采购需求

（采购需求如与拟签订的合同文本有矛盾，均以采购需求为准。）

说明：

1.当采购项目涉及政务信息系统时，采购需求应当符合《政务信息系统政府采购管理暂行办法》（财库〔2017〕210号）的相关要求。

2.采购人及采购代理机构应关注财政部门会同有关部门制定发布的需求标准，结合具体应用场景，根据对应《需求标准》确定采购需求。

已发布的需求标准如下：

《关于印发〈商品包装政府采购需求标准（试行）〉、〈快递包装政府采购需求标准（试行）〉的通知》（财办库〔2020〕123号））

《绿色数据中心政府采购需求标准（试行）》（财库〔2023〕7号）

《台式计算机政府采购需求标准（2023年版）》（财库〔2023〕29号）

《便携式计算机政府采购需求标准（2023年版）》（财库〔2023〕30号）

《一体式计算机政府采购需求标准（2023年版）》（财库〔2023〕31号）

《工作站政府采购需求标准（2023年版）》（财库〔2023〕32号）

《通用服务器政府采购需求标准（2023年版）》（财库〔2023〕33号）

《操作系统政府采购需求标准（2023年版）》（财库〔2023〕34号）

《数据库政府采购需求标准（2023年版）》（财库〔2023〕35号）

《物业管理服务政府采购需求标准（办公场所类）（试行）》（财办库〔2024〕113号）

如有更新或增加，以财政部门发布为准。

一、采购标的

1. 需求一览表

包号	标的名称	数量	是否接受进口产品投标
1	详见投标邀请	详见投标邀请	详见投标邀请

二、商务要求

1.交货期和交货地点

1.1交货期：详见投标邀请合同履行期限

1.2交货地点：采购人指定地点

三、技术要求

说明：

1. 以下技术指标及要求中如出现设备或产品品牌或指向某个品牌，仅作为参考该设备或产品所需达到的具体技术性能要求，不作为该设备或产品的品牌要求。

2. 下列“★”技术要求条款为不可负偏离项，如有任何实质性偏离需明确，将做无效投标处理；“▲、*、#”技术条款及其它一般技术条款仅为评审打分项，不作为无效投标条款。

具体技术指标要求如下：

（一）防统方系统

指标项	参数要求
审计能力	1.SQL 审计处理能力（吞吐）峰值不低于 1000Mbps，SQL 审计处理能力（速率）峰值不低于 60000SQL/S，日志在线存储不低于 192 亿条，不限制数据库实例数。
部署与管理	1.支持旁路部署方式，无需改造既有网络、无需在服务器上安装插件、对服务器零干扰、不影响服务器性能、无需服务器账号信息，从而确保业务连续不中断。
	2.针对虚拟化环境以及小型云场景，支持以虚拟交换机的 VEPA 模式完成部

	署，适配 vmware、kvm、openstack 等常见虚拟化平台。
	3.支持在目标数据库安装 Agent 引流，解决云环境、虚拟化环境等内部流量无法镜像场景下的数据库审计。支持通过 Agent 对流量进行过滤，端口、IP 地址等关键内容均能按需定义，进而有效减少网络负载。在运行过程中，Agent 的 CPU 占用率维持在 3%以下，内存占用量小于 100M，程序文件大小不超过 5M。
	4.具有成熟的云平台对接技术，提供 SDN 架构下无插件引流方案，可与各大主流云平台进行对接。
审计功能	1.支持 Oracle、SQL Server、Mysql、DB2、PostgreSQL、Cache、IRIS、Sybase、Hive、MongoDB、Informix、DM、Kingbase、LibrA、GaussDB、GBase、Highgo（瀚高）、Oscar（神通）等数据库的审计，且支持多种不同的数据库同时审计。
	▲2.全面支持后关系型数据库 Caché的集成工具 Terminal、Portal、Studio、Sqlmanager、MedTrak 工具的审计，其中查询 Global 有返回结果，Sqlmanager 支持提取 SQL ID 实现审计， Terminal 能审计到 SQL 语句和返回结果，并支持本地审计，基于 C/S 的 MedTrak 工具能审计到操作报表的具体返回结果。（提供加盖原厂公章的截图电子件）
	▲3.全面支持后关系型数据库 IRIS 的集成工具审计，查询 Global 有返回结果；Terminal 能审计到 SQL 语句和返回结果；Studio 可以审计到操作语句。（提供加盖原厂公章的截图电子件）
	▲4.支持主流业务协议操作的审计，如：Samba、NFS、Portal、Http、pop3、https、ssh、SMTP、Telnet、FTP 协议审计。（提供加盖原厂公章的截图电子件）
	5.同时支持 IPv4/IPv6 网络环境流量的审计。
	6.支持通过网络流量识别或端口扫描方式，自动识别网络中未被发现的主流数据库资产，一键添加到保护对象中进行审计。
	7.系统内置有多级缓存机制，能够实现流量超出审计速率 30%时支持时间不低于 2 小时。
	8.系统应支持多层过滤功能，支持网络流量驱动级 IP 过滤，根据过滤的条

	件（如源地址 IP/目的地址 IP）定义规则，对网络流量进行扫描，对无需审计的信息从网络层进行过滤；根据系统语句（SQL 语句）和白名单（条件为 IP/MAC/应用账户/数据库账户/审计对象/操作语句）定义规则进行应用层过滤，将客户关注的信息进行保留，避免无用信息的堆砌造成磁盘空间的浪费和性能的耗损。
	9.支持数据库绑定变量审计、函数审计(sum 求和函数等）。
	10.支持端口重定向的审计，实现端口重定向情况下的数据不漏审计。
	11.支持超长操作语句审计，针对传统型数据库，支持 8 万字节审计而不截断。
	12.支持对执行时间超过 6 小时操作的审计。
	13.支持通过手动添加或主动发现数据库中的存储过程、触发器，并对其具体操作进行行为审计，存储过程审计可审计到调用行为及具体操作风险；触发器审计可审计到触发行为及其具体操作风险。
审计策略	1.支持操作语句系列的组合规则，可根据某一客体的操作行为集合进行规则审计告警。
	2.支持 20 种以上元素的审计，可支持数据库操作命令、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、会话 ID、关键字、时间等。（提供加盖原厂公章的截图电子件）
	3.支持有规律性操作的统计审计规则，可根据在特定时间范围间内，某项操作重复达到设定的统计次数时，可触发规则进行告警。
应用审计	▲1.支持 B/S、C/S 应用系统三层架构 http 应用审计，可提取包括应用系统的人员工号（账号）在内的“六元组”身份信息，并可获取 XML 返回结果。（提供加盖原厂公章的截图电子件）
	▲2.支持带 COM、COM+、DCOM 组件的三层架构应用审计，可提取包括应用层工号（账号）之内的“六元组”身份信息，精确定位到人。（提供加盖原厂公章的截图电子件）
	3.支持通过部署插件实现 java web 环境准确关联，支持框架：tomcat、

	weblogic、jboss；支持 B/S 业务系统三层关联审计；支持 B/S 三层架构下的应用账户、终端信息关联审计。
审计查询	▲1.基于大数据全文检索技术，检索效率高达亿条数据秒级响应，快速定位相关的审计内容。支持按时间、审计对象、风险级别、IP 地址、命中的风险规则名称、操作类型、关键字等不少于 30 种维度进行检索查询。（提供加盖原厂公章的截图电子件）
防统方功能	▲1.支持杭创、健讯、金蝶/金医慧通、用友、重庆中联、天健、厦门智业、科进、天网、方正众邦、金仕达、东软、启天医星、力锦、成电医星、北大医信、和仁、信通网易、久远银海、万达、互惠、医惠、创业慧康、易联众、创星、行心、康博嘉、九明珠、弘扬、鑫亿、九阵、惠侨、慧扬、嘉和美康、众阳、金唐、南京德朗诺、尚荣、坐标、联众、新八达、新星、长信、新益华、军卫一号、海泰、启天医星、振邦、同步远方 his 中间件防统方。（提供加盖原厂公章的截图电子件）
	2.系统自带各种常见 HIS 防统方规则库，规则数量≥700 条以上，支持自定义防统方规则。
统方分析及监控	1.支持统方确认，点击查看某条审计记录，能够进行统方确认，更新其处置状态，并纳入统方报表进行行为趋势分析，同时支持生成统方报告，并存档以留存记录，供后续事件追溯使用。
	2.支持对疑似统方行为的进行人工处置，支持对同类型、同规则的行为进行批量处置或一键处置。
	3.支持统方风险日志数、已确认统方事件数、本日/本周新增涉及统方人员数量的监控与展示。
	4.支持统方风险趋势、统方风险日历、统方风险占比、统方风险排名、最近统方风险的监控与展示。
	5.支持对特定的重点关注人员、特权账号的统方行为进行监控，并针对一段时间内的统方风险数进行统计。
	6.支持查询时间段内的统方人员排名。
	7.支持对人员的统方行为进行分析，统计并展示统方行为在风险统计占比、人员行为画像分析、访问时间趋势等规律分析。

态势感知	▲1.具备自动构建数据库操作行为基线的能力，可自动识别超出行为基线之外的陌生 IP、陌生工具访问行为，并进行告警。（提供加盖原厂公章的截图电子件）
统计及报表	1.内置用户访问情况、IP 访问情况、风险统计情况、统方事件报表，并支持自定义报表，支持 Word、PDF、Excel 格式导出报表。
	2.支持立即、按周、按月生成报表，生成的报表支持通过邮件自动发送。
审计配置管理	▲1.翻译功能：支持在审计时将审计结果翻译成自然语言，支持系统定义和用户自定义翻译，便于审计人员方便、简单的获得并了解数据库审计的结果。（提供加盖原厂公章的截图电子件）
	2.支持对访问工具、IP 地址、客户端 MAC、操作系统主机名、操作系统用户名、应用账户名、规则生效时间、数据库对象、操作类型、存储过程与触发器进行集合配置，在审计规则中进行引用。
	3.支持对组织下的人员信息进行配置管理，包括科室；支持工号、访问者信息翻译时与人员组织进行关联。
	4.支持对所有防统方系统管理人员的操作行为进行审计记录，如系统管理人员的登录登出、规则修改、规则启用等，并由审计人员进行查询和审计，具有自身审计功能。
	5.支持审计规则配置的导入导出。
	6.支持工号提取配置，可按关键字、绑定变量、返回结果以及关联符等设置工号提取规则。
审计数据管理	1.提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持本地、远程备份方式，支持通过 FTP 上传或外置存储备份；手动备份文件支持密码加密。
配置监察	1.支持针对白名单、规则信息的变化情况进行监察记录。
	2.支持对系统异常、系统关闭、网线插拔异常相关的信息进行记录与告警。
组织架构管理	1.支持对组织架构的管理，能够对组织下的人员信息进行管理，支持工号、访问者信息与人员组织进行关联匹配。
攻击行为检测	1.支持对 SQL 注入、XSS 攻击等 web 攻击的识别与告警。
	2.系统应具备防范非法 IP 地址、防范暴力破解登录等异常行为检测。

	3.系统通过审计规则的设置，对于统方和破坏数据库的危险行为如：登录失败、删表、EXP 备份导表等行为自动识别和告警。
旁路阻断防护	1.支持旁路阻断功能，支持根据访问 IP、账号、客户端工具名、时间、客户端 MAC、主机名、操作回复信息等指定规则进行阻断；不改变被审计对象的网络结构、不在数据库操作系统中安装插件，审计系统异常不影响网络。
	2.阻断模式具备“严格模式”与“宽松模式”；宽松模式可对单一会话危险操作阻断，危险操作特征外的其他操作不影响；严格模式可对同类型危险操作持续阻断，源 IP 操作的所有请求直接阻断。
监控与告警	1.提供系统 CPU、内存使用率异常告警、网络和网卡异常、引擎状态异常、磁盘存储容量不足等情况时的自动报警提醒。
	2.系统支持管理界面告警、Syslog 和 SNMP trap 告警、邮件和短信告警。
	3.支持告警策略配置，针对高危事件、中危事件、低危事件、关注事件等风险分别设置告警策略，可选择邮件、短信、Syslog、SNMP 等告警方式通知对应告警信息接收人，每个告警策略中，告警事件类型、通知方式等可设置一个或多个；系统记录告警通知日志，可查看历史告警信息。
系统管理	1.支持系统安全策略配置，支持密码过期时间、密码复杂度、连续登录失败锁定、界面超时自动退出等安全策略。
	2.系统本身具备访问防火墙，对于系统的异常访问，能有效防范非法 IP 地址、防范暴力破解登录用户密码、设置访问黑白名单等安全功能。
	3.支持系统时间与 NTP 服务器同步。
服务要求	▲1.提供三年原厂售后服务：原厂提供 7×24 小时电话及远程支持服务。系统出现故障时，在接到电话故障报告后 60 分钟内做出实质性响应，如需现场服务的需原厂工程师在 4 小时内到达故障现场，系统部署、系统培训、版本升级、故障定位、运行巡检、策略优化和应急响应等服务。
	▲2.提供针对此项目的原厂售后服务承诺，并加盖原厂公章

（二）数据流动治理平台

指标项	参数要求
数据资产梳理	▲1.应用资产梳理：支持自动化持续梳理应用资产，应用资产总览包括：应用 IP/域名、今日访问量、总访问量、API 资产数、文件数、数据标签数、账号数、

	资产来源、责任人。(须提供≥上述 5 项一一对应的截图证明，并要求在同一界面；不足 5 项则视为此项不满足，提供加盖原厂公章的截图电子件)
	2.应用资产详情包括：API 总数、风险 API、弱点 API、敏感 API 数量和趋势分析、账号总数、风险账号数量的趋势分析、数据标签总数和趋势分析。
	3.API 资产梳理：通过流量解析的方式自动梳理 API 列表、应用地址、API 路径、请求类型、敏感数据类型、发现时间等，支持通过列表模式展示最近 7 天请求次数、最近 7 天访问 IP 数、最近一次访问时间、是否涉敏、接口状态等。
	4.API 类型识别支持：支持识别 HTTP 和 HTTPS 业务中的 API 接口资产；支持识别 RESTFul、SOAP、MQTT、Websocket、GraphQL、JSON-RPC、XML-RPC、Dubbo 等 API 协议。
	▲5.API 资产总览包括：API 接口清单、安全风险等级评估、脆弱性等级评估、敏感等级评估、今日调用量、总调用量、上线状态、活跃状态、API 标签。(须提供≥上述 5 项一一对应的截图证明，并要求在同一界面；不足 5 项则视为此项不满足，提供加盖原厂公章的截图电子件)
	6.自定义支持：内置 API 识别规则并支持自定义、内置 API 版本规则并支持自定义、内置 API 合并规则并支持自定义、内置 API 活跃规则并支持自定义、内置 API 敏感等级规则并支持自定。
	▲7.数据库类型支持：数据库类型至少包括常见 MySQL、Oracle、SQL Server、Caché、IRIS 等，支持自动或手动匹配数据库，支持基于数据源的连接和授权，获取其下库、表、字段的层级结构。(须提供加盖原厂公章的截图电子件证明)
	8.资产图谱支持：支持资产图谱梳理，支持应用关系梳理，可展示应用、API、用户、账号、文件、数据标签等之间的关联关系，并支持按关系链路进行查询分析。
数据安全风险评估	1.风险发现：支持 API 风险自动持续发现，支持内置规则包括数据泄露类风险识别规则，Web 攻击类风险识别规则，账号安全类风险识别规则等，至少包含：IP 单次获取大量敏感数据标签、账号单日多 IP 访问、用户一分钟内频繁登录、用户非工作时间获取大量敏感数据小时、IP 执行 SQL 注入、IP 撞库攻击。
	2.脆弱性评估：可按照 OWASP API Security TOP10 进行分类识别，至少包含：请求密码透出、响应密码透出、接口缺乏速率限制、跨站请求伪造、接口返回

	大量敏感数据、接口返回大量敏感数据标签、配置文件泄露、权限更新不合理、IP 水平越权等规则。
	3.基线学习：通过基线学习能力学习正常业务行为，通过智能技术建立数据返回量、数据返回类型、访问频次等基准线体系库，达到降低风险误报的效果。
	4.加密流量透视：旁路镜像模式下，无需导入业务系统的 SSL 证书亦可实现对 TLS1.3 加密流量的解密还原。
	▲5.主动扫描漏洞:漏洞规则库包括 CNVD 等信息安全漏洞、CVE 常见漏洞与风险、安全漏洞、敏感信息泄露、域名劫持、默认账号登录、配置错误、暴露管理面板、物联网设备安全漏洞等；支持自定义扫描目标，可指定业务系统、指定 API 接口等；支持自动生成漏扫报告：含漏洞名称、漏洞 ID、风险 API 路径等内容。(须提供≥上述 5 项一一对应的截图证明，并要求在同一界面；不足 5 项则视为此项不满足，提供加盖原厂公章的截图电子件)
用户识别与审计溯源	▲1.用户调用安全：支持自动识别和整理用户使用的源 IP，形成用户源 IP 清单；支持根据用户源 IP 与关联账号风险行为进行用户源 IP 安全评分、评估用户 IP 风险等级；支持查看用户详情，对用户进行分析，包括关系图谱分析、行为分析、轨迹分析、风险分析等。(须提供加盖原厂公章的截图电子件证明)
	2.账号安全：支持查看账号详情，对账号进行分析，包括行为统计、行为轨迹、风险分析、使用浏览器等信息。
	3.数据泄密溯源分析：支持在医院发现数据泄露事件时，通过输入或导入已泄露的数据集，自动在流量中匹配相关访问行为，并支持图形化展示数据访问路径，具体呈现 IP-用户-账号-API-数据的完整链路。
	4.溯源结果展示：支持展示数据泄露关联日志数、可疑 IP 数量、高可疑 IP 数、涉及应用数、涉及 API 数、涉及用户数、涉及账号数等信息。
	5.专项审计：支持资产专项、用户专项等专项审计，支持按资产、用户、账号、API、事件等维度开展专项审计分析，支持审计结果留痕、导出和报告生成。
敏感数据识别与动态数据分类分级	1.敏感数据识别：内置不少于 300 种医疗行业专属数据标签识别规则，包括但不限于个人身份信息数据：身份证、社保卡号；联系方式：手机号、邮箱等；支持自定义添加数据标签识别规则。
	2.支持自定义敏感数据发现规则：可根据请求行、请求头、请求体、响应行、

	响应头、响应体等识别位置，基于正则表达式识别敏感数据，且支持忽略规则。
	3.支持自定义涉敏行为发现规则：可根据敏感数据类型、数据量、数据标签总数、数据标签类型数等进行匹配识别。
	▲4.支持导入数据分类分级标准:如国家标准“GB/T39725-2020 信息安全技术健康医疗数据安全指南”或院内自定义标准等；支持导出指定数据资产清单，需要包括动态指标：今日访问量、数据量与变化；支持关联数据分布应用及风险事件等。(须提供截图证明并加盖原厂公章的截图电子件证明)
文件识别与治理	▲1.文件识别：支持从流量中自动识别出文件资产，支持识别文件的文件名称、文件格式、MD5 值、文件大小、所属应用、上传次数、下载次数、敏感等级、数据标签、入库时间、最近活跃时间。(须提供≥上述 8 项一一对应的截图证明，并要求在同一界面；不足 8 项则视为此项不满足，提供加盖原厂公章的截图电子件)
	2.格式支持与相似度分析：支持识别 xlsx、pdf、txt、dps、log、xltm、docm、csv、pptx 等文件格式，支持基于机器学习、智能分词、相似度算法等对文件进行相似度分析和相关性分析。
	3.文件分类分级：支持对识别出来的文件基于内容进行分类分级及敏感数据标注。
	▲4.文件画像：支持对文件资产从文件构成、文件相关性、文件热度、文件操作记录等维度进行分析与可视化呈现，构建文件基础画像。(须提供截图证明加盖原厂公章的截图电子件证明)
部署方式与环境适配	1.部署方式：支持软件化部署，支持旁路镜像部署和串接代理部署通过交换机镜像流量对医院业务访问流量进行识别、分析、审计与治理，不改变现有业务访问链路。支持旁路部署时对 TLS1.1、TLS1.2、TLS1.3 加密流量解密。支持串接部署在网络链路中，对用户进出业务系统的流量进行识别、分析、处置、治理等。
	2.处置能力：支持拒绝、放行、仅记录、数据脱敏、二次鉴权、数据水印、API 签名等多种处置方式。
	3.环境要求：软件支持不低于 1G 数据吞吐量，支持软件化部署，适配不少于 2 种主流国产化环境；系统采用数控分离架构设计，实现数据处理转发面与控制

	管理面的完全解耦，控制管理面负责策略配置、状态监控等功能，数据转发面负责数据包的接受、处理和转发，互不影响。
	4.可配套多个威胁追踪反制物理硬件探针：支持 7*24 小时持续监测感知内网安全威胁，利用欺骗伪装技术，通过在关键入侵路径上部署诱饵和陷阱，诱导攻击者攻击伪装目标，远离真实资产，并且对攻击者做取证和追踪溯源；内置不少于 70 种虚拟服务，包括但不限于 OA、ERP、数据库、邮件等核心业务系统。
可视化能力	1.数据态势大屏功能：提供数据流动整体态势看板，含资产、用户、风险、治理等态势看板；直观展示风险主体 TOP5、风险事件 TOP5、实时安全告警事件等；大屏汇总转发机和管理机数据和流量，并支持国内国际两个视角绘制数据流转地图。
	2.数据流动看板：支持直观查看数据流动整体情况，包括但不限于整体数据流动情况、互联网访问情况、跨境访问情况、局域网访问情况、数据流动趋势等。可详细分析数据流向的分布，包含但不限于流动区域分布、访问源分布、访问用户分布等。可详细分析涉及敏感数据流动 TOP 5 的应用、数据、用户、账号等。
	3.多种看板满足业务需求：支持提供资产看板、风险看板、用户看板、系统看板、治理看板以满足医院对敏感资产、数据防泄漏及高风险人员账号的监控需求。
	▲4.风险报告导出：能够根据系统分析结果产出报告。报告内容至少需包括报告概览、资产分析、用户分析、安全分析、运维分析、安全等级评估标准、总结建议七部分。支持按单次、每天、每周、每月生成安全报告并发送医院指定邮箱。(须提供加盖原厂公章的截图电子件证明)
服务要求	▲1.提供三年原厂售后服务：原厂提供 7×24 小时电话及远程支持服务。系统出现故障时，在接到电话故障报告后 60 分钟内做出实质性响应，如需现场服务的需原厂工程师在 4 小时内到达故障现场，系统培训、版本升级、故障定位、运行巡检、策略优化和应急响应等服务。
	▲2.提供针对此项目的原厂售后服务承诺，并加盖原厂公章；承诺由原厂提供软件部署实施服务，支持 1G 吞吐能力配置，支持旁路镜像部署调试、业务系

	统联调、上线保障、管理员培训和验收配合。

（三）终端管理系统

需求名称	需求具体内容
基本要求	1.提供一套终端管理软件。 提供 1000 个点的移动端(（安卓、pda、平板）管理授权； 提供 500 个点的 PC（Windows、 Linux、国产化）终端管理授权； 支持对 Linux 终端(ubuntu 22 版本以上 ，centos 7.9 版本以上)管控。
PC 终端网络配置管控	1.能够实时监测终端 IP 地址、MAC 地址、DNS 配置等相关网络信息，支持对应信息的实时绑定，当 IP 或 MAC 发生改变时能够强制恢复至修改前。
PC 终端安全基线	▲1.产品支持终端安全基线检查，包括对计算机名称、软件名单、系统服务、系统共享等进行检查，并针对检查项设置安检分值，基于分值决定违规处理措施，处理包括告警、断网、锁屏、重启、关机等。（提供加盖原厂公章的截图电子件）
PC 终端外设管控	1.USB 管理:U 盘注册、U 盘加密、读写管控、对移动存储设备的读、写操作进行审计，包括文件创建、复制、删除、修改、改名等操作。移动存储介质的插入和拔出动作的详细记录，包括事件类型，移动存储介质的名称、用户、计算机 IP 地址和事件时间。
	2.USB 端口、光驱、软驱、打印机、调制解调器、串行口、并行口、1394 控制器、红外设备、蓝牙设备、PCMCIA 卡、手机等。
资产管理	1.产品必须具备采集硬件资产信息功能，能够获取硬件资产信息，并对资产变动进行预警。
	2.产品必须具备采集软件资产信息功能，能够获得计算机软件安装信息，并支持对软件的远程卸载。
	3.产品需具备设备未关机走势图功能，统计一定时间内未关机设备的走势图以及设备列表，并提供 TOP10 的饼图，可通过 TOP10IP 查询未开机设备记录时间信息。
PC 端软件分发	1.产品需要提供文件分发，支持可执行程序、MSI 安装包或者文档数据文件自动下发与安装。

	2.文件分发需要支持立即执行，周期（每天/每周/每月）执行，自定义执行分发任务，分发后可以对终端的软件进行判断，能够自动统计分发成功率及软件安装成功率，支持进程、安装路径等多种参数判断方式。
PC 终端运维展示平台	1.支持在运维工作台卡片终端上展示设备故障信息，并可通过颜色不同区分设备故障状态。
PC 终端远程运维管理	1.产品具备远程管理功能，管理员可通过管理控制台和客户端方式进行远程控制，支持远程查看、控制、文件传输、重启等；
	▲2.产品的远程管理功能，需要支持 windows、国产化、不同设备间互相远程。（提供加盖原厂公章的截图电子件）
	3.产品的远程管理功能，支持 windows 用户侧在终端上主动发起，同时远程查看、远程控制可以根据管理需要和网络状况，选择、配置适合管理员的窗口分辨率、显示比例等。
	▲4.产品的远程管理功能，远程管理支持穿透 NAT 或 VPN 的远程屏幕控制。（提供加盖原厂公章的截图电子件）
PC 终端弱口令检查	1.产品支持对终端弱口令的检测，提供密码字典，支持弱密码字典的导入导出功能，可以实现自定义添加口令进行检查，同时支持冗余账户禁用，弱口令账户设置过期等修复方法。
PC 终端违规外联	▲1.产品需支持对 windows 操作系统、国产操作系统、等终端设备是否存在违规外联上网行为进行检查，对于存在的违规外联行为,给予相应处理，包括断网、重启、关机、提示信息、截屏、锁屏、修复代理等处理动作。（提供加盖原厂公章的截图电子件）
	▲2.产品需支持在发现违规外联上网行为后，可以自动配置执行处理动作的时间，可配置时间范围在 1 分钟-24 小时之间。（提供加盖原厂公章的截图电子件）
	3.支持检查当前计算机是否存在双网卡连接行为,发现阻断，防止外联。
PC 终端主机防火墙	▲1.支持终端主机防火墙控制，可以对访问的 IP 地址段、域名、端口、进程进行管控。（提供加盖原厂公章的截图电子件）
PC 终端网络访问控	▲1.支持网站访问进行控制，支持 URL 地址的黑/白名单配置，支持 URL 的地址导入导出。（提供加盖原厂公章的截图电子件）

制	2.支持对系统网站访问的审计功能，包括 IP 地址、访问域名、标题、访问时长、开始时间等。
PC 终端屏幕审计	▲3.产品需支持屏幕监控，支持截图的形式录制终端的操作行为，支持基于桌面程序窗口的录制，可指定录屏窗口。（提供加盖原厂公章的截图电子件）
	▲4.产品截屏审计需要支持对截屏间隔时间、图像质量、录制状态进行配置。（提供加盖原厂公章的截图电子件）
移动终端客户端安装	▲1.支持通过提供 windows 安装程序，在打开 USB 调试模式，连接数据线，通过 windows 系统进行一键安装。（提供加盖原厂公章的截图电子件）
移动端软件资产管理	1.支持对移动终端设备进行安装软件信息的采集展示，并能对采集的软件进行分类管理，支持快捷的一键资产导出。
移动终端权限管理	▲1.对于截屏、相机、Wifi，USB、SD 卡等功能的管控，需要通过提权的方式管控。同时在终端锁屏界面提示“此设备由您所属单位管理”以警示使用者。（提供加盖原厂公章的截图电子件）
移动终端蓝牙控制	1.支持对 Android8.1 以上移动终端蓝牙连接进行控制，限制移动终端的蓝牙连接，使其只能连接指定蓝牙设备或者强制关闭蓝牙。
移动终端 SD 卡控制	1.支持对移动终端 SD 卡使用进行控制，禁止移动终端使用外置 SD 卡，防止设备数据泄密。
移动终端时钟管控	▲1.支持对移动终端设备时间进行检测，能够实现强制 NTP 校时并禁止人为手动更改移动终端系统时间。（提供加盖原厂公章的截图电子件）
移动终端数据防泄漏	1.支持控制移动终端截屏功能使用，防止通过截屏功能数据外泄。
	2.支持控制移动终端相机的使用，防止移动终端通过拍照方式将敏感数据泄密。
移动终端水印能力	1.产品需支持移动端屏幕水印功能，对于通过屏幕截屏和被拍照等泄露的信息进行追溯。
	▲2.支持在移动终端中实现屏幕水印功能，全屏展示必须可以显示使用人、设备名、IP 地址、MAC 地址、部门名称等内容。（提供加盖原厂公章的截图电子件）
	3.启动水印功能，可以支持对水印字体大小、字体颜色、透明度、横纵向间距和倾斜度的自定义配置。

移动终端 USB 管理	▲1.支持对移动终端 USB 连接进行控制，限制移动终端与 PC 的 USB 数据传输，防止移动终端随意连接 PC 设备导致数据泄密。（提供加盖原厂公章的截图电子件）
移动终端 SIM 卡管理	1.支持对移动数据的使用提供审计功能，对移动终端使用 SIM 卡联网行为进行日志记录。
移动终端应用 APP 管控	▲1.支持对 Android 8.1 及以上版本移动终端的应用安装实施黑白名单管控。支持批量导入指定软件名单，可配置终端仅允许安装白名单应用，或禁止安装黑名单应用，有效防范非法应用对移动终端造成安全风险。（提供加盖原厂公章的截图电子件）
移动终端软件下发	▲1.支持对移动终端进行软件分发与卸载操作，可向终端下发 APK 安装包并实现静默安装，同时支持对已安装应用执行静默卸载，帮助用户便捷完成软件的推送安装与卸载管理。（提供加盖原厂公章的截图电子件）
移动终端防丢失	1.支持对 Android 8.1 及以上版本移动终端提供丢失检测能力，设备丢失后可执行强制锁屏、自动周期重启、恢复出厂设置等安全防护操作，避免因设备丢失造成数据泄露。
移动终端审计能力	1.支持对 SD 存储的使用进行有效审计，记录移动设备的 SD 卡插入取出行为。支持对 USB 存储的使用进行有效审计，记录移动设备的 USB 卡插入取出行为。
服务要求	▲1.提供三年原厂售后服务：原厂提供 7×24 小时电话及远程支持服务。系统出现故障时，在接到电话故障报告后 60 分钟内做出实质性响应，如需现场服务的需原厂工程师在 4 小时内到达故障现场，系统平台部署、系统培训、版本升级、故障定位、运行巡检、策略优化和应急响应等服务。
	▲2.提供针对此项目的原厂售后服务承诺，并加盖原厂公章

（四）资产梳理与安全咨询服务

指标项	参数要求
服务器与存储设备梳理	服务内容：全院服务器、存储设备资产梳理
	统计信息：1.物理位置（物理机）；2.宿主机（虚拟机）；3.品牌、型号，序列号（物理机）；4.采购时间（物理机）；5.维保情况（物理机）；6.设备接线情况；7.标签补打；8.系统版本；9.主机名；10.系统承载应用；11.命名规划；12.网络配置情况；13.安全软件安装情况；14.系统资源配置；

	15.系统资源使用情况
有线网络设备	服务内容：有线网络设备资产梳理
	统计信息：1.物理位置；2.设备品牌、型号，序列号；3.采购时间，维保情况；4.设备用途；5.IP 地址（管理 IP）；6.设备命名；7.设备接口数量；8.互联接口和设备接线情况
无线网络设备	服务内容：无线网络设备资产梳理
	1.物理位置；2.设备品牌、型号，序列号；3.设备 MAC 地址；4.设备管理 IP；5.设备命名；6.设备互联网接口和接线情况（AC）；7.采购时间和维保情况；
安全设备统计	服务内容：安全设备资产梳理
	1.设备名称；2.物理位置；3.逻辑位置；4.品牌、规格、型号、序列号；5.采购时间；6.授权到期时间；7.设备接口和连线；8.系统版本；9.安全策略配置情况
有线终端统计（PC、自助机等）	服务内容：有线终端资产梳理
	1.设备命名；2.物理位置；3.IP 地址；4.品牌、规格、型号、序列号；5.采购时间和维保时间；6.设备接线情况；7.操作系统版本；8.安全软件安装情况
无线终端类设备统计	服务内容：无线终端资产梳理
	1.设备命名；2.使用科室；3.IP 地址；4.品牌、规格、型号、序列号；；5.采购时间和维保时间；6.系统版本
资产报告整理	整理、统计各子项内容，生产各分类的资产报告
网络拓扑图绘制	基于精确的资产梳理结果，绘制符合以下要求的全院网络拓扑图： 图标标准化：不同类型设备（如核心交换机、防火墙、服务器、终端等）使用不同且统一的图标。 结构清晰化：清晰体现整体网络结构、关键设备、单/双链路、安全域边界及安全域交换机等。 信息完整化：标注核心业务系统服务器名称及数量；明确标识互联网出口、关键设备端口及 IP 地址。 可维护性：建立拓扑图更新机制，确保其能随网络变更而动态调整

制度梳理和补充	依据《信息安全技术 网络安全等级保护基本要求》、《数据安全法》等法律法规及行业最佳实践，对现有安全制度体系进行全面审视与完善： 制度检查：评估现有制度的覆盖范围、执行情况及修订需求。 体系补充：重点补充和完善系统安全类与数据安全类管理制度。 系统安全类：涵盖授权审批、人员管理、系统运维、机房安全、密码使用、日志留存、事件应急响应等全方位管理制度。 数据安全类：建立覆盖数据全生命周期的管理体系，包括数据分类分级、权限管理、传输加密、备份恢复、合作方管理、安全审计、事件应急等实施细则与操作指南。 层级构建：形成由总体方针、管理办法、操作规范到记录表单的四级文件体系，确保制度可落地、可执行、可追溯。
网络安全差距分析	结合资产台账、网络拓扑图及安全设备策略配置情况，对医院现有安全防护状况进行深度分析： 信息调研：全面收集资产、配置、策略等信息。 差距识别：对照国家等级保护等合规要求，识别存在的安全问题与风险点，形成《安全问题清单》。
网络安全差距分析报告编制	风险评价：对识别出的风险进行分析与评价，明确其潜在影响。 整改建议：针对每个风险点，提出具体、可操作的整改建议。 成果交付：最终形成《网络安全差距分析报告》，为后续安全建设提供明确的行动路线图。
工具部署	部署必要的技术工具，采用工具加人工的方式完成项目执行

四、其他相关要求

（一）整体服务要求

1.集成服务要求

投标人需要承担新购产品部署与原有环境的融合改造集成任务

具体包括：

负责新购产品平台部署，将新购产品连接到用户现有业务网络；实施前提供设计方案

编写设计、产品配置和运行维护技术文档；

投标产品必须兼容目前医院现有网络、业务系统，实施过程中不可对医院正常业务造成任何不良影响；

项目实施过程中不论是产品出现集成与连接的技术问题，全部由投标人负责解决，由此产生的费用均由投标人承担；

投标人必须承诺保证提供原装产品，若发现有非原装产品，则无条件退货，并赔偿由此引起的一切损失。

投标人应指定一名项目经理，负责项目的管理工作，合理安排项目进度，并对项目风险进行控制。

2.咨询服务要求

投标人需按照招标要求，完成资产梳理与安全咨询服务。要求服务过程中，不可对医院业务造成影响，不可影响业务科室的正常办公。做好资料保密工作，所有涉及医院的资料与文档，不可泄露给项目无关人员。

3.其他要求

在本项目服务期内，投标人需对本项目部署的系统进行现场巡检，巡检频率不低于每年 12 次。

对于投标人承诺的符合要求的产品，采购人有权利在签订采购合同前，对参数的每项指标均进行功能有效性验证，以确保产品实际质量及交付功能满足需求，投标人应予以配合。若中标产品有一项功能未能通过测试，将取消中标资格并追究其所有相应责任（需提供承诺书并加盖投标人公章）。