项目名称	数量	主要技术规格及要求
官网安全防护	1年	支持云防护模块、可用性监测、防篡改模块、实时攻击监测模块、一键关停、永久在线、手机 APP、安全防护报告、7*24 小时安全运维，防护节点 2 个，防护带宽 10Mpbs，智能识别扫描器攻击，快速封锁扫描 IP，专业团队根据网站调整防护规则，提供网站实时受攻击情况展示大屏，专家团队 24 小时监测门户网站安全状况，支持短信、邮件等安全告警，在监测发现安全事件后，及时通报事件发生具体情况，并协助对事件进行处置。每月输出网站安全报告，按我院需求输出年度网站安全报告。
安全设备续保	1年	1、大数据智能安全平台一台（安恒 DAS-ABL-A800）及网络流量综合探针一台（安恒 DAS-ABL-SP600）特征库、规则库升级授权。 2、WEB 应用防火墙一台（深信服 WAF-1000-B1200）云智订阅软件(特征库)升级授权。 3、上网行为管理一台（深信服 AC-1000-D600）应用识别&URL 库升级授权。
网络安全服务	1年	一、资产及业务梳理：1、主要梳理内容包括物理环境、网络拓扑，网络设备、安全设备、系统服务器、设备接口互联及陈列情况，补齐线路互联标识等。2、根据业务流程，主要梳理内容包括安全设备的管理方式，网络及安全设备的策略配置，通过访谈、收集并分析相关设备的配置，梳理业务走向。3、每次完成服务后，须编制《资产及业务台帐》。4、服务周期（年/次）：一年 1 次。 二、网络安全巡检：1、运维人员按照检查表依次对信息系统涉及物理环境、网络平台、主机系统、应用系统和安全设施进行全面和严格的专项巡检，检查结果留存归档。包括设备版本与基本配置、接口配置与状态、日志信息状态、访问控制策略、报警信息等关键工作指标进行例行监控。2、根据业务系统流程，对现有的设备做策略优化及更新。3、对于现有的设备进行版本升级、规则库升级、病毒库升级、证书更新等。4、对于现有的客户端进行扫描、查杀或者其他病毒查杀的操作，发现无法查杀的潜在威胁进行现场及时处理。5、每次完成服务后，须编制《网络安全巡检报告》。6、服务周期（年/次）：一年 12 次。 三、故障处理：巡检过程中，发现设备故障后，为了确保组织业务系统的持续运行，立即对故障进行处理。2、每次完成服务后，须编制《故障分析处理报告》。3、服务周期（年/次）：按需提供。 四、信息设备安全审计：1、网络及安全设备日志的收集与分析，进一步分析整体的安全情况。2、服务器、存储设备日志的收集与分析，重点在于运行的稳定性和安全性。3、主要对业务系统权限控制的有效性及操作行为的合理性。4、每次完成服务后，须编制《安全审计报告》。5、服务周期（年/次）：一年 4 次。 五、安全通告：1、定期提供最新病毒的防御方案、最新系统漏洞信息及其修复方法、最新发生的安全事件等内容的安全通告报告，并及时按照我院需求进行落实修复工作。2、每次完成服务后，须编制《安全通告》。3、服务周期（年/次）：按需提供。

		六、安全应急响应：1、10 人以上应急保障团队，出现安全事件，两小时内现场应急。主要包括一下 3 种情况的应急响应：1）、病毒和蠕虫事件；2）、黑客入侵事件；3）、误操作或设备故障事件。根据安全事件的影响级别启动应急响应级别。事前帮助我院建立应急响应组织、应急响应流程、应急响应实施方案。事中安全事件现场处理，减少事件影响。事后对安全事件溯源，包括事件后消除，弥补系统脆弱行，分析原因，总结教训，完善安全策略，服务和过程。2、为保证服务质量及专业性要求，响应供应商需提供由中国网络安全审查技术与认证中心颁发的信息安全应急处理服务资质进行佐证。3、每次完成服务后，须编制《安全事件处理报告》。4、服务周期（年/次）：按需提供。 七、应急预案：1、根据信息系统及其承载业务信息的重要性，以及我院网络环境和业务特点，结合国家、地区和行业等最新信息安全政策和标准，协助我院制定适用于我院的应急预案，明确应急响应组织以及预防、预警机制，针对可能的安全事件编制规范的应急处理流程。2、每次完成服务后，须编制《安全应急预案》。3、服务周期（年/次）：一年 1 次。 八、应急演练：1、根据应急预案规定的应急处理流程协助我院编制符合我院场景的应急演练方案，并进行相应模拟演练，一方面使相关方熟悉应急响应流程，提高对安全事件的响应能力；另一方面验证预案正确性和适用性，进行总结分析，根据需要对应急预案进行修订。使得相关人员了解应急流程和自己的责任，在安全事件发生时，能够有条不紊开展工作，最大程度降低安全事件带来的负面影响和损失。2、每次完成服务后，须编制《安全应急演练方案》和《安全应急演练总结报告》。3、服务周期（年/次）：一年 1 次。 九、安全加固：1、通过风险评估确认优化需求后，制定一个完备且适合的安全策略，在运行过程中，根据现有的策略基础做优化调整。2、针对网络安全设备、主机系统、应用系统等设备的口令策略、账户权限、网络服务、访问控制、我院鉴别等加固项进行加固。3、服务周期（年/次）：一年 4 次。 十、基线检查：1、根据既定的检查规范及方法，采用人工检查用表（checklist）、脚本程序或基线扫描工具对评估目标范围内的主机系统安全、数据库安全、中间件安全等进行系统的策略配置、服务配置、保护措施以及系统和软件升级、更新情况，是否存在后门等内容进行检查。2、通过 web 后门检查工具，针对网站所有文件进行安全扫描，发现网站上可能存在的 webshell、网页后门等恶意文件。3、每次完成服务后，须编制《基线检查报告》。4、服务周期（年/次）：一年 4 次。 十一、网络安全风险评估：1、基于我院信息系统现状，参照国家信息安全风险评估规范，对资产、威胁、脆弱性、安全措施进行识别和分析，确定风险计算模型，从物理层、网络层、系统层和应用层进行评估，全面分析系统面临的信息安全风险。2、为保证服务质量及专业性要求，响应供应商需提供由中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质进行佐证。3、每次完成服务后，须编制《风险评估报告》。4、服务周期（年/次）：一年 2 次。 十二、风险处置：1、风险评估后，通过风险转移、风险规避、风险接受、风险降低等系统化方法处置所发现的风险。2、每次完成服务后，须编制

		《风险处置报告》。3、服务周期（年/次）：一年 2 次。 十三、数据安全风险评估：1、根据国家数据安全法，提供专业的数据安全专家通过相关工具或测试，对全院数据的运行转态、资产情况、分级分类、数据库运行安全、数据运行的脱敏状态、敏感数据危险操作防范状态、数据库撞库防御状态、识别 SQL 注入攻击的能力状态、数据威胁等方面的能力进行深度排查评估，并给出相应的解决方案或建议。2、每次完成服务后，须编制《数据安全风险评估报告》。3、服务周期（年/次）：一年 2 次。 十四、渗透测试：1、通过模拟黑客使用的工具、分析方法对网站及业务系统进行安全测试，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误以及其他专项内容。2、为保证服务质量及专业性要求，响应供应商项目经理需提供由中国信息安全测评中心颁发的注册渗透测试工程师或注册渗透测试专家服务资质进行佐证。3、每次完成服务后，须编制《渗透测试报告》。4、服务周期（年/次）：一年 1 次。 十五、重保服务：1、大型活动安全保障服务。针对重大会议、网络安全攻防演练、国家规定的法定节假日、政治活动或其它具有广泛影响的活动，按照我院需求派遣专业安服人员以现场或远程值守的方式提供网络安全保障服务，协助处理信息安全事件。包括前期重要业务的检查、安全扫描、网络安全加固等准备工作，确保在重要敏感时期的网络安全。2、每次完成服务后，须编制《重保安全服务实施报告》。3、服务周期（年/次）：按需提供。 十六、网络安全培训：提供注册信息安全专业 CISP 一个方向的现场实训及所有考试费用，提升安全人员综合安全能力来保障业务安全稳定的开展，以满足关键信息安全岗位人员的能力要求。3、服务周期（年/次）：一年 1 人次，提供 1 张 CISP 认证证书。 十七、安全意识培训：1、面向单位内全员开展专业的网络与信息安全意识培训，提高职工个人隐私保护、常规攻击防护、信息安全管理等能力，增强个人网络安全防护意识，规避网络攻击风险。2、每次完成服务后，须编制《网络信息安全培训 PPT》。3、服务周期（年/次）：一年 1 次。 十八、安全运维培训：1、提供面向运维人员关于安全配置、安全防护、安全处置等安全运维知识的专项培训。2、每次完成服务后，须编制《网络安全运维培训 PPT》。3、服务周期（年/次）：一年 1 次。 十九、网络安全管理制度体系建设：1、根据会昌县人民医院实际情况，按照中央网信办对落实网络安全工作责任制的要求，为我院建立起一整套符合三级医院评审要求和相关法律规定的、能够促进医院安全管理水平提高的网络信息安全管理制度。2、每次完成服务后，须编制《网络信息安全管理制度》。3、服务周期（年/次）：一年 1 次。 二十、网络安全总结：1、根据我院现场网络安全情况，从安全策略与制度、技术防护体系、安全意识培训、安全事件回顾和风险评估漏洞管理等多个方面总结过去一段时间内（如年度、季度或特定项目周期）的网络安全工作，分析当前面临的网络安全威胁与挑战，评估已实施的安全措施的有效性，并提出未来改进和优化的方向。为我院提供清晰的网络安全态势

		感知，促进安全策略的持续完善与执行。2、内容包括不限于网络安全工作成果、网络安全策略、规章制度及其实施情况，安全设备的部署与运行状况，网络安全意识培训情况等以及相关防护数据统计表、图表等辅助材料，按我院需求输出报告。3、每次完成服务后，须编制《网络安全总结报告》。4、服务周期（年/次）：一年 2 次。 二十一、等级保护咨询服务：1、按照等级保护定级备案流程，协助我院进行定级备案工作，遵照等级保护基本要求，通过对我院系统的技术与管理的角度进行差距分析，并提交整改方案，协助整改，最终帮助我院系统符合等级保护的要求。2、每次完成服务后，须编制《等级保护建设方案》。3、服务周期（年/次）：按需提供。