毕方数据库安全审计系统

技术白皮书-V1.0

北京协推信息技术有限公司

2019 年 12 月

声明

本白皮书由北京协推信息技术有限公司编制，内容涉及毕方数据库安全审计系统的技术架构、功能特点及应用场景。未经本公司书面许可，任何单位或个人不得以任何形式复制、传播或摘录本手册内容。本公司保留对文档内容进行更新和修改的权利，最新版本请访问官方网站获取。

公司联系方式：

北京协推信息技术有限公司

目　　录

1 概述

毕方数据库安全审计系统是北京协推信息技术有限公司自主研发的新一代数据库安全审计产品，具备细粒度审计、精准行为回溯、智能风险识别、全方位风险控制等能力。系统采用旁路部署方式，实时监控数据库访问行为，支持主流数据库与国产数据库协议解析，适用于政府、金融、电信、能源等对数据安全要求极高的行业。

2 用户需求分析

2.1 合规性需求

随着《网络安全法》《数据安全法》《个人信息保护法》等法律法规的落地实施，企业必须建立健全的数据安全审计机制。等级保护 2.0、ISO27001、SOX 法案等标准均明确要求对数据库操作进行审计。毕方数据库安全审计系统可帮助企业满足多维度合规要求，提供完整的审计记录与报表输出。

2.2 安全性风险

数据库作为核心数据资产的承载平台，面临来自内外部的多重威胁，包括 SQL 注入、权限滥用、越权访问、敏感数据泄露等。毕方系统可实时监控并识别异常行为，及时阻断潜在风险。

2.3 可用性风险

数据库性能波动或故障可能导致业务中断，影响企业运营。毕方系统具备性能分析与故障诊断能力，帮助运维团队快速定位问题，保障业务连续性。

2.4 审计风险

缺乏有效审计机制将导致安全事件无法追溯、责任无法认定。毕方系统提供全量操作记录与可视化回溯能力，支持事中告警与事后取证。

2.5 传统安全技术的盲点

传统防火墙、IDS/IPS 主要防御外部攻击，难以识别内部威胁。而数据库自身日志审计功能开启后对性能影响大，且日志易被篡改或删除。毕方系统通过旁路监听、协议解析、行为建模等技术，弥补了传统安全手段的不足。

3 系统架构与技术原理

毕方数据库安全审计系统采用旁路部署方式，通过交换机镜像端口或 TAP 分流器获取数据库流量，实时解析 SQL 操作并生成审计日志。其技术原理如图 1 所示。

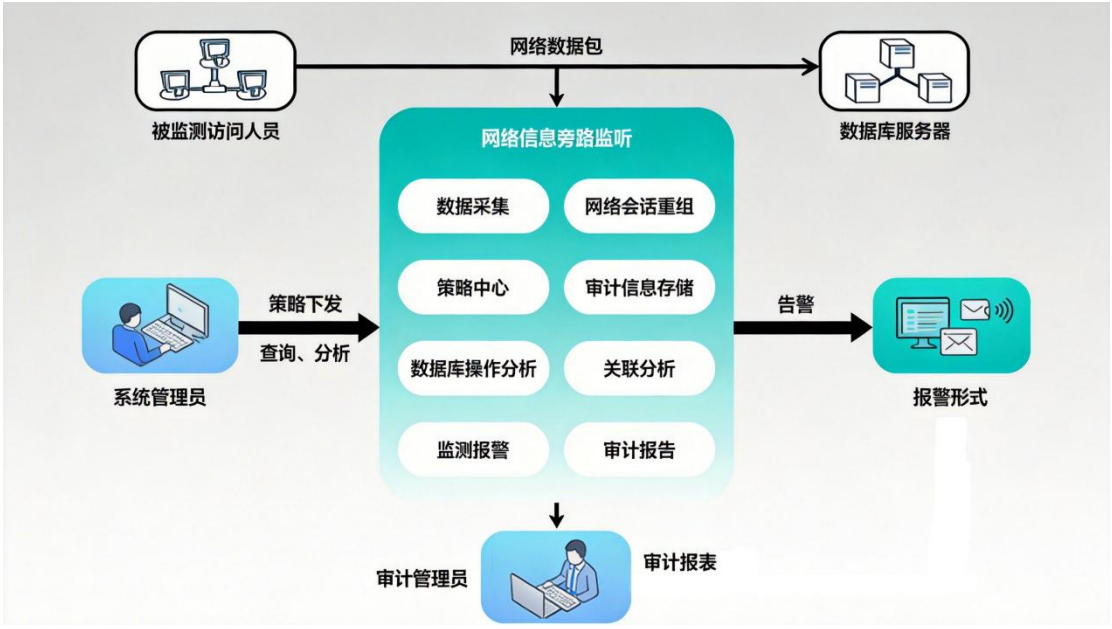

图 1 毕方数据库安全审计系统技术原理图

系统核心组件包括：

数据采集引擎：支持多种数据库协议解析，覆盖 Oracle、MySQL、SQL Server、达梦、人大金仓等；

策略管理中心：提供灵活的策略配置与告警机制；

Web 控制台：基于 RIA 技术，支持多维度查询、报表生成与系统配置。

整体体系架构如图 2 所示。

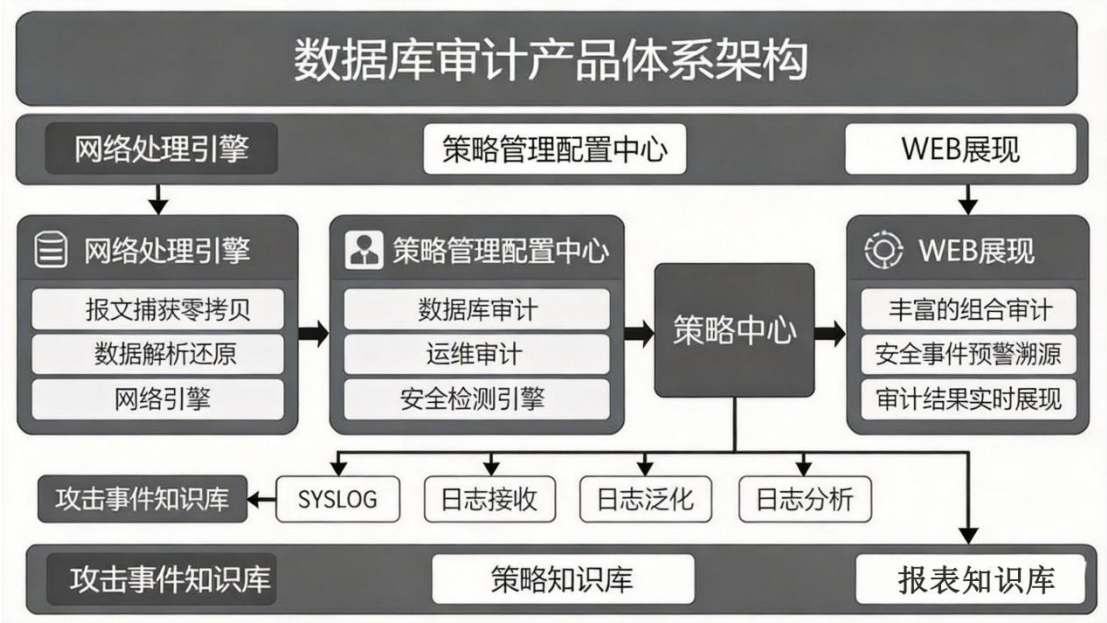

图 2 毕方数据库安全审计系统体系架构图

4 核心功能

毕方数据库安全审计系统具备四大核心功能，如图 3 所示。

图 3 毕方数据库安全审计系统核心功能

- **全量审计**：记录所有数据库操作，包括增删改查、权限变更、登录登出等；
- **双向审计**：不仅审计请求内容，还记录返回结果，支持敏感数据追踪；
- **三层关联审计**：支持中间件与数据库操作关联，精准定位业务用户；
- **动态基线建模**：自动学习用户行为习惯，识别异常操作；
- **漏洞与攻击检测**：内置攻击特征库，支持 SQL 注入、暴力破解等检测；
- **性能分析**：支持 SQL 延迟分析、死锁检测、资源占用监控；
- **报表系统**：内置合规报表模板，支持自定义报表导出。

5 产品优势

- **自主可控**：核心解析引擎自主研发，支持国产数据库与国产化部署环境；
- **精准溯源**：三层关联技术可精确到业务用户，提升追溯能力；
- **智能建模**：基于用户行为建立基线，自动识别异常；
- **全面覆盖**：支持 Oracle、MySQL、SQL Server、达梦、人大金仓、GaussDB 等；
- **易用性强**：支持 SQL 中文翻译、敏感信息脱敏、一键排障；
- **高性能架构**：采用高效协议解析与存储压缩技术，支持大规模并发场景。

6 用户价值

- **防止权限滥用**：对高权限用户操作进行全面审计，防止内部数据泄露；
- **降低运维风险**：审计临时账户、远程维护操作，提升安全性；
- **保护敏感数据**：对核心表、关键字段进行重点监控；
- **满足合规审计**：提供完整的审计日志与合规报表，助力通过等保、SOX 等审计；
- **促进制度落地**：将管理制度与技术手段结合，提升执行效率。

7 典型应用场景

毕方数据库安全审计系统适用于以下场景：

政府单位：满足等保 2.0、政务数据安全要求；

金融机构：满足银保监会、人行数据安全监管要求；

医疗机构：保护患者隐私数据，满足 HIPAA、电子病历规范；

企业集团：实现数据资产统一监控与审计；

云环境：支持虚拟化、容器化部署，适配云原生架构。

典型部署方式如图 4 所示。

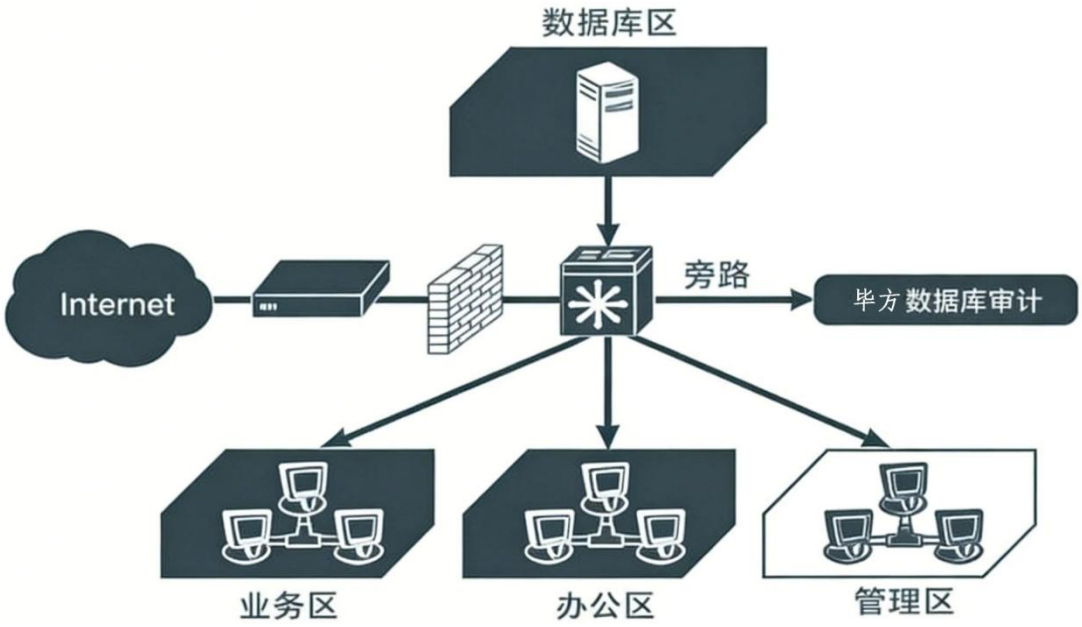

图 4 毕方数据库安全审计系统典型部署示意图

系统通过旁路监听方式接入网络，不影响现有业务，快速实现数据库操作的全量审计与风险监控。

如需获取更多技术资料或申请试用，请联系北京协推信息技术有限公司。