**数据库审计技术指标**

**数量：1台。质保：3年。**

**资质要求：**

* 提供自主知识产权证明文件（软件著作权、软件产品登记）。
* 提供与需求单位同类HIS系统的三甲医院数据库审计的销售案例。
* 中标供应商必须在成交结果公示后按照用户要求提供为期15个工作日的产品测试，如中标供应商不组织或测试过程中发现其投标时的响应内容和测试结果有出入、以及所投产品不满足招标文件规定的，将按照有关规定取消其中标资格并追究中标供应商递交虚假资料的法律责任。

**系统部署：**

* 采用旁路部署方式对原有网络不造成影响，审计产品的故障不影响被审计系统的正常运行。
* 审计工作不影响数据库的性能、稳定性或日常管理流程。
* 审计结果存储于独立存储空间。
* 独立完成审计数据采集，不依赖于数据库自身的日志系统。

**审计功能：**

* 支持Cache、Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL等数据库的审计，满足所有信息化系统数据库的安全审计需要。
* 支持大数据体系的数据库审计，如hadoop体系，mongodb等。
* 可支持同时审计多个不同类型的数据库,审计数据统一存储、查询、分析、统计。
* 支持Cache数据库集成工具terminal、portal、studio、MedTrak工具的审计。
* 支持双向审计，要支持对数据请求的报文进行审计，同时应对请求的返回结果进行审计，如操作回应、作用数量、执行时长等内容，并能够根据返回的回应进行审计策略定制。
* 支持绑定变量审计。
* 支持服务器虚拟化的审计。
* 支持虚拟桌面操作的审计。
* 支持Telnet、FTP协议的审计。
* 支持访问数据库的源主机名、源主机用户的审计。
* 实时审计数据库访问的各项要素，如执行的SQL命令、请求内容、包长度、操作回应、作用数量、执行时长；以及客户端及主机端IP、MAC地址、客户端操作系统用户名、主机名、端口、工具、及数据库登录用户名等内容。
* 支持数据库账号登陆成功、失败的审计。
* 支持数据库操作成功、失败的审计。
* 能够对SQL语句转换成中文自然语言的描述功能。

**审计策略：**

* 审计规则库，用户可自定义审计策略。
* 可提供通过子对象模式多级关联跨表跨字段的组合规则。
* 审计策略支持数据库客户端操作系统主机名及用户名、客户端进程、客户端MAC、客户端IP等作为条件。
* 审计策略支持数据请求的报文、数据库操作返回内容、返回行数作为条件。
* 审计策略支持数据库操作关键字作为条件。

**规则分析、统计、追踪：**

* 实时监控，提供实时告警信息，可对当前会话进行详细察看，有助于管理员及时处置。
* 审计数据支持18种以上查询条件，可支持按数据库操作命令（包括select、create等14个命令）、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（包括开始、结束日期）等为条件进行查询。
* 支持按自定义关键字作为查询和统计条件。
* 支持条件之间的与、或、非逻辑组合查询。
* 实现对所有违规事件出现频率进行图形化的汇总统计分析，并提供对汇总结果的实时查询功能；可以对客户端使用的程序、客户端IP、用户名进行图形化排名展示，并生成报表。
* 支持以Word、PDF、xls等格式的报表导出。
* 可对可疑监控对象的操作语句进行回放，方便追溯。

**安全管理：**

* 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。
* 采用B/S管理方式。
* 提供系统升级功能。
* 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。
* 能够实现对自动备份、手动备份审计数据的恢复还原。
* 支持对审计数据存储容量达到一定阀值后，对老记录的自动删除功能。
* 提供磁盘存储容量不足、磁盘Raid故障等自动邮件报警。
* 提供设备自身CPU、内存、磁盘、网口、运行时间、运行状态等信息的监视功能。
* 提供审计策略和配置的导入导出。

**响应方式：**

* 完整真实地记录及存储审计事件信息。
* 系统管理界面告警。
* Syslog告警。
* SNMP trap告警。
* 短信告警。

**硬件配置：**

* 采用独立的标准机架式硬件架构，软硬件一体化系统。
* 性能指标：峰值事件处理能力不低于30000条语句/秒，日志存储最低1年。
* 机架式。