采购需求及技术规格要求

一、总体要求

1.本项目报投标总价，投标总价包含完成本项目所产生的一切费用，合同履约期间采购人不再追加任何费用，投标人自行考虑报价风险。

2.下列采购需求中：标注▲的产品为核心产品，中标的核心产品的名称、品牌、规格型号、数量、单价等将予以公布。

二、项目技术需求

（一）技术需求重要性表述

标识重要性	标识符号	代表意思
关键指标项（基础项）	无标识项	**有不满足要求的，将导致投标无效。**
重要指标项	★	评分项，具体评分细则详见第四章评标方法和标准。
注：本项目所有技术要求无标识项内容要求投标人须全部响应满足，投标人须如实响应；如在后期合同履约过程中，发现有虚假响应情况，采购人有权解除合同、不予退还履约保证金、不予支付合同款项，且上报监管部门并追究中标人给采购人带来的一切损失。		

（二）项目概述

本项目旨在建设覆盖多院区的集团化全网络终端安全管理平台，实现终端准入控制、安全防护、统一运维及数据防泄漏等功能，满足医疗行业网络安全合规要求，提升内网终端安全防护能力。

（三）总体要求

1. 覆盖范围：集团多个院区，终端客户端需提供场地授权，兼容有线、无线网络及哑终端（如医疗设备、IOT 设备）。
2. 架构要求：

2.1. 管理平台需支持中心-分院区二级级联部署，在中心部署一级集中管理服务器，总院和各分院区独立部署二级服务器管理节点和准入网关，数据本地

化存储，关键日志加密上报中心。

3. 兼容性：

3.1. 支持 Windows、Linux（含 ARM/MIPS 架构）、Android 4.0+、国产化操作系统（银河麒麟、统信 UOS 等）。

3.2. 适配老旧系统及无客户端的哑终端。

▲（四）软件产品功能需求（所属行业：软件和信息技术服务业）

1. 整体要求

1.1. ★网络准入控制、终端安全管控、数据防泄密、移动终端管理功能等功能模块一体化，一个客户端。一套平台实现 Windows 和主流信创 PC 终端的统一管理，无需单独部署服务器系统。后期根据院方需求扩容防病毒、文档加密、终端检测响应等。

1.2. 对服务器自身设备进行监控维护，可维护信息包括服务器名称、IP 地址、当前版本、运行状态、磁盘空间、CPU 负载、内存使用率等。

1.3. 客户端自我防护机制，客户端文件、进程、注册表、服务等都无法停止、修改、删除；客户端正常运行情况下安装目录隐藏；客户端安全模式下运行，客户端策略依然生效；客户端功能在线调整，在功能调整、问题验证等场景下客户端文件（配置文件、DLL 等）实时替换，无需覆盖安装、重启终端。

2. 网络准入控制

2.1. 准入方式：

2.1.1. ★支持 802.1x、MAB、端口镜像、策略路由、Portal 等多种准入控制技术混合使用。

2.1.2. 无客户端准入（基于 IP/MAC 绑定、设备指纹识别）。

2.1.3. 准入未放行前 web 重定向、邮件重定向方式引导；准入控制阻断和提醒模式，提醒并帮助用户自助安装。

2.2. 身份认证：

2.2.1. 多种身份认证源实现入网实名认证：内置账户、AD/LDAP 集成，单点登

录（SSO）认证对接。

2.2.2. 访客/外协用户管理，访客自助填写放行时长、受访人等信息，管理员审批、指定人员审批、自动审批、受访人扫码审批等多种审批流程。

2.3. 安全检查：

2.3.1. 终端合规性基线检查（防病毒软件安装与病毒库更新时间、终端软件安装、补丁更新、高危端口禁用、是否启用 Guest 账号、是否存在弱口令检测、终端防火墙检测、基于注册表、文件、进程、系统、服务进行自定义检查等）。

2.3.2. 违规终端自动隔离并引导修复。

2.4. 哑终端管控：

2.4.1. ★基于设备指纹，对设备进行免检准入，并对免检设备进行仿冒检查，可基于设备行为特征的仿冒检查，并可将仿冒设备隔离。

2.4.2. 自动发现并分类哑终端（打印机、医疗设备等）。

3. 终端安全管控

外设管理：

3.1.1. 禁用高风险接口（USB 存储、蓝牙、光驱），授权设备白名单。

3.1.2. 提供 AES256、国密 SM4 算法加密程序对市面移动存储介质进行安全性质加密，备份安全 U 盘的登录密码到系统后台，对安全 U 盘读写操作进行审计或审批。

违规外联防护：

3.1.3. 同时禁止使用多个网卡、禁止移动上网卡、禁用终端电脑开启 Wi-Fi 热点，Wi-Fi 黑白名单控制，支持无线 SSID 仿冒检测；

3.1.4. 离线策略生效，断网时仍可执行安全策略。

系统加固：

3.1.5. 禁用组策略编辑器、注册表修改、控制面板、禁止设置网络属性等高危操作，支持对指定系统服务的启动类型进行设置。

3.1.6. 终端安全基线检查，包括支持共享检查、密码策略检查（复杂度、长度、时长、密码历史）、防病毒安装和病毒库更新检查、共享检查、DNS 检查、DHCP 检查、网络连接状态检查、终端软件黑白名单检查、终端必须安装

软件检查、软件版本检查、系统磁盘和数据盘磁盘剩余空间检查、检查屏幕保护策略与最大屏保时间、统一设置屏幕保护背景；

3.1.7. 进程黑白名单、高危软件检测与阻断；能对重要进程运行状态进行监视；

4. 数据防泄漏

水印管理：

4.1.1. ★屏幕动态水印（明文/矢量水印/截图盲水印）、打印水印，明文水印内容包含用户身份、终端信息、时间信息等，支持自定义水印显示位置、字体、字号、水印密度、水印颜色、透明度、对齐方式等。

4.1.2. 对截屏审计与盲水印溯源终端信息、用户信息、时间信息等。

文件管控：

4.1.3. 敏感内容识别，识别方式包括关键字内容检测、正则表达式、文件名称、文件 MD5、文件类型、加密码文件、文件大小等；支持至少主流文件类型真实格式与内容的识别，识别文档的原有格式，不受后缀名称的影响；支持对不低于 10 层文档嵌套的敏感文件检查；支持 OCR 识别；

4.1.4. 对终端上的敏感文件访问控制，禁止非法复制、粘贴、另存为、重命名、写、删除等操作；支持自定义文件源和目的设备类型，设备类型包括：本机硬盘、U 盘、网络共享、光盘、软盘、智能设备等。

5. 移动设备管理

准入与管控：

5.1.1. ★移动设备接入医院 WLAN 时，移动设备管理客户端与网络准入控制联动，自动使用 NACC 或 802.1x 等方式进行网络准入控制认证。

5.1.2. ★安卓、iOS、鸿蒙系统设备专机专用：安卓、鸿蒙设备支持启用安全桌面，安全桌面锁定在前台，用户无法自行退出，安全桌面支持自定义显示应用，安全桌面时间与服务器时间同步；iOS 设备支持单一应用模式。

5.1.3. 针对安卓设备、鸿蒙系统设备上应用安装、卸载或使用限制，防止设备安装使用不合规应用；

5.1.4. 移动设备需通过安全隧道访问内网资源。

应用管理：

5.1.5. ★私有化应用商店，支持应用的全生命周期管理，支持对应用进行创建、编辑、下发、强制更新、删除、黑白名单设置、明细查询、增量更新等；支持应用多版本管理，可根据不同APP、不同用户灵活设置不同的发布策略。支持建立应用上架、下架审核流程，规范应用管理流程。

5.1.6. 移动端设备级明文水印和矢量水印，明文水印内容包含用户身份、终端信息、时间信息等，支持自定义水印显示位置、字体、字号、水印密度、水印颜色、透明度、对齐方式等；

5.1.7. 设备实时操作，包括：远程擦除数据、推送消息、锁定设备及设备定位功能。

6. 统一运维管理

资产管理：

6.1.1. 支持SNMP、主动扫描、客户端作为探针监听等多种方式发现全网终端资产；对接入网络的终端进行发现和定位，显示设备所在接入交换机及端口位置信息；自动识别接入设备的类型，包括：PC设备、网络设备、服务器、移动设备、IoT设备等，自定义添加设备类型识别规则条件，以操作系统、开放端口、设备名、MAC地址前缀、MAC地址厂商、IP地址范围等条件设置权重，自动将设备匹配归纳到新添加的设备类型列表中。

6.1.2. 采集设备硬件信息、操作系统信息、软件信息，生成软硬件资产报表，支持对设备的等硬件设备和软件配置变更行为进行监控，展示设备配置变更信息等。

远程协助：

6.1.3. ★Windows、Linux、国产系统及移动终端的远程桌面控制与文件传输。

软件分发：

6.1.4. 在管理员后台向终端推送一个或多个软件并自动安装，支持软件静默安装、断点续传及带宽控制。

6.1.5. 对每次分发任务的应用总数、软件安装成功数、安装失败数、下载失败数、用户取消任务数、不需要安装数进行统计，并对任务进行完成率和异常率的统计；

软件管理

6.1.6. 可以对终端的软件安装情况进行详细统计，能够收集所有或则特定单个软件的安装情况，并生成相应的统计报表；支持对 Windows 终端绿色软件资产信息进行采集，采集方式包括主动扫描和运行时采集；

6.1.7. 软件安装、卸载审计控制，可审计用户软件安装卸载行为，可禁止用户软件安装、卸载行为；支持软件安装\使用黑\白名单管理；支持绿色软件黑白名单管理；

6.1.8. 支持对商业软件的采购订单进行录入管理；

6.1.9. 软件使用统计，对网站标题、网站 URL、进程文件路径、网站访问次数、应用程序使用次数、网站访问时长、应用程序使用时长进行统计；

6.1.10. ★自动识别终端安装的高风险软件，支持识别的高风险软件至少包括：易侵权软件、恶意软件、流氓软件、易造成敏感数据泄露软件等；高风险软件识别规则自动关联软件黑名单策略，自动处置高风险软件；当员工安装了高风险软件，管理员可以第一时间接受到弹窗告警，方便管理员及时处置高风险软件；高风险软件识别规则支持云端自动更新。

软件商城

6.1.11. 构建内部软件商城，员工可在软件商城自助下载安装软件。管理员在管理平台页面上传软件安装包，并自动获取软件名称、版本等信息；支持软件商城内软件分类展示；对软件自定义软件安装、卸载命令；针对不同部门发布不同软件；

补丁管理：

6.1.12. Windows 终端补丁无需额外搭建微软补丁服务器实现终端的补丁安装情况进行检查、强制修复、闲时安装；支持对信创终端补丁的分发；统计补丁安装情况；补丁分发支持智能中继等措施降低网络带宽压力；

消息推送：

6.1.13. 对指定的范围内终端发送纯文本、富文本、HTML 文件等通知，终端弹框提示，向终端指定目录分发文件；可管控推送范围。

7. 分级分权管理

总院拥有全局视图及策略下发权限，分院管理员仅管理本区域终端。

自定义管理员角色权限（如策略配置、审计日志查看）。

（五）性能指标

1. 处理能力：

1.1. 管理平台单节点支持不低于 20Gbps 流量吞吐，一级管理服务器支持 5 万终端并发管理，总院、西区、南区、北区二级服务器支持 20000 终端并发管理，感染病医院住院部、门诊二级服务器支持 5000 终端并发管理。移动设备管理组件需支持 5000 点移动设备强管控。

1.2. 提供多种型号准入控制器，满足不同院区的准入需求，型号 1 单台支持不低于 20000 终端接入，型号 2 单台支持不低于 5000 终端接入。

2. 扩展性：

2.1. 横向扩展，可通过集群部署提升管理容量。

3. 稳定性：

3.1. 故障自动切换（如双活数据中心），准入服务故障时需具备逃生机制。

3.2. 智能应急逃生方式，系统检测到运行中出现的异常和故障支持自动应急：一定时间内连续出现多台终端准入失败自动临时放行且阈值可自定义（分钟级别），确保企业网络的可用性；

（六）部署要求

1. 硬件资源（所属行业：工业）

序号	用途	配置要求	台数
1	一级集中管理平台	冗余电源，CPU≥36 核，内存≥128GB，硬盘≥4*2T，SSD≥480GB，以太网口≥4，万兆光口≥2，RAID 5，支持 50000 终端并发管理。	1
2	二级管理节点型号 1	冗余电源，CPU≥36 核，内存≥128GB，硬盘≥4*2T，SSD≥480GB，以太网口≥4，万兆光口≥2，RAID 5，支持 20000 终端并发管理。	4
3	二级管理节	冗余电源，CPU≥20 核，内存≥64GB，硬	2

	点型号 2	盘≥4*2T，SSD≥240GB，以太网口≥4，万兆光口≥2，RAID 5，支持 5000 终端并发管理。	
4	移动设备管理节点	冗余电源，CPU≥8 核，内存≥32GB，硬盘≥2*2TB，以太网口≥4，RAID 1，支持 5000 点移动终端管。	2
5	准入网关型号 1	冗余电源，网口≥6，万兆光口≥2，最大支持 20000 台终端准入控制。	4
6	准入网关型号 2	冗余电源，网口≥6，万兆光口≥2，最大支持 5000 台终端准入控制。	5

2. 网络架构：

2.1. 旁路部署，不改变现有网络拓扑，避免单点故障。

3. **此部分内容均包含在投标总价内，但需单独报价，且价格合计不得高于 30 万元。**

（七）服务要求

1. 实施服务：提供部署方案设计、系统联调及人员培训。

1.1. 须根据甲方的网络、资源、业务等实际现状设计合理的实施方案，包括但不限于软硬件部署、网络拓扑、项目推广方案、培训实施方案等；

1.2. 合同签订生效后，接甲方通知后 30 个自然日内设备到货，并在供货后 365 个自然日内完成本项目全部软硬件的安装、测试、部署实施，并验收合格；

1.3. 乙方需为本项目提供原厂实施队伍，原厂实施团队确保在本项目中投入项目经理、关键实施人；

1.4. 如未在规定期限内完成项目交付，投标人应按照项目延迟天数按照合同总价款的每日万分之四向招标人支付违约金。投标人未在指定期限内进行修正的，招标人有权解除合同。

2. 售后服务：

2.1. 7×24 小时技术支持，故障响应时间≤2 小时。

2.2. 提供不少于5年的软件及硬件的升级及质保服务。

2.3. 验收通过后提供1人2年期驻场服务，未经甲方同意不得更换驻场人员。驻场人员具有3年以上工作经验，具有责任心，能独立进行终端安全问题排查及处理，独立撰写事件处理报告。