**医院网络安全等级保护建设整改项目采购需求参数**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **技术参数要求** | **数量** | **单位** | **备注** |
| **一、等保安全整改建设内容** | | | | | |
| 1 | 态势感知平台 | 1、产品配置接口≥4电口，内存≥4\*16GB，盘位数≥8，硬盘容量≥4\*4TB，带宽≥1Gbps，配置BMC诊断模块 2、支持大屏可视化功能，支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势、设备运行态势，支持页面跳转到对应态势大屏，并具备大屏告警能力。 3、支持大屏展示业务脆弱性态势，包括漏洞风险态势、漏洞类型TOP5、高危漏洞TOP5、业务总览、脆弱性业务TOP5、实时脆弱性监测。 4、★支持大屏展示正常横向访问和正常外连监控数据；正常横向访问监控包括被访问最多的业务TOP5、最活跃终端TOP5、应用TOP5、实时访问监控等，正常外连监控包括外连最多的业务TOP5、外连最多终端TOP5、外连态势、外连国家TOP5,并支持国际、国内地图切换。（需提供第三方检测报告证明并加盖原厂商公章）。 5、支持综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势、正常横向访问监控、正常外连监控、设备运行态势等11个大屏展示功能，并支持大屏轮播，可自定义大屏轮播顺序。 6、支持感知业务/服务器资产，可定义IP地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息，并支持基于流量支持识别操作系统、开放的服务与端口。 7、★支持检测15类以上常见协议的弱密码,包括HTTP、FTP、LDAP、VMWARE、ORACLE、VNC等类型协议，检测列表包含账号、密码、服务器、所属分支和业务、最近登录源IP、类型、最近发现时间等信息，密码星号显示需超级管理员才可查看，并支持储存数据包。（需提供第三方检测报告证明并加盖原厂商公章）。 8、支持基于流量检测业务服务器的配置不当功能，检测列表包含服务器、所属业务、所属分支、配置不当类型、风险等级、发现时间等，支持配置不当类型下钻，展示配置不当详情，提供解决方案和数据包举证。 9、★支持实时漏洞分析功能，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、目录遍历漏洞、OpenLDAP等操作系统、数据库、Web应用等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。（需提供第三方检测报告证明并加盖原厂商公章）。 10、支持安全域维度展示安全风险，包含安全域列表、安全域评分、事件类型TOP5、IP地址、IP类型、风险等级、关键风险、状态等信息。 11、支持具备独立威胁情报分析模块，内置威胁情报数量不少于120W，支持展示威胁情报命中数、今日命中数、命中威胁情报类别TOP10、命中趋势、活跃威胁情报TOP20等。 12、支持具备独立文件威胁鉴定模块,集成静态文件检测引擎和智能分析检测引擎，可统计分析当前文件的文件进度，包括恶意文件数、未知恶意文件数、待分析文件数、安全文件数。 13、支持检索安全日志，可基于时间、攻击类型、严重等级等选择项进行组合查询，可基于具体设备、来源/目的所属、IP地址、特征ID、URL进行具体条件搜索。 14、支持对等级保护建设整改过程中系统定级、差距评估、备案、整改、测评过程中产生的文档结论进行统计归档，并使用可视化的统一界面进行展现与管理，最大程度发挥安全措施的保护能力 15、★支持通过SNMP协议对网络中网络设备、安全设备的运行状态进行监控，包括设备机器名、CPU负载、内存和流量等。（提供截图证明并加盖制造商公章）。  16、支持独立的第三方接入管理模块，支持接入第三方安全设备、网络设备、DHCP服务器、蜜罐、中间件等日志接入和解析功能，并支持导入正则文件解析主流设备日志，支持syslog、wmi、https接入方式；  17、支持具备多种分析引起引擎，包括不限于安全日志分析引擎、DnsFlow行为分析引擎、HttpFLow分析引擎、NetFLow分析引擎、MailFLow分析引擎、SmbFLow分析引擎、威胁情报分析关联引擎、第三方安全检测引擎、文件威胁检测引擎等 18、产品制造商具备信息安全风险评估服务资质 19、产品制造商具备CMMI 5级认证证书 | 1 | 台 | 三年质保，三年软件升级 |
| 2 | 潜伏威胁探针 | 1、吞吐量≥1Gbps，配置≥6个千兆电口，配置≥2个万兆光SFP+.  2、支持报文检测引擎,具备IP碎片重组、TCP流重组、应用层协议识别与解析等功能。 3、支持对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等异常通信行为分析能力； 4、支持对网络通信行为进行还原和记录，以实现运维人员取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为； 5、支持对网络内部终端受远控木马或者病毒等恶意软件入侵进行检测，能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；（提供截图证明，并加盖厂商公章） 6、支持通过设备对流量进行抓包分析，定义抓包数量、接口、IP地址、端口或自定义过滤表达式； 7、★支持无缝接入至医院已部署态势感知平台中，实现对产品的统一升级，可展示当前所有接入产品的规则库日期、是否过期等，并支持禁用指定探针的升级。（提供无缝接入承诺函，加盖厂商公章） 8、支持对敏感数据泄密检测功能，支持对敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤 9、支持将流量还原的文件发送至沙盒进行静态检测和动态模拟执行，可支持第三方沙盒对接。 | 1 | 台 | 三年质保，三年软件升级 |
| 3 | 日志审计系统 | 1、授权资源数≥200个，配置≥4千兆电口，支持接口扩展，尺寸≥1U机架；存储空间容量要求保存日志≥180天。 2、支持添加、修改、删除资产，并对资产的基本属性进行维护，支持资产增加自定义属性。 3、支持对IP对象的自动发现功能，支持IPv6功能，对自动发现的设备可以转资产或删除。 4、支持Syslog、Syslog-ng 、SNMP Trap、文件、WMI、FTP、数据库、SMB、Console、镜像流量等方式采集日志。 5、支持从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段。 6、支持对安全事件重新定级，根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义 7、支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索。  8、支持审计对象的定义，包括：审计目标对象、审计行为对象、审计行为执行者对象、审计来源对象、审计时间段对象等 9、支持对所有审计管理员操作审计系统的动作进行审计；审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明； 10、支持业务管理配置，可以导出系统内报表、策略、采集器、资产等业务数据，供新设备导入配置， 11、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。 12、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。 | 1 | 台 | 三年质保，三年软件升级 |
| 4 | 准入控制系统 | 1、★支持用户分权管理，操作员可以管理各自的用户群组和策略组，只有上级管理员才能管理全部的用户组和策略；（提供功能截图并加盖原厂鲜章） 2、★一体化客户端，使用同一个客户端实现网络准入、用户认证、终端安全状态检查、桌面资产管理等所有功能，避免多个客户端带来的管理不便；（提供功能截图并加盖原厂鲜章） 3、支持802.1x、Portal、L2TP IPSec VPN、无线等多种网络环境的身份认证，支持基于端口的802.1x和基于MAC地址的802.1x，可管理HUB或非智能交换机下的多个用户； 4、★支持exe文件安装、AD域登录脚本安装、静默安装、网页下载等安装方式。为启动认证的用户上网时自动重定向到安装网页，弹出exe安装文件或者Java安全插件，帮助用户下载相关安全客户端，并自动对终端用户进行病毒、补丁等安全状态的检查；（提供功能截图并加盖原厂鲜章） 5、对于服务器或打印机、IP话机等哑终端的接入端口可放行，自动学习网络中服务器或打印机的IP/MAC地址信息，允许服务器或打印机在指定的交换机接口上面认证接入网络，在非指定区域无法接入网络，非法终端通过服务器或打印机端口接入网络时，可以根据策略让其接入端口立即关闭或延时关闭，防止终端盗用打印机等端口接入网络，提高网络接入安全；（提供功能截图并加盖原厂鲜章） 6、用户的接入权限，可以在认证通过后下发给接入设备，由设备动态控制用户的访问权限，限制用户对内部敏感服务器和外部非法网站的访问； 7、可以对源/目的IP、源/目的掩码、源/目的网段等九元组进行控制，实现流量管理；在网络设备ACL资源不足的情况下，仍然可以实现终端网络访问权限灵活控制；（提供功能截图并加盖原厂鲜章） 8、★提供安全违规处置能力：可基于不同安全检查项设定不同的违规处置模式，如下线模式、隔离模式、VIP模式、访客模式和监控模式。当用户违反多个安全检查项时，采用各个安全检查项中最高的安全模式进行处理，安全模式级别由高到低为：下线、隔离、提醒、监控；（提供功能截图并加盖原厂鲜章） 9、客户端可检测IP流量、网卡流量、广播报文流量、TCP/UDP连接数等异常流量，并且执行隔离、下线、提醒等管理措施； 10、支持对软件进行监控、对进程进行监控、支持对服务进行监控。支持纯白软件管理，终端用户只能安装该纯白软件列表中的软件，不能安装该纯白软件列表之外的软件。支持MD5方式进程检查，即使修改进程名也无法逃避检查。支持配置组内关系配置，与关系表示组内配置软件、进程、服务、文件必须同时满足。支持延时检查进程； 11、桌面资产管理，支持对客户端软硬件资产信息的编号、收集、统计、变更情况告警等，支持通过HTTP、FTP、文件共享等方式进行软件分发，在终端用户需要帮助时可提供远程协助；  12、★支持和20种以上主流防病毒软件联动，可以检测杀毒软件引擎版本，检测病毒库版本。支持不同的用户检测不同的防病毒软件，不同的引擎版本和病毒库版本，确保系统处于最新防护状态；（提供功能截图并加盖原厂鲜章） 13、配置2000点终端准入控制授权。 | 1 | 套 | 三年软件升级 |
| 5 | 网络运维管理系统 | 1. 支持分布式部署：要求资源拓扑、告警、性能等功能模块支持多服务器分布式虚拟化部署，可实现负载分担，满足大规模网络环境的统一管理。单套软件可管理的节点数可达15000个； 2. ★支持自定义用户主页：管理员可以首页中通过拖拽，自定义需要在首页展示页面，同时支持Widget扩展；（提供功能截图并加盖原厂鲜章） 3.可以为不同的管理员设置不同的用户名、密码，并限制管理员的管理权限和管理范围，实现用户分权管理； 4. ★支持自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等；（提供功能截图并加盖原厂鲜章） 5.支持对全网设备告警的实时监控和统一浏览；支持多种提醒方式，如告警实时提醒（告警板）、告警音响提示；支持多种转发方式，比如转E-mail，转短信，转上级网管或其它网管等。支持告警分析，可以屏蔽重复告警、闪断告警，支持告警自动确认功能； 6. 支持告警智能分析，包括告警分类关联分析、告警多源关联分析、告警拓扑根源分析、告警网络影响度分析； 7. 支持提供直观的设备的面板视图：支持设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态；并提供基于设备面板的设备、单板、端口配置功能；  8. ★支持设备配置集中管理：配置库包括配置文件和配置片断，配置内容可带有参数，在部署时根据设备的差异设置不同的值；配置文件可部署到设备的启动配置或者运行配置；配置片断只能部署到设备的运行配置；（提供功能截图并加盖原厂鲜章） 9. 支持批量的设备配置备份和恢复。支持向导方式或者任务方式（周期性任务、一次性任务或立即任务）批量的备份、恢复完整的配置文件，也可以批量的下发配置片断；（提供功能截图并加盖原厂鲜章）  10.支持设备与用户统一管理：支持网络管理与用户管理联动，如通过点击拓扑楼层接入交换机图标，可查看该设备所有接入用户帐户信息，查询在线用户列表、强制用户下线、下发消息、总在线用户数统计、不安全用户数统计等；  11. 支持设备软件智能升级。支持网络运行设备的软件版本查询功能，支持先备份后升级，保证一旦升级失败后可以恢复到原有设备软件版本，支持对整个升级过程的可靠性检查，如设备软件版本和设备是否配套，flash空间是否足够等，确保用户的整个升级操作万无一失。支持不间断业务的软件升级ISSU；（提供功能截图并加盖原厂鲜章）  12. ★支持VLAN拓扑功能以可视的方式对网络中的VLAN资源进行管理，查看拓扑视图中所有设备节点和链路是否允许某个特定VLAN通过；（提供功能截图并加盖原厂鲜章）  13. 网络资产自动发现：在设备增加到网络资产管理的同时，系统还会自动发现该设备上可以管理的配件信息，并将这些配件加入到网络资产中进行管理，网管员可以根据不同的查询条件查询网络资产信息；对资产进行变更审计；（提供功能截图并加盖原厂鲜章） 14. 本次配置150个设备管理授权； | 1 | 套 | 三年软件升级 |
| 6 | 应用管理软件 | 1.★为保障架构稳定型与数据互通性，软件产品及组件为自主研发统一产品，不得采用OEM第三方产品或组件，提供软件著作权登记证书并加盖原厂鲜章；  2.自动发现拓扑：自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等。  3.支持动态性能阈值，学习设备性能指标的历史数据（默认5周以上），动态自学习计算出设备该性能指标的最佳阈值，当性能指标偏离于学习到的最佳阈值时，平台产生性能告警通知运维人员。  4.支持多种提醒方式，如告警实时提醒（告警板）、告警提示音、微信告警、APP告警  5.系统支持灵活定制告警级别，并支持持续出现、重复发生以及超过规定处理时间仍未解决的告警，指定升级告警的告警级别，支持重复告警过滤。  6.★可发现和定位设备深度故障，可接收分析各类SNMP trap告警，完成格式的解析，并入库，系统预定义解析超过8000种的trap类型，例如光模块失效告警、硬件故障告警等。  7.★支持通过智能算法模型对操作系统内疑似内存泄露的进程进行检测、分析并告警。同时支持从不同维度检测占用资源高的进程并发送告警，包括TopN CPU利用率进程、TopN 内存利用率进程等，并显示其变化趋势。支持对僵尸进程的数量统计以及每个僵尸进程详细信息的监控。（提供功能截图并加盖原厂鲜章）  8.★支持通过HMC对小机进行管理，包括小机逻辑分区、虚拟处理器、镜像内存等信息的监控。（提供功能截图并加盖原厂鲜章）  9.★数据库管理：提供对常见数据库服务器的监控管理,包括MySQL、Oracle、MS SQL、DB2、Informix、PostgreSQL、Sybase、Cache、达梦、虚谷、人大金仓、HBase等；  10.★支持SAP HANA 2.0数据库的监控，对OracleRAC 的服务在各个节点的启用和运行信息的监控；  11.★中间件管理：提供对常见中间件服务器的监控管理，支持对性能、状态等信息的监控，包括WebLogic、WebSphere、Tomcat、JBoss、GlassFish、TongLink、WebSphere MQ、Office Sharepoint、Active MQ、Hadoop等；  12.Web应用管理：提供对常见Web服务器的监控管理，包括Apache、IIS、Nginx、SOAP 服务、Rest 服务；  13.★平台需具备扩展性，支持自定义应用监控，不用修改原系统的任何代码，按照规则增加配置文件及脚本即可生成一种新的监控应用类型。指标的采集方式、展现形式及页面布局均可通过配置文件指定。支持手动输入shell脚本的方式进行自定义数据的采集并展现；（提供功能截图并加盖原厂鲜章）  14.★支持重要指标通过自学习的方式生成动态基线阈值，并允许手工指定某些时间段的基线值，以符合指标实际的运行情况；（提供功能截图并加盖原厂鲜章）  15.★支持对系统业务应用url序列监控及录制功能，实现对应用可用状态及响应时间的监控，提供url序列录制工具，通过点击访问多个不同的应用系统ulr地址或者同一业务系统的多个页面，完成url访问顺序的脚本录制，脚本可导入到系统，系统自动根据录制的脚本进行url序列监控，可监控录制的每个url的访问的执行耗时、http状态码、http状态值、URL可用性、页面响应字节数，并可设置页面关键字并统计关键字出现的次数；（提供功能截图并加盖原厂鲜章）  16.★可通过SMI-S协议、SNMP协议或者RESTful协议对华为、H3C、DELL、IBM、EMC、Hitachi等存储设备进行集中监控管理。DELL必须支持SC、Equallogic PS系列；IBM必须支持DS、Storwize系列，EMC必须支持ISILON、CLARiiON、VPLEX系列，华为必须支持OceanStor系列，H3C必须支持P5730存储设备和OneStore零存储设备；（提供功能截图并加盖原厂鲜章）  17.本次配置50个应用管理授权。 | 1 | 套 | 三年软件升级 |
| 7 | 服务器管理软件 | 1、平台需具备全面性，必须支持通过IPMI、SNMP和RESTful协议带外方式对主流厂商服务器进行硬件层面的精细化管理，例如服务器序列号、硬件型号、产品ID、风扇状态/风速、温度、电源功率/状态/模式、处理器状态/缓存/速度、内存大小/状态/频率、网卡状态相关信息的监控以及服务器远程控制。同时支持服务器硬件系统事件的采集，包括硬件错误事件，并支持将服务器系统事件转换为运维平台的告警信息。（提供功能截图并加盖原厂鲜章）  2、本次配置50台服务器硬件管理授权。 | 1 | 套 | 三年软件升级 |
| 8 | 移动安全网关（VPN） | 1、支持移动终端数量≥200个，加密数据流量≥200Mbps，并支持扩展为SSL VPN使用，具备≥4个电口。 2、支持在Android终端上基于沙盒技术生成隔离的安全工作区域，提供安全的办公环境，支持网络VPN专线功能，开启之后禁止个人App访问互联网，只允许工作App通过VPN访问内网资源 3、支持对封装应用的文件系统进行安全隔离，使得封装应用和个人应用的存储目录完全隔离，无法相互访问各自的文件 4、支持对封装应用的分享功能进行控制隔离，安全应用的分享功能仅在隔离区域生效，无法将文件和数据分享到个人应用中，保障数据安全。 5、支持水印保护，对截屏和拍照泄密行为进行追溯，后台可定义应用保护水印内容，包括时间戳、工号或姓名、自定义内容等信息，水印的文字大小、边框大小、字体演示、边框颜色、透明度、倾斜度均支持自定义。 6、★支持Local DB 、短信认证、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、短信认证或动态令牌的多因素捆绑认证。（提供界面配置截图） 7、★支持设备信息查看，要求能查看到设备注册时间、用户、设备名称、设备型号、手机号码、系统存储空间、是否越狱/ROOT、IMEI/UDID、WiFi MAC地址、OS版本、设备应用状态(应用名称、版本号、大小、类型、是否违规)、设备目前状态(失联|违规|擦除等)（提供界面配置截图） 8、支持密码策略设置，要求强制用户必须将密码设置为带有字母和数字的复杂密码；可强制手机超时自动锁屏；可设置修改密码规则；可设置密码有效周期，例如1一个月要重新设置一次密码；可防止暴力破解，在多吃输入错误密码时删除所有数据。 9、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。 10、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。 11、支持第三方移动App的自动封装，并发布到应用商店中，避免二次开发。 12、支持系统管理员的分级分权，对不同用户账号和资源的独立管理 13、产品制造商具有CMMI5级认证证书 | 1 | 台 | 三年质保，三年软件升级 |
| 9 | WEB应用防火墙 | 1、吞吐量≥4Gbps，并发连接数≥1000000；新建连接数≥20000，,配置接口≥6千兆电口，配置接口≥2千兆光口，支持虚拟网线以及混合部署方式。 2.、支持IPV6环境部署，包括接口/区域配置、路由配置等网络适应性功能，支持核心常用安全功能，包括僵尸网络，IPS漏洞防御，WEB应用防护等均支持IPV6技术环境。  3、支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略，负载均衡算法不少于4种。 4、★支持一键分析当前访问控制策略异常问题（包括策略风险访问、冗余、冲突、重合、端口放通过大等），并针对异常问题划分不同等级，提供问题描述、危害、以及解决方案和关系图例说明。（提供功能截图证明并加盖制造商公章）  5.、支持模拟策略匹配的访问控制规则，即输入源目的IP、端口、协议五元组信息，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；  6、支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制。 7、★支持采用安全智能检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测（提供功能截图证明并加盖制造商公章） 8、支持网络访问控制，配置特定网络区域只允许指定的IP地址或IP范围对外进行访问，防止内部伪造源IP对外DoS攻击的情况； 9、支持蜜罐检测功能，定位网络中感染僵尸网络病毒的真实主机IP地址； 10、支持对已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。 11、产品具备独立的入侵防护漏洞规则特征库，特征总数在7400条以上； 12、★支持非法进程链展示，通过对进程进行溯源，对违规的进程呈现给安全管理员，比如主进程释放子进程，子进程调用文件等行为进行细粒度展示，并可在防火墙界面通过联动一键处置恶意进程（提供功能截图证明并加盖制造商公章） 13、支持基于勒索病毒的攻击链提供勒索病毒防护配置向导，包含防护对象、勒索病毒常用端口、漏洞、弱口令的自定义定时识别。 14、★支持自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证；（提供功能截图证明并加盖制造商公章） 15、支持针对用户安全的风险汇总，将失陷类的安全事件按照已失陷、高风险、中风险、低风险等优先级展示，并通过威胁性和确定性的维度展示失陷主机风险的分布情况； 16、支持高级威胁事件分析，并展示热点事件详情，如全网威胁情报、高级黑客、持续性攻击、网站存在后门、黑链、感染僵尸网络、病毒感染、外发攻击等，并将高危事件推送到运维管理员手机微信端进行预警； 17、产品制造商是国家互联网应急响应中心网络安全应急服务国家级支撑单位 18、产品制造商具备CMMI 5认证证书 | 1 | 台 | 三年质保，三年软件升级 |
| **二、等保安全运维服务** | | | | | |
| 1 | 网络安全巡检服务 | 提供周期巡检服务，每季度一次例行网络安全巡检，巡检内容为网络安全系统定期升级更新、网络安全告警日志分析、网络安全整改建议、网络安全策略优化等，出具相应的巡检报告。提供三年服务。 | 1 | 项 | 三年服务 |
| 2 | 网络安全应急处置 | 提供1年网络安全应急处置服务，一旦医院发生网络安全事件，一般事件半小时内远程响应技术指导，重要事件2小时内现场响应处置，防止网络瘫痪、系统中断等对医院运营带来影响。提供三年服务 | 1 | 项 | 三年服务 |
| 3 | 重大节日网络安全保障 | 提供重大节日网络安全保障服务，全国两会、国庆、春节等重大节日期间，网络安全服务机构提供远程值守，24小时待命，发生网络安全事件可及时远程响应，根据事件严重程度可随时赴现场响应处置。提供三年服务 | 1 | 项 | 三年服务 |
| 4 | 网络安全培训 | 针对全院人员进行国家网络安全法普法培训和医院职工安全用网培训，提升网络安全意识、提高安全用网技能。每年一次，提供三年服务。 | 1 | 项 | 三年服务 |
| 5 | 网络安全应急演练 | 服务方应参照等保要求协助需方制定完善应急预案，开展应急演练，每年一次，提供三年服务，按流程处置突发安全事件： （1）服务方应协助需方制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容,进行应急预案的演练； （2）服务方应针对突发的安全事件，及时进行评估风险，按需对高危对象进行紧急安全策略加固； （3）服务方应针对突发的安全事件，对病毒或恶意代码进行安全扫描与紧急查杀，并采取其他措施消除安全风险； （4）服务方在安全事件报告和响应处理过程中，应按流程进行汇报，分析和鉴定事件产生的原因，收集证据，记录处理过程。 | 1 | 项 | 三年服务 |