一、总则与范围

本项目为网络安全设备采购与部署项目，包含本文件中所有列明的硬件设备、软件授权、系统集成、施工安装、测试验证、培训与售后服务的全部工作，须形成完整、可交付、稳定运行的网络安全防护体系。

二、总体要求

本次项目采用交钥匙工程模式。中标供应商须独立完成项目从深化设计、到货、安装调试、系统集成、施工改造（如光纤线路）、最终验收及培训的全过程所有工作。院方不参与具体技术实施，仅提供必要的现场配合与最终验收。投标报价为一次性闭口包干价，应包含但不限于完成本项目所有工作所需的设备购置费、软件授权费、材料费、施工费、运输费、保险费、税费、利润、风险费、质保期内所有升级维保费用等。合同签署后，未经院方书面同意，不得以任何理由追加任何费用。项目验收通过后，中标供应商须向甲方完整移交所有相关文档资料。

三、采购设备清单

序号	设备名称	技术规格与性能要求	数量	单位
1	空调	1.核心性能：总制冷量≥10.5kW，显冷量≥10.0kW，显热比≥0.95。 2.硬件配置：室内机为 G4 等级回风过滤，风机采用离心式设计，内风机支持 AC/EC 可选，风量≥3000m³/h，运行噪声≤65dB(A)，外壳材质为热镀锌板，节流部件为电子膨胀阀；室外机压缩机为转子式，风机采用 AC 无极调速，运行噪声≤58dB(A)，制冷剂采用 R410A。	1	台
2	态势感知平台	1、核心性能：存储容量≥14.4TB，原始流量存储时长（1Gbps 带宽）≥900 天。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 硬件配置：标准 2U 机架式，内存≥96GB，系统盘≥480GB SSD，数据盘≥4×4TB，冗余电源，接口≥4 千兆电口+4 万兆光口。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2、核心功能：	1	台

		2.1 支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示，支持不少于 15 个业务展示界面，支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便单位结合自身业务需求进行个性化设置。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.2 提供多源数据关联分析、灵活的威胁建模、丰富的上下文信息展示能力，帮助提升威胁检测的精准度。 2.3 持资产责任人管理，覆盖资产全生命周期：自动发现、入库审核、离线识别、图库自动匹配、手动导入及退库、自定义命名等。支持设置全局退库周期与数据更新频率，并提供主机资产分级及责任人绑定能力。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.4 支持跨三层取 MAC 地址，识别资产 MAC 地址。 2.5 支持展示服务器的脆弱性风险分析、详情，热点漏洞情况。 2.6 支持勒索专项检测页面，统一展示和管理勒索安全告警，按感染途径分类（常用端口、漏洞、RDP 爆破、病毒感染、黑客攻击、C&C 通信等），展示受害资产及 TOP5 攻击数，列表呈现勒索事件详情（时间、描述、定性、风险等级、受害者 IP、攻击次数等），帮助单位有效应对勒索风险。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.7 具备实时告警分析能力，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面分析。 2.8 提供 Web 登录行为智能识别能力，支持基于响应状态码、响应内容、URL、关键字、IP 地址、资产组等灵活配置登录成功规则；并通过机器学习引擎持续学习，自动优化登录成功判定模型。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。		

		2.9 支持可视化展示威胁影响面，通过大数据分析清晰呈现失陷主机对其他主机的影响及受损情况，便于快速处置；支持首页搜索框输入 IP/域名/URL/端口/通信对进行检索，列表展示横向攻击、违规访问、风险访问、可疑行为等详情，构建全方位持续检测能力；支持入口点溯源，分析首次失陷、疑似入口点、首次攻击等信息，帮助管理人员快速定位攻击入口。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.10 具备实时告警分析能力，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面分析。 2.11 支持从不同维度呈现处置报告，且能够快速基于月、季、年维度生成报表，报告的导出方式支持至少包括 ppt、pdf、doc 三种方式，满足单位不同场景的汇报需求。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。		
3	潜伏威胁探针	1、核心性能：网络层吞吐量≥500Mbps，应用层吞吐量≥160Mbps。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 硬件配置：标准 1U 机架式，接口≥6 千兆电口。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2、核心功能： 2.1 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。 2.2 支持命令注入、XSS、SQL 注入、Webshell 上传、XXE、PHP/JAVA 代码、反序列化等十余种攻击检测的自定义启停，针对命令注入、SQL 注入等核心检测项，可灵活切换高检出或低误报模式。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.3 支持自动发现网络中的拓扑设备并生成网络拓扑图，直	1	台

		观呈现网络整体架构。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.4 支持敏感信息检测功能，内置敏感信息库。 2.5 支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断。 2.6 支持以源目 IP、源目端口和日志类型、日志来源来进行白名单审计。 2.7 内置 IPS 漏洞特征识别库、应用识别库、WEB 应用防护库、僵尸网络识别库、实时漏洞分析识别库。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.8 提供三权分立的用户管理能力：系统管理员、审计管理员、安全管理员、普通管理员四个角色相互独立。 2.9 内置简单命令行管理窗口，便于基础运维调试。		
4	Web 应用防火墙(WAF)	1、核心性能：网络层吞吐量≥4G，HTTP 应用层吞吐量（WAF）≥300M，HTTP 新建连接数≥6 万，HTTP 并发连接数≥150 万。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2、硬件配置：标准 1U 机架式，接口≥8 千兆电口+2 千兆光口。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 核心功能： 2.1 支持虚拟 WEB 应用防火墙的创建、启动、关闭、删除功能；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、安全策略等功能。 2.2 支持 NAT44 、NAT64、NAT66 地址转换方式。 2.3 具备路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式，适用于现网不同的边界防护需求。 2.4 产品支持根据路由和协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，	1	台

		至少包括带宽比例、加权流量、线路优先等。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.5 支持账号风险检测，支持检测多余入口、弱口令、暴力破解、失陷账号。 2.6 支持 OWASP 定义 10 大 web 安全威胁防护，保护服务器免受基于 Web 应用的攻击，SQL 注入防护、XSS 攻击防护、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，内置超过 4500 中 WEB 应用攻击特征。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.7 支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御。支持对 15 层及以上的压缩病毒文件进行检测和拦截。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.8 支持 https 解密功能，支持 TCP 代理和 SSL 代理。 2.9 支持用户账号全生命周期保护，包括多余入口、弱口令、暴力破解及失陷账号检测，防止账号被暴力破解导致非法提权。 2.10 支持对 SYN、UDP、ICMP、DNS、HTTP、TCP、IP 等进行 DDOS 防护。 2.11 支持联动云端智能运营平台，实现流量日志分析、事件聚合及云端专家研判，安全事件预警和处置可通过移动端实时接收与处理。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.12 支持 IPv4/IPv6 双栈工作模式，以适应 IPv6 发展趋势。		
5	终端安全管理系统	1、核心性能：支持软件化部署；支持虚拟化部署；支持多操作系统。服务器授权≥10 套，PC 授权≥200 套。 2、核心功能： 2.1 支持资产台账管理，全面记录资产详细信息。支持 USB	1	套

		设备管控。 2.2 支持弱密码检测，系统内置弱密码规则库，可自定义弱密码规则库。 2.3 支持显示攻击事件命中的 ATT&CK 相关技术，便于用户了解攻击者的操作行为和目的，评估整体影响面。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.4 支持安全策略一体化，单条策略即可覆盖多项安全功能的配置。 2.5 支持客户端错峰升级，可自定义同时升级的最大终端数量，防止大规模终端集中更新引发网络拥塞或 I/O 风暴。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.6 具备资源智能识别能力，可自动识别老旧设备及设备资源占用状态，动态调度监控与扫描任务。 2.7 支持基于 SSVC 决策树模型的优先级排序,综合漏洞属性、外部情报及资产暴露面等多维度，在 CVSS 评分基础上进一步收敛高危漏洞数量，输出响应、关注、观察三级结果，辅助单位快速聚焦优先处置的漏洞威胁。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.8 提供查杀工具的管理中心派发能力，可在管理端一键批量下发到内网各终端，快速清除威胁。 2.9 提供勒索病毒防护体系入口，直观展示近七天防护成效，包括已处置恶意文件、拦截可疑行为、阻止未知进程操作及暴力破解攻击次数。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。 2.10 支持 windows 服务器远程连接保护，可开启远程连接二次身份验证机制，以防止黑客对服务器的入侵。【提供包括但不限于检测报告、技术白皮书、彩页、官网截图等任意一种证明材料】。		

6	铠装光纤改造	施工要求：对指定的住院楼（1-8 层）网络骨干光纤进行更换，全部采用室外铠装单模光纤。乙方负责新光纤的敷设、熔接、标签制作、链路测试，并确保新线路性能指标完全满足并优于现有业务传输要求，所有废旧线路由乙方负责清理。	1	批
7	安全设备检测	依据院方提供文档对所有安全设备、服务器、交换机进行全面登记、检测、评估工作。对现有安全设备提供一次密码重置服务。	1	批

四、工程施工与集成要求

1.现场勘查：合同签订后，乙方须进行详细的现场勘查，并在 5 个工作日内提交经甲方确认的《施工图纸》。

2.安装部署：所有硬件设备在机房内按要求完成标准机架安装、固定、接线。各安全设备与医院现有网络设备（交换机等）完成互联互通配置。终端安全管理系统客户端需在医院指定的 200 台 PC 和 10 台服务器上完成静默部署与激活。如现有机房机柜不满足安装要求，厂家自行配置相应机柜。

3.本楼层中部已布设空调供电主回路，需从该主回路单独接引一路专用供电线路至机房区域，线路配置需完全满足精密空调及机房整体安全用电规范要求，该线路部署涉及的全部耗材、配件采购及施工费用，统一纳入本项目整体预算范畴。

4.系统联调与策略配置：态势感知平台须与潜伏威胁探针、WAF 完成数据对接和策略联动调试。根据医院网络现状，完成所有设备的初始安全策略配置，形成基线。

5.测试验证：乙方须进行不少于 48 小时的系统连续稳定运行测试，并提供《系统测试报告》，报告应包含功能性、性能及稳定性测试结果。

6.培训：乙方须对甲方相关技术人员进行不少于 8 学时的现场培训，内容涵盖系统日常操作、策略维护、日志查看和应急处理。

五、交付成果与资料要求

项目最终验收时，乙方必须向甲方提交以下全套纸质及电子版（PDF+DOC 可编辑格式）文档资料：

1.技术文档：产品出厂检测报告、原厂授权证明、产品操作手册、管理员手

册。

2.设计实施文档：深化设计方案、设备安装部署点位图、网络拓扑图、IP地址规划表。

3.工程记录文档：到货签收单、设备安装调试记录、各系统配置文件（电子版）。

4.测试与验收文档：光纤链路测试报告（OTDR 报告）、系统联调测试报告、连续稳定运行测试报告、项目最终验收报告。

5.培训文档：培训教材、培训签到表、培训效果评估表。

6.管理资料：项目全套设备及软件清单（含序列号）、售后服务承诺书、服务工程师联系表。