

合同包一：2025 年业务上云及弱电运维服务项目

一、业务上云服务

序号	服务名称	技术标准	数量	单位
1	适应医院整体化信息要求	详见附件 1	1	项
2	运营商专线要求	详见附件 2	1	项
3	人员配备要求	详见附件 3	1	项
4	云机房资源租用及安全服务要求	详见附件 4	1	项
5	医院网络资源服务（互联网、医院外网官网）等业务云资源服务	详见附件 5	1	项

附件 1：适应医院整体化信息要求

序号	具体技术（参数）要求		服务期限
1	基础设施运维	对不同专线接入云资源、链路及相关设备进行运维。	一年
2	容灾备份中心建设服务	对容灾机房设备及环境进行运维（不包含设备及软件更新、设备及软件重新购置等）。对云业务部署的数据中心与内蒙古中医医院数据中心形成的同城灾备进行运维，保证关键业务能够在中医院现有的数据中心正常接管运行。	
3	容灾备份要求	提供 7×24 小时容灾备份技术支持和故障维护服务，确保备份的完整性，一旦发生业务、设	

		备、线路、故障或平台故障，及时恢复备业务及平台运行。故障恢复时间不大于 180 分钟。
4	数据安全实施服务	上云的核心虚拟机进行秒级别数据保护，且具备根据用户要求恢复虚拟机的数据的服务。通过专线还可以将云上的数据备份到用户本地。并提供技术方案。提供技术方案证明，需具备基于现有环境，检查现有业务的数据安全现状，生成检查报告，并设计、规划、本异地可行的备份方案。
5	业务资源调配服务	采购人具有宿主机控制权限。虚拟机的 CPU、内存、硬盘大小等资源可以根据采购人需求调配（36c/448G/296T 资源可由实际需求进行自由调配）。调配后对虚拟机业务的影响时间范围为 0 到 5 分钟。
6	云兼容性服务	要求兼容主流虚拟化厂商。能跨云平移虚拟机
7	云安全及云网络服务	中标方能够对虚拟机的操作系统进行维护，包括系统级别的安全、配置和软件包更新。中标方能够根据采购人需求对网络进行调整，包括进行端口级映射，ACL 调整等。可以根据用户需求对资源的配比进行调整，对虚拟机资源调度进行整合等，协助云上应用的部署工作等。
8	技术对接服务	能够实现专属云平台与采购人网络中心私有云平台的平滑对接，对接后可以实现跨三层网络虚拟机迁移而业务不受影响，真正实现自由上云，自由下云，并可以提供详细的技术实现方案。
9	网络安全	提供 IPS, IDS, DDOS, WAF 等网络安全设备进行上云虚拟机的必要防护，同网段虚拟机之间需要通过云安全软件进行安全隔离避免虚拟机之间的相互攻击。并提供技术方案。
10	云资源的运维运营服务	针对我院现有在运行全部业务系统进行运维，并与本地容灾机房实现高可用保障。
11	运维成本分析服务	实时、动态分析当前资源占用及配比，针对云上资源运行成本进行分析及优化。
12	资产管理服务	需提供不少于 1 次全面的准备及工作调整，提升快速适应资产、威胁及脆弱性动态变化的能力，具备第一时间应急止损的能力。

13		<p>针对医院指定的重要业务系统，根据每个应用系统实际部署情况，提供符合每个应用系统情况的资产管理、运维事件、安全事件、拓扑图、技术指标监控、自动化巡检、应用档案、应用探针实施运维运营服务；提供应用系统用户授权管理，提供每个被纳管的业务系统分别进行授权的能力，可以通过用户权限管理为业务部门、外包外协等用户提供多级授权机制，以满足业务部门、外包单位日常工作需要；提供监控一张图看板调研和制作服务，为每一个应用系统单独梳理和实施并展示。一张图中应该包括：软硬件监控指标、软件运行 kpi 指标、关键业务数据、常态化安全巡检等内容。一张图应该同时制作和提供拓扑图和详细指标看板两种形式供业务部门和相关厂商运维人员使用；</p>
14	应用系统监控和看板	<p>监控一张图看板能够提供多种可编排组件来进行看板制作，组件包括图表组件、统计组件、表格组件、测量组件、文本组件、热力图等组件，最后可以通过可视化配置工具配置完成。实施人员能够通过标准的查询语言以自定义方式将数据展示在组件中，通过拖拽，灵活布局组件的方式配置看板，以使用户和维护人员随时通过可视化配置功能进行调整。为保证工期和降低后期成本，不接受通过二次定制开发方式进行指标扩展。</p>
15		<p>要求提供不低于 50 种常用软件探针清单，要求探针可以独立部署。探针需包括：常见操作系统>3 种、常见数据库>5 种、常见 NOSQL>10 种、常见消息中间件>5 种、常见大数据平台、常见云平台、常见应用服务器、JVM、Docker、K8S、容器云、nvidia gpu 等，并且要求提供 SNMP、IPMI、RedFish 探针，以满足医院要求；提供应用拓扑图绘制服务，绘制好的拓扑图允许用户自行修改，支持将中间件、数据库、网络设备、服务器设备、安全事件、用户体验感知设备、外部接口等涉及应用系统相关的元素通过配置整合到应用拓扑中，并可以为每个元素自定义指标。指标需支持纯文本、进度条，连接线需支持实线、虚线、动画，动画速度可根据线条属性的数值进行动态变化。</p>

16		提供应用系统日志实时分析服务，在不收集日志的前提下，对分布式应用各个位置的业务日志、错误日志进行实时分析，从日志内的指定事件产生到在监控看板上体现、并形成告警的事件，整个过程应小于 60 秒；提供应用系统与流程引擎的结合能力，为应用系统提供配置流程服务；提供资产应用系统综合大屏开发服务，包括：接入应用数量、纳管资产数量、巡检设备情况、事件告警情况、应用系统运行情况、24 小时动态、应用系统出口流量、用户体验统计。
17	运维和安全事件集成服务	提供集中化的事件中心开发集成服务，提供集中处置运维事件和安全事件服务。要求能够集成第三方网管工具、应用监控工具、安全态势感知、漏洞扫描、堡垒机、虚拟化云平台等系统的安全告警、运维事件，以实现事件集成和集中处置。
18		提供事件等级定义服务，根据管理需要协助医院进行运维事件等级分类管理，并集成来自不同平台的告警事件自动归集到同等级事件中；提供事件超时自动关闭功能，可配置事件超时规则，系统能够根据超时规则自动关闭过期事件，减少运维人员工作量；提供安全和运维事件全生命周期日志，包括事件的产生、规则匹配情况、自动或人工处置记录、事件关闭等全过程信息的审计；
19		提供事件处置规则引擎，根据事件标签定义对事件自动匹配，并可设定规则有效期、消息模板、优先级，同时支持电话外呼、自动派工单；提供事件消息模板自定义功能，包括：信息模板、电话模板，模板中的标题、接收人、内容均需要支持宏定义能力。
20		提供智能告警规则配置，根据业务需要，进行告警规则合并和抑制；抑制指标的偶发性波动；一个故障原因导致的多设备和系统故障，只报源头；关联性故障，可以只报源头，也可以回溯告警；系统维护期间，可以设置静默时间段，不告警。
21		提供短信、电话、微信、企业微信、钉钉等多种方式的告警通知能力；需要支持根据事件规则，触发不同类型的流程工单、工单标题需要支持宏定义，可将多个告警标签组合作为工单标题，以便接单人通过工单标题快速了解问题；提供告警事件关联资产、应用

		的功能，事件能够自动归集到资产和系统档案中，便于业务人员查看和处理。
22	CMDB 资产梳理服务	提供 IT 资产 CMDB 数据库梳理服务，能够提供自定义资产大小类别定义，可根据实际情况设置资产的大小类别，提供资产类别关联资产属性模板，以实现资产属性的灵活定义。
23		资产模板需通过可视化的方式进行配置，以满足资产精细化管理，可视化属性设计器需要支持：单行文本、多行文本、日期控件、时间控件、下拉控件、文本描述、表格控件，控件属性需支持：控件默认值、是否必填项、数据格式、验证规则、长度等。
24		资产小类提供状态监测通用规则，通过输入规则，来展示资产的在线情况、存活状态等，监测规则需要支持宏定义；提供资产的新增、删除、编辑、复制、拆分、导入、导出、脱保统计、报废统计、使用年限统计功能；提供基于 PN 码的产品库，用于资产快速录入，通过输入 PN 码，快速获取资产详细信息，并可更新 PN 产品库。
25		提供多维度资产管理视图，可通过商务维度、位置维度、网络维度进行维护管理资产，并提供卡片&列表多种展现形式；提供告警事件、安全风险、资产档案、点巡检、自动巡检等资产数据聚合，在资产视图可以直观的查看围绕资产的相关信息；
26		提供资产与安全态势感知、杀毒软件等系统对接，并在资产管理界面展示相关数据；提供资产与流程引擎的结合能力，可以为每一类资产配置多类流程；提供资产展示大屏，包括：仅 30 天事件趋势、仅 30 天事件等级、资产分类统计、未关闭事件、目前告警资产、资产等级占比等。
27	自动化运维服务	针对医院指定的重要业务系统，提供自动化运维实施服务，并提供服务有效期内的无限次自动化运维脚本维护服务。要求运维脚本能够基于系统的脚本模板管理功能，能同时支持 ssh、stfp、winrm 多种管理协议。支持在一个任务模版中不同协议的多段脚本混合定义，脚本段执行顺序可定义。提供脚本执行超时定义及采集行数的配置功能。

28		提供模板管理功能，模板支持版本管理，可通过历史版本进行切换版本，并提供发布模板、禁用模板、导入模板、导出模板；为保证自动化脚本运行的安全性，需对脚本模板、自动化作业数据进行加密和数字签名，防伪造、防篡改。要求使用国密算法进行加密和数字签名；提供任务管理模块，通过任务关联模板可进行设备的自动化运维，任务需支持是否对比基线类型，支持自动告警功能，并可设置任务执行周期。
29		提供任务队列查看，可查看当前队列中所有任务，对于未执行的任务，可进行暂停、重启操作，并可追踪历史任务；提供配置文件基线监测、操作系统安全基线自动核查、虚拟机环境准备、上线前自动化检查、数据库备份检查等多种自动化巡检功能，支持通过规则进行按分钟、小时、天等多种周期的监测；提供基线文件的在线对比功能，支持文本对比、时间对比、MD5 对比，将文件差异以颜色标注，支持将新配置文件的版本设为基线。
30		引擎和管理平台需要分离部署，集群化部署，满足高可用和负载均衡需求。提供以应用系统维度查看自动化巡检任务的视图，在应用系统中仅看涉及本系统的所有巡检情况，并直观的显示出所有巡检任务、所有被巡检设备及每个设备的巡检统计情况。
31	人工巡检和 标准化作业 书管理	提供基于精益管理 TPM 模型的人工每日巡检、周期点检、精密点检管理服务，并记录巡检结果及处理结果；支持通过流程引擎自定义每日巡检单、可自行配置，并可设置不同审批环节，以适用于不同场景；巡检单支持自动引用系统中的资产数据，并可以将巡检过程中的异常资产数据自动归集至资产病历卡中。
32		周期点检提供：每周一次、每月一次、每年一次年度报告三种点检周期，并可自行设定具体月份，系统根据周期自动形成点检计划，并记录巡检结果及处理结果；周期点检可设置：点检方案、点检路线、被点资产、所属合同，可根据资产类型添加标准化作业书，可按照项目、部门进行逐项检查，并支持一键检查；周期点检、精密点检需按照遵

		循 TPM 精益管理八定原则，点检方法需要在 5S 标准进行设置。
33	等级保护工作管理服务	根据等保安全法，系统需内置提供 1-5 级等保测评指标，并根据管理要求、技术要求、控制点、分类展示详细指标项，包括：测评标准、测评对象、判定条件、是否高风险项、权重、参考文件；提供应用系统等保自评功能，通过选择应用系统、安全等级，自动拉取测评项，并可以自行增加测评项；支持测评项分配责任人，责任人可通过工作台进入测评，附入佐证材料、流程、文档，并选择测评结论，结论包括：满足、部分满足、不满足、不适用，每项结论均影响测评分数。
34		提供安全等保测评分数计算，通过安全等保测评评分标准及公式，最终得出测评分，便于进行针对性的安全保障；支持以应用系统维度查看等保测评任务，可根据安全管理、安全管理人员、安全运维管理、安全管理机构、安全管理制度、安全区域边界、安全计算环境、安全通讯网络、安全物理环境、安全管理中心进行过滤显示。
35	信息化管理流程实施服务	要求使用 WEB 方式、面向业务人员的可视化、拖拽式、所见即所得的表单设计器，无需安装专用设计工具或插件。支持原有纸质 A3/A4 / 自定义三种格式选择，可手动调整表单的宽度和高度来制作各种样式的文档，100%还原纸张大小，支持高保真还原表格，可生成正式制式标准文档。表单设计器能够使用表单控件快速编辑生成各类简单或复杂的表单，满足不同业务的需要。支持从 Word、Excel 中复制已经设计好的页面，只需把表单控件放置在对应填表位置上即可。支持 HTML 代码方式，提供高级用户对表单页面的全面控制支持；表单设计器需同时提供两种不同类型的设计器，方便普通业务人员使用的无格式互联网化的流式表单设计器和模拟纸质样式、打印格式良好的复杂表单设计器。
36		表单设计器要求提供单行文本、多行文本、附件控件、头像控件、单选框组、多选框组、下拉菜单、超链接控件、签章控件、位

	置坐标、富文本编辑器等标准控件，支持多维度人员选择控件、多维度组织机构选择控件、编号控件、二维码控件、图片验证码控件、文件编辑控件等特殊控件；还需要提供自定义表单业务控件功能，在预定义控件时可以配置数据源，并通过分配业务控件权限的形式达到数据源隔离的目的。
37	要求具备“表单多行”控件，即能够在表单列上动态添加或删除单行文本、多行文本、下拉选择框、日期时间、附件、组织机构等多种类型控件用于加载行列数不固定的动态数据，所有表单列字段均应支持可视化数据源联动；要求控件支持可视化数据源联动与控件联动配置，通过一个控件赋予的值，来联动其他控件；
38	流程引擎需支持顺序审批、并行审批、组合审批等多种流程模式；应支持简单条件分支、复杂条件分支、多重分支组合条件分支；提供多人并行审批、并行审批竞争和多人全部处理等流转控制；支持抄送、转发、撤销、附入新流程；支持流程环节指定办理人处理、全部人员审批才可通过及任意一人审批即可通过、退回、取回（允许审批后取回）、接收办理消息、中止、终止、终止重发，流程环节知会人员（审批前知会、审批后知会），流程催办、转办（多级转办）、续办、加签、委托代理等高级业务处理功能；流程引擎支持可选择退回到发起人、退回到上一环节、退回到指定环节三种退回方式。退回到发起人是发起后退回后可以修改表单，修改附件，重新提交。系统可配置退回后重新提交是按流程固定顺序重新流转，还是可以直接提交到上次退回的环节，直接审批通过；退回到上一环节是指只允许退回到已审批通过的上一环节重新审批或发起；退回到指定环节是指退回到已审批通过的任意环节重新审批或发起；流程引擎需支持环节超时设置功能，启用超时设置后，能够设定流程环节最大办理时限，超时未办理可自动给流程环节办理人发送超时消息提醒。超时提醒可设定消息提醒上限、消息提醒频率、提醒时间范围，以及周末是否免发消息提醒；

39		<p>流程节点应支持自动审批，当某节点办理时间超过预设时长后，自动触发办理事件并将本次处理类型标记为超时自动处理。流程节点还可以设置完成权限，拥有完成权限的工作人员可以直接完成该流程，流程将不再进行后续环节，并视为该流程已办结；支持通过可视化配置方式实现表单数据自动采集入库，要求系统能够在流程处理中的任意环节配置采集规则、执行数据采集。支持将表单数据采集到关系型数据库，支持插入式采集、更新式采集（根据关键字更新部分数据字段）或插入更新式采集（存在则更新，不存在则插入），支持将同一个表单数据同时采集到多张表（支持主从表）中；</p>
40		<p>提供数据采集过程的异常监控和处理功能，可全程监控数据采集过程中的异常或警告，并自动添加在异常日志队列中。对日志记录中因采集规则配置不当导致采集失败的可进行单独的人工干预重采、也可将同一批次的异常数据批量执行重采，直至所有数据采集成功；发出警告的表单数据可正常采集入库。管理员可以监管流程使用情况，监测流程事项的发起情况，流程服务的频次，时长，效率等流程汇总信息，出现异常的流程将自动提醒管理员，管理员可直接进行人工介入干预流程。</p>
41	自动拨测探针	<p>提供和软件系统配套的硬件拨测探针设备，以满足医院内多位置、多协议、多节点，基于专用硬件设备的自动化拨测功能。拨测需支持 ICMP\TCP\HTTP 协议，并且可以根据业务需要随时扩展。要求提供通过脚本配置，进行模拟登录后对需要认证的业务页面进行拨测的能力；拨测设备要求$\geq 2\text{GB}$ 内存、不低于 64 位双核 CPU、双千兆以太网端口，支持远程管理；服务期内，提供只换不修服务。</p>
42	自动拨测服务	<p>要求针对每个需要拨测的业务系统提供实时统计图，图表内容包括：http 连接时间、服务器处理时间、http 解析时间、tls 连接时间、http 传输时间；提供统计百分位图，包括 p99、p95、p90、p75、p50，直观的查看用户体验效果，并支持去除超时等异常数据；提供拨测数据包括：平均耗时、最小耗时、最大耗时、标准差等数据，便于观测数据。</p>

43		对分布在医院各处的硬件探针，进行拨测作业自动下发，无需在探针上自行设置，以便随时对拨测作业进行调整和增加。提供在业务系统管理界面中的用户自定义体验感知配置功能，可进行指定业务系统的探测指标、协议类型、数值阈值颜色自定义等设置。
44	运维工具软件要求	运维工具软件需要同时提供 PC、微信、企业微信、医院自用 APP 等多种方式提供业务访问；负载均衡集群；运维工具软件要求支持基于负载均衡技术的多活集群技术，能够通过简单增加服务器（虚拟机）方式进行业务并发能力的扩展和高可用（高可用，即所有业务节点都可以同时工作，任何一个节点出现故障均不会停止服务），要求具备集群令牌、集群缓存功能。
45		大数据存储和 TSDB 数据库要求：运维工具软件使用大数据分布式存储技术和专业 TSDB 来提供海量运维数据的高速分布式存储和访问。
46		工作条件要求：软件应是一个开放的且符合业界技术标准的系统平台；支持在 Window、UNIX、Linux 或同等及以上档次操作系统上部署；要求使用全文检索技术提供知识库、要求使用专业时序数据库 TSDB 保存时序数据。考虑到运维大数据保存和分析需要，拒绝使用关系数据库保存时序数据的产品。软件使用的应用服务器，支持 Tomcat、Weblogic 等中间件。架构要求采用 B/S 架构模式，通过浏览器能稳定可靠使用。能够兼容常用的浏览器；各浏览器访问前后台功能均无需安装任何插件。本项目，无论用户使用 PC、APP、微信企业号、钉钉，均提供无限系统用户数、网元设备数量以及流程许可限制。开发能力要求：平台应遵循 OAuth2.0 标准，为用户以及第三方提供基于 RestFul 方式的数据接口、所有业务数据等开放 WEB Services 服务，第三方可以使用 Java、PHP、.NET、Python 等语言开发应用；要求平台提供 SDK 接口和二次开发手册，满足第三方扩展功能的需要。
47		安全要求：数据传输安全，支持高安全的 SSL(Secure Sockets Layer 安全套接层)/TLS(Transport Layer Security 传输层安全)协议。其他要求：本次服务涉及到产品

		和服务，均需提供无限制系统用户数、网元设备数。	
--	--	-------------------------	--

附件 2：运营商专线要求

序号	具体技术（参数）要求		服务期限
1	专 线 提 供 服 务	需满足全部主流运营商互联网、专线、裸光纤、接入路由空间，满足未来的网络连接。云部署的物理机房通过 2 条裸光纤分别以不同路径的物理路由连接医院机房两台核心交换机上，两条裸光纤互为主备、相互负载，在满足医院对网路链路需求的同时，实施网络组件和路径冗余，以支持可用性和负载分配，避免单点故障，提高链路的高可靠性和利用效率。通过防火墙实现逻辑区域隔离，应该按照流量类型对网络流量进行逻辑分离，将内部网络划分为业务网络、存储网络、管理网络，加强云平台内部网络的安全性，数据链路延时≤10 毫秒，主用链路为裸光纤。裸光纤带宽为 1G、2G 各一条。	一年

附件 3：人员配备要求

序号	具体技术（参数）要求		服务期限
1	驻场运维人员运维工作要求	<p>1. 在我院主要领导的具体指导下，承担网络机房运维日常工作安排部署，相关技术方案制定，网络规划及地址分配，设备日常巡检及安全服务巡检和更新维修以及协助院机关各业务处室的部分技术支撑工作；</p> <p>2. 承担互联网规划、局域网网络拓扑结构变动和调整，结合在用信息系统需求，提出网络系统硬件的基本选型、配置要求，提供网络所需的相关应用服务、映射地址、端口号、公网地址等。</p> <p>3. 承担部分核心交换机、楼层交换机、磁盘阵列、数据备份、防火墙、路由器等常用设备的管理及日常配置。</p> <p>4. 积极与运营商沟通，做好管理本单位租用的互联网 IP 地址网段，并数量掌握地址分配情况。</p> <p>5. 承担与自治区卫健委管理部门积极沟通，定期核查委机关在用信息系统外网 IP 地址使用情况。</p> <p>6. 协助办公室做好终端设备的安全自查和日常维护。</p> <p>7. 指导驻场运维服务人员的日常管理和调配，每日查看网络的运行使用状况，做到发现问题，适时处置并及时报告。</p> <p>8. 接受中心领导指派的其他工作任务。</p> <p>9. 服务级别：7*24 小时驻场技术服务。提供不低于 4 名工程师驻场技术服务（为保障驻场运维工程师办公需求，办公场地由采购人提供）；另组建不低于 20 名工程师的技术服务团队，其中包括 1 名项目负责人及 19 名一、二线工程师；另提供不低于 10 名三线专家服务团队提供远程服务。</p>	一年
2	服务报告	需提供 ≥ 1 次总结业务运行和服务约定履约情况，提出风险预报、整改方案及未来优化方向。服务次数： ≥ 1 次	
3	知识库	需以用户为单位建立专属知识库、由现场人员进行知识库维护，二线专家团队进行内容审核，下设客户现场各类型常见故障处理流程及方案，故障发生后 2 小时内极速处理。亦可确保发生人员变动可在 3 天内快速进入角色。	
4	培训服务	需提供 ≥ 2 次向用户提供培训服务，由资深技术专家培训与客户业务相关技术，与维保设备服务方设备运行特性、日常设备维护技巧，常见设备故障处理、关键设备性能。	

5	基础架构优化服务	需解决不同厂商设备互通时的异构问题以及不同的服务提供商之间的配置差异问题，以提高运维效率，降低配置不规范引发的设备运行风险，减轻运维工作量，提升工作效率，确保业务系统稳定运行，制订统一规划提供储备。
6	数据库性能优化服务	需通过数据库自带或三方工具综合分析数据库运行情况。找出性能瓶颈，提供相应的优化服务方案。

附件 4：云机房资源租用及安全服务要求

序号	具体技术（参数）要求		服务期限
1	整体要求	为保障我院数据的安全、稳定运行，供应商提供的所有资源空间及物理承载设备必须为我单位专属使用，不得和其他用户共用或混用。提供的资源空间必须高效稳定的支撑医院内网业务。包括我院现有在运行全部业务系统。	一年
2	资源量级要求	云端虚拟化资源； 2410 核-2.9THz 内存不低于 4.5TB 裸磁盘容量不低于 383.02TB 物理资源； 6 颗 5220R(2.2GHz/24 核/35.75MB/150W) 处理器 768GB 内存最高速率 2933MT/s，支持 RDIMM 或 LRDIMM 集中存储裸空间 36TB	
3	存储要求	平台必须支持直接备份或归档到基于 S3 接口的对象存储，归档到 S3 对象存储的数据可支持直接挂载打开读写使用，用于快速恢复数据之用处；支持管理平台节点（包括存储服务器、客户端）的设备运行情况（状态、容量使用情况等）进行统一监控；对于所有操作进行审计，记录配置修改、登录成功/失败、数据恢复等操作；支持对用户密码的安全策略管理，可设置密码的复杂度、有效期等；	
4	移动办公 VPN 接入服务	最大理论加密流量 $\geq 100\text{Mbps}$ ，最大并发用户数 ≥ 300 ，设备最大吞吐量 $\geq 150\text{Mbps}$ ，整机最大并发会话数 $\geq 35\text{w}$ ；服务设备不少于 4 个 10/100/1000M 以太网电口，支持 2 个 USB 口和 1 个 RJ45 串口，支持单电源；内存 $\geq 2\text{G}$ ，硬盘容量 $\geq 64\text{G SSD}$ ；专业 VPN 设备，采用标准 SSL、TLS 协议，同时支持 IPSec VPN、SSLVPN、PPTP VPN、L2TP VPN；支持 IPv6 的接入；支持 IPv6 的浏览器访问 IPv4 的 web 资源；支持 IPv6 的 windows 端访问 IPv4 的 13vpn 资源、TCP 资源支持 IPv6/IPv4 双协议栈；	
5		支持对基于 HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH 等的所有 B/S、C/S 应用系统，支持基于 TCP、UDP、ICMP 等 IP 层以上的协议的应用；支持 PC 终端使用包括 Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux 等主流操作系统来登录 SSLVPN 系统，并完整支持该操作系统下的各种 IP 层以上的 B/S 和 C/S 应用；支持主流操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的 SSL VPN 接入；移动	

	<p>端支持通过 PPTP、L2TP VPN 方式接入；支持终端使用包括 IE6、7、8、10、11 或其他 IE 内核的浏览器，以及最新版本的非 IE 内核浏览器，最新版登录 SSLVPN 系统，登录后可完整支持各种 IP 层以上的 B/S 和 C/S 应用；支持国产化终端使用来登录 SSLVPN 系统，并完整支持该操作系统下的各种 IP 层以上的 B/S 和 C/S 应用；服务设备应支持的密码算法包括：AES、AES192、AES256、DES、3DES、MD5、SHA1、SHA2-256、SHA2-384、SHA2-512、DH、RSA</p>
6	<p>可支持个性化登录策略，在一台设备上配置不同的访问域名、IP 地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果；支持用户登录界面、服务界面的完全自定义，上传单独的 Web 页面作为用户登录界面、服务界面；支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访；支持 Web 参数修正，可针对 Flash、Java、Applet、或视频播放器对象所引用资源路径进行修正，避免无法播放的问题；服务设备应提供环境检测、自动修复工具，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响 SSL VPN 的使用，减轻运维工作。</p>
7	<p>支持断线重连自动技术，防止用户误操作关闭浏览器导致 VPN 隧道断开；防止用户在无线网络环境下网络正常切换时 VPN 隧道断开。服务设备必须支持防中间人攻击，服务设备可在用户登录 SSLVPN 时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象；提供 HTTPS 驱动病毒查杀工具，支持对 Windows 环境下的针对 HTTPS 拦截监听的驱动病毒进行扫描查杀，避免因为 HTTPS 驱动病毒导致无法正常接入和使用 SSL VPN；设备内部必须支持自建 CA 中心，便于数字证书认证平台搭建；支持与基于 PKI 体系的第三方 CA 进行结合认证，可根据 CA 某字段将通过 CA 认证的用户自动映射到指定用户组，方便进行权限授权配置；支持 CRL 证书撤销列表；</p>
8	<p>单台 VPN 设备可扩展同时支持 5 套以上 CA 根证书；支持与第三方认证服务器对接；支持动态令牌认证，支持无需部署令牌认证服务器实现动态令牌认证。</p>
9	<p>服务设备支持与本方案中终端安全软件联动管理，通过防火墙服务设备界面完成网络中的终端安全软件的安全策略统一管控，实现终端病毒查杀功能。（提供证明截图）</p>
10	<p>支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式；支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度。支持针</p>

		对不同的 web 页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。基于互联网专线的延伸服务，通过再客户端部署专用网络安全设备与云端系统配合，实现“云+管+端”全场景的网络安全防护，保障客户网络安全和稳定，并提供配套准段 SIM 卡	
11		支持 HTTP 快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议。（ 需提供服务设备截图证明 ）	
12	互联网出口入侵防御服务 1 套	服务设备要求采用非 X86 多核架构，配置双交流电源，具备独立的攻击检测引擎与病毒检测引擎；服务设备要求提供 3 年 IPS/AV/ACG 特性库升级授权，支持本地、在线两种升级方式；服务设备要求全威胁业务 UDP 吞吐量 ≥9Gbps；应用层吞吐量 ≥4.5Gbps；服务设备要求配置 ≥14 个千兆电接口，≥12 千兆光接口，≥4 万兆光接口；配置 4 个千兆多模模块；服务要求支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置；服务要求支持策略冗余分析，冲突策略分析以及命中率统计；服务要求支持应用风险调优，通过应用层检测引擎智能地分析安全策略允许通过的流量中存在的潜在风险。	一年
13		服务要求攻击特征库数量 ≥8500、病毒特征库数量 ≥600W、支持的协议识别数量 ≥5500、WEB 攻击特征库 ≥3500（ 提供功能截图 ）	
14		IPS 检测到攻击报文或攻击流量后，支持 Web 重定向、黑名单等响应方式，以实现第一时间隔离有安全威胁的主机；服务设备提供海量预分类的 URL 地址库，支持根据 URL 类别实现 URL 过滤，URL 过滤可以基于时间、主机，能够精细到单一 IP 地址，设备提供海量预分类的 URL 地址库，支持管理者自定义新的 URL 地址和 URL 分类支持 URL 黑白名单	
15		提供服务基于用户名（或用户 IP 地址）实现对用户行为统一分析界面，采用饼状图对访问应用流量、网站访问集中分析展示，包含基于时间轴的访问行为轨迹（应用账号、行为内容等），关联账号（微信、QQ）等相关用户行为审计内容。（ 提供功能截图 ）	
16		服务设备同时支持串接部署模式以及旁路部署模式，支持配置备份和回滚功能，支持软硬件 bypass，支持外置 bypass 主机等方式保障设备掉电网络直通；要求服务设备支持虚拟入侵防御功能：支持虚拟入侵防御的创建、启动、关闭、删除功能；可独立分配 CPU/内存等计算资源；可独立管理，独立保存配置；具备独立会话管理、NAT、路由等功能。服务设备支持 2 台设备堆叠成一台设	

		备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署。为保证投标服务设备厂商在安全漏洞方面的整体研究水平和及时预防能力。具备网络安全漏洞统一收集验证、预警发布及应急处置体系，进而提高服务设备的安全性。	
17		服务设备应具有入侵抵御系统《软件著作权证书》， 提供有效证书复印件	
18		服务设备需支持 IPV6 协议，应具备 IPV6 证书， 提供有效证书复印件	
19	互联网出口上网行为管理服务 1 套	服务设备要求为机架式独立硬件设备，系统硬件为全内置封闭式结构，稳定可靠，加电即可运行，启动过程无须人工干预；服务设备要求为多核架构设计，不允许采用 X86 架构，采用模块化结构设计；服务设备要求为最大功率≤300W；内置软件 Bypass 模块，内置两路电口 Bypass；在设备流量异常时，可自动切换到 Bypass 状态，当设备恢复时，可自动切换回工作状态；双电源；服务设备要求为支持 10M/100M/1000M 自适应电接口数量≥12，支持千兆 SFP 光接口数量≥12，接口无路由/交换/LAN/WAN 等固化区分，均可作为二三层接口使用，支持多桥组部署；服务设备要求为吞吐量≥5Gbps；行为审计&应用控制适用用户规模≥2000 人；无线非经支持最大 AP 数量≥512；服务设备要求支持 DDNS 客户端以及域名 IP 绑定功能；	一年
20		服务设备要求支持静态路由、策略路由、RIP、OSPF、ISP 路由，其中 ISP 路由支持自定义，并可提供基于应用的策略路由， 提供 web 配置界面截图	
21		服务设备要求支持一键化快速审计策略配置。服务设备支持 http、邮件、即时通讯、基础协议、娱乐股票、网络应用六个大类维度的用户应用审计。http 类审计支持网页访问、网络社区（微博、论坛）、网页搜索、http 外发文件、http 文件下载、web 网盘上传文件、web 网盘下载文件等细粒度的审计。	
22		服务设备要求支持 portal 服务器联动 portal 服务器故障全部用户逃生；服务设备要求支持针对特定域名的 APP 缓存，只要是该域名传输的 APP 全部缓存；服务设备支持文件缓存，支持安卓和 IOS 形式的文件，主动缓存文件形式不限于视频、APP 等；服务设备要求支持主流厂商的对接；	
23		服务设备支持通过 udp 9999 同步在线用户、支持 radius 同步在线用户、支持深澜、城市热点、PPPoE、安美等认证方式的在线用户同步；支持基于 http 协议获取在线用户同步；服务设备要求支持预定义的入侵攻击特征类，包含最大事件集、常规事件集、应用事件集、攻击事件集。	

24		服务设备支持大于 6000 条预定于入侵攻击特征，包括 Web 服务器防护，包括网页防爬虫、网页防篡改、HTTPS 防护、DDoS 攻击防护、Web 攻击过滤、漏洞防护等，提供配置界面	
25	互联网出口防火墙服务 2 套	服务设备规格性能规格：网络层吞吐量 $\geq 4G$ ，应用层吞吐量 $\geq 2G$ ，并发连接数 ≥ 200 万，HTTP 新建连接数 ≥ 6 万。服务设备：内存 $\geq 4G$ ，硬盘容量 $\geq 128G$ SSD，电源：单电源，网络接口 ≥ 8 千兆电口+2 个千兆光口；服务设备部署方式：支持路由，网桥，虚拟网线，旁路镜像，单臂以及混合部署方式、主备、双机部署模式，实现双机高可用。	一年
26			
27		▲服务设备 VPN 能力：支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换。提供产品功能截图证明并提供检测报告证明功能有效性	
28		服务设备认证方式：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；服务设备双栈协议：支持 IPv4/IPv6 双栈工作模式，支持 IPv6 环境的应用控制策略设置，能针对 IPv6 的 IP 地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。	
29		▲服务设备入侵防御：支持内置不低于 12000 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。提供产品功能截图证明和第三方检测报告	
30		服务设备虚拟防火墙：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；服务设备访问控制策略：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。	
31		▲Web 应用防护 1：支持内置不低于 4000 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。提供功能截图第三方检测报告	
32		▲Web 应用防护 2：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。支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。提供产品功能截图证明和第三方检测报告	
33		防病毒：支持独立的勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略，支持在设备首页独立展示勒索风险板块。提供功能截图并提供关于“勒索病毒”的软件著作权证明功能有效性	

34		DDoS 防御：支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 等泛洪类攻击防护，支持 IP 地址扫描和端口扫描攻击防护；支持 ARP 欺骗类攻击防护；IP 封锁：支持对请求报文头 XFF 字段检测，并对非法源 IP 进行日志记录和联动封锁；应用控制：支持应用的识别和控制，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。生命周期管理：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。服务设备提供开放 API 接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。	
35		云威胁情报分析：互联网场景下支持云威胁情报网关技术，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。支持云端未知威胁主动探测技术，实现分钟级内未知威胁情报全网设备下发。 提供功能截图或第三方检测报告	
36	互联网区 web 应用防火墙服务 1 套	服务设备要求配置≥8 内存，≥1T 硬盘，≥2 个以太网千兆管理接口，配置≥6 以太网千兆电口，≥8 个以太网千兆光口，支持≥2 个接口扩展槽位；4 个千兆多模模块；服务设备要求应用层吞吐量≥1Gbps，HTTP 并发连接数≥600000；保护网站站点数量无限制；服务设备支持透明流模式、透明代理模式、反向代理模式、路由牵引模式、镜像检测模式及镜像阻断模式；	一年
37		服务设备支持旁路镜像模式下，对检测到的攻击进行旁路阻断；服务设备支持通过 BGP 方式对流量进行牵引，并在清洗攻击后回注，回注过程支持设置 SNAT 策略；服务设备支持 HTTP 协议校验，可根据实际网络状况自定义协议参数合规标准，过滤非法数据；服务设备支持设置扫描陷阱，防止恶意扫描；服务设备支持爬虫防护；	
38		服务设备支持文件上传、下载过滤；服务设备支持网站批量离线、网站批量恢复、网站一键断网、网站一键恢复操作；服务设备支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标服务器、攻击类型、攻击趋势、流量趋势及实时事件的动画统计；态势监测支持对监测范围、防护区域和防护对象的自定义设置；	
39	网闸服务 1 套	要求服务设备提供内网≥6 个 10/100/1000M RJ45 接口，≥2 个 1000M 的 SPF 光口；外网≥6 个 10/100/1000M RJ45 接口，≥2 个 1000M 的 SPF 光口；服务设备网络吞吐量：≥700Mbps；系统整体时延：< 1ms；	一年

40		要求服务设备采用 2+1 架构，专用传输隔离部件完全自主开发且外部无法编程控制， 要求提供截图 ；内外端机为 TCP/IP 网络协议的终点，阻断 TCP/IP 协议的直接贯通；内外端机之间采用专用硬件和专用协议进行连接，不可编程。网闸以软硬件结合的方式，有效地隔断内外网络间直接连接，防止信息无限制交换；	
41		服务设备只能通过内端机上的管理口对网闸进行配置，外端机上禁止配置管理；提供服务设备安全的文件传输功能，支持 FTP、NFS、SMB 等文件传输协议；提供服务设备对多种主流数据库 数据库系统的安全访问；支持用户查询、修改、添加、删除等操作；服务设备支持全表复制、增量更新、全表更新等；	
42		服务设备支持各种实例访问；服务设备基于专用客户端与网闸安全连接方式，提供多种主流数据库 的单、双向数据交换；为保证网闸安全性，管理端和审计端需独立与管理口连接使用，禁止使用内端机或外端机上的通讯口对网闸进行配置管理，禁止在外端机上具有管理接口；	
43		服务设备默认包含主机审计许可证书数量 ≥ 50 ，最大可扩展审计主机许可数 ≥ 150 ，可用存储量 $\geq 1\text{TB}$ （RAID1 模式），平均每秒处理日志数（eps）最大性能 ≥ 1200 。服务设备规格：2U，内存大小：8G，硬盘容量：64GB minisata+1TB SATA*2，电源：单电源，接口：6 千兆电口。支持 Syslog、SNMP Trap、数据库、文件、SMB、WMI、Console、日志导入、镜像流量等方式采集日志，审计中心可以支持多个日志采集器	
44	互联网区 日志 审计 服务 1 套	支持各类设备的日志采集要求，主要包括：安全设备：国内主流防火墙等； 操作系统；数据库等；应用系统：Apache、Tomcat、IIS、Weblogic 等；网络设备：主流的路由器、交换机、负载均衡等网络设备主流网络设备；服务设备支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件；支持根据设备类型，按日期展示日志的接入情况，包含不同级别日志数量统计；支持精确的专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询	一年
45		服务设备支持全球地理位置库，支持不同设备相同 IP 的日志识别；服务设备支持列表的方式展示告警；告警声音设置；告警过滤策略；支持实时监控，滚动显示实时的日志接入信息；服务设备支持关联、审计策略命中后定义告警，响应方式包括：SYSLOG、邮件、自定义命令行。服务设备支持挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，关联的类型包括基于规则和基于统计的。	

46		支持根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如系统管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，安全审计员只负责查看相关的审计结果及告警内容；安全管理员只负责完成对系统本身的用户操作日志管理；服务设备支持 DNS、DGA、解码错误、解码失败、解码超时的网络会话分类展现；服务设备支持 HTTP 网页标题、BBS、威胁情报、DGA、搜索关键词的网络会话分类展现；支持 TLS 会话、数据库会话、邮件会话、FTP 会话、Telnet 会话，即时通讯会话的展现；服务设备支持定义部门和人员的对应关系，支持定义人员与账号的对应关系	
47		要求服务设备采用非 X86 多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块；要求服务设备吞吐量 $\geq 25\text{Gbps}$ ，并发连接数 ≥ 1000 万；提供 ≥ 15 个 SSL VPN 并发授权；要求服务设备 ≥ 14 个千兆电接口； ≥ 8 个千兆光接口； ≥ 8 个万兆光接口（含模块）；配置冗余电源；支持 4 个扩展插槽，支持国密板卡扩容；服务设备实现路由模式、透明（网桥）模式、混合模式。实现静态路由、策略路由、RIP、OSPF、BGP 等路由协议。	
48	数据中心 防火墙服务 2 套	服务设备实现一对一、多对一、多对多等多种形式的 NAT，实现 DNS、FTP、H.323 等多种 NAT ALG 功能。NAT 地址池支持动态探测和可用地址分配；服务设备提供海量预分类的 URL 地址库，支持根据 URL 类别实现 URL 过滤；设备支持管理者自定义新的 URL 地址和 URL 分类；服务设备支持联动云端 URL 地址库进行全面实施核查。服务设备实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于 MAC 的访问控制列表，802.1q VLAN 透传等功能。服务设备支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置；支持策略冗余分析，冲突策略分析以及命中率统计。	一年
49		▲服务设备支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。（提供功能截图）	
50		服务设备支持不低于 6000 条以上的应用识别，且提示风险类型及风险级别，便于用户根据实际情况进行上网行为管理。当终端流量流经服务设备时，设备可以分析并提取出终端信息，并支持在终端信息发生变更时向用户发送日志，提示用户。服务设备支持 SNMPv1、SNMPv2、SNMPv3、RMON 等网络管理协议，并且支持通过网管软件	

		远程进行设备软件升级、配置等。为了保证整个网络的可靠稳定，要求本次提供的安全设备支持 A/S, A/A 方式部署，支持配置同步和会话同步；提供开放 API 接口（RESTful, NetConf），可编程管理防火墙，不再仅依赖网管软件。	
51		服务设备支持 2 台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署，提供报告复印件	
52	内网准入及审计服务 1 套	服务设备网络层吞吐量 $\geq 3.6\text{Gbps}$ ，应用层吞吐量 $\geq 450\text{Mbps}$ ，带宽性能：300Mb，并发连接数 ≥ 150000 ，每秒新建连接数 ≥ 4000 ，支持用户数 ≥ 1500 ，准入终端数（默认客户端授权数） ≥ 800 ，包转发率 45Kpps；内存大小 $\geq 4\text{G}$ ，硬盘容量 $\geq 1\text{T}$ SATA，电源：单电源，接口 ≥ 6 千兆电口+2 千兆光口 SFP。服务设备支持两台及两台以上设备同时做主机的部署模式；服务设备支持部署在 IPv6 环境中，设备接口及部署模式均支持 IPv6 配置，所有核心功能（应用控制、流量控制、内容审计、日志报表等）都支持 IPv6；	一年
53		服务设备支持发现私接路由（或者共享软件等）共享网络的行为：1. 支持自定义配置终端数量和冻结时间。2. 支持“仅统计电脑”和“统计所有终端”两种模式。3. 支持可选“冻结 IP”还是“冻结用户名”。4. 支持添加信任列表 5. 支持显示以 IP 或用户名的维度统计一段时间内的趋势图。6. 支持例外排除功能：如冻结条件是 2. 指定例外条件 1 台 PC，2 个终端。当 PC 或终端数超过例外条件才会被判定为共享。7. 支持在数据中心报表中可查询通过共享上网的 IP、用户，并能导出报表；（提供产品界面截图）	
54		服务设备支持 DNS 透明代理，能够基于用户、域名、目标 DNS，指定代理策略生效，代理策略可以设置为：重定向至 DNS 服务器、解析为 IP、丢弃、重定向至制定线路；服务设备支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载；支持使用 VPN 做专线备份；支持链路故障检测；服务设备支持 LDAP、Radius、POP3、Proxy 等第三方认证；支持 ISA\lotus ldap\novel ldap\oracle、sql server、db2、mysql 等数据库等第三方认证；	
55		服务设备支持首页分析显示接入用户人数、终端类型、认证方式；泄密风险、违规访问等行为风险情况；服务设备支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持下钻设置线路流控策略；服务设备支持 radius、AD、POP3、Proxy、PPPOE、H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制	

	指定用户、指定 IP 段的用户必须使用单点登录；服务设备支持图形化查看当前内网 IP 使用情况，帮助管理员减少人工维护 IP 表的工作量；
56	服务设备自动发现网络里面的终端，并获取 IP、Mac、厂商、操作系统、开放服务、开放端口等信息，支持根据 IP 段、MAC、使用者过滤用户，以便和其他过滤方式一起组合来搜索或获取终端信息；（提供服务设备界面截图）
57	服务设备 1. 对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 2、支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；3. 支持查看终端类型分布；服务设备支持以图表方式显示移动终端接入趋势；服务设备支持短信认证方式，用户输入手机号作为用户名，通过短信猫或短信平台发送验证码；
58	服务设备支持 802.1x 认证，支持对接本地和 AD 域用户源，支持在旁路模式部署下准入生效；支持未认证前推送认证客户端下载页面，减轻客户端分发工作量；（提供服务设备界面截图）
59	服务设备支持二维码认证，担保人扫描访客的二维码后对其网络访问授权；支持访客填写信息、担保人填写信息、免填写信息三种模式；服务设备支持哑终端通过 MAC 认证的方式接入网络，必须支持在终端管理列表批量绑定设备 IP/MAC 快捷放通入网；服务设备支持基于 802.1x 的外部 CA 证书认证，同时支持在线证书状态查询（OCSP）；不同用户推送不同认证页面，该认证页面可自定义，编辑内容包括文字、颜色风格、图片，且图片支持轮询播放；服务设备限制某个新用户只能在某个 IP 段、MAC 段范围内登录；认证成功的用户支持页面跳转：1. 跳转到用户原本输入的 URL 地址；2. 跳转到管理员指定的 URL 地址；3. 跳转到注销页面；
60	支持基于用户组、位置、终端类型、URL 类型配置流量管控策略；支持 FTP 协议上传、下载文件的审计，支持 FTP 传输客户端的外发附件审计，包括 WinSCP、XFftp, FileZilla、SecureFX
61	服务设备支持根据标签选择应用，标签分类不低于包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖 6 大类；支持给每个应用自定义标签；支持根据标签选择一类应用做控制；支持对每一种应用的定义和解释，帮助客户快速定位应用的分类；支持给每一种应用列上图标，易于客户了解应用的特征。（提供服务设备界面截图）

62		服务设备支持允许用户登录 Webmail 收邮件，而禁止发送 Webmail 邮件的功能；服务设备支持对加密 HTTPS、SMTP-SSL、SMTP 的邮件进行关键字过滤，支持基于关键字、发件人地址、关键字过滤；支持针对特权用户配置免认证 key、免审计 key、免控制 key；设备必须内置业界知名杀毒引擎；支持检测 SYN Flood、ICMP Flood、UDP Flood 等泛洪类攻击防护，支持发现异常后告警、封锁主机、推送终端安全软件修复处置；支持防 ARP 欺骗，支持告警；支持定时广播静态 ARP 表项；服务设备支持对 HTTP、HTTPS、FTP、SMTP、POP3、IMAP 协议进行病毒检测和查杀；支持告警通知；支持与云端联动对未知文件进行检测，在设备界面显示云端检测结果。支持识别、阻断、冻结（指定时长）僵尸主机	
63		支持查询和导出基于指定时间段/用户/用户组的防共享接入日志、移动终端发现日志、准入日志、登录注销日志等行为日志，支持共享接入、终端类型、接入用户数的排行和趋势分析；支持基于用户和事件类型等维度的上网安全日志统计分析（需提供服务设备功能截图证明）	
64	数据库审计服务 1 套	要求服务设备硬件配置 $\geq 4G$ 内存， $\geq 2T$ 硬盘，支持 2 个管理接口，业务接口 ≥ 6 个以太网千兆电口； ≥ 8 个以太网千兆光口，同时支持 ≥ 2 个接口扩展槽位，支持万兆口扩展；服务设备 SQL 峰值处理能力 ≥ 4 万条/秒，日志存储数量 ≥ 9 亿条，可支持审计 4 个业务系统，每业务挂载数据库数量不限；服务设备支持对医院的 HIS、LIS、EMR、PACS 等信息资产全方位监控，对患者就诊信息的篡改、敏感患者就诊信息非法调阅进行追踪告警；内置不同 HIS 系统的防统方规则库，内置 HIS 系统不少于 9 个。	一年
65		支持独立于系统管理员、系统审计员、系统安全员的纪检用户角色，可根据需求配置不同权限的纪检子帐号集，展示纪检用户关心的统方数据。服务设备提供监察人员使用的监察视图，可展示今日、本周以及本月统方事件，同时可根据工号为对象进行二次钻取，展示统方事件分布	
66		支持查看返回值信息，可一键查看统方事件中的返回值信息，且返回值内容可自动翻译，敏感字段自动提前展示，帮助使用人员直观看到语句执行结果，辅助判断审计结果（需提供服务配置界面截图）	

67	<p>服务设备支持医生处方查询分析，可依据时间、帐号、次数进行 topN 查询分析，结果以表格及分布趋势图展示，并支持三个月的统计对比分析；支持医护人员工号关联展示，通过统方事件中医护人员工号关联展示分析，辅助判断，监察人员可迅速确认统方事件，快速定位相关责任人；服务设备支持统方事件告警，发现统方行为。提供统方事件追踪页面，通过事件关联追踪排查事件，多维度定位事件状态，包括地点追踪、屏幕录像，且屏幕录像与该事件一一对应，支持快捷规则配置；服务设备支持事件告警，发现异常或非法行为。提供事件追踪页面，通过事件关联追踪排查事件，多维度定位事件状态，包括地点追踪、屏幕录像，且屏幕录像与该事件一样对应。支持快捷规则配置；同时，支持对审计数据的多种响应方式，包含过滤、记录、windows 消息、邮件、syslog、SNMP、屏幕录像、网关联动等多种事件告警和提示方式，第一时间向负责人发送告警信息</p>	
68	<p>支持与物理设备面板一一对应的网卡模拟展示，可根据实际连线情况实时展示网卡当前状态，包含光/电口识别、网卡连通、数据收发、网卡信息等状态，并以水量方式展示网卡当前负载，且支持面板与表格模式切换（需提供服务配置界面截图）</p>	

附件 5：医院网络资源服务（互联网、医院外网官网）等业务云资源服务

序号	具体技术（参数）要求		服务期限
1	专属计算服务	▲本项目需提供专属硬件资源，可用资源要求如下：VCPU ≥124、内存≥320GB、高性能块存储（可用容量）≥7TB，订阅时长≥12 个月。 提供承诺函并加盖投标人公章。	一年
2		▲为了确保本次项目业务的数据安全性，本次采购的云服务需采用硬件独享的模式，云厂商需要提供物理资源独享方案，同时满足本项目资源物理隔离、安全合规等（ 需提供截图证明，并盖章 ）；	
3		用户可以在专属计算资源的配额内随意创建不同云主机的规格；为了保障本单位业务运行的高可靠性，要求云厂商的云平台在物理资源独享的基础上需提供免费的 HA 公共备机资源，当本单位的独享服务器宕机后，可自动将公共备机加入到宕机集群中，在备机上恢复云主机的运行状态，并保证故障主机和备机物理介质隔离；	
4		为了匹配本单位业务快速发展的需求，要求云厂商提供的云平台需支持云主机在线扩容功能同时满足“热添加”模式，即在业务运行状态下，可以动态增加 vcpu 和内存的大小；（ 需提供截图证明，并盖章 ）	
5		为保障数据就近接入性，所提供资源的云节点需要在呼和浩特；云平台允许支持数据重建优先级调整，在故障数据重新恢复时，可由我单位指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性；	
6		承诺云上资源独占、资产可控（独属于客户的专属云服务器）、专属服务器大屏可视、并且在本地就近接入。（ 提供承诺函并加盖公章 ）	
7	互联网带宽服务	配置互联网带宽 100M，订阅时长 12 个月；	
8	弹性 IP	为了满足本单位网络与外部网络通信需求，云厂商提供的网络需支持弹性 IP 功能，云主机、虚拟路由器均能绑定和解绑弹性 IP；配置公网 IP 地址不少于 2 个，订阅时长 12 个月；	
9	网络能力要求	为了满足本单位网络安全的需求，云厂商需提供 VPC 内的分布式防火墙，对虚拟机的东西向流量做防护，实现虚拟机之间的微隔离，对数据中心内部流量进行 L3-L4 层安全防护；为了满足本单位业务进行统一流量审计，云厂商提	

		供的网络需满足端口镜像功能，支持 VPC 网络流量（如：内部云主机）镜像到虚拟安全设备、物理设备；支持跳转连通性探测页面，可以设置探测对象信息，包括网口、对象类型、IP 地址，可以点击开始探测按钮查看探测页面信息，可以在网络连通性探测页面查看网络探测是否成功；
10		▲云平台能够通过图形化管理平台的拖放操作完成虚拟网络拓扑的创建和管理，能够通过同一界面中的功能按键，实现虚拟网络连接、开启和关闭等操作；（需提供具有 CNAS/CMA 认证的国家级第三方测试机构的证明材料，至少包含材料首页，对应功能页和材料尾页，材料加盖公章）
11		▲性能要求：应用层吞吐量 $\geq 100\text{M}$ ，并发会话数（七层） ≥ 80 万，每秒新建会话数 ≥ 4 万；订阅时长 12 个月；
12		具备链路故障检测功能，支持通过 ARP、DNS、PING 协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率；支持基于 IP 地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等；产品内置应用特征识别库，支持不少于 10000 种应用规则，支持对游戏、P2P 下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制；支持对 HTTP、FTP、SMB、SMTP、POP3、IMAP 协议进行病毒检测和查杀，支持最大 16 层的压缩文件查杀；
13	下一代防火墙服务资源	产品内置 IPS 检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过 7000 种特征规则；支持僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证；产品内置 Web 应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含 SQL 注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL 后面攻击、跨站请求伪造、目录遍历攻击、WEB 整站系统漏洞等应用层攻击行为，支持超过 3000 种 Web 服务器漏洞特征规则；
14		▲支持对 HTTP 异常请求协议检测和防护攻击，检测内容包含 HTTP 请求信息的方法及参数长度等；（需提供产品功能截图证明并盖章）
15		具备识别与阻断扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵；支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞；支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用；支持 Web 服务器自动侦测功能，根据 Web 服务器在线状态、端口使用状态、Web 服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级；

16		▲性能要求：HTTP 应用层吞吐量≥100Mbps；HTTP 并发连接数≥8W；订阅时长 12 个月；
17	WEB 应用防火墙	协议合规检测：产品支持对 HTTP 协议包中各项参数进行合规性控制，通过自定义阈值与参数访问控制相结合的方式，对 HTTP 数据进行第一层安全控制，从最开始杜绝非法数据包传输。Web 攻击防护：产品通过预置 Web 细粒度的防护特征库，可以有效的对 OWASP TOP10 攻击行为进行拦截，全面覆盖了 WEB 应用安全存在的主要威胁，并可根据特定的攻击字段自定义特征，通过匹配的方式对可能出现的攻击执行相应的处理。Web 业务控制：产品采用行为分析算法，针对访问行为分析，实现无特征行为的攻击防护，基于访问行为分析可以有效阻断爬虫，黑链，盗链，恶意文件的上传下载等行为。
18		Web 敏感信息保护：产品通过中件间信息保护、数据库信息保护、敏感文件保护、代码错误信息保护、隐私信息保护、敏感词防护等诸多敏感信息检测技术，防止敏感信息被泄露。Web 业务加固：产品提供深入到具体应用业务内部的专项的加固保护能力，并为每种所支持的应用程序提供专门的检测防御模块，并综合提供多层面的多种检查、控制，从而保护业务的安全性。DDoS 攻击防护：产品采用数据采集模型，对经过流量进行分发调配，并配合多核处理架构合理利用系统资源，提升自身处理和清洗能力。
19	运维安全管理服务	可管理资源数≥10 个；系统各模块支持以 B/S 方式管理，采用 https 加密方式访问；订阅时长 12 个月；针对远程终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端 IP、客户端 IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息；支持字符协议：SSHv1、SSHv2、TELNET；支持图形协议：RDP、VNC；支持文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板；支持通过协议前置机进行协议扩展，至少支持扩展 KVM、Vmware、数据库、http/https、CS 应用等；
20		▲支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入（提供截图并盖章）；
21		▲用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD 域认证、Radius 认证等认证方式；并支持各种认证方式和静态口令组合认证（提供截图并盖章）；

22		支持 Windows AD 域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号；内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴；支持 RDP 安全模式（RDP、NLA、TLS、ANY）设置，以适应 RDP-Tcp 属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合 FIPS 标准等加密级别；支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问；
23		▲支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批（提供截图并盖章）
24		支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作；支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式；支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开；
25	终端 安全 服务	提供不少于 15 个服务端授权；订阅时长 12 个月；支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、僵尸网络、WebShell 后门数量、高危漏洞及其各自影响的终端数量；支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组；支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描，及时发现尚未纳入管控的终端；支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示；
26		▲可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低 3 种防护级别（需提供产品截图证明并盖章）；
27		支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件 Hash 值，文件大小，文件创建时间；可配置 WebShell 实时扫描，一旦发现 WebShell 文件，可自动隔离或仅上报不隔离；基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（需提供产品截图证明并盖章）；提供内存扫描（挖矿

		病毒巡检)工具,支持通过内存、进程和启动项来检索病毒相关信息;提供勒索病毒整体防护体系入口,直观展示最近七天勒索病毒防护效果,包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数;(需提供产品截图证明并盖章);支持按“最近7天”“最近30天”“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒TOP5排行榜,并展示对应的事件数及终端数;
28		资产授权数不少于10个;订阅时长12个月;支持主动、被动相结合的数据采集方式,支持通过Agent采集日志数据,支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka(截图证明)等多种方式完成日志收集;支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析,支持对解析结果字段的新增、合并、映射;(需提供截图证明并加盖原盖章);支持对每个日志源设置过滤条件规则,自动过滤无用日志,满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数,减少对网络带宽和数据库存储空间占用;支持对单个/多个日志源批量转发,支持定时转发,可通过syslog和kafka方式转发到第三方平台,并且支持转发原始日志和已解析日志的两种日志;支持接入TLS加密方式的日志,支持对日志传输状态、最近同步时间进行监控,可统计每个日志源的今日传输量和传输总量;
29	日志 审计 服务	▲支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索;可根据时间、严重等级等进行组合查询;可根据具体设备、来源/目的所属(可具体到外网、内网资产等)、IP地址、特征ID、URL进行具体条件搜索;支持可设置定时刷新频率,根据刷新时间显示实时接入日志事件;(需提供截图证明,并盖章)
30		支持解码小工具,按照不同的解码方式解码成不同的目标内容,编码格式包括base64、Unicode、GBK、HEX、UTF-8等;(需提供截图证明,并盖章);支持单条事件进行展开,显示事件详细信息和事件原始信息,支持事件详情中任意字段作为查询条件无限制进行二次检索分析;支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则,内置关联分析规则数量达到350条以上,支持自定义关联分析规则;日志进行归一化操作后,对日志等级进行映射,根据不同日志源统计不同等级下的日志数量;支持可视化展示,包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等,可提供设备专项分析场景。如防火墙外部攻击场景

		分析、VPN 账号异常场景分析、Windows 服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析；
31		数据库流量(单向)不小于 300Mb/s、数据库无限制；订阅时长 12 个月；采用 B/S 管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务；精细化日志秒级查询，通过 SQL 串模式抽取保障磁盘 IO 的读写性能；分离式存储 SQL 语句保障数据审计速度快（需提供截图证明，并盖章）；
32		▲TB 级日志秒级查询、支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多 SQL 语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询（需提供截图证明，并盖章）；
33	数据库安全审计服务	自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果；支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询；支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行；数据库威胁分析：可以通过自定义交互分析设置正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数这几个维度实时监控内网数据威胁态势并且提供交互式分析视图帮助单位快速溯源；
34		▲内置大量 SQL 安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等；（需提供截图证明，并盖章）

35	业务探测服务	▲为持续监控公网业务在全国范围内的可用性与连续性，需支持公网场景下的健康检查，可针对业务公网 IP 地址选择合适探测点发起探测，可选择探测点不可少于 5 个，且需提供不少于 10 万次探测免费次数；（需提供产品功能截图，并盖章）
36		根据客户业务实际情况，探测任务需支持 HTTP/HTTPS、TCP、ICMP 等监测协议；支持设置响应头、响应体、状态码、响应时间等断言条件对业务进行实时探测；支持定时拨测，支持设置探测频率，探测频率最高 30 秒；支持查看拨测失败的响应内容；支持监控信息图表可供查看实时以及历史的拨测趋势图；线上运维管理服务可允许用户登入云上智能运维管理平台，支持用户通过移动端小程序查看业务拨测情况以及用户资源（包括云主机、数据库、服务器、资源池）的监控指标信息；订阅时长 12 个月；
37	安全基线服务	▲业务系统上线前的安全检查比较复杂，为了避免业务系统上线后由于弱密码、高危端口等脆弱性问题导致业务系统受到攻击，要求云厂商上线前提供弱密码、高危端口的整改闭环服务；（需提供承诺函并加盖公章）
38		为保障业务安全，针对用户核心业务弱密码检测规则需包括长度规则、字符规则、字典序、web 空密码、账号白名单、密码白名单等，承诺 24 小时内发现弱密码。检测到弱密码问题后，服务团队需每周一次跟进业务部门闭环弱密码问题；为保障业务安全，针对用户核心业务进行高危端口检测，高危端口类型需包括外网及内网业务，承诺 24 小时内发现高危端口。检测到高危端口问题后，服务团队需每周一次跟进业务部门闭环高危端口问题；为了避免本单位业务因中勒索病毒遭受重大经济损失，要求云厂商提供的云平台支持勒索病毒防护，通过定时快照服务实现，所有满足条件的虚拟机都按系统定义的频率执行自动快照。发现勒索事件后，专属管家需 30 分钟内介入，基于存储快照协助恢复数据；（需提供截图证明与承诺函，并盖章）；要求云平台内置自动化安全基线核查工具，支持每周自动扫描并修复不符合等保要求的配置并辅助用户闭环；订阅时长 12 个月；
39	运维监控服务	云厂商需每季度提交巡检报告，从稳定性、性能、容量等方面对云上资源进行巡检，展示运行风险，并提供整改和优化建议；为了满足本单位的在处置疑难问题时的时效性和安全性，要求云厂商支持代维功能，云厂商的运维人员可通过代维协助本单位完成云主机、NFV 的配置修改或问题处理，同时本单位可在事后进行录屏下载回看；为满足本单位运维监控的便利性，平台告警和资源状态需支持微信小程序查看；在小程序中能够监控云平台资产和安全设备的告警和资源状态，（提供产品功能截图并盖章）；为了保障本单位的服务体验效果，云厂商需为本单位创建

		专属运维群，且专属运维群支持范围与工单支持范围一致，提供 7x24 小时技术支持，专属群 10 分钟内响应。订阅时长 12 个月。	
40	云上备份服务	▲为有效防止数据丢失，保障在系统故障或攻击后的业务连续性和数据恢复能力，确保关键数据安全，需提供不少于 4600GB 的数据高可用备份空间；订阅时长 12 个月；	
41		为了更好的保护用户数据，支持设置定期全量备份，支持用户灵活配置备份策略，备份文件保留时间最高可以达到 15 年；支持免代理恢复虚拟机整机，也支持对虚拟机文件系统进行解析，以在必要或应急时对虚拟机中的文件、文件夹等进行临时提取；	

二、弱电运维服务

序号	具体技术（参数）要求		服务期限
1	响应服务时间需求	<p>收到医院保修电话或通知，驻场服务人员要第一时间到达，并展开排查工作；如驻场人员 1 小时内无法及时解决故障，必须上报公司，公司在 2 小时内安排故障排查小组入驻；</p> <p>一级故障：影响整体子系统运行的或涉及重点业务区域内的网络系统故障，应在接到报修通知 30 分钟内恢复，属重大技术问题的，要在 1 小时内修复，如不能修复的，要给予合理解释，并约定修复期限。</p> <p>二级故障：办公楼区域内的监控、门禁、报警系统的各别点位故障，但不影响系统运行的，应在报修通知 8 个小时内恢复，如需跟换设备，需与甲方约定到货更换日期。</p> <p>三级故障：楼内的信息发布、楼宇自控、大屏幕等日常办公使用的系统各别点位故障，但不影响系统运行的，应在报修通知 24 小时内恢复。</p> <p>经维护检测属设备损坏无法维修的，维保人员在规定时间内完成设备配件更换工作。</p> <p>7×24 小时提供驻场技术服务。</p>	一年

2	维保人员需求	提供≥1 名工程师驻场技术服务。遇重大会议、活动和季末、年终等节假日重要时间点，可要求临时增派现场维护人员，以保障期间维护工作的顺利进行。
3	技术培训需求	每季度针对我院各类系统的常见问题解决方法及操作使用举办专场培训会议。 培训目标：对使用操作人员进行应用功能培训，使其能熟练使用系统完成日常业务。 培训方法：提供全面技术讲解，通过讲练相结合的教学方式让用户学员学习本系统的操作使用。 交付成果：包括但不限于《设备使用说明书》、《使用方法文档截图》、录制培训视频等。
4	定期巡检、保养服务需求	按国家有关规范和要求派专业人员对系统定期检查、测试、保养、维修、确保设备正常运行。 1、每季度对维保项目内的系统和主要设备进行≥1 次综合检查工作，对系统和主要设备的运行情况做详细的检查测试，如发现问题第一时间通知相关使用管理部门，并提出合理化解决方案。 2、对指定的设备做定期维护保养，包括：系统软件、必要的机械设备、电子部件的除尘清洗，定期保养至少每半年 1 次。 3、每个月对系统软件的数据文件至少进行备份 1 次。 4、维保单位应向医院主管部门提交详细的工作计划与工作安排，对每次巡检、保养工作做好记录，并移交相关负责人签字； 5、具体巡查维护次数如下： 1) 按周巡检：会议室配电系统、视频监控系统、门禁系统、LED 大屏、UPS 电源系统、精密空调、机房环境监控系统的巡检记录。 2) 按月巡检：扩声系统、数字 IP 网络广播系统、综合布线及信息网络维护、护理呼叫系统、分诊排队系统与取号叫号设备与系统、时钟系统、入侵报警系统、电子巡更管理系统、安防设备及系统、智能照明系统、信息发布平台与设备的巡检。 3) 按季度巡检：弱电井柜、智能 AP 电源、楼层交换机的巡检的关键数据的备份情况并形成巡检报告。 4) 按每半年维保：弱电井除尘、数据机房除尘并形成巡检报告。
5	配件更换服务	提供弱电系统相关配件（包括但不限于安防设备、监控设备、叫号设备等），年度总费用上限为人民币贰拾万元整（¥200,000），由服务方承担；若实际费用超出该限额，超出部分经院方书面确认后由医院据实支付。服务商需按月提供费用明细及发票供甲方审核，未经医院同意的超额支出由服务商自行承担。

三、医技、住院部护理呼叫平台升级服务

序号	具体技术（参数）要求		服务次数
1	智慧病房信息交互软件升级	<p>数据对接：数据整合：基于标准应用的业务模型和客户自定义的业务，从 HIS、CIS、LIS、PACS 等信息系统数据库中进行基础业务数据、指标数据的获取和转换，分层处理与存储，形成支撑业务应用的主题数据集，支持数据分析的实时计算，支持与主流数据库进行视图对接，支持 WebService、视图等多种方式进行协议对接。数据质量：支持数据接口和数据内容检测并生成检测报告，包括主键唯一性、字段非空检查、外键一致性检查等，记录数据错误类型和严重等级。</p> <p>数据安全：采用国产化操作系统部署，支持医院信创建设。</p> <p>提供含“智慧病房”关键字样的软著证书复印件。</p> <p>辅助决策：针对病床周转、病人构成等方面的日常动态进行挖掘分析，支持指标的趋势、同比、环比、占比分析。统计分析展示支持时段、科室、病区多个维度的统计分析，并且可导出统计结果。病床周转分析：支持分析各病区病床使用率和周转率、各个时段入住率和周转率的变化趋势。病人构成分析：分析病人病情程度分布、年龄段分布、性别占比。入住周期分析：分析各科室、病区病人入住周期，及入住周期的趋势变化。呼叫服务分析：分析入住期间病人呼叫服务的次数、时段分布、护士响应率、要求服务类型。</p>	1次
2		<p>★兼容性：与医院现有病房护理对讲系统软硬件无缝兼容；（需提供截图证明与承诺函，并盖章）；</p>	
3	智慧病房数据接口软件升级	<p>支持与医院 HIS，EMR 等系统无缝对接。</p> <p>支持与 Oracle、SQLServer, DB2, MYSQL 等大型数据库。</p> <p>支持数据库视图、中间表、WebService、Webapi 等多方式实现与 HIS 系统及其他信息系统的数据交换。支持数据对接的可视化调试，支持异常检测，支持对接 HIS 状态监控，数据表，数据字段异常监控和提醒。</p>	
4	智慧门诊信息交互	<p>数据对接：数据整合：基于标准应用的业务模型和客户自定义的业务，支持从 HIS、CIS、LIS、PACS 等信息系统数据库中进行基础业务数据、指标数据的获取和转换，分层处理与存储，形成支撑业务应用的主题数据集，支持数据</p>	

	软件升级	<p>分析的实时计算。数据质量：支持数据接口和数据内容检测并生成检测报告，包括主键唯一性、字段非空检查、外键一致性检查等，记录数据错误类型和严重等级。</p> <p>数据安全：采用国产化操作系统部署，支持医院信创建设。</p> <p>提供含“智慧门诊”关键字样的软著证书复印件。</p>	
5		<p>★兼容性：与医院现有排队叫号系统软硬件无缝兼容（需提供截图证明或承诺函，并盖章）；</p>	
6	门诊排队管理软件升级	<p>诊区与科室灵活配置：支持根据医院导诊台布局自定义诊区，允许同一科室在多个诊区同时开诊，亦支持单个诊区容纳多个科室，满足复杂门诊布局需求。</p> <p>叫号语音个性化设置：可按诊区独立设置叫号音量、语速；支持患者姓名1-3次重复呼叫；针对嘈杂环境或老年患者，可自定义姓名多音字读音；支持根据诊间空间大小设定诊间等候区容纳人数（1-人）。</p> <p>显示屏内容灵活配置：支持手动编辑叫号屏界面风格，医生信息、叫号信息、诊室信息、医生简介、患者队列等内容可按需选择显示或隐藏。</p> <p>可视化界面自定义工具：系统内置图形化界面编辑器，将显示屏视为画布，支持用户自由绘制、编辑界面内容与风格，兼容横屏、竖屏显示模式。</p> <p>精细化样式控制：支持对各功能区域进行样式精细化设置，包括背景颜色、区域形状、字体大小、字体颜色、加粗、闪烁效果、文字对齐方式等。</p> <p>弹窗提醒机制：支持按诊区启用叫号弹窗提醒，弹窗背景图、叫号内容可自定义编辑；弹窗显示时长与语音播报时长自动同步。</p> <p>多模式入队机制：支持预约号按时自动入队、非预约号自动入队、患者自助签到入队、护士人工签到入队等多种入队方式。</p> <p>诊区级规则配置：支持以诊区为单位独立配置排序规则、签到规则、叫号规则及分诊规则。</p>	
7		<p>智能标签自动识别：支持自定义患者标签规则，当患者数据表中某字段满足条件时（如年龄 > 75），系统自动为其打上指定标签（如“老人”）。</p> <p>标签差异化排序：不同标签可配置独立排序策略，例如“预约”标签按票号排序，“回诊”标签按签到时间排序。</p> <p>排队规则可视化表达：支持自动生成当前诊区排队规则的逻辑表达式，直观展示规则配置，避免人工逐项核对。</p> <p>特殊人群优先标识：对军人、军属、残疾人、老年人等法定优先人群，系统自动标记并在显示屏上以特殊标识（如“军”）及颜色区分。</p> <p>病情等级优先机制：支持按病情严重程度设置叫号优先</p>	

		<p>级；同优先级患者可按票号、签到时间等次序叫号。</p> <p>预约超时处理策略：预约患者未按时签到，可配置惩罚策略，如排至当前时段末位、顺延 N 位等。</p> <p>过号自动顺延机制：患者过号后自动顺延 N 次，超限后需重新签到方可入队。</p> <p>回诊智能分配：回诊患者签到后优先分配至原接诊医生；若原医生不可用，系统可自动分配同级别医生，或由护士人工干预分诊。</p> <p>“一号管三天”模式：支持初诊未签到及回诊患者在挂号后 72 小时内完成签到并就诊。</p> <p>▲软件著作权要求：须提供中华人民共和国国家版权局颁发的、登记名称中包含“门诊排队”关键字的计算机软件著作权登记证书复印件。</p>	
8	医技排队管理软件升级	<p>用户可根据医院导诊台分布情况设置诊区，可自定义诊区名称，选择该诊区所管科室，一个诊区可管理一个或多个科室，以满足医院导诊台对不同科室的管理需要；</p> <p>支持手动编辑叫号显示屏的界面风格，医生信息及叫号信息等内容可选择性显示，包括诊室信息、医生介绍、患者队列等信息。</p> <p>支持拖拽拉伸更改界面布局比例，更改界面各个区域所要展示的内容。</p> <p>支持对界面各部分内容，如电子门牌、医生介绍、叫号信息、跑马灯信息等，各自设置背景内容、字体大小、字体颜色等个性化设置。</p> <p>支持预约号到预约时间后自动进入队列和非预约号自动进入队列，以及患者自助签到进入队列，护士操作签到进入队列等多种患者进入队列的方式。</p> <p>支持按号票大小排序、按签到时间排序、预约时段先后等多种排序方式，可设置预约号优先及迟到惩罚机制。</p> <p>支持不同号别（急诊、预约、普通、住院等）、不同环节（初诊、过号召回等）的患者设置不同的排序规则，各个诊区可自由组合形成本区的排队规则。</p>	
9		<p>软件应提供中华人民共和国国家版权局颁发的“医技排队”关键字样的计算机软件著作权登记证书复印件；</p>	
10	门诊排队导诊软件升级	<p>手动挂号与：支持手动录入患者姓名、性别、就诊卡号、科室、挂号类别、医生等信息，并打印号票。</p> <p>多方式患者识别：支持外接扫码器、读卡器等设备，通过社保卡、身份证、电子健康卡等快速识别患者，实现签到、状态查询、排序调整、转诊、插队等操作。</p> <p>队列全景监控：可实时查看当前诊区各科室/医生队列详情，包括队列名称、等候人数、患者姓名、号票、性别、年龄、卡号、挂号类别、分诊类型、备注、过号记录、预约时段等。</p> <p>特殊人群优先调序：支持对老、幼、军人、离休等患者手</p>	

		<p>动提升排序；显示屏同步显示备注标识（如“军”）并以醒目颜色区分，提升公众理解度。</p> <p>票号冻结管理：护士可对已签到但暂不能就诊的患者票号进行冻结，冻结期间医生无法呼叫；支持自定义冻结时长，到期自动解冻，亦支持手动提前解冻。</p> <p>绿色通道机制：支持为急诊、抢救等特殊患者开启绿色通道，无需排队直接进入诊室。</p> <p>人工广播与定时播报：支持导诊台人工喊话广播及自定义内容的定时语音播报；广播期间自动暂停叫号语音，结束后自动恢复。</p> <p>导诊-诊室双向对讲：支持导诊台与诊室医生之间实时双向语音通话，实现岗位间高效协同。</p>	
11		<p>软件著作权要求：软件须提供中华人民共和国国家版权局颁发的、登记名称中包含“排队导诊”关键字的计算机软件著作权登记证书复印件。</p>	
12	医技排队导诊软件升级	<p>支持外接扫码器、读卡器等外设，通过社保卡、身份证、电子健康卡等方式快速查找患者，进行手动签到、状态查询、排序调整、患者转诊、患者插队等操作。</p> <p>支持查看当前诊区的每个科室和医生队列就诊患者情况，包括队列名称、人数统计、患者个人信息、排队序号、接诊医生等，患者信息包括患者姓名、号票、性别、年龄、就诊卡号、挂号类别、分诊类别、备注信息、过号记录、预约时间段等；</p> <p>支持对老、幼、军人、离休等患者手动调序，同时显示屏可显示此类患者备注信息，如“军”，并用其他颜色以示区别，让其他患者能够关注和理解。</p> <p>支持查看当前诊区的每个科室和医生队列就诊患者情况，包括队列名称、人数统计、患者个人信息、排队序号、接诊医生等，患者信息包括患者姓名、号票、性别、年龄、就诊卡号、挂号类别、分诊类别、备注信息、过号记录、预约时间段等；</p> <p>患者在一个诊区有多个检查项目时，支持一次签到操作即进入多个队列的功能，同时具备当其中一个诊室呼叫患者，其他诊室自动暂停对该患者进行呼叫，当患者其中一个诊室检查结束后，其他未检查项目再对患者进行呼叫，避免过号产生；</p> <p>支持绿色通道统能，即针对“特殊”患者无需进入排队队列，直接进入诊室检查；</p> <p>支持与诊室叫号软件相互呼叫并通话，实现诊室医生和分诊台护士在不离开各自岗位情况下的及时语音沟通。</p> <p>支持对侯检区进行定时语音广播和喊话广播，广播时暂停叫号语音，结束后自动恢复。</p>	
13		<p>软件提供具有中华人民共和国国家版权局颁发的“排队导诊”关键字样的计算机软件著作权登记证书复印件；</p>	

14	智慧 门诊 数据 接口	数据获取：支持与第三方系统数据交互，包括视图、webservice、推送接口等多种对接方式，获取系统运行所需的基础数据，包括医护人员信息、患者信息、药品信息等。	
15	软件 升级	数据推送：支持将子系统运行产生的数据推送给第三方系统，包括排队队列信息、统计数据、设备运行状态等。	

注：★核心技术参数，不满足将导致投标无效；▲为重点指标，需提供相应佐证材料，无标记为一般技术指标。