黄山市第三人民医院安全等级保护建设及等保测评服务采购项目采购需求

一、服务要求

（一）项目描述

1、项目背景

随着网络安全形势的日益严峻，网络与信息安全已被提升为国家战略，习总书记提出了“没有网络安全就没有国家安全”的重要论述，明确要求“全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。”国家有关部门先后出台了一系列文件，明确了等级保护的重要性。

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施，其中第二十一条规定“国家实行网络安全等级保护制度”。等级保护工作正式入法，等级保护制度已成为新时期国家网络安全的基本国策和基本制度。所有网络运营者和关键信息基础设施运营者均有义务按照网络安全等级保护制度的要求对系统进行安全保护。2018 年 6 月 1 日，“2018 年网络安全执法检查工作电视电话会议”在北京主会场召开，会议进一步明确了网络安全的重要性，并需要展开执法检查。为了履行国家《网络安全法》法律义务，满足行业监管机构的合规要求，有效规避网络安全合规风险，各单位需要积极开展等级保护建设工作。

随着 2019 年 5 月 13 日《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》标准的正式发布国家网络安全等级保护工作正式进入 2.0 时代。等保 2.0 充分体现了“一个中心三重防御“的思想。一个中心指“安全管理中心”，三重防御指“安全计算环境、安全区域边界、安全网络通信”，在等级保护的规范下，网络系统需要按照符合备案级别对应的安全标准进行安全建设。应落实网络安全等级保护相关要求，加强网络系统安全防护能力以及核心数据的保护建设工作。

2、建设目标

本次安全加固建设将对黄山市第三人民医院云上业务进行安全加固，确保相关业务持续稳定运行。通过新增下一代防火墙（含 IPS、AV、WAF 模块）、主机安全、数据库审计共同构建网络系统安全防护体系。针对本项目中一套系统做一次三级等保，并确保通过测评。

（二）采购清单及参数要求

序号	产品名称	产品配置	数量	单位
1	下一代防火墙	1、带宽性能≥200Mbps，新建会话/秒（七层）≥20000，并发会话数（七层）≥1000000； 2、具备链路故障检测功能，通过 ARP、DNS、PING 协议等	1	套

		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； 3、具备静态路由和多播路由，支持 RIP、OSPF、BGP 等动态路由协议； 4、★产品内置应用特征识别库，支持不少于 9000 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；**（需提供产品功能截图证明）** 5、具备基于国家/地区维度的流量管理功能； 6、★支持对 HTTP、HTTPS、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；**（需提供产品功能截图证明）** 7、具备僵尸网络检测功能，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； 8、支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性； 9、★支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维；**（需提供产品功能截图证明）** 10、支持对当前应用控制策略异常分析，包括策略风险访问、策略冗余、策略冲突、策略重合、端口放通过大等问题，并提供相关解决方案便于用户快速调优； 11、支持实时检测当前网络的整体安全状况，显示当前安全风险问题，并提供建议方案便于快速开展日常安全运维； 12、所投产品生产厂商获得国家互联网应急中心认证的甲级网络安全应急服务支撑单位。**（需提供相关证明材料）**		
2	主机安全软件授权	1、本次要求产品纯软交付。包括控制平台，并提供 26 个服务器授权；	1	套

		2、产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；同时也支持硬件管理平台交付； 3、★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；**（需提供产品功能截图证明）** 4、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； 5、★支持基于系统内置弱密码字典和自定义弱密码字典的检查功能，弱密码检测支持至少包括 SSH、RDP、MySQL、Tomcat、Redis 等应用类型，可按照空密码、自定义弱密码、密码长度小于 8、字符种类小于 3 等常见弱密码类型进行分类查看；**（需提供产品功能截图证明）** 6、通过智能识别终端环境情况（低配硬件、老旧设备等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整客户端的资源占用（CPU、IO 等），为业务让出资源，不卡业务，对业务零摩擦； 7、具备基于本地缓存信誉检测与全网信誉检测，构建全网信誉库的检测引擎，做到内网一台威胁，全网感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率，减少终端资源开销； 8、★支持禁止黑客工具启动，包含：xuetr、ProcessHacker、PCHunte、Mimikatz 等自启动，可以防止黑客攻击；**（需提供产品功能截图证明）** 9、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； 10、支持 windows 服务器 RDP 远程登录保护，可开启 RDP 远程登录二次认证，以防止黑客对服务器的入侵；**（需提**		

		供产品功能截图证明） 11、统计单个攻击源及分布式攻击源的暴力破解检测，支持按照 RSSH、SMB 和 MSSQL 类型进行封堵并自定义爆破阈值，可对封停时间进行自设置； 12、支持 agent 安装目录的文件保护，可以保护 agent 目录和文件实时监控驱动文件，可以保护 agent 的服务/进程/文件不被恶意删除，以免影响正常功能，导致用户的终端受到病毒入侵； 13、所投产品的生产厂商具备云安全成熟度成熟度模型 CS-CMMI 5 认证。**（需提供证书复印件）**		
3	数据库审计	1、本次提供实例授权数：4 2、支持主流大数据平台数据库的解析与审计，包括 Hbase、MongoDB、elasticsearch 等；**（需提供产品功能截图证明）** 3、支持同时对传统数据库和大数据平台数据库进行审计； 4、支持基于深度协议解析技术自动对数据库进行风险评估，并且提供分值参考，便于用户直观发现威胁状态；**（需提供产品功能截图证明）** 5、★支持对执行时间、数据库账号、来源 IP、来源端口、来源 MAC、客户端工具、目标 IP、目标端口、目标 MAC、数据库实例名、SQL 语句、执行时长、SQL 类型、SQL 命令、操作对象、二级操作对象、SQL 行数、SQL 状态等至少 25 个条件进行审计；**（需提供产品功能截图证明）** 6、★支持自动将 SQL 语句分为 login、logout、DDL、DML、DCL、TCL、privilege 等操作类型；**（需提供产品功能截图证明）**	1	套
4	等保测评	一套系统完成一次三级等保测评。	1	套

5	服务器	配置 2 个 Intel Xeon 银 4208 (2.1GHz/8 核/11MB/85W) 处理器，最多可支持 2 个处理器；配置 2*32GB 2Rx4 DDR4 内存，最多可支持 24 根 DDR4 内存；配置 RAID0/1/10/5；配置 3 块 1.92TB 6G SATA 2.5in EV SSD 通用硬盘模块；2 个板载 1GB 以太网端口，可选高级网络适配器选件；配置 2 个 550W 热插拔电源（94%转化率），可选冗余；标配导轨；2U 机架式。	1	台

二、商务要求

序号	内容	要求
1	**合同签订地点**	黄山市第三人民医院
2	**提供服务的期限**	合同签订并接采购人通知后 10 天内完成等级保护建设工作，等级保护建设完成后 10 天内出具《整改建议》，采购人整改完成后，中标人进行复测并在 20 天内出具《测评报告》。
3	**验收**	完成后验收，确保通过三级等保要求，出具正式测评报告。
4	**付款**	**付款人：**黄山市第三人民医院 **付款方式：**合同签订后支付合同总额的 50%，验收合格后付清余款。
5	**履约保证金**	**是否收取履约保证金：** **√否； □是**