支持，并至少提供不少 4 人的运维团队，1 名项目经理、1 名主机存储工程师、1 名网络安全工程师、1 名驻场工程师 2.驻场工程师要求大专以上学历，精通网络技术，具有三年以上从业经验，精通 CISCO、华为、VMware、深信服等设备的配置和系统维护。熟悉病毒防范，熟悉防火墙、入侵检测等网络安全系统设备的配置和维护，熟悉主流网络操作系统、服务器的运维。熟悉 VLAN，STP，OSPF，BGP，MPLS VPN，SSL VPN 等协议及技术。了解网络监控工具，监控网络设备的各项性能，能发现潜在问题。熟悉 Linux 系统的基本操作，熟悉 SQL Server 语句。 3.驻场工程师主要负责信息化设备的日常维护，需要配合管理机房内所有相关设备，保障其安全、稳定运行。做好机房设备、人员进出机房的登记管理，协助完成机房的值班执勤，并做好其他系统的日常维护。需组织协调并有效、快速的解决本次招标维护保修范围的各类故障，同时要尽量保证人员的稳定。如在维保期间，招标人认为投标人工程师能力有限，可要求投标人更换工程师，投标人需按招标人要求执行。 **4.提供人员简介、相关资格证书及在本公司的近一年社保证明材料，**

		并加盖投标人公章。
	服务期限	提供5年机房运维服务（机房所有硬件设备的维护、数据维护以及网络安全维护，含利旧第三方软硬件），1人现场驻点服务3年

5.5 设备部署及系统集成服务

技术指标	服务要求
设备安装部署服务	新购及利旧设备的集成，将各个子系统连接成整体运行平台，包括整个项目实施、安装、调试、虚拟化平台搭建、数据库安装、网络配置等，含第三方软件系统厂家技术服务费。
系统集成服务	1、提供双活机房（超融合和网络）方案设计、医院整体内外网络方案规划设计、网络安全方案规划、核心业务系统数据库及存储双活方案设计、云桌面超融合扩容方案设计、新院区容灾方案设计、应用虚拟化集群、容灾机房虚拟化集群、灾备机房利旧改造方案设计及实施工作； 2、对原有的虚拟桌面瘦客户终端可充分利旧、无缝对接，利旧使用原有安全设备，对原有安全设备进行策略加固和部署模式调整，使其安全防护能力充分利用起来；同时对利旧服务器虚拟化及操作系统软件版本升级加固； 3、将各个子系统连接成整体运行平台，包括整个项目实施、安装、调试、虚拟化平台搭建，数据库集群搭建等，含第三方软件系统厂家技术服务费； 4、中标方负责协调现有应用软件（HIS、EMR、LIS、PACS等）的迁移工作，包括与应用软件厂商的交流和方案确定。所产生的所有费用均需中标方承担。硬件平台的搬迁由中标方负责，所涉及原有硬件设备的搬迁所产生的第三方费用均由中标方承担。 5、为保障数据无丢失以及停机时间为零。此次项目的系统迁移、双活数据中心、容灾需设备原厂工程师现场实施及保障。 保障新老存储在原双活系统中的整合，容灾系统的实施与持续数据保护系统的恢复测试，数据中心交换机的更新，保证数据无丢失以及应用零停机，保障

	在任意时刻无论是服务器还是存储出现故障不会影响核心业务系统的使用。 6、投标时需根据用户现场实际方案出具调研报告及详细的数据迁移方案（包括现有设备型号、配置架构以及如何与新设备如何平滑过渡的实施方案）。 7、投标人在系统升级割接过程中需确保过程顺利进行，系统割接过程须具有可回溯性，确保应用割接失败的回退。 8、项目实施后必须满足通过信息系统安全等级保护三级测评要求。
★测试和备件	为了保证设备性能和可靠性，中标后5个工作日内，中标人需提供招标设备和系统用于现场功能和性能测试，由第三方出具测试报告，所涉及的测试费用由中标承担，如测试结果与投标参数不符，中标人承担一切责任。
	在保修期内发生的软硬件故障全部提供免费服务。采购方有权要求提供与本次项目服务器和存储相同档次设备，放在采购方做备件，当在线运行设备故障宕机时第一时间更换。当有部件故障（包括CPU、内存、电源、硬盘等配件），必须以最快的速度无条件进行更换。
	投标方必须确保备件符合系统技术要求，在接到报修通知后，在可能需要使用相关备件的紧急情况下，其他备用设备在2小时内必须到达，如果发现投标方使用二手部件或兼容设备进行维修，将视为违约，并有权对投标响应方进行处罚或终止保修合同的执行。**（提供服务承诺函）**
人员配置	本项目实施团队成员不得少于6人，项目实施经验不少于三年，至少包括1名OCM工程师、1名VCP工程师、1名网络工程师、1名主机存储工程师，项目经理要求具有信息系统项目管理师（软件证书）工程师担任，投标时项目组人员一经确认未经采购人允许不可更换，并承诺以上工程师在质保服务期内可随时响应并到现场解决采购方的实际技术问题。**（提供以上工程师证书复印件及投标公司近一年社保证明材料，并加盖投标人公章）**

5.6 搬迁服务

技术指标		服务要求
系统及数据搬迁迁移服务	迁移范围	医院原有的 Vmware 虚拟化、超融合集群；阿里云服务器集群；医院网络、安全设备；外网、专网链路等
	主机系统迁移	原机房虚拟化服务器迁移及搬迁 1.迁移原虚拟化服务器到改造后的超融合平台； 2.提供详细的系统迁移方案及相应的应急预案； 3.迁移过程不允许业务停顿，因迁移工作导致的业务停顿所带来的损失由中标人全部承担。
		原机房云服务器迁移 1.迁移原云服务器到改造后的超融合平台； 2.提供详细的系统迁移方案及相应的应急预案； 3.迁移过程不允许业务停顿，因迁移工作导致的业务停顿所带来的损失由中标人全部承担
		容灾搬迁改造 1.配合医院原机房主机、存储相关软硬件的搬迁、集成实施等工作； 2.完成医院主机系统异地到搬迁后的灾备机房的系统容灾备份、恢复、演练等服务。
	数据库迁移	1.新采购存储安装、部署实施；存储双活故障切换、容灾切换演练等工作； 2.实现新机房核心 ORACLE 数据库及容灾数据库部署实施；完成医院原 HALO6 应用系统、oracle 数据库云主机迁移涉及的 Oracle 软件安装； 3.完成原HIS、EMR等核心数据库数据迁移以及涉及到的Oracle 单机、RAC 等安装部署服务； 4.完成新机房 HIS、EMR 等核心数据库备份、容灾涉及的 Oracle DG 等安装部署服务； 5.提供详细的系统数据迁移方案及相应的应急预案；迁移过程不允许

		业务停顿，因迁移工作导致的业务停顿所带来的损失由中标人全部承担。
		原数据库服务器、核心存储利旧改造 1.配合完成医院原数据库服务器、存储改造升级
		2.医院整体搬迁过程在非业务高峰时间段进行，提供必要的技术支持、现场保障以及可能涉及到的实施服务，做好异常情况应急保障工作，保障医院整体搬迁过程中业务正常和业务安全。
	网络系统割接	完成医院外网网络割接
	迁移对接服务	中标人负责协调现有应用软件（包括HIS、EMR、LIS、PACS等所有业务系统）的迁移工作，包括与应用软件厂商交流和方案确定以及原厂人员现场支持协调，无条件配合整个医院的搬迁工作，和第三方紧密配合
机房搬迁服务	搬迁范围及目标	1.需要对医院原有机房设备搬迁到新机房内。整体搬迁包括搬迁前的调研、方案制定和评审、关键系统连续性保障方案及相应硬件设备免费提供、搬迁过程中的设备拆卸、下架、打包、保护、搬迁后的备上架、安装、验证、恢复各业务系统、保证搬迁设备的正常运行等。 2.本次搬迁必须满足专业系统正常运行条件，在整个搬迁过程中确保专业系统数据和设备不损坏、不崩溃，保障在全部搬迁后系统可以最短时间内恢复运行。具体设备清单以调研核对后的清单为准，核准涉及的多余费用由中标人承担
	机房搬迁规划	1.机房搬迁前勘察，在开始搬迁之前，需要完成机房搬迁所需要的调研、评估、风险分析，对迁移方案进行规划，制订详细的迁移实施步骤和应急预案，并进行测试； 2.搬迁方案的设计，根据评估结果，制定详细的搬迁方案，包括搬迁目标及保障措施、搬迁的时间、流程、人员、设备、数据备份和恢复、搬迁包装设计、运输车辆及保障措施等，分析各种风险因素制定相应应急方案应急预案和安全措施，并规划搬迁的关键设备在搬迁过程中

		的搬迁应急备件。
	设备搬迁服务	（一）搬迁准备阶段 1.对医院原机房内设施进项设备梳理、系统调研、标签登记、系统关联分析、风险分析等工作，并设计分次搬迁方案，保证现有机房内系统平滑无缝过渡； 2.根据招标人提供的新机房功能分布架构，规划、设计各设备在新机房内的位置分布，提供新机房系统及网络架构图； 3.规划、设计机房搬迁时各系统和各相关设备的下电、拆除、包装、运输、安装、上架、上电、连接和调试等详细搬迁步骤，并提供详细实施文档。重要的搬迁步骤要求有完善的回退应急方案，一旦某个环节失败，能够根据应急方案及时恢复，确保系统不受影响； 4.搬运前需要对设备进行健康检查，并由中标人和招标人共同确认设备运行状况，对于搬迁前已出现的故障由招标人负责协调维修； 5.协助用户做好搬迁前各系统关键数据的备份工作，包括各操作系统配置、各应用系统配置、各类数据的备份； 6.做好搬迁前的线缆、需拆卸硬件的标签工作以及设备清单的清点工作，所有设备清单需经投标人与招标人共同确认； 7.为本次搬迁设备提供备品备件应急服务。 （二）搬迁阶段 1.搬迁阶段指自系统和设备开始下电，至设备搬迁至新机房，全部设备安装调试完毕并通过招标人验收为止。 2.在招标人规定的各时间窗内完成机房的搬迁工作，包括所有系统和设备及其附件的下电、拆除、包装、运输、安装、上电、调试等机房搬迁全过程。搬迁过程中，要对搬迁设备进行妥善的包装和安全的运输，搬迁过程中任何损坏的设备，均由中标人负责更新或更换备件； 3.确保设备搬迁完成后，各类硬件及系统的完整性、可用性和一致性。机房搬迁期间由于运输原因出现故障或不可预测的意外情况，中标人按照事先的应急预案在招标人规定的时间窗内恢复系统正常运行，并

		尽快完成故障件修复。 4.搬迁期间，中标人要协助招标人进行应用系统恢复测试工作，包括应用系统部署、测试方案制定、协调软件厂商到场等。 （三）搬迁收尾阶段 1.按照方案进行分次搬迁后，完成机房架构调整，最终达到新机房架构设计要求，并配合进行冗余、故障热切等演练； 2.配合招标人完成业验证工作，完成新机房设备部署图的制定； 3.协助招标人完成老机房的清理工作； 4.应由中标人完成的搬迁后的其他工作； 5.搬迁后需要确保硬件的完整性，保证搬迁后硬件通电测试运行正常，保证系统、数据的完整性，配合招标人恢复信息系统上线正常运行； 6.搬迁到新机房后，重要业务必须 1 天内提供正常服务，其他应用系统 3 天内提供正常服务。

5.7 利旧设备改造

技术指标	服务要求
延保要求	所有利旧设备的改造及安全软件安装与配置，延续三年维保；
其他要求	利旧日志审计新增200个原厂授权； 利旧堡垒机新增200个原厂授权； 利旧的2台网闸同步维保时间并延续三年

附：利旧设备清单

序号	产品	数量	单位	品牌型号	现有授权与维保到期日
1	网闸	2	台	金电网安 FerryWay V2.0	2024-05-08/2026-05-08
2	日志审计	1	台	安恒 DAS-log-1000	200 资产 2024-03-17
3	上网行为管理	1	台	深信服 AC-1000	2024-03-24
4	堡垒机	1	台	思福迪 LogBase-B1000Y	300 授权 2025-05-07

5	态势感知系统	1	套	天融信 SASE-81030	2024-12-6
5	虚拟化服务器	4	台	Dell EMC R740	2025-05-24
6	PACS 存储	1	台	Dell PowerVaultDM3600F	2025-05-24
7	虚拟桌面服务器	4	台	Dell PowerEdgeR740	2023-10-04
8	服务器安全防护	22	CPU	亚信安全/AsiaInfo Deep Security20.0	2026-2-26

五、实施及管理要求

1.项目组织管理要求

（1）投标人应充分考虑满足投标项目的建设要求，提出完整的项目管理、培训、项目施工、项目验收、售后服务方案。

（2）投标人在投标文件中，应根据对项目的理解作出项目的人员配置管理计划，包括组织结构、项目负责人、组成人员及分工职责；阐述项目建设中招标人方和建设方的职责。

（3）招标人有权监督和管理投标项目的测试、安装、调试、故障诊断、系统开发和验收等各项工作，投标人必须接受并服从招标人的监督、管理要求，按要求提供中间过程工作成果。

（4）根据《湖州市卫生健康委网络信息安全和信息化工作管理办法》要求，项目建设需执行《湖州市卫生健康领域信息化建设规范》，实现与湖州市健康大脑的“互联互通”为实质响应项。

2.计划与进度管理要求

(1)投标人在投标文件中应根据对项目的理解作出项目实施的初步计划，成为中标人后必须提交正式工作方案，明确招标项目工作的方式、过程步骤、按阶段分解的详细计划、对应计划应提交的工作成果、需要招标人协调与配合的事项，并经招标人审核、批准。

(2) 投标人在项目实施过程中必须分别按周、月提交进度报告，对项目问题及进度延迟原因进行说明，制定合理的解决措施并有效执行。

(3)投标人必须在投标文件中阐述项目沟通计划，确保投标人与招标人之间信息沟通顺畅。

3.质量管理要求

(1)投标人应按 ISO9001 质量管理体系规范要求，针对招标项目实施过程及交付结果进行质量规划、管理、控制。

(2)中标人在项目实施过程中应开展质量保证活动，所提交的进度报告应包括质量报告内容，对质量问题制定改进措施并有效执行。

(3)中标人必须接受招标人的质量监督检查，提供真实有效的相关质量活动记录、证据，接受招标方提出的合理的质量问题整改要求，承担质量责任及因质量问题导致的进度延迟责任。

(4)投标人必须提供详细测试方案，包括采用测试技术、测试方法和测试报告提交形式。

4.文档交付要求

应用系统应严格按照国家软件工程规范进行，中标人必须根据开发进度及时提供有关文档，包括：

①准备阶段：《实施计划》；

②需求分析阶段：《需求分析说明书》；

③设计阶段：《概要设计说明书》、《数据库设计说明书》；

④测试阶段：《测试计划》、《测试报告》；

⑤上线阶段：《试运行/上线报告》；

⑥培训文档：《培训计划》；

⑦交付使用：《用户手册》；

⑧与工程相关的其他文档。

六、商务要求：

1、服务期：5 年

2、服务地点：由招标人指定地点

3、支付方式：

根据《保障中小企业款项支付条例》、省财政厅《关于坚决打赢疫情防控阻击战进一步做好政府采购资金支持企业发展工作的通知》（浙财采监【2020】3 号）要求， 制定如下付款方式：

（1）合同生效及具备实施条件后 7 个工作内支付合同金额的 40%作为预付款；

（2）机房建设后支付合同金额的 40%（预付款扣回）；

（3）项目初步验收完成且合格后支付至合同金额的 60%；

（4）项目经招标人最终验收通过后支付至合同金额的90%；

（5）余款待项目终验合格后一年内付清。

注：签订合同时中标人明确表示无需预付款或者要求降低预付款比例的，招标人可在合同中另行约定。

4、服务要求：

（1）在服务期内，中标人应负责对其提供的软硬件进行现场维修、损坏件更换，不收取额外费用，响应时间必须满足系统正常运行的要求。

（2）服务期内，要求中标人7×24小时电话响应技术咨询；除非招标文件另有规定，中标人须在接到招标人维修要求电话后，在4小时内做出响应，在24小时内派人到现场进行故障处理。

（3）中标人在投标文件中须说明服务内提供的服务计划。

5、培训：

（1）中标人应对招标人的操作人员及维修人员提供技术培训，使其能对设备进行日常操作和维护保养及能对一般故障进行维修。

（2） 旨在提供更好的其他方式培训。

6、送货调试：

（1）送货地点：按招标人要求。

（2）质量标准：符合我国国家有关技术规范要求和技术标准。

（3）送货、调试过程中发生的费用由中标人负责。

（4）中标人应在投标文件中提出其送货调试过程中使用单位需配合的内容。

7、数量调整

招标人保留在签约时调整部分方案及定购软硬件数量、配套设备、备件和服务的权力，中标人应对系统方案中设备和服务明细报价，按投标单价不变的前提下进行调整，双方不得拒绝。

8、验收方案：

(1)验收内容：中标人实际完成的情况是否符合招标文件要求和在投标文件中的商务、技术承诺。验收中发现达不到验收标准或合同规定的性能指标，中标人必须在征得招标人认可后进行更换，并负担由此给招标人造成的损失，直到验收合格为止。

（2）验收标准：中标人已经按招标文件要求和在投标文件中的商务、技术承诺完成项目执行。中标人应提供有效的检验文件，经招标人认可后，与提供的性能指标一起作为合同验收标准，并在验收中提供招标人认可的相应检测手段，验收标准应符合中国有关的国家、地方、行业的标准。

（3）验收时中标人应在现场，验收完毕后作出验收结果报告；验收产生的全部费用由中标人承担。

9、工作范围：

根据招标文件，各投标人须按国家有关标准及规范完成下列工作：

1、产品及相关附件的提供、运输、装卸、就位、安装、调试、检验、通过验收；

2、完成各项调试、检验、测试工作，并在招标人的配合下通过的验收；提供各种数据资料；直至通过验收。

3、对最终使用单位的操作人员及维修人员进行技术培训；

4、质保期内的维保及维修；

5、售后服务的措施及承诺。

第三章 投标人须知

前附表

序号	内容、要求
1	项目名称：湖州市中医院新院迁建数据中心建设项目
2	采购内容及数量：详见第二章招标需求
3	投标报价及费用：1、本项目投标应以人民币报价；2、不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用；3、本项目代理服务费按肆万零玖佰柒拾伍元整计取由中标人支付。在确定中标人后，领取中标通知书前，由中标人全额支付，请各投标人自行考虑计入投标报价中。
4	答疑与澄清：投标人如认为招标文件表述不清晰、存在歧视性或者其他违法内容的，可以在知道或者应知其权益受到损害之日起 7 个工作日内，以书面形式向招标人、招标代理机构提出质疑，根据《中华人民共和国财政部令第 94 号-政府采购质疑和投诉办法》第十条第二款规定，投标人在法定质疑期内须一次性提出针对同一采购程序环节的质疑，否则招标代理机构有权拒绝第一次质疑以外其他所有质疑。答疑内容是招标文件的组成部分，并将在网上发布补充（答疑、澄清）文件，潜在投标人应自行关注网站公告，招标人不再一一通知，投标人因自身贻误行为导致投标失效的，责任自负。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。
5	采购预算：1498 万元。
6	1、投标文件的制作：本项目实行电子招投标。 2、投标人应按要求提供电子投标文件及数据电子备份投标文件，具体内容如下： （1）电子投标文件：按政采云平台项目采购-电子交易操作指南及本招标文件要求制作、加密并递交，超过上传时间的视为放弃投标资格，作未递交投标文件处理； （2）数据电子备份投标文件：以 U 盘形式提供的数据电子备份投标文件格式及内容须与政采云平台项目采购-电子交易操作指南中制作、加密并递交的电子投标文件格式及内容一致。数据电子备份投标文件制作成一个 U 盘，但须密封、包装，不按此规定密封、包装的数据电子备份响应文件均按未提供处理。 （3）数据电子备份投标文件递交方式： 数据电子备份投标文件应通过邮寄快递方式送达，邮寄地址为：科信联合工程咨询有限公司湖州分公司[湖州市清远路 699 号福美达科技大厦 4 楼]，联系电话：0572-2566197。邮寄截止时间：投标人应于 2024 年 3 月 11 日 12:00 时前准时送达，逾期不予受理。截止开标时间前，招标代理机构统一负责接收。投标人

	须留足投标文件邮寄时间,确保数据电子备份投标文件于规定的时间前送达指定地点，未按时送达的，均按未提供处理。 注：（1）投标人应权衡利弊考虑是否提供数据电子备份投标文件，招标人及招标代理机构不做强制性要求，若因下一条款（第 3 条）原因须启用数据电子备份投标文件时，而投标人未提供的，视为放弃投标资格，作作未递交投标文件处理；（2）投标人应对提供的数据电子备份投标文件进行密封处理，若需要启用数据电子备份投标文件时，由招标人或招标代理机构启封并进行解密；（3）若投标人未提供数据电子备份投标文件,招标公告及招标文件中关于数据电子备份投标文件的要求及内容不再适用。
7	投标截止时间：2024 年 3 月 11 日 14:00 时； 投标地点：（1）本项目通过“政府采购云平台（www.zcygov.cn）”实行在线投标响应（电子投标）； （2）投标人应当在投标截止时间前，将生成的文件格式“.jmbs”的“电子加密投标文件”上传递交至“政府采购云平台”实行在线投标响应。投标截止时间以后上传递交的投标文件将被“政府采购云平台”拒收，作未递交投标文件处理。
8	评标办法及评分标准：附后
9	中标结果公告：招标人依法确定中标后 2 个工作日内，并公告 7 个工作日。 公告发布网址如下： 浙江政府采购网：http://zfcg.czt.zj.gov.cn/; 湖州市公共资源交易信息网：http://ggzyjy.huzhou.gov.cn/
10	中标通知书：在发布中标结果公告的同时，向中标人发中标通知书。
11	签订合同时间：中标通知书发出后30日内。
12	履约保证金的收取及退还：本项目不适用。
13	投标文件有效期：60 天
14	解释：本招标文件的解释权属于招标人
15	在确定中标人后,签订合同前,中标人须提供二份完整的纸质投标文件给招标人,纸质投标文件须与电子投标文件格式及内容一致。
16	特别说明：政采云公司如对电子化开标及评审程序有调整的，应按调整的程序操作。

一、总 则

（一）适用范围

本招标文件适用于湖州市中医院新院迁建数据中心建设项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

（二）采购预算：1498万元。

（三）定义

1. 招标人系指组织本次项目招标的**湖州市中医院**；招标代理机构系指招标人授权委托代理本项目招标程序的**科信联合工程咨询有限公司**。

2.“投标人”指向招标人提交投标文件的单位。

3. “产品”系指投标人按招标文件规定，须向招标人提供的一切产品、保险、税金、备品备件、工具、手册及其它有关技术资料和材料。

4.“服务”系指招标文件规定投标人须承担的安装、调试、技术协助、校准、培训、技术指导以及其他类似的义务。

5.“项目”系指投标人按招标文件规定向招标人提供的服务。

6.“书面形式”包括信函、传真、电报等。

7.“▲”系指实质性要求条款。

（四）采购方式

本次招标采用公开招标方式进行。

（五）投标费用

1. 投标人应自行承担投标过程中的所有相关费用，不论中标与否，招标人在任何情况下不承担有关费用。

2. 本项目代理服务费由中标人在中标后、领取中标通知书时由中标人支付给招标代理机构，按肆万零玖佰柒拾伍元整计取,该费用请投标人自行考虑计入投标报价中。

（六）联合体投标

本项目不接受联合体投标。

（七）转包与分包

本项目不允许转包与分包。

特别说明：

▲1.投标人投标所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人所拥有。投标人投标所使用的招标项目实施人员必须为本法人员工。

▲2.投标人应仔细阅读招标文件的所有内容，按照招标文件的要求提交投标文件，并对所提供的全部资料的真实性承担法律责任。

▲3.投标人在投标活动中提供任何虚假材料,其投标无效，并报监管部门查处；

（八）质疑和投诉

根据《中华人民共和国财政部令第 94 号-政府采购质疑和投诉办法》第二章规定。

1.投标人认为招标文件、采购过程、中标或者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 7 个工作日内，以书面形式向招标人、招标代理机构提出质疑。招标文件可以要求投标人在法定质疑期内一次性提出针对同一采购程序环节的质疑。

2.提出质疑的投标人（以下简称质疑投标人）应当是参与所质疑项目采购活动的投标人。潜在投标人已依法获取（依法获取指：投标人按本项目招标公告要求在政采云系统上获取并报名成功）其可质疑的招标文件的，可以对该文件提出质疑。未按照规定方式依法获取招标文件的，不得对招标文件提起质疑投诉。对招标文件提出质疑的，应当在获取招标文件或者招标文件公告期限届满之日起 7 个工作日内提出。

3. 投标人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：

（1）投标人的姓名或者名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期。

投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代理人签字或者盖章，并加盖公章。

3. 招标人、招标代理机构不得拒收质疑投标人在法定质疑期内发出的质疑函，应当在收到质疑函后 7 个工作日内作出答复，并以书面形式通知质疑投标人和其他有关投标人。

5. 投标人对评审过程、中标或者中标结果提出质疑的，招标人、招标代理机构可以组织原评标委员会、竞争性谈判小组、询价小组或者竞争性磋商小组协助答复质疑。

6.质疑答复应当包括下列内容：

（1）质疑投标人的姓名或者名称；

（2）收到质疑函的日期、质疑项目名称及编号；

（3）质疑事项、质疑答复的具体内容、事实依据和法律依据；

（4）告知质疑投标人依法投诉的权利；

（5）质疑答复人名称；

（6）答复质疑的日期。

质疑答复的内容不得涉及商业秘密。

7.招标人、招标代理机构认为投标人质疑不成立，或者成立但未对中标、中标结果构成影响的，继续开展采购活动；认为投标人质疑成立且影响或者可能影响中标、中标结果的，按照下列情况处理：

（1）对招标文件提出的质疑，依法通过澄清或者修改可以继续开展采购活动的，澄清或者修改招标文件后继续开展采购活动；否则应当修改招标文件后重新开展采购活动。

（2）对采购过程、中标或者中标结果提出的质疑，合格投标人符合法定数量时，可以从合格的中标或者中标候选人中另行确定中标、中标人的，应当依法另行确定中标、中标人；否则应当重新开展采购活动。质疑答复导致中标、中标结果改变的，招标人或者招标代理机构应当将有关情况书面报告本级财政部门。

二、招标文件

（一） 招标文件的构成。本招标文件由以下部分组成：

1.公开招标招标公告

2.招标需求

3.投标人须知

4.评标办法及标准

5.合同主要条款

6.投标格式与附件

7.本项目招标文件的澄清、答复、修改、补充的内容

（二）投标人的风险

投标人没有按照招标文件要求提供全部资料，或者投标人没有对招标文件在各方面作出实质性响应是投标人的风险，并可能导致其投标被拒绝。

（三）招标文件的澄清与修改

1.投标人应认真阅读本招标文件，发现其中有误或有不合理要求的，投标人应当在获取招标文件或者招标文件公告期限届满之日起七个工作日内提出，否则逾期视为默认。招标人对已发出的招标文件进行必要澄清、答复、修改或补充的，应当在招标文件要求提交投标文件截止时间十五日前，在财政部门指定的政府采购信息发布媒体上发布更正公告，并以书面形式通知所有招标文件收受人；不足十五日的，招标人或者招标代理机构应当顺延提交投标文件的截止时间。

2.招标人、招标代理机构必须在网上公布答复投标人要求澄清的问题，并将不包含问题来源的答复网上公布通知所有购买招标文件的投标人。

3.招标文件澄清、答复、修改、补充的内容为招标文件的组成部分。当招标文件与招标文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的网上公告文件为准。

4.招标文件的澄清、答复、修改或补充都应该通过本招标代理机构以法定形式发布，招标人非通过本招标代理机构，不得擅自澄清、答复、修改或补充招标文件。

三、投标文件的编制要求

（一）投标文件的组成（如无格式、格式自拟。）

投标文件由《资格文件》《技术、商务、资信及其他文件》《报价文件》三部分组成。

1. 资格文件主要包括下列内容：

（1）有效的营业执照、税务登记证、组织机构代码证或“三证合一”的营业执照或“五证合一”的营业执照；

（2）法定代表人有效身份证明书及身份证或法定代表人授权书及授权人身份证；

（3）授权代理人最近一个月个人社保缴纳证明文件；

（4）投标承诺书；

（5）信用承诺书；

（6）其他招标文件要求提供的或投标人认为需要说明的资格文件内容。

2. 技术、商务、资信及其他文件主要包括下列内容：

投标人自评分索引表；

（1）技术部分（包含但不限于技术评分内容）：

①产品技术参数；

②项目总体方案；

③服务方案和质量；

④应急预案；

⑤人员配置；

（2）商务、资信及其他部分：

①商务响应表；

②售后服务；

③培训计划；

④优惠承诺；

⑤企业实力；

⑥企业业绩；

（3）其他招标文件要求提供的或投标人认为需要说明的技术、商务、资信及其他文件内容。

3.报价文件：

（1）投标函；

（2）开标一览表；

（3）报价明细表；

（4）中小企业声明函/监狱企业声明函/残疾人福利性单位声明函；（如有）

（5）招标代理服务费承诺函；

（6）投标人针对报价需要说明的其他文件和说明。

（二）投标文件的语言及计量

1.投标文件以及投标人与招标人就有关投标事宜的所有来往函电，均应以中文汉语书写。除签名、盖章、专用名称等特殊情形外，以中文汉语以外的文字表述的投标文件视同未提供。

2.投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元），否则视同未响应。

▲（三）投标报价

1.投标报价应按招标文件中相关附表格式填写。投标报价为本招标项目全部工作内容的报价，所有报价均应使用（人民币元）表示。

2.投标报价是履行合同的最终价格，应包括产品、包装、运输、装卸、保险、税金、货到就位、安装、调试、培训等一切税金和费用。投标报价为签订合同的依据。因投标人失误的错漏项均视为已包含在总报价中。

3.投标文件只允许有一个报价，有选择的或有条件的报价将不予接受。

4.投标人的最终报价由投标人自担全部风险责任，中标后不得以任何理由调整报价或追加任何费用。

5.投标人所有优惠条件和优惠费用不得降低和影响本招标项目质量。

6.投标人对招标文件里有关投标报价的全部内容应仔细确认，若有个别异议，应在开标前提出修改意见，否则视同全部确认。

7.报价如单价与总价不符时，以单价为准；大写与小写不符时以大写为准。

8.投标人在报价中应充分考虑所有可能发生的费用，否则招标人将视报价总价中已包括所有费用。

9.投标人对在合同执行中，除上述费用及招标文件规定的由中标人负责的工作范围以外需要招标人协调或提供便利的工作应当在报价文件中说明。

（四）投标文件的有效期

▲1.自投标截止日起60天投标文件应保持有效。有效期不足的投标文件将被拒绝。

2.在特殊情况下，招标人可与投标人协商延长投标书的有效期，这种要求和答复均以书面形式进行。

3.投标人可拒绝接受延期要求。同意延长有效期的投标人不能修改投标文件。

（五）投标文件的签署和份数

1、电子投标文件：

投标人应根据“政采云投标人项目采购-电子招投标操作指南”及本招标文件规定的格式和顺序编制电子投标文件并进行关联定位，若因投标文件内容不完整、编排混乱导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任。凡是参加两个或者以上标项投标的，投标文件必须按标项分别制作。

2.数据电子备份投标文件：

电子投标文件的备份文件（.bfbs格式）可以U盘形式存储。数据电子备份投标文件格式及内容须与政采云平台项目采购-电子交易操作指南中制作、加密并递交的电子投标文

件格式及内容一致。投标人应将数据电子备份形式的投标文件密封、包装，不按此规定密封、包装的数据电子备份投标文件均按未提供处理。

3.其他：

3.1 投标文件需按招标文件要求的格式填写并签字盖章。

3.2 投标文件不应涂改或行间插字和增删，如有修改，修改处须加盖投标人的公章或由法定代表人或其授权委托人签字或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人负责。

（六）投标文件的包装、递交、修改和撤回

1.投标人应当在投标截止时间前完成电子投标文件的传输递交，并可以补充、修改或者撤回电子投标文件。补充或者修改电子投标文件的，应当先行撤回源文件，补充、修改后重新传输递交，投标截止时间止未完成传输的，视为撤回投标文件。投标、响应截止时间后送达的投标、响应文件，将被政采云平台拒收，作未递交投标文件处理。

2.数据电子备份投标文件：以 U 盘形式提供的数据电子备份投标文件格式及内容须与政采云平台项目采购-电子交易操作指南中制作、加密并递交的电子投标文件格式及内容一致。递交方式：

数据电子备份投标文件应通过邮寄快递方式送达，邮寄地址为：科信联合工程咨询有限公司湖州分公司[湖州市清远路 699 号福美达科技大厦 4 楼]，联系电话：0572-2566197。邮寄截止时间：投标人应于 2024 年 3 月 11 日 12:00 时前准时送达，逾期不予受理。截止开标时间前，招标代理机构统一负责接收。投标人须留足投标文件邮寄时间,确保数据电子备份投标文件于规定的时间前送达指定地点，未按时送达的，均按未提供处理。

3.整个开标过程中若因投标人问题造成电子投标文件无法正常解密的，均认定为未提交电子投标文件，作未递交投标文件处理。若因网络或者其他非投标人问题造成电子投标文件无法正常解密的，启用数据电子备份投标文件，因投标人自身原因造成数据电子备份投标文件无法打开的，作未递交投标文件处理。若正常解密成功，则数据电子备份投标文件不予开启。在下一顺位的投标文件启用时，前一顺位的投标文件自动失效。

4.投标人应将以数据电子备份形式提供的投标文件一份密封、包装。数据电子备份投标文件的包装封面上应注明投标人名称、投标人地址、投标文件名称、投标项目名称、标项及项目编号，并加盖投标人公章。未按规定密封、包装或标记的数据电子备份投标文件将被拒绝，由此造成数据电子备份投标文件被误投或提前拆封的风险由投标人承担。

（七）投标无效的情形

实质上没有响应招标文件要求的投标将被视为无效投标。投标人不得通过修正或撤消不合要求的偏离或保留从而使其投标成为实质上响应的投标，但经评标委员会认定属于投标人疏忽、笔误所造成的差错，应当允许其在评标结束之前进行修改或者补正（可以是复印件、传真件或扫描件等，原件必须加盖单位公章）。修改或者补正投标文件必须以书面形式（政采云系统递交）进行，并应在中标结果公告之前查核原件。限期内不补正或经补正后仍不符合招标文件要求的，应认定其投标无效。投标人修改、补正投标文件后，不影响评标委员会对其投标文件所作的评价和评分结果。

1.在评标开始前，评标委员会或招标代理机构对投标人的资格进行审查，如发现下列情形之一的，投标文件将被视为无效，不在进行下一步评审：

（1）未提供有效的营业执照、税务登记证、组织机构代码证或未提供“三证合一”的营业执照或未提供“五证合一”的营业执照；

（2）未提供法定代表人有效身份证明书及身份证或未提供法定代表人授权书及授权人身份证或与法定代表人授权委托人身份不符的；

（3）未提供法定代表人授权委托人社保的；

（4）未提供投标承诺书的；

（5）未提供信用承诺书的；

（6）资格证明文件不全的，或者不符合招标文件标明的资格要求的。

2.在符合性审查和商务评审时，如发现下列情形之一的，投标文件将被视为无效：

（1）投标文件未按招标文件要求签字或盖章；

（2）投标文件格式不规范、项目不齐全或者内容虚假的；

（3）投标文件的实质性内容未使用中文表述、意思表述不明确、前后矛盾或者使用计量单位不符合招标文件要求的（经评标委员会认定并允许其当场更正的笔误除外）；

（4）未实质性响应招标文件要求或者投标文件有招标人不能接受的附加条件的。

3.在技术评审时，如发现下列情形之一的，投标文件将被视为无效：

（1）未提供或未如实提供投标货物的技术参数，或者投标文件标明的响应或偏离与事实不符或虚假投标的；

（2）明显不符合招标文件要求的规格型号、质量标准，或者与招标文件中标有“▲”的技术指标、主要功能项目发生实质性偏离的；

（3）投标技术方案不明确，存在一个或一个以上备选（替代）投标方案的；

（4）与其他参加本次投标投标人的投标文件（技术文件）的文字表述内容相同连续 20 行以上或者差错相同 2 处以上的。

4.在报价评审时，如发现下列情形之一的，投标文件将被视为无效：

（1）未采用“人民币元”报价的或未按照招标文件表明的币种报价的；

（2）报价超出采购预算金额或者最高限价的；

（3）投标报价具有选择性，或者投标报价未按照招标文件规定的价格进行报价的。

5.被拒绝的投标文件为无效。

6.投标人有下列情形之一的，视为投标人串通投标，其投标无效：

（1）不同投标人的投标（响应）文件由同一单位或者个人编制；

（2）不同投标人委托同一单位或者个人办理投标事宜；

（3）不同投标人的投标文件或响应文件载明的项目管理成员或者联系人员为同一人；

（4）不同投标人的投标（响应）文件件异常一致或者投标报价呈规律性差异；

（5）不同投标人的投标（响应）文件相互混装。

7. 投标人有下列情形之一的，属于恶意串通，其投标无效：

（1）投标人直接或者间接从招标人或者招标代理机构处获得其他投标人的相关情况并修改其投标（响应）文件；

（2）投标人按照招标人或者招标代理机构的授意撤换、修改投标（响应）文件；

（3）投标人之间协商报价、技术方案等投标（响应）文件的实质性内容；

（4）属于同一集团、协会、商会等组织成员的投标人按照该组织要求协同参加政府采购活动；

（5）投标人之间事先约定由某一特定投标人中标、成交；

（6）投标人之间商定部分投标人放弃参加政府采购活动或者放弃中标、成交；

（7）投标人与招标人或者招标代理机构之间、投标人相互之间，为谋求特定投标人中标、成交或者排斥其他投标人的其他串通行为。

8.出现以下情形，导致电子交易平台无法正常进行，或者无法保证电子交易的公平、公正和安全时，中止电子交易活动：

（1）电子交易平台发生故障而无法登录访问的；

（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；

（3）电子交易平台发现严重安全漏洞，有潜在泄密危险的；

（4）病毒发作导致不能进行正常操作的；

（5）其他无法保证电子交易的公平、公正和安全的情况。

出现以上规定情形，不影响采购公平、公正性的，招标代理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数据电子备份投标文件形式进行；影响或可能影响采购公平、公正性的，重新采购。

（八）废标的情形

在采购活动中，出现下列情形之一的，应予废标：

(1)符合专业条件的投标人或者对招标文件作实质性响应的投标人不足三家的；

(2)出现影响采购公正的违法、违规行为的；

(3)投标人的报价均超过了采购预算，招标人不能支付的；

(4)因重大变故，采购任务取消的。

四、开标

（一）开标准备

招标代理机构将在规定的时间和地点进行开标，并按照招标文件规定的时间通过“政府采购云平台”组织开标、开启投标文件，所有投标人均应当准时在线参加。

（二） 电子招投标开标及评审程序

1.开标由招标人或者招标代理机构主持，邀请投标人在线参加。评标委员会成员不得参加开标活动；

2.主持人宣布开标会议开始，并按照规定的时间通过政采云系统组织开标，所有投标人应当准时在线参加；

3.投标截止时间后，投标人应登录政采云平台，在收到电子加密投标文件【开始解密】通知后，通过“项目采购-开标评标”模块对电子投标文件进行在线解密；

4.在开标结束后（评标开始前），由招标人或招标代理机构进行资格审查。资格审查后在系统上公布资格审查结果；

5.由评标委员会对资格审查通过的投标人进行技术、商务、资信及其他部分评审，符合性审查及评分结束后，由主持人公布无效投标的投标人名单、投标无效的原因，并在系统上公布其他有效投标的评审结果；

6.由主持人在系统上公布的投标人名称及在其投标文件中承诺的投标报价、投标内容以及其他有必要宣读的内容；

7.报价部分符合性审查及评分结束后，由主持人公布无效投标的投标人名单、投标无效的原因，并在系统上公布其他有效投标的评分结果；

8.最终在政采云系统上公布评审结果；

9.开标会议结束。

特别说明：政采云公司如对电子化开标及评审程序有调整的，应按调整的程序操作。

五、评标

（一）组建评标委员会

本项目评标委员会由政府采购评审专家及招标人代表共5人组成。

（二）评标的方式

本项目采用不公开方式评标，评标的依据为招标文件和投标文件。

（三）评标程序

1.形式审查

在开标结束后（评标开始前），招标人或代理机构负责对投标人的资格和投标文件的完整性、合法性等进行审查。

2.实质审查与比较

（1）评标委员会审查投标文件的实质性内容是否符合招标文件的实质性要求。

（2）评标委员会将根据投标人的投标文件进行审查、核对,如有疑问,将对投标人进行询标,投标人要向评标委员会澄清有关问题,并最终以书面形式（政采云系统内）进行答复。投标人未在规定时间内澄清或者拒绝澄清或者澄清的内容改变了投标文件的实质性内容的，评标委员会有权对该投标文件做出不利于投标人的评判。

（3）评标委员会完成评标后,按评标原则推荐中标候选人同时起草评标报告。

（4）评标委员会按评标原则通过电子系统向招标人及招标代理机构提交评审报告。

（四）澄清问题的形式

评审中需要投标人对投标文件作出澄清、说明或者补正的，评标委员会和投标人应当通过电子交易平台交换数据电文。给予投标人提交澄清说明或补正的时间为30分钟，投标人已经明确表示澄清说明或补正完毕的除外。

（五）错误修正

投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

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；

2.大写金额和小写金额不一致的，以大写金额为准；

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；

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。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价应当采用书面形式并加盖公章或者由法定代表人或其授权的代表签字。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。经投标人确认后产生约束力，投标人不确认的，则其投标将作为无效投标处理。

（六）评标原则和评标办法

1.评标原则。评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与投标人接触。

2.评标办法。本项目评标办法是**综合评分法**，具体评标内容及评分标准等详见《第四章：评标办法及评分标准》。

3.评标过程中凡是属于审查、澄清、评审和比较的有关资料以及授标建议，任何人均不得向投标人或其他无关人员透露。

（七）评标过程的监控

本项目评标过程实行全程录音、录像监控，由湖州市公共资源交易管理办公室进行现场监督。投标人在评标过程中所进行的试图影响评标结果的不公正活动，可能导致其投标被拒绝。

六、定标

（一）确定中标人。本项目由招标人确定中标人。

1.招标代理机构在评标结束后 2 个工作日内将评标报告交招标人。招标人应当自收到评标报告之日起 5 个工作日内，在评标报告确定的中标候选人名单中按顺序确定中标投标人。中标候选人并列的，由招标人或者招标人委托评标委员会按照招标文件规定的方式确定中标投标人；招标文件未规定的，采取随机抽取的方式确定。

2.招标人在收到评标报告 5 个工作日内未按评标报告推荐的中标候选人顺序确定中标人，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标人。

3.招标人依法确定中标人后 2 个工作日内，招标代理机构以书面形式发出《中标通知书》，并同时在相关网站上发布中标结果公告。

七、合同授予

（一）签订合同

1.招标人与中标人应当在《中标通知书》发出之日起 30 日内签订政府采购合同。招标人与中标人签订合同后在规定时间内依法发布合同公告。同时，招标代理机构对合同内容进行审查，如发现与采购结果和投标承诺内容不一致的，应予以纠正。

2.中标人拖延、拒签合同的,将被取消中标资格。

（二）中标通知书

1.确定中标人后，招标代理机构将以书面形式发出中标通知书，通知中标的投标人其投标被接受；

2.中标通知书为双方签订合同的依据；

3.中标人应根据中标通知书中规定的时间内，由法定代表人或其授权代理人与招标人签订合同。

（三）履约保证金：

本项目不适用

八、其他内容

1、为有效破解当前中小微企业面临的“融资难、融资贵”困局，充分发挥好政府采购扶持小微企业发展的政策功能，本项目中标人可凭中标通知书等材料至“绿贷通平台”网页（www.lvdt.huzldt.com）或“政采贷”平台网页（www.zcygov.cn）申请相关融资产品。具体操作方式可在“绿贷通”或“政采贷”平台网站查询，也可向“绿贷通”或“政采贷”平台电话咨询（“绿贷通”联系电话：0572-2392590、“政采贷”联系电话：0572-2151055、18698580797）。

第四章 评标办法及评分标准

为公正、公平、科学地选择中标人，根据《中华人民共和国政府采购法》、《政府采购货物和服务招标投标管理办法》及相关法律、法规等规定，并结合本项目的实际，制定本办法。

本办法适用于湖州市中医院新院迁建数据中心建设项目的评标。

一、总则

本次评标采用综合评分法，总分为100分，其中价格分10分、技术商务资信及其他部分90分。合格投标人的评标得分为各项目汇总得分。本项目由招标人确定中标人，中标候选资格按评标得分由高到低顺序排列，得分相同，按技术部分得分由高到低顺序排列。技术部分得分仍相同的，由招标人采用随机抽取的方式决定，排名第一的投标人为第一中标候选人,其他投标人中标候选资格依此类推。第一中标候选人放弃中标或者因不可抗力提出不能履行合同，招标人可以确定第二中标候选人为中标人，排名第二的中标候选人因前款同样的原因不能签订合同，招标人可以确定排名第三的中标候选人为中标人，招标人也可选择重新采购。评分过程中采用四舍五入法，并保留小数2位。

各投标人最终得分=价格分+技术分、商务、资信及其他分得分

二、评标内容及标准

（一）价格分10分

价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，价格分为满分，其他投标人的价格分按照下列公式计算：

价格分=（评标基准价/投标报价）×10%×100

落实政府采购政策：

1.根据财政部、工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知（财库【2020】46号），对小型和微型企业的产品投标报价给予20%的扣除，并用扣除后的价格计算价格评分。

符合以下所有要求的投标人被认定为小型、微型企业：

1）投标人按照《关于印发中小企业划型标准规定的通知》（工信部联企业【2011】300号）的所属行业规定为小型、微型企业【按《政府采购促进中小企业发展管理办法》的通知（财库【2020】46 号）规定提供《中小企业声明函》，不提供不予认可】。

2.监狱企业参加投标【提供《监狱企业声明函》及其相关的证明材料】，视为小型、微型企业，享受小微企业政策扶持，监狱企业属于小型、微型企业的，不重复享受政策。

3.残疾人福利性单位参加投标【提供《残疾人福利性单位声明函》及其相关的证明材料】，视为小型、微型企业，享受小微企业政策扶持，残疾人福利性单位属于小型、微型企业的，不重复享受政策。

投标人按照规定提供声明函内容不实的，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。

此项由评审小组集体核实后统一打分。

（二）技术分、商务分、资信及其他分 90 分

本项目设技术、商务、资信及其他分 90 分。

（三）技术分、商务分、资信及其他分的计算

技术、商务、资信及其他按照评标委员会成员的独立评分结果汇总数的算术平均分计算，计算公式为：

技术分、商务分、资信及其他分=（评标委员会所有成员评分合计数）/（评标委员会组成人员数）

附件：评分表格式

序号	评审内容	评分标准	分值
技术分			62 分
1	产品技术参数	产品性能、技术指标：根据投标人提供的设备性能质量、技术指标和系统功能要求进行评定,满足招标文件要求得30 分。技术参数中打打“▲”号的指标为实质性指标，不得负偏离，打“★”号的指标为重要性指标，每负偏离一项扣 1 分，其他一般指标负偏离的每偏离一项扣 0.5 分，最多扣 29 分。 须提供相关证明材料，未提供视为负偏离。	30 分
2	项目总体方案	项目实施方案设计具有完整性、先进性和可行性，具有合理的进度安排、组织架构，具有良好的进度控制、风险控	8 分

		制管理、质量保障措施、信息安全管理措施、文档管理措施以及项目验收方案，得 8 分。方案措施有欠缺、不科学合理的、不利于招标人、不利于本项目或与本项目不相关的每处扣 0.5 分，最多扣 7 分。 **以上方案不提供不得分**	
3	服务方案和质量	投标人提供针对本次项目服务方案科学完整，对项目需求的充分理解和把握，符合招标人实际需求，包括但不限于服务方案的科学性、先进性、可靠性、成熟性、合理性和扩展性，提供的服务质量保证措施是否完善有效，以上内容相应地满足或优于本项目需求的得 8 分，方案有欠缺、不科学合理的、不利于招标人、不利于本项目或与本项目不相关的在紧急情况下展开的每处扣 0.5 分，最多扣 7 分。 **以上方案不提供不得分**	8 分
4	应急预案	根据投标人针对本项目提出的应急方案（包括但不限于应急演练方案、应急响应时间、故障排除时间、应急处置措施）进行评分，应急预案内容完整、方案可行、措施有效的得 8 分，方案措施有欠缺、不科学合理的、不利于招标人、不利于本项目或与本项目不相关的在紧急情况下展开的每处扣 0.5 分，最多扣 7 分。 **以上方案不提供不得分**	8 分
5	人员配置	项目负责人： 1、拟派本项目项目负责人具备国际项目管理师（PMP）项目管理或信息系统项目管理师（软考证书）证书的得 1 分。 **需提供相关证书证明材料及近一个月社保缴纳证明复印件并加盖投标人公章，缺项或不提供均不得分。** 拟派项目团队成员（除项目负责人外）	8 分

		2、具有系统集成项目管理工程师（软考证书）或数据中心（机房）运维管理工程师或数据中心（机房）规划设计工程师证书的得 1 分； 3、具有网络专家高级认证（HCIE、CCIE 等同类证书）证书或网络规划设计师（软考证书）的得 1 分； 4、具有国产云计算架构高级认证（ACP、ACE、TCE、TCP、H3CSE、HCIP 等同类型证书）证书的得 1 分； 5、具有注册信息安全专业人员（CISP）证书或信息安全保障人员认证（CISAW）证书的得 1 分； 6、具有 OCP Oracle 认证专家证书、OCM Oracle 认证大师证书、红帽认证工程师（RHCE）、虚拟化认证工程师（VCP）、麒麟或 UOS 操作系统应用工程师认证证书的，每提供一个得 1 分，同一证书不重复计分，本项最高得 3 分； **需提供相关证书证明材料及近一个月社保缴纳证明复印件并加盖投标人公章，缺项或不提供均不得分。**	
商务分、资信及其他分			**28 分**
6	售后服务	根据投标人提供的售后服务方案（包括但不限于售后服务管理体系、售后服务响应时间、售后服务人员安排、售后服务保障措施、后续技术支持等）进行评分，售后运维团队强，服务方案全面周到的得 8 分，售后服务不全面、不利于招标人、不利于本项目展开或与本项目不相关的每处扣 1 分，最多扣 7 分。 **以上方案不提供不得分**	8 分
7	培训计划	根据投标人提出的培训计划（业务人员应用培训和管理员级培训）、地点、组织、人员配备、软硬件资料等内容完整、科学合理的得 8 分，与本项目要求不符合的、不利于招标人、不利于本项目展开或与本项目不相关的每处扣	8 分

		0.5 分，最多扣 7 分。 **以上方案不提供不得分**	
8	优惠承诺	根据投标人提供的优惠承诺进行评分，每提供一条优于本项目需求且具有实际价值的优惠承诺得 1 分，本项最高得 3 分。 **与本项目需求无关联为无效承诺的或不提供均不得分。**	3 分
9	企业实力	1、投标人具有有效的 ISO 9001 质量管理体系认证证书得 1 分。 2、投标人具有有效的 ISO 20000 信息技术服务管理体系认证证书得 1 分。 3、投标人具有有效的 ISO 27001 信息安全管理体系认证证书得 1 分。 4、投标人具有有效 ISO 27701 隐私信息管理体系认证证书得 1 分。 5、投标人具有有效的 ISO27017 云服务信息安全管理体系认证证书得 1 分。 6、投标人具有有效的 ITSS 信息技术服务标准体系认证证书得 1 分。 **提供有效认证证书复印件及全国认证认可信息公共服务平台网站证书信息截图加盖投标人公章，否则不予认可。** 7、根据投标人提供的 2020 年 1 月 1 日至今有效的政府行政职能部门或行业主管部门或所属行业协会授予的投标企业荣誉证书（荣誉与本项目特征相关）进行评分： 国家级，包含国务院所属的部、委、办、局或所属行业协会授予的荣誉得 2 分； 省级，包含省政府所属的部、委、办、局（厅）或所属行业协会授予的荣誉得 1.5 分； 市级，包含市政府所属的部、委、办、局或区、县政府或	8 分

		所属行业协会授予的荣誉得 1 分。 分值不重复计算，本项最高得 2 分。 **提供相关证书复印件并加盖投标人公章，否则不予认可。**	
10	企业业绩	投标人自 2020 年 1 月 1 日以来（以合同签订日期为准）承担过同类项目（数据中心建设）业绩的，每提供一个得 0.5 分，最高得 1 分。 **提供合同及用户验收报告扫描件并加盖投标人公章，缺项或不提供均不得分。**	1 分

第五章 合同主要条款

（仅供参考，以正式合同为准）

财政审批编号：HZCG[2023]680 号

甲方（招标人）：

乙方（中标人）：

甲、乙双方根据科信联合工程咨询有限公司关于湖州市中医院新院迁建数据中心建设项目公开招标的结果，签署本合同。

1.定义

本合同中的下列术语应解释为：

1.1“合同”系指供需双方签署的、合同格式中载明的供需双方所达成的协议，包括所有的附件、附录和构成合同的所有文件；

1.2“合同价”系指根据合同规定，甲方在乙方完全履行合同义务后应付给的价格；

1.3“货物”系指乙方根据合同规定向甲方提供的一切货物、质量保证书和其他技术资料及技术参数等；

1.4“服务”系指根据合同规定乙方承担与供货有关的辅助服务，如运输、装卸、安装、保险以及其他的服务，例如安装、调试提供技术援助、培训和其他类似的义务；

1.5“甲方”系指具体使用货物和接受服务的使用单位；

1.6“乙方”系指根据合同规定提供采购项目货物和服务的具有法人资格的公司、企业或实体；

2.合同项目与内容

2.1 合同项目：湖州市中医院新院迁建数据中心建设项目

2.2 内容：湖州市中医院新院迁建数据中心建设

2.3 合同价：

3.服务时间与服务地点

服务时间：由甲方指定。

服务地点：由甲方指定。

4.签署合同的要求

4.1、乙方必须按照招标文件和询标过程中承诺的条款以及中标通知书中规定的时间、地点与甲方签订合同；

4.2、所签订的合同内容不得对招标文件和乙方的投标文件作实质性修改；

4.3、甲方不得向乙方提出任何不合理的要求，作为签订合同的条件，不得与乙方私下订立背离合同实质性内容的协议；

5.技术规范

5.1 本合同执行国家及本省、市现行项目实施及验收规范及有关条例、实施办法等。

5.2 提供和交付的服务技术规范应与招标文件规定的技术规范相一致。

5.3 招标文件、投标文件、招标答疑、技术澄清及询标答复的所有内容是构成合同不可分割的部分，与本合同具有同等法律效力，当文件有相矛盾之处，以时间在后者为准。

6.知识产权

乙方保证所提供的服务及货物均不存在知识产权纠纷。乙方应保证甲方在使用时不受第三方提出侵犯其专利权、商标权等知识产权的诉讼。

7.付款方式

根据《保障中小企业款项支付条例》、省财政厅《关于坚决打赢疫情防控阻击战进一步做好政府采购资金支持企业发展工作的通知》（浙财采监【2020】3 号）要求， 制定如下付款方式：

（1）合同生效及具备实施条件后 7 个工作内支付合同金额的 40%作为预付款；

（2）机房建设后支付合同金额的 40%（预付款扣回）

（3）项目初步验收完成且合格后支付至合同金额的 60%

（4）项目经甲方最终验收通过后支付至合同金额的 90%

（5）余款待项目终验合格后一年内付清。

注：签订合同时乙方明确表示无需预付款或者要求降低预付款比例的，甲方可在合同中另行约定。

8.支付：支付应使用人民币；

9.技术服务

乙方应负责安排甲方相关人员进行操作、维修的培训。具体时间及培训内容在投标时由乙方提出建议；

10.售后服务及承诺

10.1 乙方应明确承诺售后服务各项内容和措施，提供详细的服务地点、联系人、电话等有关资料；

10.2 服务期：详见招标文件要求。在服务期内，因服务质量所发生的一切费用均由乙方承担；

11.验收方案

11.1 验收内容：乙方实际完成的情况是否符合招标文件要求和在投标文件中的商务、技术承诺。验收中发现达不到验收标准或合同规定的性能指标，乙方必须在征得甲方认可后进行更换，并负担由此给甲方造成的损失，直到验收合格为止。

11.2 验收标准：乙方已经按招标文件要求和在投标文件中的商务、技术承诺完成项目执行。乙方应提供有效的检验文件，经甲方认可后，与提供的性能指标一起作为合同验收标准，并在验收中提供甲方认可的相应检测手段，验收标准应符合中国有关的国家、地方、行业的标准。

11.3 验收时乙方应在现场，验收完毕后作出验收结果报告；验收产生的全部费用由乙方承担。

12.违约责任

12.1 甲方无正当理由拒收接受服务的，甲方向乙方偿付合同款项百分之五作为违约金。

12.2 甲方无故逾期验收和办理款项支付手续的,甲方应按逾期付款总额每日万分之五向乙方支付违约金。

12.3 乙方不按约定提供服务的，每日向甲方支付千分之六违约金。逾期提供服务超过约定日期 10 个工作日的，甲方可解除本合同。乙方因逾期提供服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值 20%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

12.4 如乙方提供的服务或与服务相关的物品存在知识产权纠纷而导致本合同无法继续履行，在甲方发函要求解决相关知识产权问题后 日内仍未解决的，则甲方有权单方终止本合同的履行，并要求乙方承担相应赔偿责任。

13.不可抗力事件处理

13.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

13.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

13.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

14.争议解决

14.1 在执行本合同中所发生的或与本合同有关的一切争端，合同双方应通过友好协商解决，经过协商仍不能解决，双方选择通过下列第_____ 种方式解决：

（1）将争端提交湖州仲裁委员会仲裁

（2）直接向甲方所在地有管辖权的人民法院起诉。

14.2 仲裁费用或诉讼费用应由败诉方负担。

14.3 在仲裁或诉讼期间，除进行仲裁或诉讼的部分外，本合同其它部分应继续执行。

15.转让或分包

15.1 本合同范围的服务，应由乙方提供，不得转让他人供应；

16.适用法律

合同适用法律有《中华人民共和国民法典》、《中华人民共和国产品质量法》和浙江省有关条例等。

17、合同生效及其它

1.合同经双方法定代表人或授权代理人签字并加盖单位公章后生效。

2.合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。

3.本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

4.本合同一式伍份，其中甲乙双方各执两份，招标代理机构一份。

甲方：	乙方：
地址：	地址：
法定（或授权）代表人：	法定（或授权）代表人：
签字日期：年 月 日	签字日期：年 月 日

第六章 投标格式

封面格式（**中标后提供的纸质版本格式**）

投标文件

资格文件/技术、商务、资信及其他文件/报价文件

项目名称：

项目编号：

投标文件名称：资格文件/技术、商务、资信及其他文件 /报价文件

投标人名称：

投标人地址：

年 月 日

目 录

1、资格文件目录（具体参考第三章投标人须知“投标文件的组成”）

……

2、技术、商务、资信及其他文件目录（具体参考第三章投标人须知“投标文件的组成”）

……

3、报价文件目录（具体参考第三章投标人须知“投标文件的组成”）

……

（本章仅提供部分标准通用表格，具体格式内容请参照本投标文件中对投标文件编制要求）

法定代表人有效身份证明书

（姓名）是（投标人全称）的法定代表人，身份证号码为 _____。

特此证明。

投标人：（盖章）

法定代表人（签名或盖章）：

日期： 年 月 日

————————————————————————————————

有效身份证明复印件粘贴处

法定代表人授权委托书

致（招标人名称）：

我（姓名）系（投标人名称）的法定代表人，现授权委托本单位（姓名）以我方的名义参加_____项目的招标活动，并代表我方全权办理针对上述项目的投标、签约等具体事务和签署相关文件。

我方对授权代理人的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。授权代理人在授权书有效期内签署的所有文件不因授权的撤销而失效。

授权代理人无转委托权，特此委托。

授权代理人签名： 法定代表人签名：

职务： 职务：

授权代理人身份证号码：

投标人公章：

年 月 日

————————————————————————————————

授权代理人有效身份证明复印件粘贴处

投标承诺书

（投标人）现参加 （项目名称）政府采购活动，我单位承诺如下：

1、符合参与政府采购活动的资格条件（符合《中华人民共和国政府采购法》第二十二条规定和浙财采监【2013】24号《关于规范政府采购投标人资格设定及资格审查的通知》第六条规定,且未被“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、没有税收缴纳、社会保障等方面的失信记录，若违背以上承诺的，我单位原因承担相应法律后果和责任，并依法依规列入严重失信名单。

承诺单位/个人：

（盖章/签名）

时 间： 年 月 日

信用承诺书

（投标人）现参加（项目名称）政府采购活动，郑重承诺如下：

对所提供的资料合法性、真实性、准确性和有效性负责；

严格按照国家法律、法规和规章，依法开展相关经济活动，全面履行应尽的责任和义务；

加强自我约束、自我规范、自我管理，不制假售假、不虚假宣传、不违约毁约、不恶意逃债、不偷税漏税，诚信依法经营；

自愿接受行政主管部门的依法检查、违背承诺约定将自愿承担违约责任，并接受法律法规和相关部门规章制度的惩戒和约束；

按照信用信息管理有关要求，本单位（个人）同意将以上承诺在信用湖州网站公示，若违背以上承诺，依据相关规定记入企业（个人）信用档案；性质严重的，承担相应法律后果和责任，并依法依规列入严重失信名单。

统一社会信用代码：

承诺单位/个人（盖章/签名）

时间： 年 月 日

投标人自评分索引表

投标人全称（公章）：

评分项目	投标文件对应资料	自评分	投标文件页码
对应第四章评分办法及评分标准（报价除外）			
……			

法定代表人或其授权代理人签字或盖章：

日期： 年 月 日

项目实施人员配备表

（项目负责人）

投标人全称（加盖公章）：

项目编号：

姓名		近3年业绩及承担的主要工作情况，曾担任项目经理的项目应列明细
性别		
年龄		
职称		
毕业时间		
所学专业		
学历		
资质证书编号		
其他资质情况		
联系电话		

注：1、此表仅提供了表格形式，投标人应根据需要准备足够数量的表格来填写；

2、请附随表相应证书等；

3、项目负责人参加投标人社会保险的证明；

4、所有材料提供原件的扫描件，加盖投标人公章。

项目实施人员配备表

（项目团队，除项目负责人以外的配备人员）

投标人全称（加盖公章）： 项目编号：

序号	姓名	性别	年龄	学历	专业	职称	本项目中的职责	项目经历	参与本项目的到位情况
							安全员		

法定代表人或授权代理人签名或盖章：

日期： 年 月 日

注：1、此表仅提供了表格形式，投标人应根据需要准备足够数量的表格来填写；

2、请附证书等；

3、项目团队人员参加投标人社会保险的证明；

4、所有材料加盖投标人公章。

技术响应表

投标人全称（加盖公章）：

项目编号：

序号	内容	招标文件要求	投标文件实际响应	响应情况	偏离原因

法定代表人或其授权代理人签名或盖章：

日期： 年 月 日

注：**▲1、投标人必须按招标需求一一对应，如实填写；**

2、此表仅提供了表格形式，投标人应根据需要准备足够数量的表格来填写。

商务响应表

投标人全称（加盖公章）：

项目名称：湖州市中医院新院迁建数据中心建设项目

项目	招标文件要求	是否响应	投标人的承诺或说明或优化方案
服务期			
付款方式			
其他要求			
.....（自拟）			

法定代表人或其授权代理人签字：

日期： 年 月 日

企业业绩

投标人全称（加盖公章）：

项目名称：湖州市中医院新院迁建数据中心建设项目

序号	项目名称	使用方	合同金额（元）	签订时间	使用方联系人	联系方式

注：此表仅提供了表格形式，投标人应根据需要准备足够数量的表格来填写。

法定代表人或其授权代理人签名或盖章：

日期： 年 月 日

企业认证

投标人全称（加盖公章）：

项目编号：

序号	证书名称	颁发机构	颁发时间	备注

法定代表人或授权代理人签名或盖章：

日期： 年 月 日

注：

1. 获得的证书(附证书原件的扫描件并加盖公章)；

2. 此表仅提供了表格形式，投标人应根据需要准备足够数量的表格来填写。

投标函

_____：

_____（投标人全称）授权_____（授权代表名称）_____（职务、职称）为授权代表，参加贵方组织的_____（项目名称）（括号内填项目编号）招标的有关活动，并对_____项目（项目名称）进行投标。为此：

1、提供投标人须知规定的全部投标文件：“资格文件”、“技术文件”、“报价文件”正本各一份、副本_____份。

2、保证遵守招标文件中的有关规定和收费标准。

3、保证诚信地执行招标人、投标人双方所签的合同，并承担合同规定的责任义务。

4、投标人已详细审查全部招标文件，包括招标文件补充文件（如果有的话）。我方完全理解并同意放弃对这方面有不明及误解的权力。如果招标文件有相互矛盾之处，我方同意按投标人的理解处理。

5、利益冲突：近三年内直至目前，我公司与本项目的投标人、招标机构没有任何的隶属关系。

6、我公司没有被本项目所在地的主管部门限制参加报价。

7、愿意向贵方提供任何与该项报价有关的数据、情况和技术资料，完全理解贵方不一定接受最低价的报价或收到的任何报价。

8、本报价文件自报价之日起60天内有效。

9、兹证明上述声明是真实的、正确的，并提供了全部能提供的资料和数据，我们同意遵照贵方要求出示有关证明文件。

以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

投标人全称（盖章）：

法定代表人（签字或盖章）：

日　　期：

开标一览表

投标人全称（加盖公章）：

项目名称：

项目编号：

报价单位：人民币（元）

序号	报价内容	投标报价
1	硬件	
2	软件	
3	安全	
4	服务	
投标总报价（1+2+3+4）		小写： 大写：

注： 1、报价一经涂改，应在涂改处加盖单位公章或者由法定代表人或授权委托人签字或盖章，否则其投标作无效标处理。

2、投标费用包括项目实施所需的材料费、人工费、服务费、购买及制作标书费、代理服务费、税费等及其他一切费用。

▲3、各投标人报价不得超过分项限价及最高限价，否则按无效标处理。

法定代表人或授权代理人签字：

年 月 日

报价明细表

序号	产品	数量	单位	单价	总价
一、硬件					
1	服务器 1	8	台		
2	服务器 2	10	台		
3	互联交换机	4	台		
4	数据中心汇聚交换机	4	台		
5	存储	1	台		
6	CDSS 服务器	1	台		
7	验章服务器	1	台		
8	光纤交换机	4	台		
9	云桌面服务器扩容	3	台		
10	云桌面终端扩容（含个 100 授权）	200	台		
11	运维大屏	3	台		
12	其他（可自行增加）				
二、软件					
1	分布式存储软件	1	套		
2	虚拟化软件	1	套		
3	超融合软件	1	套		
4	虚拟化容灾备份系统	1	套		
5	数据库容灾系统	1	套		
6	IT 综合运维监管平台	1	套		
7	IT 综合运维服务平台	1	套		
8	数据支撑平台	1	套		
9	业务性能保障与优化系统	1	套		
10	桌面管理软件	1	套		
11	文件安全交互系统	1	套		

12	其他（可自行增加）				
三、安全					
1	专网防火墙	4	台		
2	外网防火墙	1	台		
3	数据中心防火墙	2	台		
4	WEB 应用防火墙	1	台		
5	数据库审计	1	台		
6	内网准入控制	1	套		
7	外网准入控制	1	套		
8	威胁探针	2	台		
9	零信任	1	套		
10	终端杀毒软件	1	套		
11	服务器防护软件扩容	1	套		
12	数据加密	1	套		
13	其他（可自行增加）				
四、服务					
1	光纤专线租赁	4	条		
2	等保测评服务	1	项		
3	安全服务	1	项		
4	运维服务	1	项		
5	设备部署及系统集成服务	1	项		
6	搬迁服务	1	项		
7	利旧设备改造	1	项		
8	其他（可自行增加）				
合计		小写： 大写：			

注：报价明细表的合计金额应与开标一览表的投标总报价一致。

中小企业声明函（工程、 服务）

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（ 单位名称 ）的 （ 项目名称 ）采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。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. （ 标的名称 ），属于（ 招标文件中明确的所属行业：信息传输、软件和信息技术服务业）； 承建（承接）企业为（ 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. （ 标的名称 ），属于（ 招标文件中明确的所属行业：信息传输、软件和信息技术服务业）； 承建（承接）企业为（ 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（盖章）：

日 期：

注：1、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。

监狱企业声明函（如有）

【非监狱企业的不用提供】

本企业郑重声明，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，本企业为监狱企业。

根据上述标准，我企业属于监狱企业的理由为:

本企业为参加(项目名称：）（项目编号：）采购活动提供本企业的产品。

本企业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(盖章）：

日期：年 月 日

监狱企业参加政府采购活动时，应当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的证明文件。

监狱企业:是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。

残疾人福利性单位声明函（如有）

【非残疾人福利性单位不用提供】

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 (招标人名称)单位的 (项目名称)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)，成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往册商标的货物)。

本单位对上述声明的真实性负责，如有虚假，将依法承但相应责任。

投标人名称(盖章)：

日期： 年 月 日

招标代理服务费承诺函

科信联合工程咨询有限公司：

根据招标文件的规定，一旦我公司中标，我公司同意按招标文件规定金额向贵公司交纳中标标项的招标代理服务费，在收到中标通知书后的当天一次性结清。

本承诺函自开标之日起至本次采购期满有效。

法定代表人或授权代理人签字：

投标人公章：

日期： 年 月 日

单位名称：科信联合工程咨询有限公司湖州分公司

税号：91330523MA28C9FX3N

帐号：52050078801000000333

开户银行：上海浦东发展银行股份有限公司湖州南浔小微企业专营支行