巴中市中医医院（巴中市巴州区人民医院）
三级等保安全整改（网络安全服务）采购项目

一、项目描述

近年来，随着信息化的快速发展，医院信息系统遭受网络安全威胁的情况日益加剧，随着互联网网络攻击事件频发，勒索病毒、暴力破解、SQL 注入、XSS 漏洞 、文件上传等攻击手段层出不穷，对网络安全、数据安全乃至国家安全形成了严重的威胁。为保障巴中市中医医院(以下简称“医院”）重要信息系统的稳定、安全、持续运行，数据的安全：医院拟对重要信息系统（以下简称“系统”）的网络安全风险做到早发现、早预防，加强医院信息系统的网络安全防护能力，本项目对我院的网络安全防护设备和防护措施进行强化，提供专业的网络安全服务及时发现并阻断系统中可能存在的安全漏洞和其他网络安全风险，加强医院内部网络安全防护制度和网络安全应急响应制度，以提高医院的网络安全防护水平。

项目建设完成后达到三级等保的要求，并无偿的为接入省级或市级互联网医院分院平台和四川省互联网医疗服务监管平台提供技术支持，能满足国家互联互通成熟度测评四甲相关要求，满足电子病历应用水平分级评价四级信息安全项目相关要求，满足四川省智慧医院三星级以上关于信息安全的评审相关要求。

二、技术服务要求

（一）服务支撑软、硬件技术规格、功能要求

服务名称	服务细项	服务内容	数量	备注
医院三级等保建设运营服务	核心链路保护服务	1．固化千兆电口≥24 个；万兆光口（SFP+）≥16 个；25G 光口（SFP28）≥8 个；40G/100G 混合端口（QSFP28）≥2 个，业务口扩展插槽≥1 个；配置可插拔电源模块，标配 1+1 冗余电源，支持高压直流输入；支持可插拔风扇模块≥2 个； 2．★MAC 地址≥64K，支持 4K VLAN ，交换容量≥2.56Tbps，包转发率≥960Mpps； 3．支持支持 Access、Trunk、Hybrid 方式，支持基本 QinQ 和灵活 QinQ,支持基于 MAC 的动态 VLAN 分配;支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议；支持 STP（IEEE 802.1d），RSTP（IEEE 802.1w）和 MSTP（IEEE 802.1s），支持 ERPS 以太环保护协议（G.8032）； 4．支持云平台和手机 APP 统一进行管理、监控和远程配置，配置≥5 年云管理授权。 5．★其他：根据服务需要提供的服务工具为双机冗余，	1 项	按需提供对应服务工具（提示：需提供两台核心交换机）

审核人：

		配置≥25G 高速堆叠模块及配套线缆，实现两套服务工具的链路聚合；软硬件维保≥5 年，提供现场安装、培训，7*24 小时远程技术支持，备用机服务。		
	网络区域边界防护服务	6. ▲标准机架式设备≥1U，实配千兆光口≥4，万兆光口≥2，千兆电口≥6；IPSec VPN 隧道≥4000，配置 AV-IPS-URL 特征库升级服务≥5 年；电源≥2。 7. 吞吐量≥4Gbps，最大并发连接数≥360 万，每秒新建连接数≥8 万，IPS 吞吐量≥1.5Gbps； 8. 设备关键芯片国产自研，保证设备安全可控； 9. 支持与第三方平台对接，实现策略的命中，冗余分析及风险调优； 10. 系统预定义 IPS 签名数量≥8000，病毒库数量≥500w； 11. 支持 HTTP、HTTPS、DNS、SIP 等应用层 Flood 攻击，支持流量自学习功能； 12. 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。 13. ★根据服务需要提供的安全服务工具为双机冗余；支持网口负载均衡，具有负载、主备等多种算法。软硬件维保≥5 年，提供现场安装、培训，7*24 小时远程技术支持，备用机服务。	1 项	按需提供对应服务工具（提示：需提供两台防火墙）
	内外边界物理隔离服务	14. 内端机≥6 个千兆电口、≥1 个控制口、≥2 个 USB 接口、≥2 个扩展槽；外端机≥6 个千兆电口、≥1 个控制口、≥2 个 USB 接口、≥2 个扩展槽；网络吞吐≥1.8Gbps；系统延时<1ms；MTBF≥50000 小时 ；最大并发连接数≥300000；无用户数限制；配置冗余双电源。 15. 提供访问控制服务，对象包括：源地址、目标地址、应用、时间、并发数等；支持内容关键字、文件类型过滤；支持病毒检测功能。 16. 提供 ping 、traceroute、telnet、抓包等服务工具方便排查故障。 17. 提供服务工具有完整的审计日志：系统日志、管理日志、访问日志、攻击日志、内容过滤日志、文件交换日志、数据库交换日志；日志支持 SYSLOG 外传。 18. ▲提供数据库应用同步服务，无需另装同步软件；支持 ORACLE、SQLSERVER、MYSQL、SYBASE、DB2、POSTGRESQL 等多种主流数据库的同步，支持国产达梦数据库、人大金仓数据库的同步。 19. ▲提供数据库应用代理访问服务，支持的数据库种类包括 ORACLE、SQLSERVER、MYSQL、SYBASE 等主流数据库；可根据 SQL 命令进行控制，如不允许 D E L E T E 等。 20. 提供文件同步服务，无需另装同步软件；支持单、双向同步；支持文件类型过滤；支持同步备份功能。 21. 根据服务需要提供的安全服务设备支持工业应用协	1 项	按需提供对应服务工具（提示：需提供两台网闸）

审核人：

		议交换，支持的协议至少包含 MODUS、OPC、DNP3、S7 等，对这些协议能进行应用指令控制，而并非只是开放端口，如只能读取，不能写入。 22. 提供时间模式配置交换策略服务，时间模式支持指定时间、指定星期，指定日期范围。 23. ★根据服务需要提供的安全服务工具为双机冗余；支持网口负载均衡，具有负载、主备等多种算法。包含≥5 年软硬件维保服务，提供现场安装、培训，7*24 小时远程技术支持，备用机服务。		
	数据库访问审计服务	24. 标配≥6 个千兆电口，≥4 个千兆 SFP 接口，≥2 个扩展槽；可支持扩展 4 口/8 口的千兆光或电模块，≥4T 硬盘，默认支持≥16 个数据库实例；最大日处理≥13000W 条 SQL 明细；入库速度≥10000(条/秒)；峰值事务处理能力≥20000(条/秒)；日志存储量≥16 亿条；配置冗余双电源。 25. 提供支持语句大小为 30MB 内的超长语句的审计与展示服务，页面不仅展示超长语句全文，还可统计出语句大小； 26. 根据服务需要提供的安全服务设备支持系统自检功能且提供独立界面，当系统自身侦测到日志存储空间不足、昨日业务数据量超标、磁盘错误、license 过期、无配置备份、系统掉电、监听网卡断开等涵盖系统运维中的各项重要消息时，独立弹窗提示用户并包含快捷处理方式； 27. 提供 SQL 模板服务，系统能自动识别并抽取数据库句式语意相同但参数不同的语句，并通过独立页面展示，同时记录该模板的状态、触发规则名、总记录数、总告警数、上次告警记录数、上次出现时间、最后出现时间，并能设置该模板别名； 28. ▲提供 HIS 厂商统方规则库，配置不同 HIS 系统的防统方服务，内置 HIS 系统≥15 个； 29. 提供数据库审计与分析服务，支持 Oracle，Microsoft SQL Server，DB2，Sybase，Informix、MySQL、Caché、Teradata、MongoDB ，人大金仓（Kingbase）、达梦(DM)、南大通用、神通等数据库的审计。可准确分析出这些数据库的协议，并支持对多种不同类型和不同版本的数据库的同时审计； 30. 提供在线回档服务，并查看历史归档数据。可通过历史数据回档客户端，在不删除现有审计数据的情况下查询设备挂载已归档数据。同时，无缝衔接系统查询模块，支持在线对归档数据多条件组合查询； 31. 提供查询服务，查询方式包含：普通查询、模糊查询、明细查询、词组查询、流水号查询等多种匹配命中方式，同时可叠加多种查询条件，其中包含会话语句种类、重复程度、耗时、数量、排除关键字及时段选择等，查询结果支持多种格式导出； 32. 提供事件告警服务，发现异常或非法行为。提供事	1 项	按需提供对应服务工具（提示：需提供一台数据库审计设备）

审核人：

		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，如将此类语句设为安全、设为统方等； 33．提供多种审计数据库响应服务，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； 34．▲为保证数据库安全审计服务的技术先进性，根据服务需要提供的安全服务设备，采用在海量 SQL 语句归并技术； 35．提供审计数据中敏感数据的模糊化处理服务，系统内置常见敏感数据的掩码规则； 36．★包含≥5 年软硬件维保服务，提供现场安装、培训，7*24 小时远程技术支持，备用机服务。		
	网络访问行为管理审计服务	37．标准配置≥6个千兆电口，≥1个扩展槽、≥2个USB，≥1 个控制口，≥1T 硬盘。适用用户数≥1000 人，网络吞吐量≥6G，最大并发连接数≥160 万，每秒最大新建连接数≥50000；配置冗余双电源。 38．提供基于轮询的多链路负载均衡算法服务，支持基于链路的下行流量自动均衡的多链路负载均衡算法，支持基于最佳路径的多链路负载均衡算法。 39．▲提供 DOS/DDos 攻击防护服务：支持 Land、Smurf、WinNuke、Ping of Death、Tear Drop、IP 数据块分片传输数据包攻击防护，支持 ARP、SYN、UDP、ICMP、DNS 洪水攻击防护，支持 IP 地址扫描和端口扫描攻击防护，支持异常报文攻击检测； 40．提供身份认证服务：支持 IP/MAC 绑定认证；支持本地身份认证、短信认证、微信认证、钉钉认证等；短信认证支持 HTTP 协议认证，包括亿美短信、互亿无线、数米科技、互亿国际等。 41．提供终端类型（PC，android，苹果等）识别服务，可识别手机操作系统和 IP 地址，并可将其添加到信任列表或者拒绝上网。 42．提供准入控制服务：能够根据 IM 监控规则、操作系统规则、进程规则、文件规则、注册表规则等相关规则设置准入策略，对不符合要求的终端禁止上网。 43．提供黑名单服务：能够对网络共享行为进行检测，并把共享 IP 加入黑名单，例如无线路由器共享、360WIFI 共享限制等；支持对流量配额、速率控制、并发会话数控制、新增会话数控制、基于时间段的控制等行为进行黑名单管控功能，同时支持多种惩罚方式、加倍惩罚机制。 44．▲提供协议剥离服务：支持将特殊协议（如 L2TP、GRE、LWAPP、CAPWAP 等）的协议头剥离掉，对特殊协议封装内的原始数据进行认证、审计和控制。	1 项	按需提供对应服务工具（提示：需提供一台上网行为管理设备）

审核人：

		45．提供详细的告警服务，包含管理员操作日志、设备状态、流量异常、违规网站、违规帖子、违规文件上传、违规邮件发送以及潜在危害的行为告警。 46．★包含≥5 年特征库升级服务和硬件维保服务，提供现场安装、培训，7*24 小时远程技术支持，备用机服务。		
	网络安全状况检测服务	47．标配≥6 个千兆电口，≥2 个扩展槽；≥2 个 USB 口，≥1 个 COM 口，≥128G SSD 固态盘，≥1T 企业级硬盘；每秒 TCP 新建连接数≥18 万，最大 TCP 并发会话数≥200 万，整机吞吐率≥8Gbps，安全检测吞吐率≥2.5Gbps，配置冗余双电源。 48．提供威胁文件展示服务，服务包含展示选定时间内的文件检测威胁趋势、危险文件总数、危险文件下载源 IP Top10、危险文件下载目标 IP Top10、病毒文件类型、文件关联邮箱、文件关联 URL、文件报告列表，提供病毒文件样本下载功能； 49．提供探测扫描展示服务，服务包含展示选定时间内的扫描探测趋势、扫描探测总数、扫描探测源 IP Top10、扫描探测目的 IP Top10、扫描探测详细信息； 50．提供事件详情查看服务，事件详情查看中以分类规整方式动态嵌入与之相关的攻击证据，并能实现证据内容的无限次数的钻取。分类方式应包括：尝试获取用户信息、疑似敏感行为、尝试获取用户权限、疑似 Web 应用攻击、疑似木马活动、病毒扫描、协议异常、网络扫描、异常连接等； 51．提供恶意外联展示服务，展示选定时间内的恶意外联趋势、恶意外联总数、恶意外联活跃域名统计 Top10、恶意外联源 IP Top10、恶意外联关系图、恶意外联类型、恶意外联详细信息等； 52．提供 Web 攻击展示服务，展示选定时间内的 Web 攻击趋势、Web 攻击总数、Web 攻击源 IP Top10、Web 攻击目的 IP Top10、Web 攻击 URL 统计、Web 攻击返回码统计、Web 攻击类型统计、Web 攻击详情等； 53．提供代理解析服务，当服务器前端部署代理设备或 CDN 时，通过配置源 IP 解析规则，获取真实的攻击源 IP 地址，支持配置规则名称、解析方法、解析字段、代理级数、规则状态等信息； 54．提供漏洞检测服务，能够识别敏感信息泄漏漏洞、Oracle SQL 注入漏洞、MySQL SQL 注入漏洞、SQL Server SQL 注入漏洞、远程代码执行漏洞、OpenSSL 心脏出血漏洞、反序列化漏洞等高危漏洞； 55．▲为保证对海量数据的风险检测能力，安全服务工具有采用在海量审计数据中发现异常的技术。 56．提供勒索病毒检测服务，能够识别 Wannacry、Satan、GandCrab、GlobeImposter 等勒索病毒； 57．提供挖矿木马检测服务，能够识别 CryptoLoot、Webmine、Coinhive 等网页挖矿行为；	1 项	按需提供对应服务工具（提示：需提供一台入侵检测设备）

审核人：

		58. ▲提供提取告警日志文件服务，支持提取触发网络入侵攻击告警的 Pcap 元数据； 59. 提供入侵检测服务，能够识别成功的 Webshell 攻击、远程代码执行漏洞攻击、命令注入等攻击行为。 60. 提供多种告警服务，支持 Syslog 告警、邮件告警、SNMP Trap、网关联动、Windows 告警、态势感知系统联动等事件响应策略； 61. ★包含≥5 年特征库升级服务和硬件维保服务，提供现场安装、培训，7*24 小时远程技术支持，备用机服务。		
	重要资产运行日志审计服务	62. 标准配置≥6 个千兆电口、≥1 个扩展槽，≥2 个 USB 口，≥1 个控制口，≥4T 硬盘；日志源授权点数≥100 点；日志处理性能≥15G/天；平均≥5000EPS，峰值≥10000EPS；配置冗余双电源。 63. 提供灵活多样的日志检索服务，可根据日志的级别、IP、端口、类型、编号、用户名、地理位置等属性进行组合精确查询；支持自建表达式的高级检索方式； 64. 提供多种日志采集服务，支持 Syslog、SNMP Trap、文件导入、WMI、SMB、数据库等日志采集方式； 65. ▲内置 500+主流厂商设备日志范式化解析策略，主机、网络设备、安全设备、中间件、数据库、应用系统、虚拟化平台主流设备自识别接入，解析设备品牌包含但不限于：华为、H3C、深信服、天融信、绿盟、黑盾、锐捷等；对 windows/linux 日志以及设备进行解析以及挖掘关联关系；针对匹配的多条解析范化策略，设置策略优先级，实现灵活操作；界面新增、删除、修改、查询解析规则；导入、导出范式化解析规则。 66. 提供日志重新定义服务，可配置策略，根据设备名、类别、级别、IP、端口、MAC、动作等组合条件对事件严重级别进行重定义； 67. 提供日志采集过滤服务，可配置过滤策略，根据设备名、类别、级别、IP、端口、MAC、动作等组合条件进行过滤，减少日志采集量； 68. ▲提供内置关联分析服务，可基于规则、基于统计等方式对日志进行关联；支持基于异常统计模型的检查分析功能，如：识别异常的流量等； 69. 提供报表模板服务，可设置报表执行周期计划，定期生成报表并发送到指定邮箱；报表支持 PDF、WORD、EXCEL、HTML 等格式； 70. ▲提供威胁情报碰撞，能够结合源 IP 情报标签、目的 IP 情报标关联分标签、源 IP 情报判定、目的 IP 情报判定，结合日志进行关联分析，提升告警的精准度； 71. 根据服务需要提供的安全服务设备支持系统数据库自动备份功能，可将数据库定期备份到 NFS； 72. ★包含≥5 年软硬件维保服务，提供现场安装、培训，7*24 小时远程技术支持，备用机服务。	1 项	按需提供对应服务工具（提示：需提供一台日志审计设备）

审核人：

	数据安全服务	73. 配置≥2 颗高性能处理器，核数≥10 核 20 线程，配置≥128GB 内存；配备≥2 块 480G SSD；≥8 块 8TB SAS HDD 数据盘，前端支持≥12 个 3.5 寸 SATA/SAS 数据硬盘，配置掉电保护功能 RAID 卡≥1 张（缓存≥2G），支持 RAID0、1、5 等多种 RAID 级别。千兆电接口网卡≥2 个，万兆光接口网卡≥2 个（含万兆多模光模块），配置冗余双电源； 74. ★配置≥50TB 备份容量授权，不限制前端个数的定时与实时备份数量；授权功能包含数据重删压缩、永久增量、数据副本、大屏监控、备份数据防勒索等功能模块； 75. 支持主流市场国内外主流虚拟化平台的免代理备份，支持 Vmware vSphere、FusionCompute、H3C CAS 等虚拟化平台的备份恢复，备份过程中无需在 VM 中安装任何代理，支持单机和集群部署环境； 76. ▲支持虚拟机快速恢复，无需恢复全量备份数据，直接挂载备份数据到云平台即可运行，支持 Vmware vSphere、FusionCompute、H3C CAS 等虚拟化平台，实现分钟级恢复，保障业务连续性； 77. ▲支持批量虚拟机备份捕获时间点状态功能，支持同时捕获后传输和分别捕获传输数据方式，满足用户对数据一致性或宿主机负载的不同需求； 78. 支持 Vmware vSphere、FusionCompute、H3C CAS 等虚拟机自定义指定磁盘备份，减少备份数据量降低后端存储占用空间； 79. 支持 Vmware vSphere、FusionCompute、H3C CAS 等虚拟机备份获取源端真实数据，减少备份数据量降低网络传输负载以及备份存储空间占用； 80. 支持主流 Windows、linux、国产 Kylin、UOS、Anolis OS、openEuler、中科方德等操作系统整机、文件备份； 81. 支持主流的数据库备份恢复，包括：Oracle、SQL Server、MySQL、MairaDB、PostgreSQL 等主流数据库的应用级备份，备份任务配置过程全部图形化向导指引完成，无需编写任何的脚本； 82. 支持 Windows、Linux 等系统的整机实时复制，可将生产服务器上数据卷的数据变化实时复制到备份系统上，数据恢复无需重新安装配置操作系统和应用软件，支持自动分区无需手动分区； 83. ▲支持主机数据库应用自动识别，支持进行整机持续保护时数据库一致点的捕获，保证数据库一致性，防止进行恢复后数据库无法启动； 84. ▲支持实时备份任务配置缓存目录空间，支持不少于两种缓存架构的配置方式，支持自定义空间大小； 85. 配置大屏实时监控功能，能够监控系统的各项关键指标，包括不限于 CPU 使用率、内存使用率、存储空间使用、任务类型、备份进度、备份速度、任务状态等，便于管理员随时掌握系统的运行状况；	1 项	按需提供对应服务工具（提示：需提供一套一体化实时备份设备）

审核人：

		86．系统具备对备份数据集进行图形化管理，可以通过标识信息追溯到备份数据时间点、备份类型、数据大小、所在位置等信息； 87．备份平台提供防勒索机制，支持备份数据的不可变存储功能，避免病毒篡改、删除数据； 88．★提供不少于五年软硬件设备的维保售后服务，提供现场安装、培训，7*24 小时远程技术支持，备用机服务。		
	终端安全管理服务	89．系统支持 C/S、B/S 等主流架构设计。支持部署在 Linux、windows 等服务器操作系统上，系统支持多台服务器部署在不同服务器操作系统上，从而实现多操作系统平台双机热备，解决服务器单点故障风险，实现跨平台备份。客户端支持 Linux、Windows、macOS、安卓、信创（如：统信、麒麟）等操作系统；软件授权数量≥800 用户，提供≥5 年系统升级维护服务，提供现场安装、培训，7*24 小时技术支持。 90．系统功能支持移动存储管理、文档防勒索、设备管理、资产管理、网络管理、终端安全配置、应用程序管控、桌面管理、补丁管理、文档安全管理等功能。 91．支持禁用 U 盘、移动硬盘、智能手机、所有 USB 存储设备和使用所有 USB 外接设备功能，同时支持指定部门/用户可以使用特定设备。USB 移动存储管理支持禁用、只读、只写和加密等管控模式。包含 USB 设备插入日志、USB 设备使用申请审批日志和 USB 设备文档操作日志。支持实名认证 U 盘注册和 U 盘使用申请，针对注册过的 U 盘可做使用权限特殊处理。加密 U 盘支持内部使用和外部授权使用两种管理模式。 92．▲支持终端文档防勒索功能，创建安全程序特征指纹库，精确鉴别应用程序身份信息，阻断一切非法程序对文档的访问。 93．支持自动收集终端计算机硬件型号、性能、品牌、出厂时间等信息，采集 CPU 内核、线程、名称、封装、工艺、规格、系列、扩展系列、型号、扩展型号、步进、修订号、指令、虚拟化、超线程、风扇速度、总线速度等信息。 94．支持流量控制功能实时限制计算机的通信流量，支持上传、下载分别控制，支持全局流量控制及应用程序单独控制。 95．▲支持禁止关闭系统防火墙、来宾账户、注册表编辑器、敏感注册表项、文件共享、控制面板、任务管理器、安全模式、截取屏幕、计算机管理、服务管理、组策略、修改 IP 地址和修改计算机名称等功能。支持与服务器系统时间同步功能。支持开启账户密码策略。 96．▲注册表防篡改支持禁止恶意程序修改敏感注册表项，系统内置关键注册表项，同时支持自定义添加敏感注册表项。 97．支持应用程序黑名单、白名单功能和支持禁止新安装软件，禁止安装软件情况下支持申请安装，支持客户端使	1 项	按需提供对应服务工具（提示：需提供一套终端管理软件）

审核人：

		用企业软件库。支持应用程序管控支持按进程名称、公司名称和唯一标识三种管控模式。支持应用程序库，自动收集全网所有应用程序及按公司名、安装目录和进程名称自动分组。 98. 支持屏幕水印设置、桌面壁纸设置、屏幕保护程序设置、自动锁屏设置、定时关机重启设置。屏幕水印支持文字水印、点阵式水印、窗口水印，同时屏幕水印支持置底显示。 99. 提供漏洞检测平台及统一分布式下发管理组件，检测终端计算机操作系统漏洞和自动更新安装操作系统补丁。 100. ▲敏感信息报警功能包含窗口标题、邮件内容、文件名称、打印文档标题、网页标题、网页搜索和聊天内容报警。支持敏感文件扫描审查，采用多关键字综合打分制，可以创建全网敏感文件审查任务，查看涉敏客户端、涉敏文件及涉敏文件上下文。 101. 支持禁止聊天程序、邮件客户端、浏览器或自定义程序发送文件，同时支持仅限制敏感文件外发和阻断和阻断时上报日志。远程调试客户端功能支持强制远程控制、交互模式、旁观模式、兼容模式和独占输入等管控模式。支持多网段、跨 NAT 及互联网环境，同时提供通过手机 App 远程操控客户端计算机。支持远程开机功能，支持定时周期远程开机设置，同时支持跨网段、跨 VLAN 远程开机。 102. 支持软件分发功能，支持断点续传及下发软件执行参数配置。支持实时文件传输、快捷键、命令行下达。支持多客户端发送远程消息，支持同时查看多个客户端屏幕，支持远程关闭、重启、卸载客户端计算机。 103. 支持磁盘管理工具，控制台在客户端无感知情况下，同 Windows 本地资源管理器方式显示磁盘信息，并对磁盘文件进行查看、打开、删除、上传、下载、加密、解密。 104. 操作系统账户管理工具，支持控制台强制启用、禁用客户端 Windows 操作系统账户，重置 Windows 系统所有账户密码。 105. 支持文档操作审计、文档打印审计、剪贴板使用审计、光盘刻录审计、邮件发送审计、即时聊天审计、上传下载审计和屏幕录像，支持审计附件原文件上传服务器。 106. 账户管理提供权限描述符功能，在已有客户端和功能授权的基础上去掉一些特殊权限，如对指定客户端的强制远程、禁止卸载客户端等。		
	一体化智能监控运维管理服务	（一）综合监控服务要求 107. ▲实现支持面向业务的监控。实现接入的监控资源总体情况，包括正常设备数、严重设备数、提醒设备数、失联设备数等。实现系统接入的设备数及各种设备类型的接入数，包括操作系统、数据库、中间件、网络设备、服务器、存储等。展示最新严重告警信息，能够快捷定位需要处理的告警事件。 108. 内置丰富的资源面板，用户可根据需求自主拖拽布	1 项	按需提供对应服务工具（提示：需提供

审核人：

		局，多维度多视角的自定义资源面板，帮助用户实现登录即工作的便捷。 109. 支持展示监控对象的总体概况，包括监控资源的基本信息、核心指标、实时状态和实时告警信息。支持根据告警级别、发生时间等条件查询监控对象的全部告警信息。 110. 支持快速切换当前业务系统的其他监控对象，便于查找分析问题。（提供系统证明截图并加盖投标人单位公章） 111. 实现展示监控对象的全部指标列表，针对每个指标支持图形化显示历史曲线。 112. 支持查看监控对象所有指标某个时刻点的数据，为分析历史故障提供决策依据。 113. 支持所有监控对象显示在一个列表中，清晰看到每类监控对象的数量和通过关键字快速查找。支持快速跳转设备的管理口功能。 114. 支持在线执行脚本，包括 ping、端口扫描、Traceroute 等。 115. 支持针对具体监控对象的监控指标和触发器的管理。 116. 支持 Windows、Linux 等操作系统的监控，支持主、被动方式。支持对 CPU 使用率、CPU 负载、队列长度、CPU 系统态使用率的监控。 117. 支持对内存使用情况监控，包括内存使用率、交换空间使用率、内存空闲率等。 118. 支持对磁盘剩余空间、磁盘 IO、传输速率、响应时间、吞吐量的监控，提供磁盘预计用完时间。 119. 支持对网络发送与接收速率、丢包率、错误包数、网卡流量进行监控。 120. 支持对进程、端口和服务进行监控。分析进程占用内存和 CPU 的相关情况，如：进程 CPU 占用前二十，进程内存占用前二十等。 121. ▲数据库监控：支持 MySQL、SQLServer、Oracle、DB2、MongoDB、Redis、ElasticSearch、Caché和达梦等数据库的监控。支持会话数、连接数、会话锁定率、活跃会话等各类性能指标的监控。支持资源和缓存等可用指标的监控。支持对阻塞和死锁等可用性监控。支持对数据库备份状态及结果监控。支持对慢查询（SQL）进行监控。支持对表空间进程监控。支持对文件进行监控，提供日志文件信息。 122. ▲中间件监控：支持对 Nginx、IIS、Tomcat、WebLogic、Resin、Apache、Zookeeper、Jboos、东方通 TongWeb 等中间件的监控。支持对 ActiveMQ、RabbitMQ、Kafka 等消息队列的监控。支持对 Zookeeper、Kafka 等集群进行监控。支持中间件的请求、会话、类、线程、堆内存、垃圾回收和资源等进行监控。 123. 支持系统可用性监控，包括响应状态和响应时间等。支持针对系统的接口可用性进行监控，包括接口响应时		一套监控运维管理服务软件）

审核人：

		间、响应码、响应状态等。支持针对系统的某些功能可用性监控，包括系统登录、重点功能、退出等。 124. 支持虚拟化平台的监控，包括虚拟化平台的宿主机、集群、虚拟机等监控。支持虚拟化平台的总体情况展示，包括虚拟机的开关机情况、宿主机的开关机情况、CPU\硬盘\内存的总体使用情况、虚拟机 CPU 使用率和内存使用率前五等。 125. 支持主机视图和虚拟机视图两种树状维度，清晰显示虚拟化平台的架构。支持虚拟机视角监控，包括虚拟机的 IP、状态、CPU 使用率、内存使用率、磁盘使用率、CPU 核数、内存大小等。 126. 网络设备监控服务要求：支持对不同品牌交换机、防火墙、入侵防护、上网行为、负载均衡等安全设备的监控。支持对不同品牌交换机端口状态、流量监控分析功能。支持对不同品牌交换机电源、风扇、电源、主板等硬件监控，CPU、内存的性能监控。 127. 物理服务器监控服务要求：支持对华为、戴尔、华三、惠普、联想、浪潮等各品牌物理服务器的监控。支持对跨平台(Windows、Linux、Unix 等) 操作系统级指标项的监控。支持读取服务器处理器、内存、硬盘、网络等的配置信息；提供 IO 分析数据。支持对物理服务器的硬件监控，包括风扇、温度、电源、电池、电流、电压和主板等。 存储监控服务要求：支持对惠普、日立、EMC、群晖、IBM、华为等各平台物理存储设备的监控。支持读取存储池和物理硬盘信息，支持对存储的分析，包括发送数、错误硬盘数、Autosupport 发送成功数等。支持读取存储的网口状态、速率、以及流量等信息。支持获取存储的背板和节点信息。 （二）报障管理模块服务要求 128. ▲IT 呼叫中心：在电话响起时，自动弹出报修页面；实时在线录音，录音文件可传至服务器永久保存，录音文件可回放，可监控多路电话；自动记录已接、未接、呼出的电话记录。 129. 值班管理：在来电弹屏时，自动解析来电号码，并根据来电号码自动识别对应的来电人或者来电客户；来电时自动提示当前客户历史报修记录，根据记录可回复客户进度和判断是否重复报修。 130. 工单管理：接单：支持手机接单、电脑接单；转交：支持工单转交给其它同事，在手机，电脑均可操作；填写处理记录：可以填写多次处理记录，支持语音自动识别为文字；完成：维修处理完成，转为待评价状态；评价：支持不同的维度评价，例如响应速度，服务态度等，三天未评价，系统默认好评；工单查询：根据关键词（故障描述、解决办法等）、报修时间、工程师和工单状态等进行综合查询和导出 EXCEL。 131. 知识库管理：实现系统自动分词进行模糊搜索；实现对知识库的评价功能；支持富文本编辑，实现图文结合的		

审核人：

		知识库，提供附件上传等功能；维修结束后，可以把维修过程自动转入知识库。 132. 移动端功能：可采用拍照、录音、文字描述、语音识别等方式进行报修；在故障处理的各个环节，系统通过微信自动把处理的实时进度信息反馈给报修人；通过手机可以派单、转交、接单、填写处理记录、完成、关闭工单等操作；通过微信扫一扫进行现场设备巡检，根据手机提示的巡检项目逐项核对并记录，然后现场拍照确保人员真正到达现场；通过微信扫一扫可以查询到设备的具体信息。 （三）资产巡检管理模块服务要求 133. 台账：资产台账整体管理，此功能为了辅助巡检管理使用； 134. 巡检标准设置：针对每种设备类型可以设置标准化的巡检作业体系； 135. 巡检记录：填写巡检记录，并现场拍照； 136. 巡检设备管理：巡检设备的设置，待巡设备的提醒等； 137. 巡检周期管理：可以针对不同类型，不同品牌，不同型号设备设置不同的巡检周期，巡检方式及内容； 138. 设备类别管理：设备类型设置，建立树型设备分类结构； （四）项目管理模块服务要求 139. 我的项目：以项目的维度，查看自己所参与的项目中产生的任务、交付物、进度、会议、动态等； 140. 任务分解：以任务的维度，查看自己所接受的任务，包括改进类、需求类、问题类、任务类，所属的项目、提出时间、截止时间、优先级、完成情况等，可对任务进行汇报，上传相关文档； 141. 项目进度管理：把控所有在进行中的项目，历史和本月任务是否解决，查看未解决的问题、相关负责人、项目所处进度、会议等； 142. 项目过程管理：对项目的大节点、里程碑进行配置； 143. 需求流程管理：新增需求、暂停需求、转派需求、终止需求、拒绝需求、完成需求、查询需求； 144. 填写处理记录：可以填写多次处理记录，支持语音自动识别为文字。修改当前进度； 145. 合同发票：实现合同、发票基本信息的维护。 （五）其他服务要求 146. ★提供系统平台所有模块功能终身使用授权，系统平台被监控对象授权数量无限制。提供≥5 年的系统升级维护服务，提供现场安装、培训，7*24 小时技术支持。		

（二）运维监测服务要求

审核人：

1、★网络安全运维监测服务

序号	名称	技术参数与性能指标
1	网络安全运维监测服务	1、向采购人提供全流量的网络安全检测、可视及响应服务；以大数据分析为核心，结合威胁情报、UEBA、失陷主机检测、大数据关联分析、NTA 流量分析、可视化等技术为基础的全流量分析服务；对全网安全进行可视，帮助用户看清业务、看到威胁、看懂风险，并辅助用户决策； 2、根据采购人的信息系统持续发展产生的安全需求，实时制定相应的安全防护策略，对采购人的安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全运维管理等方面提供为期≥3 年的远程及现场技术支持服务、季度巡检服务、应急响应服务及故障恢复服务； 3、在采购人软件系统或者网络架构发生变化，需要调整网络及安全设备部署时，根据采购人需求完成设备的硬件迁移、策略重构及重新部署上线； 4、远程及现场技术支持服务要求：按需提供，7*24 小时响应；确保当天的问题单当天有回复，能解决的 4 小时内解决，不能及时解决的应回复原因并提供具体的解决时间，服务完成后向采购人提交《现场服务记录表》； 5、季度巡检服务要求：提供季度巡检服务，针对安全设备进行巡检，做好系统补丁更新、特征库更新、软件版本升级服务，分析其性能和工作状态，做好预防性措施，发现问题及时处理；针对网络安全状况进行巡检，掌握采购人业务系统面临的病毒、攻击、漏洞等威胁情况，发现并消除潜在威胁；巡查处置完成后向采购人提交《季度巡检报告》； 6、应急响应服务要求：15 分钟电话响应，3 小时内到达现场；服务完成向用户提交《应急响应报告》； 7、故障恢复服务：若医院突发网络安全事故造成业务中断，业务恢复时间小于 12 小时；恢复过程中所需备件及维修维护费均由成交供应商承担（包含且不限于人工费、运输费、税费等）。

2、网络安全运维监测服务考核

采购人每年对成交供应商是否达到服务数量及质量按照以下办法进行考核，对达到要求的服务应予以确认，未经确认的服务，相关分数不予计算（本项成交供应商须单独提交承诺函，并加盖公章）。

序号	考核项目	考核内容及分值	考核标准
1	人员配置	配置专职运营维护人员和服务技术人员≥1 人，须具备相关专业资质并提供相关证件。（5 分）	能满足需要得 5 分，否则得 0 分；
2	培训服务	按用户需求提供相关培训手册及培训服务。满足使用人员对系统使用及操作要求，双方确认培训服务成效。每年不低于1 次培训服务。（5 分）	因供应商原因导致培训服务不达标，扣 5 分；

审核人：

3	巡查服务	每月对项目系统和设备全面巡查1次并解决潜在的问题，避免发生系统性风险。同时提供巡查报告。（12分）	巡查率应为100%，每少一次巡查扣1分，扣完为止；
4	设备及平台维护	每月保证设备整体正常运行率不得低于95%。每月平台正常运行率不得低于98%。（12分）	每少一个百分点扣2分，扣完为止；
5	系统运行报告	供应商每个季度前5天内汇报上个季度系统运行情况，出具书面系统运行巡查、分析报告、风险处置报告，统计数据表册。（12分）	未按时提交报告报表的每次扣3分；
6	故障申报热线电话应答	提供7×24小时的故障响应：一般情况下，在15分钟以内响应；如电话连续3次以上拨打无人接听，视为无响应。（10分）	无响应或超时响应每次扣2分；
7	故障处理时效	一般故障4小时内恢复，重大故障12小时内恢复。（30分）	超出时效范围的，按照受影响的前端点位数进行扣分，2分/点位数；
8	系统更新服务	供应商必须每季度前20个工作日内给采购人提供和安装最新的系统升级包、补丁包、特征库等。（8分）	未及时更新，每次扣2分；
9	其他服务	每个服务年内，供应商应当协助采购人完成并通过三级等保测评备案。（6分）	配合但未完成，每次扣2分，不配合扣6分，供应商已配合采购人开展测评，但因采购人自身原因导致未通过则不扣分
10	考核结果应用	如果服务提供商年考核得分在90分及90分以上，视为服务合格；考核得分在90分以下，服务商须提交整改报告并扣除全款10%的服务费。	

三、商务条款

序号	商务要求名称	商务要求内容
1	设备上线时限	政府采购合同签订之日起，45个工作日内完成本项目所需软、硬件设备配套上线（含相关设备软件升级）。
2	服务期限	成交供应商对该项目的服务期限最长不应超过三年（期间服务内容及金额均按照招标文件内容执行）。每年服务期满后进行《网络安全运维监测服务考核》，考核合格后续签下一年服务合同。网络安全运维检测服务考核不合格，待服务商提交整改报告，一个月后验收小组复核，复核合格后续签下一年合同；若连续3次整改后依旧未通过考核，服务中止。
3	服务地点	巴中市中医医院（巴中市巴州区人民医院）。
4	验收、交付标准和	成交供应商与采购人严格按照《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》（中华人民共和国国务院令第658号）以及

审核人：

	方法	《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）等国家和行业现行法律法规、规章、标准，结合本项目谈判文件、成交供应商响应文件、政府采购合同要求进行验收。
5	相关设备归属权	本服务项目涉及的相关软、硬件设备所有权归医院所有。
6	支付方式及比例	年度服务费根据当年度《网络安全运维监测服务考核》最终得分按约定一次性支付；
7	付款进度安排	在供应商向采购人出具合法有效完整的完税发票及凭证资料后的15个工作日内进行支付结算。
8	违约责任与解决争议的方法	违约责任： （一）成交供应商在政府采购合同履约期间，因自身原因造成政府采购合同终止的，因此产生的所有经济损失由成交供应商自行承担，如给采购人造成经济损失的，采购人将依法追究其法律责任； （二）采购人和成交供应商必须遵守本项目各项规定，保证本项目的正常履行。如因成交供应商工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给采购人造成损失或侵害，包括但不限于采购人本身的财产损失、由此而导致的采购人对任何第三方的法律责任等，成交供应商对此均应承担全部的赔偿责任； （三）未经采购人书面同意，供应商擅自将本项目合同下权利或义务部分或全部转让任何第三方时，采购人有权单方面解除合同； （四）如供应商根据本项目合同约定应向采购人支付违约金或应赔偿采购人的损失的，采购人有权从其应向供应商支付的合同款中扣除，不足部分，供应商应予以补足。 争议解决： （一）供应商与采购人双方应通过友好协商，解决在执行本项目合同所发生的或与本项目合同有关的一切争议。如协商不能解决争议，任何一方均可将争议提交采购人所在地有管辖权的法院，通过诉讼解决争议； （二）在诉讼期间，除正在进行诉讼部分外，本项目合同其它部分应继续执行。
9	其他	（一）本项目的报价是服务商响应采购项目要求的全部工作内容、最终用户验收合格后的总价体现，包括且不限于完成本项目所需的一切费用、税费、人工费、运输费或其他费用。该项目成交后报价不做调整，并且在合同履行过程中是固定不变的； （二）在服务期中，所有的安全生产责任和法律风险均由中标供应商承担（提供承诺函并加盖投标人公章）； （三）供应商应保证本项目所提供的所有服务、成果不涉及侵犯任何第三方的专利权、商标权或著作权等（提供相关证明文件或承诺函并加盖投标人公章）； （四）供应商需配合采购人完成针对主管、协管、及其他三方部门反馈的漏洞风险提供整改支持服务（提供承诺函并加盖投标人公章）； （五）供应商应同采购人签订安全保密协议，对在本项目履约过程中获知的信息及履约后产生的成果附有保密责任； （六）每个服务年内，供应商应当协助采购人进行三级等保测评备案（提供承诺函并加盖投标人公章）； （七）为保证项目生命周期延续，需供应商提供服务期合同外维保价格，

审核人：

		提供的价格需可量化（如：年度维保费不超过合同总金额的 2%）或按服务模块分段报价，该报价作为后期采购维保、升级服务价格的参考依据。最终报价单能计算出每个服务类别单项报价。

备注：

1、以上条款中带★为实质性要求，不允许负偏离且需提供承诺函并加盖投标人单位公章。

2、以上条款中带▲条款为重要参数，提供相应的证明材料（界面截图、检测报告等）或承诺函并加盖投标人单位公章。

3、以上商务要求为实质性条款，均不允许负偏离，负偏离视为非实质性响应投标文件，做无效投标处理，有明确要求的须按要求提供证明材料，所有商务要求均须按招标文件要求在商务响应表中予以应答。

审核人：