用户需求书

一、项目概况

1、项目名称：白沙县人民医院网络安全项目

2、项目编号：HNJC2022-065

3、采购预算：79.3 万元

4、资金来源：财政资金

二、采购需求清单、参数

序号	设备名称	单位	数量	备注
（一）	安全感知管理平台一体机(SIP 一体机)	1	台	报价中必须包含所有货物及服务的价格及运输保险、装卸、培训辅导、质保期售后服务、全额含税发票、雇员费用等，合同的执行以交付时间为准。
（二）	医保网出口防火墙	1	台	
（三）	日志审计	1	套	
（四）	全网行为管理及准入	1	台	
（五）	服务器区防火墙	1	台	
（六）	终端安全管理系统	1	台	
（七）	超融合一体机	1	套	
（八）	计算服务器虚拟化软件	2	套	

（一）、安全感知管理平台一体机(SIP 一体机)

1、设备采用外观≥1U 的机架式服务器，配置 4TB 企业级硬盘，标配≥6 个千兆电口，≥2 个万兆光口，配置单电源；

2、支持自动识别网络内部主机网段和外网网段；支持通过流量中的应用内容自动区分网络内部网段 IP 是属于 PC 还是服务器；

3、支持基于流量实时漏洞功能，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（提供产品界面截图并加盖厂商公章）；

4、支持自动识别已知服务器，通过被动检测机制，对经过探针的流量进行分析，识别已知服务器对外提供的所有服务、已开放端口及端口传输的协议/应用等；

5、支持通过云端沙盒对全球威胁情报源进行验证，提取有效信息形成规则定期更新到僵尸网络识别库，增量提升检测能力；支持 DNSFlow 分析引擎，利用机器学习算法结合威胁情报，能够从大量的样本中进行学习，总结其伪装的规律，从而发现伪装的恶意 DNS 协议；

6、支持对服务器、客户端的各种应用发起的漏洞攻击进行检测，包括 20 种攻击类型共 9000+以上规则；

7、具备安全日志分析引擎、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（提供产品界面截图并加厂商公章）；

8、支持检测主机与 C&C 服务器通信行为，支持区分国内外区域；支持检测从未知站点下载可执行文件、访问恶意链接、使用 IRC 协议进行通信、浏览最近 30 天注册域名、下载文件格式与实际文件不符、基于行为检测的木马远控、比特币挖矿等可疑访问行为，支持区分国内外区域和显示可疑行为访问趋势（提供产品界面截图并加盖厂商公章）；

9、支持接入防火墙、上网行为管理、终端 EDR、WAC 无线控制器、DAS 数据库审计和潜伏威胁探针等设备,并支持在页面中显示安全组件接入的数量和状态（提供产品界面截图并加盖厂商公章）；

10、为了保证设备间的功能联动性，需支持与本项目上网行为管理设备进行联动响应，同步上网行为管理设备认证用户，实现与安全事件关联（提供产品界面截图并加盖厂商公章）。

（二）、医保网出口防火墙

1、性能指标：网络层吞吐量≥6Gbps，应用层吞吐量≥2Gbps，防病毒吞吐量≥800M，IPS 吞吐量≥500M，全威胁吞吐量≥400M，并发连接数≥180 万，新建连接数≥6 万；硬件指标：1U 规格，硬盘容量≥64G SSD，单电源，标配≥6 个千兆电口+4 个千兆光口；

2、支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持静态路由，ECMP 等价路由；支持多播/组播路由协议；

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路由选路功能（提供产品界面截图，并加盖厂商公章）；

4、支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换；

5、访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，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、设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间（提供产品界面截图，并加盖厂商公章）；

7、支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；

8、设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在 50 万条以上；支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；支持对终端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（提供产品界面截图，并加盖厂商公章）；

9、支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护；

10、支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息（提供产品界面截图，并加盖厂商公章）；

11、支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况。

（三）、日志审计

1、性能指标：主机审计许可证书数量≥50，平均每秒处理日志数≥1200 条/秒；硬件指标：2U 规格；可用存储空间≥2TB；单电源；标配≥6 个千兆电口，≥2 个万兆光口；

2、支持展示关联事件类型分布 TOP5、对象 IP 统计 TOP5、事件等级分布、事件趋势、事件列表；点击查看日志可自动跳转到日志检索；

3、基于审计总览形式，展示整体的审计状况，包括当前存储空间、关联事件、审计事件、日志传输趋势（提供产品界面截图并加盖厂商公章）；

4、支持日志进行归一化操作后，对日志等级进行映射，根据不同设备会统计不同等级下的日志数；

5、内置 40+条审计策略，包括操作系统、数据库；可启用/禁用策略，默认匹配上后都会产生页面告警；

6、支持批量或者单台设备数据转发，且可支持同时转发给多台设备，使用的是 syslog 转发，支持对接同品牌安全感知平台（提供产品界面截图并加厂商公章）；

7、支持按照不同的解码方式解码成不同的目标内容，编码格式包括 base64、Unicode、GBK、HEX、UTF-8 等（提供产品界面截图并加盖厂商公章）；

8、为了保障安全体系的兼容性和一致性，日志审计系统产品需与本项目安全感知平台、防火墙、全网行为管理为同一生产厂商

（四）、全网行为管理及准入

1、性能指标：网络层吞吐量≥4.8Gbps，并发连接数≥40W，新建连接数≥8000，支持用户数≥3000；硬件指标：1U 规格；存储≥ 1TB；单电源；标配≥4 个千兆电口，≥4 个千兆光口；

2、支持网关模式、网桥模式、旁路模式、多路桥接模式，以及两台及两台以上设备同时做主机的部署模式；

3、支持 P2P 智能流控，通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；（提供产品界面截图，并加盖厂商公章）

4、支持绑定 IP 认证、绑定 MAC 认证，及 IP/MAC 绑定认证等；支持当用户 MAC 地址变动时，需要重新认证；

5、支持基于时间段的带宽划分与分配策略；支持对单个用户/用户组设置日流量、月流量配额功能；

6、支持二维码认证，管理员扫描访客的二维码后对其网络访问授权；（提供产品界面截图，并加盖厂商公章）

7、支持基于通道流速、通道总用户数、通道活跃用户数等维度的流速趋势分析报表；支持基于时间/用户/用户组/上行/下行/总体等维度的域名流量、域名访问排行；

8、支持 Web 访问质量检测，针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单（提供产品界面截图，并加盖厂商公章）；

9、支持给应用识别规则库里的每一种应用列上图标，至少能识别 2700 种主流应用，且能将识别的应用智能分类，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖 6 大类；易于管理员了解应用的特征和进行策略配置；（提供产品界面截图，并加盖厂商公章）

10、支持基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中；（提供产品界面截图，并加盖厂商公章）

11、针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）；（提供产品界面截图，并加盖厂商公章）

（五）、服务器区防火墙

1、性能指标：网络层吞吐量≥6Gbps，应用层吞吐量≥2Gbps，防病毒吞吐量≥800M，IPS 吞吐量≥500M，全威胁吞吐量≥400M，并发连接数≥180 万，新建连接数≥6 万；硬件指标：1U 规格，硬盘容量≥64G SSD，单电源，标配≥6 个千兆电口+4 个千兆光口。

2、支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持静态路由，ECMP 等价路由；支持多播/组播路由协议；

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路由选路功能；（提供产品界面截图，并加盖厂商公章）

4、支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换；

5、访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，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、设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间；（提供产品界面截图，并加盖厂商公章）

7、支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；

8、设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在 50 万条以上；支持恶意域名重定向功能，用于 DNS 代理服务器场景

下定位内网感染僵尸网络病毒的真实主机 IP 地址；支持对终端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；（提供产品界面截图，并加盖厂商公章）

9、支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护；

10、支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息；（提供产品界面截图，并加盖厂商公章）

11、支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况；

（六）、终端安全管理系统

1、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；

2、支持展示跟同品牌下一代防火墙、安全感知平台、上网行为管理，云端 SOC 平台，SAAS 化管理平台的联动状态；（提供产品界面截图，并加盖厂商公章）

3、支持以安全策略模板方式对指定终端组快速部署安全策略，安全策略模板支持默认模板和自定义模板；（提供产品界面截图，并加盖厂商公章）

4、支持对主机账号信息进行梳理，可按照“7 天”、“30 天”展示登录历史，了解账号风险，包括是否存在隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、半夜登录、多 IP 登录等，并可以将存在风险账号的主机列表导出

5、支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等；（提供产品界面截图，并加盖厂商公章）

6、支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议；

7、支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截；（提供产品界面截图，并加盖厂商公章）

8、构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行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；（提供产品界面截图，并加盖厂商公章）

（七）、超融合一体机

1、规格：2U 的机架式服务器，可以放入 42U 标准机柜。

2、处理器：配置≥2 颗 16 核 CPU Gold 6226R 处理器，主频≥2.9GHZ。

3、内存：配置≥8*32GB DDR4 2933 内存；内存插槽数量≥24 个，最大内存可扩展至 1.5TB；具备内存回收机制，实现内存资源的动态复用，保障服务器的性能。

4、硬盘：配置≥4 块 3.5 寸 8T SATA 数据盘、≥2 块 240G SSD 系统盘（不占用前置硬盘槽）、≥2 块 960G SSD 缓存盘，支持热插拔 SAS/SATA 硬盘，兼容 2.5 英寸和 3.5 英寸硬盘；

5、设备最多支持≥5 个 PCIe 扩展插槽，配备≥6 个千兆电口和 2 个万兆光口，配置冗余电源。

6、RAID 功能：提供 raid 0/1/10 并支持直通。

7、包含免费 3 年硬件保修服务。

（八）、计算虚拟化软件

1、虚拟化软件非 OEM 或贴牌产品，禁止借用第三方软件的整合，以保证功能的可靠性和安全性；

2、虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 IP 地址、MAC 地址等；

3、为了更好的保护数据，需要支持设置定期自动备份，支持用户灵活配置备份策略，备份文件保留时间最高可以达到 15 年；

4、每个虚拟机都可以安装独立的操作系统，为获得良好的兼容性操作系统支持需要包括 Windows、 Linux，并且支持国产操作系统包括：红旗 linux、中标麒麟、中标普华等（提供产品界面截图，并加盖厂商公章）；

5、具有合理的内存调度机制，支持内存回收机制，实现虚拟化平台内存资源的动态复用，并支持手动设置内存超配机制，能够实现内存的过量使用，保证内存资源的充分利用；

6、支持无代理跨物理主机的虚拟机 USB 映射，需要使用 USB KEY 时，无需在虚拟机上安装客户端插件，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的 USB 资源，对于业务的自适应能力、使用便捷性更佳（提供产品界面截图，并加盖厂商公章）；

7、为尽可能保障数据中心断电场景下的业务，支持 UPS 联动，并在市电断电通过 UPS 临时供应电量，当 UPS 电量过低时，按照虚拟机优先级先将不重要的虚拟机进行软关机；

8、支持双向迁移，可将 VMware 虚拟机在运行状态下迁移到超融合平台上，也可将超融合平台上的虚拟机在运行状态下迁移到 VMware vCenter 的集群中（提供产品界面截图，并加盖厂商公章）；

9、支持纳管第三方主流虚拟化平台，提供对 Vmware 平台上的虚拟机进行管理；（提供产品界面截图，并加盖厂商公章）

10、支持平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态（提供产品界面截图，并加盖厂商公章）。

注：以上产品需求中的技术参数及其性能(配置)仅供参考作用，主要目的是为了满足项目采购单位工作的基本要求，投标产品满足（实质相当于）或优于谈判文件的采购需求均可。

三、项目售后服务及其他要求：

1、项目质保期不少于二年,自项目验收通过之日起计算（技术参数中有特殊要求的以技术参数为准）。质保期内免费提供使用指导、软件升级及巡检、维护、维修、故障排除、系统优化、应急服务在内的各项服务。质保期满后,仍须按采购人要求继续提供售后运维服务,售后运维所需的零配部件及服务费用按市场优惠价计收。

2、提供及时有效的售后服务，成交单位应提供有不少 2 名技术人员的售后服务

技术支持团队（提供成员名单及相关证书（如有）），并提供 7*24 小时的电话、远程等技术支持服务，针对突发应急事件提供 4 小时内到现场处置的服务响应保障，问题解决后 24 小时内，提交问题处理报告，说明问题种类、问题原因、问题解决中使用的方法及造成的损失等情况。

3、培训要求：

3.1、成交供应商须向项目采购单位提供免费培训，培训方式应包括理论培训和操作培训。成交单位须在响应文件中提出全面、详细的培训计划。

3.2、培训内容包括但不限于：基础培训、系统管理培训、应用系统操作培训、系统维护培训。

3.3、培训费用：供应商应将所有培训费用（含培训教材费），计入投标总价；实际培训时间、地点按成交供应商与项目采购单位商定的为准。

4、合同履行期限：自合同签订之日起10个工作日交付。

5、交付地点：白沙黎族自治县人民医院。

6、验收标准：符合国家、地方、行业标准及采购文件的规定。

7、付款方式：1)合同签订后3个工作日内，成交供应商向采购单位支付合同总额的5%作为质保金，质保期自甲方验收合格之日起算二年，质保期满且产品无质量或者保修问题，甲方在收到乙方的付款申请函后7个工作日内一次性无息将质保金支付给乙方。2)所有货物到达指定地点后且验收合格，甲方在10天内支付合同总价的100%。具体合同条款，以甲乙双方签订为主。