**附件1 采购需求**

**“防统方系统”技术服务要求**

**注：**

1. **带“★”项目为实质性条款，负偏离将作废标处理；**
2. **带“▲”项目为重点参数，非“★”号和非“▲”为一般参数，负偏离将按照扣分规则进行扣分，响应人虚假参选按作废处理并承担相应的法律责任。**

|  |
| --- |
| **防统方系统功能及参数** |
| **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硬件架构，软硬件一体化系统，安全操作系统，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。 |
| CPU>=4核；内存>=32GB；>=6\*100/1000M 电口，其中镜像端口不低于4个；硬盘存储HDD>=4T，SSD>=256G，采用SSD、HDD多级存储架构，系统和业务数据分离，实现高效、安全存储； |
| 性能指标：SQL审计处理能力（吞吐）峰值500Mbps，SQL审计处理能力（速率）峰值12000SQL/S，日志在线存储16亿条。不限制数据库实例数（授权数不低于128个数据库实例）。 |
| 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。（提供截图并加盖投标人公章） |
| ▲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；（提供分布式管理软件、防统方集中管理平台软件或相同功能类型软件的著作权登记证书并提供功能截图加盖投标人公章） |
| 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。（提供面向多类型的高性能审计系统软件或相同功能类型软件的著作权登记证书并提供功能截图加盖投标人公章） |
| 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。（提供截图并加盖投标人公章） |
| 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；  |
| 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Cache数据库审计软件或相同功能类型软件的著作权登记证书并提供功能截图加盖投标人公章） |
| 支持数据库绑定变量审计、函数审计(sum求和函数等）；（提供截图并加盖投标人公章） |
| 支持端口重定向的审计，实现端口重定下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；（提供截图并加盖投标人公章） |
| 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；（提供截图并加盖投标人公章） |
| 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；（提供截图并加盖投标人公章） |
| 支持主流API协议解析，包括Restful、JSON-RPC、XML-RPC、Web Service、Dubbo、Motan、Grpc。 |
| ▲支持对访问时间、接口地址、应用地址、状态码、请求方式、返回结果、应用账号、源/目的端口、客户端MAC、客户端主机名、客户端端口、操作系统用户名、操作系统用户名、风险编号、请求内容、返回内容等条件以上进行审计；（提供截图并加盖投标人公章）。 |
| 支持设置接口调用的单向审计、双向审计及按规则审计。 |
| 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。（提供截图并加盖投标人公章） |
| ▲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；（提供截图并加盖投标人公章） |
| 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；（提供截图并加盖投标人公章） |
| 审计配置管理 | 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。（提供截图并加盖投标人公章） |
| 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； |
| 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；（提供截图并加盖投标人公章） |
| 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；（提供截图并加盖投标人公章） |
| 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；  |
| 第三方接口功能 | 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； |