

功能需求及参数	
名称	技术参数及要求
硬件规格及性能	采用独立的标准机架式 2U 硬件架构，软硬件一体化系统，全操作系统，内嵌数据库，用户无需另外安装操作系统及数据库管理系统。
	内存>=64GB；>=6*100/1000M 电口；>=1*10Gbps 光口；硬盘存储>=8TB，采用 SSD、HDD 多级存储架构，系统和业务数据分离，实现高效、安全可靠存储、冗余独立磁盘阵列；满足医院未来 6 年的使用。
	性能指标：峰值事件处理能力不低于 18000 条语句/秒，日志存储不低于 16 亿条。
	评估对现有业务系统的影响，每条语句的执行影响不高于 100ms。
工作模式	旁路部署方式，对原有网络不造成影响，产品本身的故障不影响被审计系统的正常运行，不得在现有服务器上安装可能带来风险的程序。
	★支持 Agent 引流，运行时 CPU 占用率低于 3%，内存占用小于 100M，程序文件小于 5M。
	★支持分布式部署方式，并支持集中管理功能，可快速查看所有防统方系统的状态、风险状态等；（提供截图并加盖公章）
使用要求	软硬件性能能够满足未来 6 年的发展升级需要，如果后期 HIS 及其它相关系统升级，要免费供兼容性维保服务。
	要有严格的保密措施和签好相关的保密协议。
	公司方需将统方规则配置完善，达到院方使用要求。
	配合使用过程的提出的功能需要，系统规则制定、权限划分需要符合现实工作情况，不干扰业务系统的正常运行。
	要求镜像流量部署成功，配置有光口
	语句翻译要人性化，纪委等非技术人员能看懂，文字简洁有概括性。
	系统中的记录要有溯源性，能够明确显示操作人的信息。
	规则要有弹性，可以按时间维度和数量次数制定风险等级，要有技术人员持续跟进维护来应付未来的新系统添加和新规则的制定。
	硬件配置要满足流量并发和存储抗风险能力高，有自动备份和系统性能的标识。
基本功能	支持 oracle、SQL Server、Mysql、DB2、postaresql、Caché、Portal、DM、informix、Kingbase、LibrA、神通、南大通用、Samba 等数据库的

	审计，且支持多种不同的数据库同时审计。
	★系统支持杭创、键讯、金蝶慧通、用友、中联、阳光用药、天健、厦门智业、科进、中天、天网、方正、东华、金仕达、东软、键讯、陕西医星、长城、广州力锦等 his 中间件审计。（提供截图并加盖公章）
	系统包括审计引擎及管理后台软件、策略管理、告警管理、权限管理、系统日志、系统配置等功能，审计数据统一存储、查询、分析、统计。
	★系统内置有多级缓存机制，能够实现超出总容量的 30%时支持时间不低于 2 小时，有多级物理存贮机制；（需提供原理性证明文件）
	★系统应支持多层过滤功能，支持网络流量驱动级过滤，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，对无用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/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；（提供截图并加盖公章）
防统方审计能力	★全面支持后关系型数据库 Cache 的集成工具 Terminal、Portal、Studio、Sqlmanager、MedTrak 工具的审计，其中 Portal 能审计到 Sql 语句、查询 Global 有返回结果，Sqlmanager 支持根据 SQL ID 提取高效审计，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；（提供截图并加盖公章）
	★支持数据库绑定变量审计、函数审计（sum 求和函数等）；（提供截图并加盖公章）
	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。
	★在无需重启被审计数据库的情况下，支持对 SQL Server 加密协议的审计，可正常审计到数据库账号、操作系统用户名、操作系统主机名等身份信息；（提供截图并加盖公章）
	支持超长操作语句审计，针对传统型数据库，支持 3 万字节审计而不截断；
	支持对执行时间超过 6 小时操作的审计。
应用审计能力	★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，精确定位到人，并可获取 XML 返回结果；（提供截图并加盖公章）
	★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；（提供截图并

	加盖公章)
防统方策略支持	系统自带各种常见 HIS 防统方规则库，且规则数量≥500 条以上，支持自定义防统方规则；
	★支持统方确认，点击查看某条审计记录，能够进行统方确认，此时该条审计记录就会从审计记录中移除，加入到统方报表中。（提供截图并加盖公章）
	防统方策略支持 18 种以上审计元素，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；语句翻译要人性化，纪委等非技术人员能看懂，文字简洁有概括性。
	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，连续操作了设定的语句集合时进行规则审计告警。
	支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数并进行告警。
	提供系统漏包告警、网络和网卡异常、磁盘存储容量不足等情况时的自动报警提醒；
	系统支持管理界面告警、Syslog 和 SNMP trap 告警、邮件和短信告警
事件查询统计	告警检索效率高达亿条数据分钟级，搜索条件支持全范围搜索（特别要求在超过亿条数据量时），一次性完成搜索的响应时间在分钟级别；
	内置用户登录情况、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；
	支持内置抗生素使用报表、高值耗材报表。展示医务人员用药情况、患者自费比例、抗生素使用情况、抗生素类型使用情况；展示耗材使用情况、科室使用情况；报表支持 Word、PDF、Excel 格式导出。
	★支持对可疑监控对象的操作语句进行会话级的事件回放，回放时间可达前后 60 分钟，方便风险及违规操作的追溯；（提供截图并加盖公章）
审计配置管理	★翻译功能：支持在审计时自动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，按照业务的行为和分类来进行信息的组织和展现，便于审计人员方便、简单的获得并了解数据库审计的结果；（提供截图并加盖公章）

	支持对 http 请求做自定义翻译,可将 http 请求翻译审计人员易看懂的语言;
	三权分立: 提供管理员权限设置和分权管理, 纪委监测用户、系统管理用户、安全规则管理用户权限分开, 相应权限的用户只能查看、管理相应的功能, 责任明确;
	系统支持对所有数据库审计系统管理人员的操作行为进行审计记录,如登录审计系统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;
	★支持系统管理人员异常操作监控,可按需选择需要告警的操作类别,未开启的操作类别不会发生告警。可以看到具体的告警日志信息,同时支持指定查询某时间段和某类型的告警日志查询。(提供截图并加盖公章)
	管理员登陆支持多因子认证: 静态口令认证, 短信验证, 支持密码的复杂性管理, 比如大小写、数字、特殊字符、长度等, 支持自定义内不操作自动锁屏功能;
	可提供审计策略和配置的导入导出;
审计数据管理	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,支持增量、全量备份方式;
	提供审计数据的导出和导入功能;
攻击检测能力	★支持对 SQL 注入、跨站脚本攻击等 web 攻击的识别与告警;(提供截图并加盖公章)
	★系统应具备自动发现未知仿冒进程工具的能力,通过对未知进程的监控从客户端工具使用的次数,客户端 IP 及次数、连接数据库次数等多维度进行安全评估和预警;(提供截图并加盖公章)
	系统应具备防范非法 IP 地址、防范暴力破解登录用户密码(能够对连续失败登陆进行自动锁定,锁定时间可设置)等安全功能;
	系统本身应自带系统级的安全设置,对于统方和破坏数据库的危险行为如: 拖库、删表、EXP 备份导表等行为自动识别和告警;
抗菌药物试剂及耗材分析模块	★支持特定时间区间内抗菌药, 药剂及耗材的种类, 型号, 规格, 用量, 价值的排名统计, 并生成报表(提供截图并加盖公章)
	支持对药物, 药剂, 耗材的全程监控, 支持模糊条件查询和精准条件查询。 支持对药物, 药剂, 耗材统计数据实时上报和告警
第三方接口功能	支持 Syslog 和 SNMP Trap 方式向外发送审计日志, 支持与第三方邮件和

资质要求	短信系统对接，可外置短信猫，支持 GSM 卡，提供接口可实现与网络设备的联动。
	提供接口可实现与网络设备的联动；
	支持与 FTP 服务器对接（备份与还原），FTP 存储进行加密处理，只有通过专门的工具进行恢复和查询浏览；
	产品须获得中国医药卫生信息技术首选品牌，中国医药卫生信息技术“金鼎奖”，中国网络安全与信息产业“金智奖”、中国数据库安全领域最佳产品奖，提供相关证书复印件，并加盖公章。
	★产品须具有《计算机信息系统安全专用产品销售许可证》，需提供相关证书复印件并厂家盖章。
	产品须具有《防统方系统》、《防统方系统集中管理平台》、《面向多类型数据库的高性能审计系统》计算机软件著作权登记证书，需提供相关证书复印件并厂家盖章。
	厂商须通过 CMMI3 级认证和 ISO27001 认证，需提供相关证书复印件并厂家盖章；
	获取 DAMA2020、2021 数据治理优秀产品奖；