哈密市中心医院

货物采购合同

项目名称：哈密市中心医院数据库安全运维及关键信息基础设施、灾备系统日常维护服务

甲　　方：哈密市中心医院
地　　址：哈密市伊州区广场北路 18 号
电　　话：0902-2265791

乙　　方：新疆联盛科技有限公司
地　　址：新疆乌鲁木齐经济技术开发区(头屯河区)凤凰山街353号2幢13层1306至1308室
电　　话：0991-4503278

合同签署地：哈密市伊州区

甲方：哈密市中心医院
法定代表人：杨建中
地址：哈密市伊州区广场北路 18 号
乙方：新疆联盛科技有限公司
统一社会信用代码号：9165010367928001X9
法定代表人：张宝林
地址：新疆乌鲁木齐经济技术开发区(头屯河区)凤凰山街 353 号 2 幢 13 层 1306 至 1308 室

为了保护甲乙双方合法权益，根据《中华人民共和国民法典》、《中华人民共和国政府采购法》相关法律法规以及甲方采购文件、乙方响应文件，经双方协商一致签署本合同，以资共同遵守。

一、采购标的

金额单位．元

序号	商品名称	品牌	型号	配置要求	采购数量	单位	成交单价
1	医院信息系统数据库运行维护	/	/	详见附件一医院信息系统数据库运行维护服务内容	1	项	196000
2	医院核心生产数据库异地灾备运维维护	/	/	详见附件二医院核心生产数据库异地灾备运维维护服务内容	1	项	200000
3	医院云灾备边界防护	太一星晨	T-Force3000-26-F	详见附件三医院云灾备边界防护技术参数	1	台	78000
4	数据库、关键信息基础设施维护	/	/	详见附件四数据库、关键信息基础设施维护服务内容	1	项	187000
	合同总价（元）661000 元						

注．合同总价包含商品到达甲方并能正常使用所需的一切费用，包括但不限于商品购置费、包装费、运输费、装卸费、保险费、安装调试费、技术服务费、培训费以及保修费、税费等。

二、资金来源及支付方式

1.资金来源性质为院内自筹资金。

2.资金支付方式为单位转账。

三、货款结算

1.本项目合同金额为人民币：￥661000，大写：陆拾陆万壹仟元整。

2.合同签订后 10 个工作日内，乙方将本合同全款的 10%做为履约保证金，电汇给甲方账户。验收合格之日起一年后无质量问题退还乙方，本项目质保期自双方签署验收报告之日起计算。

3.合同签订生效后，乙方向甲方提交合同金额 100%增值税普通发票，甲方在收到乙方相应发票后 30 个工作日内向乙方支付合同金额的 40%，即人民币 264400.00 元（大写：贰拾陆万肆仟肆佰元整)。

4.合同签订半年后，乙方向甲方提交合同金额的 40%收据，甲方在收到相应收据后 30 个工作日内向乙方支付合同金额 40%，即人民币 264400.00 元（大写：贰拾陆万肆仟肆佰元整)。

5.合同到期前一个月乙方向甲方提交全年安全服务维护报告后，乙方向甲方提交合同金额的 20%收据，甲方在收到相应收据后 30 个工作日内向乙方支付合同金额 20%，即人民币 132200.00 元（大写：壹拾叁万贰仟贰佰元整)。

6.转账信息

户名：新疆联盛科技有限公司

账号：3002012009024545547

开户行：中国工商银行股份有限公司乌鲁木齐人民路支行

如果乙方的上述账户资料发生变更，须提前 10 个工作日书面通知甲方，否则一切后果乙方承担。

四、货物包装与交付

1.货物的包装应适于长途运输和反复装卸，并且乙方应根据货物不同的特性和要求采取防潮、防雨、防锈、防震、防腐等保护措施，以保证货物安全无损地到达甲方指定地点。乙方将承担因包装不当导致交付的合同标的物受损的责任。

2.乙方在交付产品的同时需向甲方提供有关货物的附随资料，包括但不限于： 商品目录、安装图纸、使用明书、质量证明及其他技术资料。

3.交货期：成交通知书下发之日起 30 工作日内

交货方式：乙方承担一切运输费用，送达甲方指定地点。

收货人：李佳，联系方式：15009027373、收货地址：新疆维吾尔自治区哈密市伊州区东河区街道广场北路 18 号。

五、安装与验收

1.安装调试：乙方负责在甲方指定的时间内，按照甲方的要求完成货物的安装调试维护服务。乙方应严格遵守安全法律法规，采取安全保障措施，保证人员安全。因乙方原因造成的人员伤亡和财产损失，均由乙方承担。

2.验收标准：甲乙双方应按照甲方采购文件、乙方响应文件及产品需满足的国家标准、地方标准或行业标准的要求进行验收。

3.到货验收:甲方应在收到货物后 10 个工作日内进行到货验收。甲方仅对产品的数量和外观进行检验，并不因此减轻或免除乙方所应承担的质量保证责任。

4.最终验收：安装调测维护服务完毕后，乙方应配合甲方进行最终验收，验收结果以甲乙双方签署的验收证明为准。

六、保修与售后服务

1.货物硬件质保期为 3 年，运行维护服务提供 1 年服务。维护自到货最终验收合格之日起至质保期届满且经甲方确认无任何质量问题时止。

2.乙方承诺所售商品 自甲方收到商品之日起 10 日内可以无理由退货， 30 日内可以免费换货。更换后的货物质保期应重新计算。

3.质保期内，乙方应当提供 7×24 小时电话支持服务。乙方接到甲方保修通知后 1 个小时内响应，8 个小时内排除故障。对于质保期内不能修复的产品/部件，乙方应在 72 个小时内免费更换备品备件。

4.质保期届满后，乙方对本合同项下货物提供终身维修服务，且维修时只收取所需维修部件的成本费，服务内容应与质保期内的要求相一致。

七、知识产权及其他民事权利的保护

1.乙方保证向甲方交付的货物、软件、技术资料等，不会侵犯任何第三人的专利权、著作权、商标权、商业秘密、其他知识产权或者其他民事权利。如乙方违反上述规定，则乙方应负责消除甲方拥有并使用乙方交付的货物、软件、技术资料等所存在的全部法律障碍，并赔偿甲方的损失。

八、保密事项

1.乙方对在工作过程中接触到的甲方的任何资料、文件、数据（无论是书面的还是电子的）以及对为甲方服务形成的任何交付物，负有为甲方保密的责任。未经甲方同意，乙方不得以任何方式向任何第三方提供或透露。

2.甲方向乙方提供的任何资料、文件和信息，在乙方服务结束后，乙方均应及时归还甲方。

3.乙方人员违反上述保密规定，甲方有权解除合同。

4.其他未尽事宜按照双方签订的《哈密市中心医院信息系统安全服务保密协议》执行。

九、违约责任

1.甲方无正当理由逾期支付货款的，自逾期之日起，向乙方每日支付合同总价款的万分之二的违约金。

2.乙方未在规定时间内完成最终验收的，每逾期一日，应向甲方支付 500 元的违约金，逾期超过 7 日的，视为乙方不能交货，甲方有权单方面解除本合同并且要求乙方支付合同金额 20%的违约金。违约金不足以弥补甲方损失的，乙方应继续赔偿。

3.因乙方交付的货物存在质量问题，导致甲方或第三方受到损害的，由乙方承担赔偿责任，甲方因此遭受第三方索赔的，有权向乙方追偿。

4.乙方违反本合同和采购文件约定的有关质量保证及售后服务等的，每发生一次，乙方应向甲方支付 500 元违约金。如甲方通知乙方 3 日后仍未履行的，甲方有权委托第三方进行维修，所产生的费用由乙方承担。

十、法律适用与争议解决

1.本合同的订立、解释、履行及争议解决，均适用中华人民共和国法律。

2.本合同履行过程中发生争议的，甲乙双方应友好协商；协商不成的，任何一方可向甲方所在地人民法院起诉。诉讼产生的诉讼费、律师费、保全费、保全保险费等为实现债权产生的一切相关费用由违约方承担。

十一、合同生效及其他

1.本合同经甲乙双方签字并加盖公章或合同章后生效。合同内容如遇国家法律、法规及政策另有规定的，从其规定。

2.本合同一式五份，甲方执四份，乙方执一份，具有同等法律效力。

3.本合同后附《哈密市中心医院供应商廉洁承诺书》，乙方签字、盖章后作为本合同一部分。

4.本合同后附《附件一医院信息系统数据库运行维护服务内容》《附件二医院核心生产数据库异地灾备运维维护服务内容》《附件三医院云灾备边界防护技术参数》《附件四数据库、关键信息基础设施维护服务内容》作为本合同一部分。

5.其他未尽事宜，按照乙方投标文件执行。

（以下为签署页，无正文）

甲方（章）：哈密市中心医院	乙方（章）：新疆联盛科技有限公司
地址：哈密市伊州区广场北路 18 号	地址：乌市经济技术开发区凤凰山街 353 号
法定代表人或委托代理人（签章）：	法定代表人或委托代理人（签章）：
联系电话 0902-2265791	联系电话：0991-4503278
签订日期：2025 年 5 月 12 日	签订日期：2025 年 5 月 28 日

附件：

哈密市中心医院供应商廉洁承诺书

一、严格遵守国家相关法律法规、医院相关规章制度规定，做到诚实守信、廉洁购销、合规经营。

二、不将任何生产或者代理的产品在医院采购未完成前交科室进行临床试用或者使用。

三、不通过打招呼或者暗中授意等不正当手段竞标采购项目，不哄抬物价，牟取暴利，扰乱医院正常工作秩序。

四、严格管理好公司销售人员，不在采购、销售、使用等环节中进行商业贿赂。

五、不进入诊室、病区和库房，不向医院工作人员打听医疗用品进、销、存量和使用情况。

六、不向医院工作人员及其亲属赠送“红包”“回扣”及礼品、钱款、购物卡、有价证券和贵重礼品等，或给予其他不正当利益。

七、不得以回扣、宴请等方式影响医院工作人员采购或使用医药产品的选择权，不得在学术活动中提供旅游、超标准支付食宿费用。

八、以上承诺本公司将严格履行，如有违背以上承诺的行为，本公司自愿承担相应责任。

承诺企业代表签字：张宝林　　承诺企业盖章

附件一:医院信息系统数据库运行维护服务内容

1.对哈密市中心医院医院信息系统数据库进行例行巡检、维护、升级、优化等服务，保证各业务系统数据库运行稳定、正常。

2.对各业务系统数据库业务需求变更及异常情况进行及时响应，包括表空间扩容、数据库连接数调整、数据库等待事件优化、数据库死锁、资源优化分配等。

3.对哈密市中心医院数据库主机及配套底层硬件（存储、光纤交换机）进行维护管理：运行状态监控、性能调优、故障诊断及应急处理、操作疑难问题解答、安装调优迁移、应急演练等，为医院信息系统业务平稳、高效运行提供基础保障。

根据数据库系统点检规程，例行对数据库系统进行点检（包括：日志查看、双机运行状态、有无异常进程、性能健康表检查、系统资源状况汇总等工作），保证数据库系统处于正常工作状态，并填写各项点检表（根据具体数据库系统定制数据库点检记录表）。

根据备份点检规程，例行对数据库系统的数据备份进行点检，填写备份点检表；并对备份操作日志妥善记录保管，定期检查，确保备份日志记录完好。

根据常见故障处理手册，对定时作业没有执行成功等常见故障进行处理。

每月根据招标人指定时间由运维工程师对所有服务数据库系统形成月报，并对该月数据库运行情况进行汇总，内容包含：性能分析、趋势预测评估、发现和预测隐患、提出解决方案、优化建议、实施风险、是否实施、实施进度、实施结果。

【1】数据库基础运维

数据库系统运行基础巡检内容	
1	核查所有实例运行
2	核查 LISTENER 正常运行
3	核查可以成功连接数据库
4	核查可以成功备份数据库
5	核查存储资源有充足的可用空间
6	查看日志文件中出现的任何错误
7	查看 SQL*Net 日志中的错误信息
8	检查数据库进程数量
9	检查会话(Session)锁状态
10	检查不可用索引(UnusableIndex)
11	管理 FlashbackRecovery 区(10g、11g)
12	查看 CPU、内存、网络、磁盘的争用情况
13	检查定义在 DBMS_JOBS/DBMS_SCHEDULER 的 JOB 状态
14	识别空间受限对象(Space-BoundObjects)
15	检查分析性能数据 Workload profile\Database Hit Ratios (数据库命中率) \TOP SQLs

【2】数据库性能优化

数据库性能优化检查任务	
1	检查 Oracle 数据库性能
2	检查数据库的等待事件
3	Disk Read 最高的 SQL 语句的获取
4	查找前十条性能差的 SQL
5	等待时间最多的 5 个系统等待事件的获取
6	检查运行很久的 SQL
7	检查消耗 CPU 最高的进程

8	检查碎片程度高的表
9	检查表空间的 I/O 比例
10	检查文件系统的 I/O 比例
11	检查死锁及处理
12	检查数据库 CPU、I/O、内存性能
13	查看是否有僵死进程
14	检查行链接/迁移
15	定期做统计分析
16	检查缓冲区命中率
17	检查共享池命中率
18	检查排序区
19	检查日志缓冲区
20	性能调优及方法
21	system_Event 事件
22	session_Event 事件
23	session_Wait
24	寻找问题根源
25	应用优化
26	进程调优
27	I/O 优化
28	竞争优化
29	操作系统监控

【3】数据库备份恢复

数据库备份恢复任务	
1	检查 Oracle 数据库备份结果
2	检查数据库备份日志信息
3	检查 Backup 卷中文件产生的时间
4	检查 Oracle 用户的执行计划

附件二:医院核心生产数据库异地灾备运维维护服务内容

对医院核心生产数据库（HIS、PACS、LIS、EMR）异地灾备进行维护，维保内容包括：

1.每周对本地、异地灾备系统数据恢复、数据同步进行例行检查。

2.每月定期全面巡检本地、异地灾备系统数据库，巡检内容包含：数据库基本信息检查，数据库状态、监听状态、配置信息、空间使用等，数据恢复情况（SQLserver 数据库）、数据库同步情况（Oracle 数据库），日志传输、日志应用等信息。

3.为保障业务系统连续性、可用性，每年提供一次对医院核心生产数据库系统灾难或故障的应急演练服务。结合医院现状提供关键数据库故障业务连续性（应急）计划。提供灾备技术方案、现状及风险评估、演练操作文档、演练脚本及演练评估总结报告。

对于灾难损失的评估报告包含：

1）基础设施故障及损失：（具体故障、损失、恢复时间）

2）数据及应用系统故障及损失：（具体故障、损失、恢复时间）

3）业务系统故障及损失：（具体故障、损失、恢复时间）

需保证云灾备环境数据的在线实时同步，要求达到一旦主生产环境数据库故障无法修复时，可通过备库对主生产业务进行修复，并能够提供正常业务运行，保证数据的完整性。

- 总体要求

要求实现主备中心之间的数据实时应用，当生产系统发生严重故障或灾难时，无法再继续提供业务时可以及时启用数据库灾备系统，减少业务系统下线时间。并要求灾备中心数据库处于 Open 状态，可用于提供数据查询和统计报表功能。

- 功能要求

（1）可以满足用户的不同性能、数据保护要求，提供多种不同数据保护模式，可实现数据零丢失；

（2）可以实现一对多的数据复制，提供多重保护；

（3）灾备系统数据库可以在很短的时间内提升到生产状态。

（4）灾备库可修复主数据库由于硬件存储错误导致的数据文件坏块。

（5）数据同步应基于事务日志解析技术获取增量数据，不侵入源系统，不依赖触发器或时间戳字段，不对源库数据表进行扫描。同步时源库业务不能停止；表结构变化时 DDL 操作也可同步到灾备端；

（6）同步所有 DML、DDL 操作，支持同步数据库的各种数据类型字段，如：各种字符、数值、日期类型，Long、CLOB、BLOB、XMLType 等大对象类型以及 Oracle 数据库中的不可见列。

- 性能要求

（1）要求数据同步速度≥1GB 每小时，能够保持数据的实时同步

（2）对生产端和灾备端的 CPU、内存占有率较低，不影响业务系统性能

- 高可用要求

数据同步需要能支持数据库高可用集群，如源库 RAC 环境下单点故障支持自动切换到其它节点继续运行而无需重新初始化，也无需人工干预启动；

序号	数据同步检查任务
1	检查灾备服务进程状态
2	检查数据日志同步状态
3	检查数据增量同步情况
4	检查增量日志应用情况
5	检查主备库灾备配置参数
6	检查主备库网络传输状态，延时情况
7	主备库数据一致性、数据库比对

- 应急演练要求

对医院核心数据库进行备份数据的恢复性验证，一年一次的容灾接管演练服务。通过实战或模拟实战的方式，让整个组织和流程“活”起来，并且在演练过程中不断的根据实际情况和变化的环境进行优化，以实现真正的技术、管理、运营三管齐下，保障数据安全建设落到实处。

■ 数据安全自查服务

数据库运维人员需要帮助医院梳理清楚哪些 IT 资产和数据资产对外提供服务或者暴露，并进行周期性的更新。资产主要内容包括但不限于敏感数据分布、各种类型(结构化、非结构化、半结构化)的数据库、权限、账号等。

通过对数据安全风险的持续监控，实现对敏感数据和高风险活动，诸如数据异常访问和潜在的泄漏风险进行有效识别和监控，并提供修复建议。对安全事件的统计和稽核、数据流转的动态监测，包括但不限于:

数据安全风险事件监测:对外接口访问(高频访问、越权访问、接口未备案)、生产运维监测(异常操作、越权访问、高危操作)等。

数据安全事件统计与稽核:安全事件的分布和处置情况(事件来源分析、事件分布统计、事件发生趋势分析)等。

定期对 API 接口进行统计分析,了解 API 数据开放情况。提前对 API 接口中存在的风险进行检测，减少 API 接口中存在的风险暴露面，降低风险事件的发生对重要 API 接口、重点数据实施重点监控，一旦发现异常数据行为，及时告警，防止数据泄漏。

附件三:医院云灾备边界防护技术参数

加强医院云灾备边界安全防护能力，购置一台边界安全网关。对云灾备网络传输数据提供完整性、机密性保障。对医院信息系统数据库灾备网络提供入侵防御、病毒防护能力。

为提升医院云灾备专网边界防护能力，有效阻断网络攻击行为，提升医院核心生产端及云灾备端数据库安全防护，提供一台边界安全网关，边界安全网关需根据医院目前实际需求进行规划部署。确保部署后的安全防护满足用户实际云灾备网络安全防护需求。

指标	指标项	规格要求
设备规格要求	专用的硬件平台	采用专用 x86 多核架构，支持并配置双电源；
	知识产权	国产品牌，具备完整自主知识产权；
	产品形态	必须独立专业防火墙设备，非插卡式扩展的防火墙设备。
	硬件规格	内置硬盘 64G SSD
		内存 8G
		板载千兆电口/光口 8GE+2SFP+2SFP+
性能要求	基础性能要求	▲防火墙 UDP 吞吐量 64 字节小包≥ 6.5Gbps 1518 字节大包≥ 20Gbps
		每秒四层新建不少于 10 万/秒
	增强性能指标	并发会话数≥500 万
		在开启 IPS、AV、应用识别及行为管理的情况下，整机 HTTP 有效吞吐≥5G
		在开启 IPS、AV、应用识别及行为管理的情况下，每秒四层新建≥1.5 万/秒
功能要求	虚拟化	产品可以同时支持基于硬件 Hypervisor 技术的底层虚拟化技术（X86 平台）以及基于 VRF 的虚拟化技术。
		可以实现虚拟防火墙之间完全隔离，相互无干扰或影响，可独立升级软件版、独立重启或实现虚拟墙之间的 HA 部署。 每个虚拟防火墙均提供完整的安全功能，包括防火墙、入侵防御、防病毒、上网行为管理和流控、VPN、IPv4/IPv6 双栈等。 每台虚拟防火墙创建可限制新建、并发、吞吐、防火墙策略数量、NAT 规则数量、对象数量等关键参数。
	访问控制	支持策略自动生成，设备可根据通过网关的流量，选择自动生成地址对象、服务对象，并生成相关策略。
		支持流量获取功能，能够从指定的策略获取相关流量数据。
		支持流量筛选功能，指定源、目的地址范围、及协议对象筛选获取的流量，提供相关界面截图。
		可根据设置的替换条件，勾选聚合条件方式优化生成策略。
		支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略
		支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。
		支持策略预编译技术，访问控制策略数量增加，防火墙性能不受影响。
		支持路由、透明及混合部署模式
		支持常见 DOS 攻击防护及 ARP 攻击防护
		支持基于协议的长连接管理
	入侵防御	支持并开通网络入侵检测及防御功能，入侵防御事件库事件数量不少于 6000 条
		支持特征库分类，包含：命令执行、蠕虫病毒、木马后门、目录遍历、缓冲溢出、跨站攻击、SQL 注入、安全绕过、请求访问、DoS 攻击、信息泄露、漏洞扫描等类别。
		可基于 IP 地址、网段、用户、时间、VLAN、协议类型等条件设定入侵防御模块的检测事件及响应方式。
		▲支持 IPS 抓包取证，可选择将产生 IPS 事件的会话所有报文进行存储，并与 IPS 日志

		关联一键导出，提供相关界面截图。
		可以设置单包抓包及扩展抓包模式，可指定抓包时间。
		具备协议自动识别功能；支持自定义事件功能；
		支持对阻断时间的设置，支持只按照事件级别（严重、高级、中级、低级）执行更新，而非更新所有事件。
	防病毒	支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能；
		支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 200 万。
		防病毒功能开启后，整机处理性能衰减不超过 30%
	恶意文件检测	支持对恶意文件的检测，阻断、日志上报。支持手动添加恶意文件 hash。
		支持恶意文件库的自动升级和离线导入
		支持手工添加、删除恶意文件特征
	弱口令检查	支持对服务器、客户端进行的口令暴力破解的攻击防护；
		支持高、中、低三种密码检查强度。
		支持对常见应用（如 HTTP、Telnet、FTP、SMTP、POP3 等）进行弱口令检查，并上报安全事件。
		支持对口令频繁暴力破解的检测。检测到暴力破解后可选择告警、阻断访问、阻断源 ip 等动作。
	Web 应用防护	支持并开通 WEB 防护功能，支持对 100 个站点制订 Web 应用防护策略；
		支持 HTTP 协议合规检查，需包含对 HTTP 各类方法（至少包含 GET、POST、HEAD、PUT、DELETE、CONNECT、TRACE、PATCH 等）、HTTP 协议版本号（至少包含 HTTP/2、HTTP/2.0、HTTP/1.1、HTTP/1.0 等）、Content-type、Content-type 字符集、文件名后缀、HTTP 请求头的检查，并可设置：请求参数的最大个数、请求参数名的最大长度、请求参数值的最大长度、请求参数值的总长度、单次上传文件的总大小、上传的所有文件的总大小的相关参数。
		支持 HTTP 请求、回应的头、体检查；
		支持自定义 WEB 安全防护事件，支持自定义检查字段（至少包含请求 URL 关键字、请求包含内容关键字、请求文件类型、请求方法、请求头部、请求参数名、请求包敏感词、Cookie、响应包关键字等），支持正则匹配，并可采用多重解码类型（至少包含 BASE64 解码、16 进制解码、HTML 解码、URL 解码、字母小写化）等进行灵活组合生成策略。
		支持检测 WEB 攻击事件，包括：SQL 注入，XSS 跨站脚本攻击，PHP 代码注入，WEBSHELL 攻击、信息泄漏等问题；
		支持独立的 WEB 特征库，不少于 1400 条，并可以自动、手工升级；提供相关界面截图
	SSL 流量解密	支持 SSL 加密流量的全面安全防护，对通过设备的 SSL 流量进行解密，并综合运用 IPS、防病毒等安全防护避免加密流量攻击，支持代理模式和透明模式两种组网；并支持客户端模式（由内向外）和服务器模式（从外到内）两种模式
		支持对 HTTS、POP3S、SMTPS、IMAPS 等应用协议进行解密过滤，提供相关界面截图
		可通过匹配源地址、URL 分类、域名做解密策略，
		支持浏览器证书主动推送
	IOT 资产防护	支持通过主动及被动探测方式，自动识别多家主流厂商（至少包含：启明星辰、网域星云、深信服、天融信、山石网科、海康威视、浙江大华、HP、爱立信、锐捷、H3C 等）的多种多种终端类型（至少包括：PC、网络打印机、网络摄像机、考勤机、串口服务器、网络电话、网络设备、防火墙、负载均衡等）。
		资产相关信息（至少包含：MAC、OS、类别、厂商、TCP 端口、指纹信息）发生变化时，能够自动产生报警。
		支持资产异常时自动从网络中隔离，避免异常资产访问网络，支持异常资产相关信息恢复后，能够自动恢复对网络的访问功能。

		支持手动设置以及一键生成资产黑名单，支持手动设置以及一键生成资产 mac 地址绑定表
		支持通过与交换机获取交换机下游资产 mac 地址列表
		超过 2000 种预定义设备指纹，可手工升级，支持自定义指纹添加，并支持根据实时扫描结果一键生成自定义指纹
		支持资产画像，展示资产的名称、IP、MAC 地址、TCP/UDP 开放端口、OS、生产厂商以及类别、指纹信息等，并可通过资产的连接关系、应用、应用流量、并发连接数等的图形化展示，
		支持对资产的行为学习，自动学习资产相关的流量以及网络连接关系，通过连接关系拓扑可以进行阻断、一键生成安全策略操作，
	威胁情报	支持对经过设备访问的域名以及目的 ip 进行威胁情报查询，如果查询威胁访问，支持告警、阻断等动作。支持根据情报的威胁值、信誉值、威胁类型等进行处置判定。
		威胁情报来源支持离线库和云查两种，本地离线库规模为 50W 条，本地查询未命中将通过云查方式继续查询。离线库支持定期自动更新。
		威胁情报支持勒索软件、挖矿软件、网银木马、窃密木马、黑客工具、后门软件、僵尸网络、蠕虫网络、APT 攻击等几十种分类
		支持对命中情报事件进行列表展示，并在整机威胁图表中展示相关内容
		支持对恶意文件的检测，阻断、日志上报。支持手动添加恶意文件 hash。
	行为管理及流量控制	支持并开通基于 DPI 和 DFI 技术的应用特征识别及行为控制，应用识别的种类不少于 1000 种
		支持并开通基于 URL 分类库的 WEB 访问管理，URL 分类库规模不少于 20 万条
		支持并开通基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套的流控界面截图。
		支持基于接口的上下行带宽管理
		支持高、中、低优先级通道设置
		支持基于应用、用户、源地址、目标地址、服务、时间的通道匹配
		支持带宽限制、带宽保障和弹性带宽
	网络特性	支持静态路由、动态路由（RIP、OSPF、BGP4）。
		支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。
		支持并开通链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法。
		支持并开通 IPSec VPN 和 L2TP VPN，投标产品实配 IPSec VPN 隧道数量不少于 2000 条
		支持并开通 SSL VPN 功能，投标产品实配 SSL VPN 并发用户数不少于 1000 个。
		支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查。
		支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT
		支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323、SQL * NET
		支持标准 DHCP 服务功能，支持 DHCP 条件下的 IP/MAC 绑定及 IP 地址排除等功能。
		支持 DNS 透明代理功能，可将指定范围内的 DNS 请求自动重定向至管理员指定的 DNS 服务器，且支持多台 DNS 服务器的负载均衡。 需提供需提供具备中国 CNAS 认证的第三方测评机构出具的测试报告，证明其投标型号支持 DNS 透明代理功能
		支持标准 DNS 服务器功能，支持多种 DNS 记录，包括 A，NS，CNMAE，TXT，MX，PTR 记录。
	SD-WAN	▲免费提供 SD-WAN 功能授权，支持两个节点或多个节点之间的加密通道互联部署，替换传统 IPSEC 组网方式。适配医院现有边界安全网关 SD-WAN 互联接入，为云灾备网络传输数据提供完整性、机密性保护。
		支持基于入接口、源地址、目标地址、服务端口、用户、应用、域名、时间的选路策略，并可支持最小延迟、最小抖动、最小丢包率、链路复制、轮询、加权轮询、源 IP 哈希、源 IP 及端口哈希的负载均衡算法。

		支持对链路质量的健康检查，可设置探测周期、探测间隔、重试次数、超时时间、抖动阈值、丢包阈值、延时阈值，探测对象可选择 IP 及域名地址。
		支持双边链路质量优化，支持对称模式部署，在链路存在丢包、延迟、抖动等因素时，通过专有的协议隧道模式，封装用户应用，并改善网络环境中的应用性能解决数据丢包、延迟等问题。
		支持链路复制技术，针对核心业务如“视频”，提供多路复制，单路收发功能，在多条链路间实现业务无缝切换
		支持链路扩容技术，实现一个 session 在多条链路上同时传输，充分利用带宽。
		支持 HTTP 压缩功能，采用工业标准的 GZIP 或 Deflate 算法来压缩 HTTP 数据，从而减少传输数据量并降低带宽消耗，缩短客户端访问的下载等待时间。
	高可用性	支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。
		支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑
		支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断
		支持双路 HA 物理心跳线，确保 HA 运行稳定可靠
		支持 HA 设备之间的配置自动同步，确保用户只需在一台设备进行业务配置
	系统管理	支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置
		支持 SYSLOG 和 SNMP v3，SYSLOG 日志支持同时发给多个日志服务器
		支持威胁可视化技术和流量可视化技术，可提供详细的分析展示图表。
		支持整机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的 TOP10 统计展示、基于具体威胁事件/威胁类型的 TOP10 统计展示等，统计展示的时间周期包括 1 小时/1 天/7 天/30 天。
		支持基于流量的 TOP100 用户和 TOP100 应用的流量曲线图，流量曲线图的统计周期包括小时、天、7 天和 30 天。
		支持基于并发会话数量的 TOP100 用户和 TOP100 应用的并发数量曲线图，并发数量曲线图的统计周期包括小时、天、7 天和 30 天。
统一管控要求	边界安全设备统一管理平台适配	为实现院区边界安全设备统一管理，批量版本升级、安全策略一键下发以及网络状况及威胁集中监控，本次提供边界安全设备需适配医院现有安全集中控制器。

附件四:数据库、关键信息基础设施维护服务内容

对医院信息系统、数据库配套软、硬件关键信息基础设施进行运维工作。

1.建立和维护软、硬件关键信息基础设施(虚拟化、服务器、存储、网络)配置信息库。

2.负责软、硬件关键信息基础设施(虚拟化、服务器、存储、网络)运行状态、性能状态、资源使用情况等健康检查。

3.负责软、硬件关键信息基础设施(虚拟化、服务器、存储、网络)故障处理工作，包括故障发现、故障隐患排查、故障处理等。

4.虚拟化平台的安装、调整、加固和备份等日常维护工作；负责制作虚拟机模板机；根据资源申请，创建、调整、回收虚拟机。负责对所有业务系统虚拟机进行维护。

5.Windows、Linux 及国产操作系统的安装、优化及安全加固。负责对物理机、虚拟化上的操作系统进行维护。

■ **基础服务**

负责建立和维护软、硬件关键信息基础设施（虚拟化、服务器、存储、网络）配置信息库。

负责软、硬件关键信息基础设施（虚拟化、服务器、存储、网络）监控，包括监控运行状态、性能状态、资源使用情况等

开展所有软、硬件关键信息基础设施（虚拟化、服务器、存储、网络）健康检查，包括资源配置情况检查、性能状况检查、备份执行情况检查等。

负责所有软、硬件关键信息基础设施（虚拟化、服务器、存储、网络）故障处理工作，包括故障发现、故障隐患排查、故障处理等。

每月提供一次巡检服务，出具巡检报告。

按需对现有软件进行配置调整，负责各类技术配置文档管理，包括所有软件的各类配置文档，操作变更记录等。

■ **业务系统支撑服务**

1. 虚拟化平台

负责虚拟化平台的安装、调整、加固和备份等日常维护工作；负责制作虚拟机模板机；根据资源申请，创建、调整、回收虚拟机。负责对所有业务系统虚拟机进行维护。

2. 操作系统

负责 Windows、Linux 及国产操作系统的安装、优化、及安全加固。负责对物理机上的操作系统进行维护。

3. 数据库软件

负责 Oracle、SQL Server 等数据库的安装、维护、备份恢复、灾备演练、数据共享等服务；协助做好 Oceanbase 等国产数据库的安装、信创测试等服务。

■ **相关硬件故障技术协助服务**

硬件巡检包括对服务器、存储系统的指示灯状态、部件工作状况、网络线路连接等情况进行常规巡检，主要检查是否有部件出现故障或可能出现故障，并对设备进行故障前检查。对故障前和故障的设备配件进行及时更换。更换配件如需停止运行相关设备需与招标方负责人沟通设备停机时间。设备需在招标方要求的时间内完成故障配件的更换并保障招标方相关系统的正常运行。

在巡检过程中如设备配件出现故障投标人会对故障配件做如下处理：

（1）质保内设备：如设备配件发生故障该设备在厂商质保期内投标人会与原厂商售后服务机构联系配合原厂商售后服务人员对设备做相关检测并与招标方协调设备是否需要停机及停机时间以配合原厂商售后服务人员更换相关故障配件，保障设备的正常运行；

（2）质保外设备：设备已达到原厂商质保年限，投标人工程师在巡检过程中如果发现设备配件发生故障，投标人工程师将设备故障信息及时告知招标方负责人，由招标方另行购买硬件备件，更换备件时，投标人将协助配合备件更换时间及设备停机时间，以保障招标方业务的正常运行；