奇安信网神数据库审计产品技术白皮书

创建时间：2020 年 6 月 30 日
修改时间：2020 年 9 月 29 日

地址：北京市西城区西直门外南路26号院1号
邮编：100044

● 版权声明

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期

状态：C-创建，A-增加，M-修改，D-删除

目 录

1 产品简介

奇安信网神数据库审计与防护系统（以下简称：数据库审计系统）是针对不同环境下的数据库操作行为进行细粒度审计的合规性管理系统。通过对业务人员、运维人员、研发人员等访问数据库的行为进行解析、分析、记录、汇报，从而帮助用户进行事前风险评估，事中行为实时监控、违规操作行为及时响应告警，事后合规报告、事故追踪溯源，同时加强内、外部数据库操作行为监管、促进数据安全的正常运营。

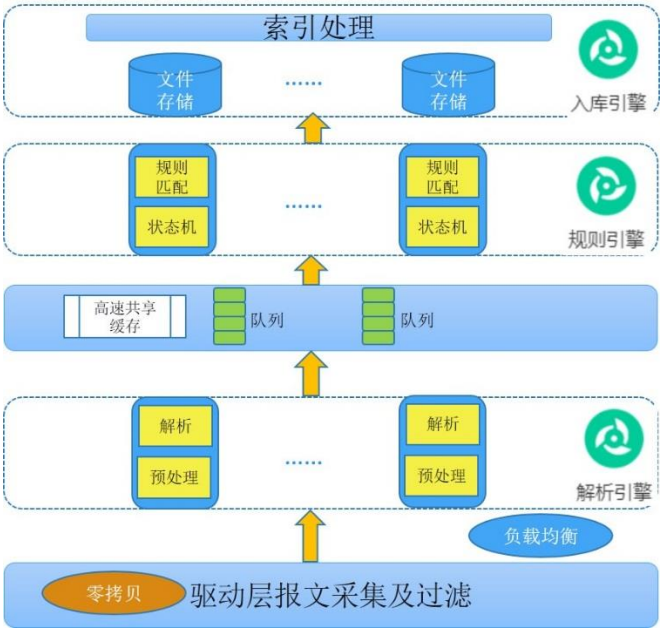
2 体系架构

2.1产品构成

数据库审计系统是既支持软硬一体化也支持纯软件适应于云/虚拟化环境的一系列产品。

数据库审计系统采用数据库深度报文协议解析技术 DPI 及动态流检测技术 DFI 等，将数据库的各种访问操作，解析还原成原始的操作语句，通过预置的安全规则匹配，即可智能分析和监控访问者的各种操作，进行实时威胁预警，并对事件统计分析记录，多重身份定位，有效支持电子取证。

2.2产品架构



奇安信网神数据库审计与防护系统架构

3 产品功能

3.1兼容性

数据库审计系统全面支持行业中主流数据库：包括主流关系型数据库、国产化数据库、后关系型数据库、大数据数据库等

3.2细粒度审计

全面性：针对业务层、应用层、数据库等各个层面的操作进行跟踪定位，包括数据库 SQL 执行情况、数据库返回值等。

细粒度：精确到表、对象、记录内容的细粒度审计策略，实现对敏感信息的精细监控；

深度检测：支持数据库中的嵌套、函数、绑定变量、长语句、返回结果集（返回数据，返回

行数，执行回应，以及执行时长）、脚本等复杂和隐秘的操作行为审计，深度识别和立体分析，不漏审、不误审，准确防范各种危险的数据库操作行为。

3.3事件准确定位

数据库审计系统可以对 IP、MAC、操作系统用户名、使用的工具、应用系统账号等一系列用户特点进行关联分析，从而定位到具体操作者。

3.4丰富策略设置

数据库审计系统根据不同的行业、不同的应用场景提供了不同的规则库，除此之外，用户可自定义设置规则，自定义策略可根据 drop、delete、alter 等高危操作指令、语句长度等信息作为设置条件。

3.5三层关联精准定位到人

数据库审计系统通过独创的三层关联技术，实现精准定位到人；支持 COM/COM+/DCOM 等 C/S 的审计，支持 Tomcat、Apache 等 B/S 的审计，比传统的时间戳匹配更加精准，避免导致高并发无法精准定位的问题。

3.6独立的审计模式

数据库审计系统采用独立的安全结构，通过交换机镜像的方式将访问数据库的流量发送到数据库审计系统，不改变原有的网络结构，真正做到对应用以及数据库零影响。

审计系统采用三权分立的模式，提供管理员权限设置和分权管理，审计用户，系统管理用户、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，相互监督，符合安全法规对审计权限的要求。

3.7别名管理

别名可以对表和字段进行别名设置，可以直观显示审计结果内容，方便非专业技术人员的查看。

3.8云架构下数据安全监控

现在越来越多的客户将应用系统及数据库服务部署在虚拟架构中，数据报文之间的流动在虚拟环境内部进行，不通过物理交换机，而现有的审计技术大多采用旁边镜像的方式，在物理架构及部署上因“看不到”数据报文无法实现对虚拟平台的数据库服务器进行审计，数据库审计系统通过报文引流技术解决“看不到”报文的问题。

3.9非法数据访问监测

数据库审计系统可根据客户意见及实际审计情况，将 IP、操作语句、账号登相关信息加入黑白名单。同时，在应用系统中，因应用系统对应后台的 SQL 语句固定，一旦发现其中含有危险信息则可将对应的 SQL 加入黑名单，而一旦应用系统中有某些语句疑似风险操作但其实际并不产生危害则可加入白名单。

3.10 绑定变量审计

在不同数据库及应用系统中，很多值得传递都是通过变量进行，如在 oracle 数据库中有绑定变量，在其它数据库中也有变量一说。如审计不到变量则无法对 SQL 指令的危险性进行判断。数据库审计系统可对不同数据库的不同变量进行审计。

3.11 事件场景还原

数据库审计系统可根据审计日志，通过事件、端口、端口等因素构建出事件的关联性及现场，通过模拟回放，模拟出整个事件的行动轨迹，通过大屏幕显示可方便分析人员及技术人员通过回放线索，直观的追溯事件的前后关联性及风险蕴含较深的操作行为。

3.12 自动发现

数据库审计系统检测到镜像数据流后，审计系统会自动的扫描数据流中的数据报文，智能识别到数据流中存在的数据库 IP 地址，端口号，以及数据库类型和版本号，并根据扫描出的数据库信息，自行添加为审计系统保护对象，自动进行审计，简化审计员的操作流程，快速部署同时避免用户因模糊记忆引起配置错误的风险。

3.13 报表分析功能

数据库审计系统根据保护对象、年份、月份进行统计以下报表：账户数最多的数据库 Top5 排名、连接数据库服务的访问者 IPTop5 排名、查询语句执行时间分布 Top5、繁忙的数据库服务器 Top5、执行时间最长的语句、同时支持 excel、word、pdf 格式报表的导出。

数据库审计系统支持合规性的报表，针对等级保护有针对性的报表，帮助用户实现快速合规，满足主管单位以及等保标准需求。

除以上的需求外还可以针对不同用户需求进行自定义报表，自定义报表支持支持按照源 IP 地址、客户端工具、帐号、告警数等源信息生成报表；支持按照数据库访问行为生成报表。

3.14 多样告警方式

数据库审计系统支持用户界面、Syslog、SNMP、邮件、短信系统等多种告警方式，第一时间告知用户人员，数据库中违规的访问情况。

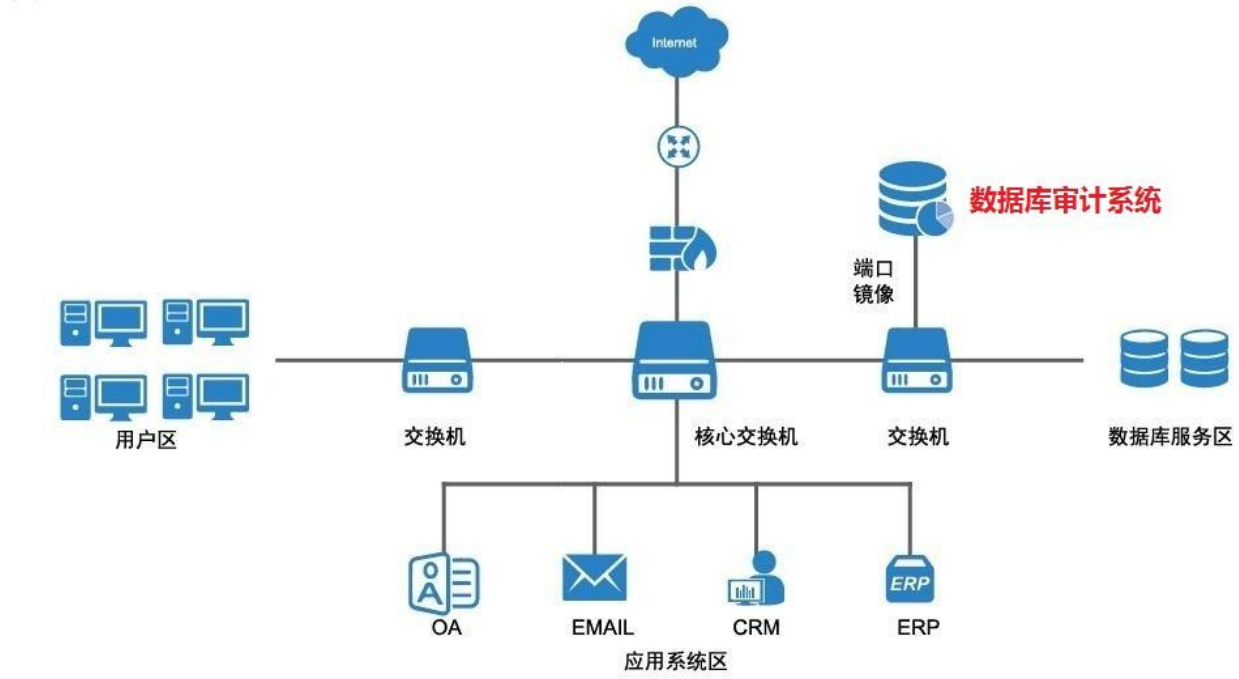
3.15 高性能检索与数据处理

数据库审计系统采用新的技术和系统架构，应用半结构化进行数据存储，检索效率大大提高，亿条数据检索数据秒级响应；同时对数据包的解析能力也大大提高，可应对如学校学生选课高峰期等高并发场景下的审计性能要求，不会因为审计性能问题导致一些数据库访问操作行为漏审。

4 典型应用

4.1旁路审计部署

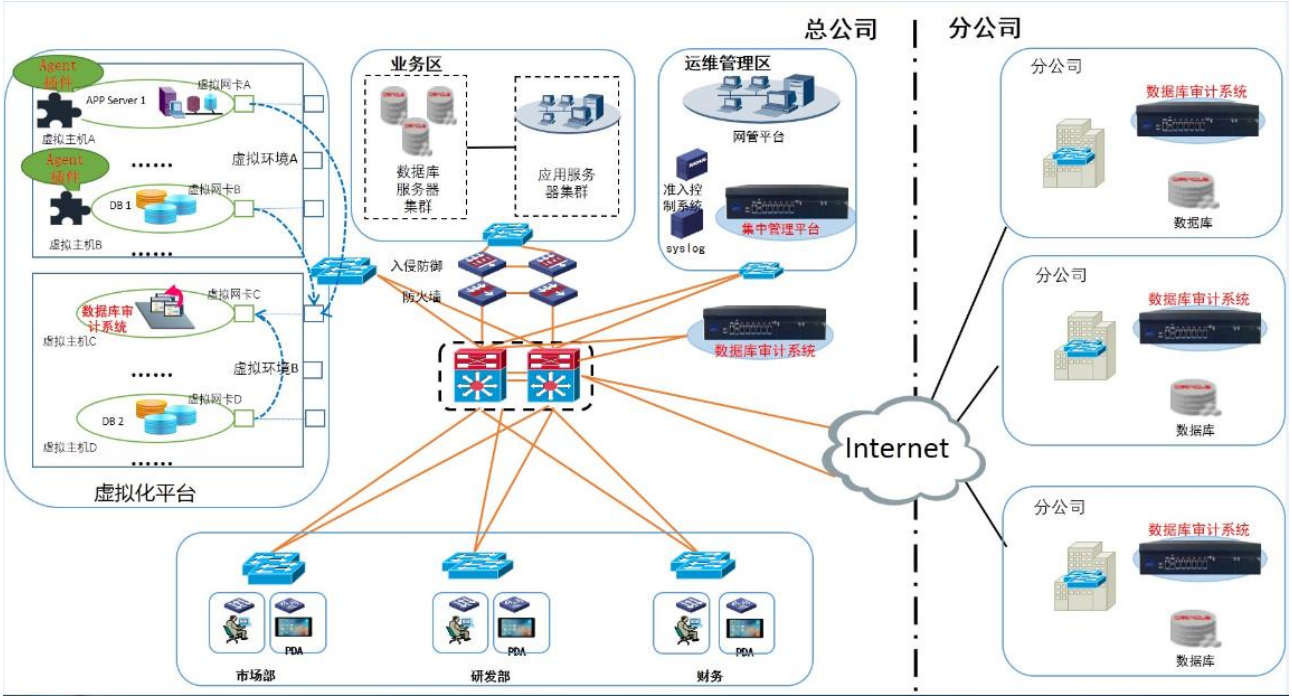
数据库审计系统支持采用旁路监听部署方式，通过交换机端口镜像，将请求数据库的双向流量镜像到审计系统中。



4.2混合部署方式

数据库审计系统提供了集中管理的技术手段，彻底解决了大型项目或大型跨区域集团企业项目面临的部署、管理、监控、预警以及日志方面的问题。

通过以上部署模式增加集中管理平台将所有的数据库审计系统统一集中管理，便于运维、解决多个产品管理困难的问题。



5 客户收益

5.1追踪溯源

便于事后追查原因与界定责任负责运维的部门通常拥有数据库管理系统的最高权限(掌握 DBA 账号的口令)，因而也承担着很高的风险(误操作或者是个别人员的恶意破坏)。审计系统能够帮助客户进行事后追查原因与界定责任。

5.2减少信息资产的破坏和泄露

通过使用数据库审计系统，能够加强对数据库的审计，从而有效地减少对核心信息资产的破坏和数据泄露。

5.3直观掌握业务系统运行的安全状况

信息化系统的正常运行需要一个安全、稳定的网络环境。对管理部门来说，网络环境的安全状况事关重大。数据库审计系统提供业务流量监控与审计事件统计分析功能，能够直观地反映网络环境的安全状况。

5.4满足合规性要求

顺利通过 IT 审计数据库审计系统为核心数据库系统提供了独立的审计解决方案，有助于完善组织的 IT 内控体系，从而满足各种合规性要求，并且使组织能够顺利通过 IT 审计。