|  |  |  |
| --- | --- | --- |
| **序号** | **分类** | **具体功能参数** |
| 1 | 医德医风 | 1-1.支持服务端、客户端纯B/S架构，不需要安装客户端软件★  1-2.支持科室信息、员工信息与医院业务系统自动同步，支持更新补充多线程方式同步,支持文件手工导入★  1-3.支持自定义角色权限，根据角色权限进行任意菜单查看、添加、删除等权限设置★  1-4.支持短信猫、短信平台接口进行配置  1-5.支持科室类型配置不同模块看不同科室数据  1-6.支持前后台分开，支持动态密码登录系统  1-7.支持自定义模块菜单名  1-8.支持系统每个页面有丰富的操作使用说明  1-9.支持科室权限，不同人员看到不同科室任务  1-10.支持日志管理，包含登录日志，同步日志，导入日志，短信发送日志，录音日志，应用服务器日志，评价器在线日志等等★  1-11.支持脱敏操作，系统自动对敏感信息加密，支持国产加密算法★  1-12.支持员工档案信息管理，包含员工基本信息、医德档案信息、医患档案信息、员工考评档案，廉政档案信息等★  1-13.支持医德档案管理，包括表扬信、锦旗、科研文章、科研项目、获奖情况、锦匾、退红包等等  1-14.支持多种级别考评方式，个人考评、科室考评、党办考评、院级考评★  1-15.支持档案多人论证，支持考评多人论证★  1-16.支持系统自动生成考评等级★  1-17.支持员工医德档案的自助服务★  1-18.支持医德事件的举报与投诉  1-19.支持科室考评，党办考评，院级考评批量操作，草稿操作★  1-20.支持考评结果的等级自定义管理★  1-21.支持考评结果归档保存，支持批量导出  1-22.支持报表统计，按系统角色的不同分别提供相应的条件组合方式的数据查询，提供针对个人、科室、医院、考评项目的多项统计功能，以数据图表的形式呈现给用户，实现数据报表的打印功能★  1-23.支持基础信息维护，基础信息维护主要完成包括职称、职务、政治面貌、科室信息、人员信息、医德考评标准等基础信息项目的更新与维护工作，实现各类基础数据的动态维护，有效保证数据的完整性与一致性  1-24.支持医德医风首页面板以及导航 |
| 2 | 防统方 | 2-1.管理、审计用户权限分开，相应权限的用户只能查看、管理相应的系统功能，责任明确。  2-2.产品既有防统方功能，又有数据库审计功能。  2-3.能够以图形方式显示服务器、数据库（如CPU、内存、接口流量等）使用情况。  2-4.系统应具备对应用程序、数据库访问者、访问者IP地址等的统计功能。并能提供按月统计每天的数据接口流量，统计出每月最大流量和最小流量的日期、终端、应用程序等，且形成趋势图。  2-5.支持多种部署方式（串接/并接）都能够阻止客户端进行疑似的统方行为。  2-6.系统支持采用旁路部署方式，不需要更改现有网络结构、服务器相关配置，系统运行不得影响现有网络和业务的正常运行。系统应能独立完成审计数据采集，不依赖于数据库自身审计日志系统，不得在现有服务器上安装可能带来风险的程序。  2-7.系统确保最小报警监控时间间隔为5秒，保证统方事件的及时告警。  2-8.系统的时间可以和关键服务器中的数据库的时间进行同步，确保记录时间的一致性。  2-9.支持加密方式的数据库连接信息分析。  2-10.支持对Oracle、MS-SQL、DB2、MYSQL、CACHE DB、POSTGRESQL和Sybase 等数据库提供自动化评估、审计和保护功能,可审计的数据库或集群数量不少于6个，并且支持单家医疗机构多种类型数据库并存的信息系统。  2-11.具备用户行为记录功能，记录用户所有的操作（业务访问、系统维护、策略配置等）。  2-12.系统从业务流程角度入手，结合核心数据特征，形成高度集成的“事前+事中+事后”数据防护手段。  2-13.系统配置文件支持导入、导出。系统支持在线升级功能，通过厂家发布的升级包可在线对系统进行软件升级和规则库升级。  2-14.系统为软硬一体机，支持千兆以上网络环境及大概至少500个客户端同时并发的监控，应达到每秒50000个以上的事务处理能力。  2-15.采用B/S架构（兼容不同种类浏览器），提供中文WEB管理界面以便于管理。并应可以根据不同的安全级别采用不同的实时告警响应方式，包括记录、消息、鸣音、邮件、短信、微信等，并能支持短信平台、微信平台。  2-16.支持包括ASCII、Unicode、UTF-8、UTF-16、GB2312、EBCDIC等编码格式，避免因编码格式不同而导致审计报表出现乱码的情况，保证审计报表的可读性。  2-17.支持集群，系统支持冗余备份。  2-18.系统预留接口以作维护，二次开发之用。  2-19.系统能够对自身的事件（包括登录、系统参数修改、系统异常等）进行审计，可以监控和审计用户对数据库中的数据库表、视图、序列、包、存储过程、函数、库、索引、同义词、快照、触发器等的创建、修改和删除等，分析的内容精确到SQL操作语句一级。  2-20.审计数据能永久保存，并支持外接存储设备进行备份。数据进行加密保管，只能通过专门工具进行恢复和查询浏览。支持数据自动备份、手动备份且可修改备份策略。  2-21.能够出具针对纪委、监察室相关人员使用的防统方审计报告（支持每天或多天生成统方审计报告，报告需简单明了，且具有主动将所有的计算机语言翻译成通俗易懂的自然语言的系统机制，支持将整条SQL语句翻译成中文，帮助建立基于内部网络的党风廉政、廉洁警示、院内敏感职权使用的防控专网，支持对接廉政风险防控系统，（需厂家截图并加盖公章）（需提防统方与廉政风险防控系统著作权证明）★  2-22.系统内置防统方知识库，具有自我学习功能。  2-23.应用云计算功能提供数据分析平台，对用户提交的数据进行自主分析，并生成报告和相关建议规则反馈给用户，帮助用户加强医德医风行为管控。（需提供虚拟云防统方与医德医风著作权证明）。★  2-24.能够获取客户端访问数据库的应用程序。根据客户端应用程序名单，实时阻止非法客户端程序或伪装正常客户端程序对关键服务器的访问。  2-25.可疑对象定位功能，可以精确定位可疑对象的物理位置（记录操作人员工号、操作类型、IP地址、客户端工具以及存放路径、操作系统用户名、主机名、MAC地址、SQL语句和操作的时间等关键信息）。  2-26.可以对某统方行为的所有操作以及操作结果关联起来，以报表的形式呈现给使用部门，便于使用部门分析和追溯统方事件。★  2-27.阻止可疑会话功能，甄别数据访问，阻止非正常数据会话。能根据预定规则阻止SQL语句的“数据库墙”功能，如根据系统设置的客户端IP/MAC黑名单，以及数据内容中的敏感信息，实时阻止黑名单中的客户端对关键服务器的访问。  2-28.统方白名单权限的设置，可对授权统方行为的操作人员工号、操作类型、IP地址、客户端工具、操作系统用户名、主机名、MAC地址、SQL语句和操作的时间范围等条件进行设置，只有通过了授权和验证才可以获得统方权限。  2-29.支持抗生素三色告警，能对指定时间内全院抗菌药物品种、剂型、规格、使用量、使用金额，使用量和使用金额分别排名前N位的抗菌药物品种进行分析，自动生成报表（需厂家截图并加盖公章）（需提供防统方与抗菌药物用量管理系统著作权证明）★  2-30.可根据用户自定义规则实时发出手机短信通知和邮件提醒等多种方式的告警信息，为了告警的及时性和稳定性，提供防统方专用短信平台模块（非SIM卡插入方式的短信模块，含短信费用），提供证明材料或厂家承诺函。★ |