

司南数据库安全管控平台

让数据使用高效而安全

产品版本： V7.0

发布日期： 2025/05/13

01

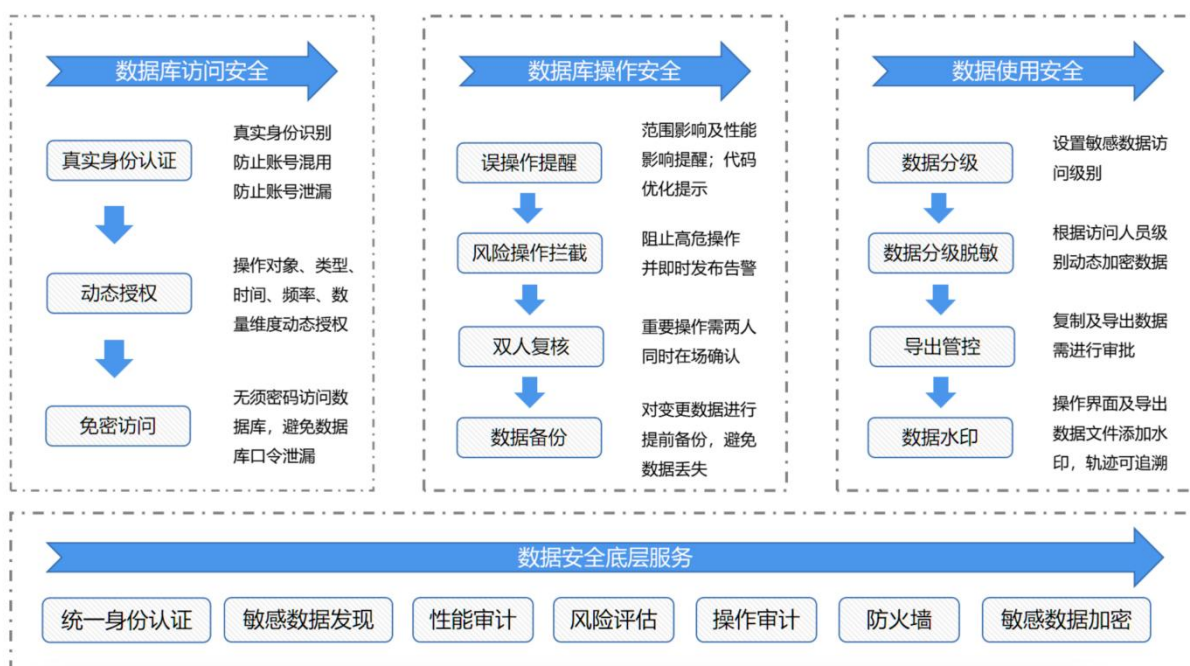
产品介绍

Product Introduction



产品简介

司南数据库安全管控平台(简称“司南”)是一款数据库权限管控类的产品，为多种商业数据库及开源数据库提供统一的访问入口，便捷精细的权限管理结合动态，静态脱敏功能，可为数据资产提供最大限度的保护；同时产品深度集成自研 SQL 审核知识库，可拦截并记录风险 SQL，烂 SQL，并提供多维度统计排行，持续帮助开发人员提升数据库设计水平。

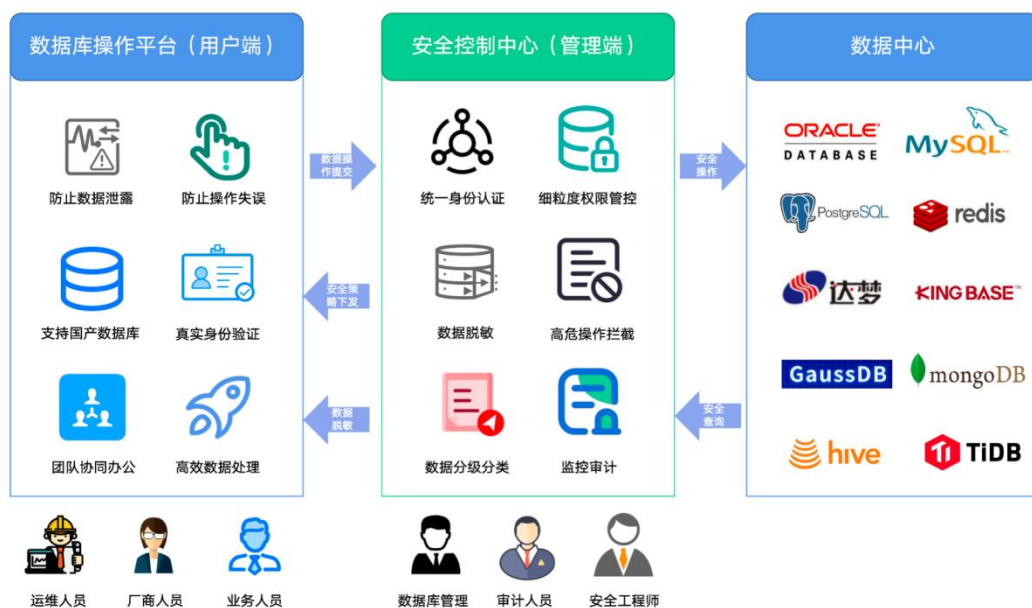


解决方案

近几年数据安全事件频发，出现诸多核心业务数据库被删除、大批量数据泄露等事件，影响巨大，令人深思。



作为业界领先的面向企业的数据库安全解决方案，司南致力于打造一站式安全可靠的数据库操作平台，旨在帮助企业安全、高效地使用数据库，提升研发与 DBA、运维的协作效率，为企业核心数据提供更安全的访问管控与审计，防止数据越权访问、数据泄露、数据误删除等。



司南从数据访问源头开始解决数据安全问题，建立了完整的事前动态管控、事中实时防御、事后快速响应的纵深防御体系，为整个数据生命周期安全性提供完整的保障。

02

产品价值

Value & advantages

■ ■ ■ ■ ■

建设数据库一站式安全访问平台，保障数据库服务连续性及数据安全，使数据库管理符合安全管理规范，夯实数字化运维的基石。



1、管理效率的提升

- **统一数据库访问入口：**提供统一的数据库开发与管理平台，实现数据库访问及管理入口统一，对数据库访问行为进行统一、安全管控。
- **统一用户管理：**对开发测试人员、运维人员、第三方公司人员实现统一的权限管控，无须每套数据库各自维护一套用户体系。
- **流程规范管理：**内置审核发布、SQL 上线、SQL 审核、提权等多套流程，帮助实现流程闭环管理，业务规范落地。
- **提升精细管控能力：**字段级细粒度权限管控，满足业务精细化管理的需要。提供操作类型、对象、时间、数量、人员的细致管控能力。
- **满足批量管控需要：**内置权限管控基础模版，多套数据库可以共用权限管控模版，实现数据库的统一管控。
- **减轻审核负担：**内置行业最佳实践 SQL 审核规则与对象级动态审核引擎，自动生成审核报告，提前发现风险，保障数据库稳定运行。

2、研发生产力提升

- **多种数据库，一个客户端：**实现在一个环境中完成多种数据库的统一管理与开发设计，无须频繁切换不同数据库客户端，提升研发效能。
- **无密码接触：**无须记忆或存储多种数据库登陆口令，使用唯一真实身份访问不同数据库。
- **提升协作效率：**多部门在线协同，共享代码，无须人为维护、线下反复沟通，促进团队合作。
- **提升 SQL 质量：**内置 SQL 审查功能，及时发现代码中的违规与潜在风险，帮助提升代码质量，提前消除潜在威胁，提高项目研发效率。
- **跨终端访问：**云原生数据库客户端，提供云端数据库操作与管理能力，提供在不同网络、不同终端中安全访问方案。
- **开发工具箱：**内置多种数据库开发工具，覆盖主要数据库开发痛点，以自动化替代手动操作。

3、高可用、高性能、高扩展性

基于 GO 语言与原生技术

部署方式	单机部署	集群部署
使用技术	Docker	Kubernetes
安装 Agent	不需要	不需要
建议环境	测试环境	正式环境
服务器	1 台	6 台
CPU	> 8 核	> 16 核
内存要求	> 16G	> 32G
硬盘要求	200G	3200G

4、支持主流数据库

司南支持 openGauss、GoldenDB、TDSQL、Gbase、Kingbase、TiDB、MySQL、SQL Server、SQLite、OceanBase、PostgreSQL、DB2、Oracle、HBASE、达梦、MongoDB 等十余种多类型数据库。

03

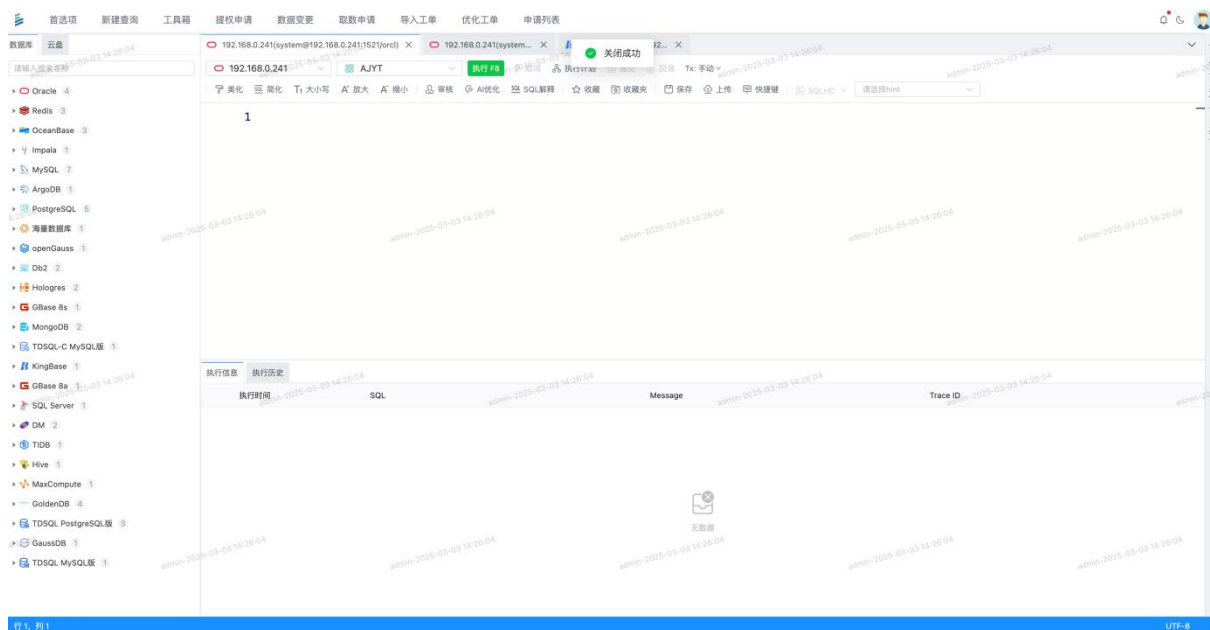
核心功能

Core Function

■ ■ ■ ■ ■

1、云数据库客户端

薄冰自研云数据库客户端，提供高效、安全、全面的数据库开发工作环境，可以在一个开发环境中完成超过 10 多种数据库的统一管理及数据库开发设计，提供高级 SQL 编辑器、命令编辑器、数据库对象管理、SQL 智能补全、数据导入及导出、结果集管理、对象搜索、SQL 审核与拦截等功能。



在**生产力提升**方面，司南针对国人使用习惯进行交互优化，同时内置效率提升工具箱、跨部门协作流程与共享工作区。

同时，司南是一款**更安全的云客户端**。管理员可设置成员的数据操作权限、导出复制权限、全局水印、敏感信息过滤等。安全可控，拒绝一切外在风险。

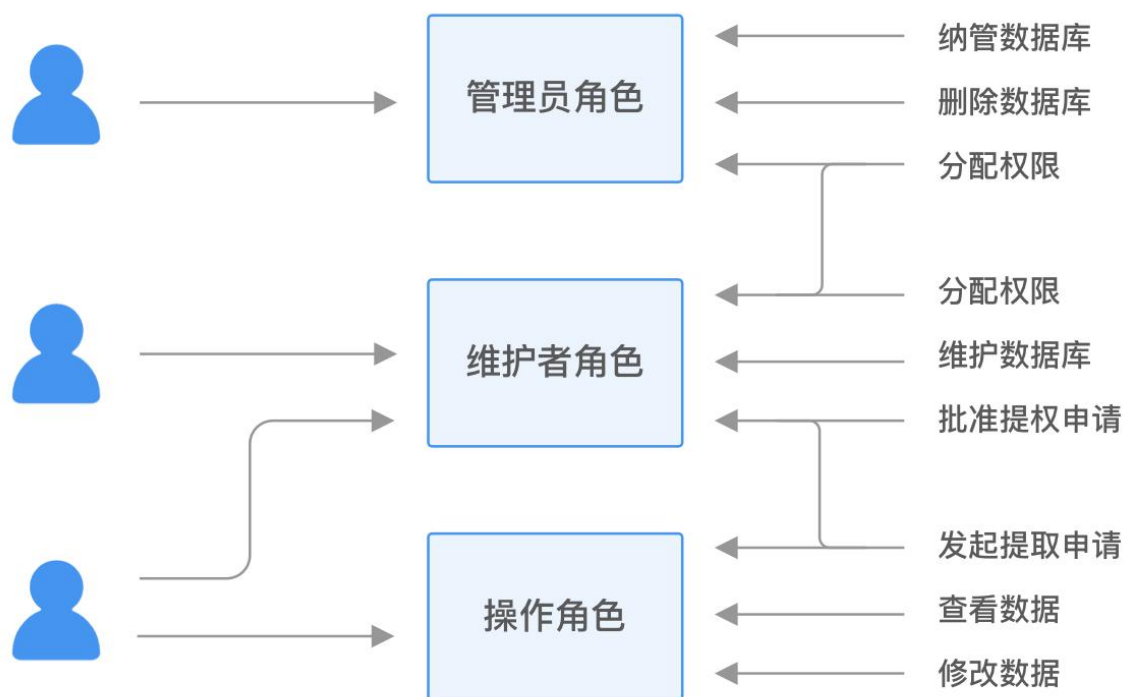
2、统一身份认证

司南对数据库访问用户的真实身份进行双因素验证，不牺牲用户体验的情况下，额外增加一层安全保护。保证访问身份的真实性，避免账号混用等现象。

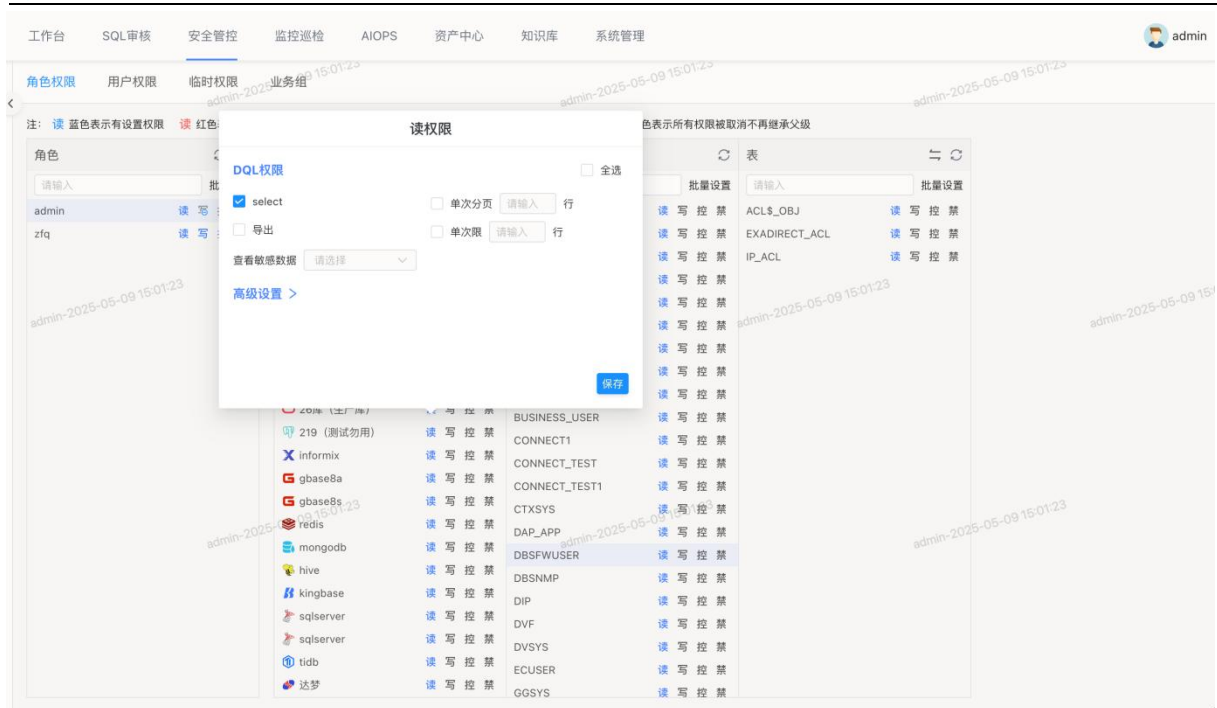
同时，用户使用唯一真实身份访问所有数据库，无须接触数据库密码，免除口令泄露风险，也避免了账号密码记忆与保存的负担。

3、细粒度权限管控

司南自主研发权限管控系统，基于角色和岗位的访问控制，实现动态、细粒度的授权，统一多类型数据库权限管理，完全替代数据库本身的权限系统。管理员可以从操作人员、操作对象、操作时间、操作类型、操作频率等维度进行自主设置，控制用户可以在什么时间，访问什么内容，进行哪些操作。



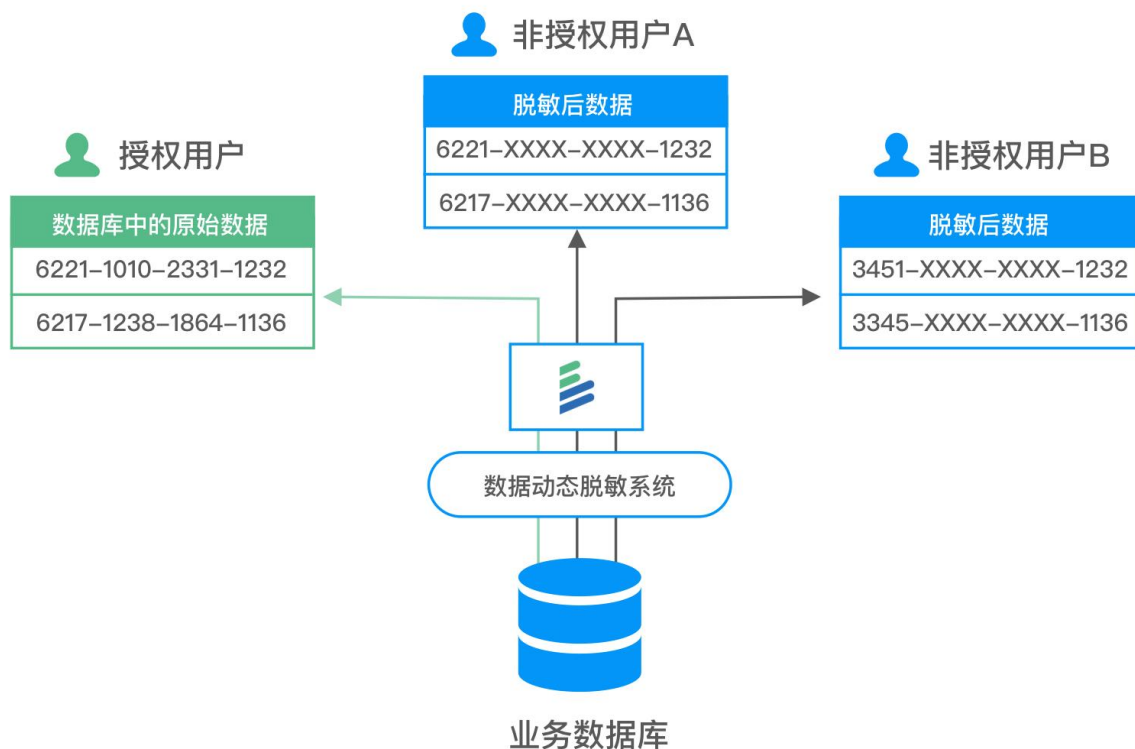
并且管理员可以基于模版、全局设置、批量设置等多种方式，对大量的数据库进行批量、统一地设置，提高数据库权限管理效率。



4、数据动态脱敏

司南可不改变数据库原始数据的情况下，根据数据访问人员级别动态显示明文或者密文。支持截断、加密、随机填充、上下浮动等多种脱敏算法，实现对客户资料、商业数据、个人隐私等多种数据进行脱敏显示。

司南内置多种脱敏规则模版，可以根据用户设置的脱敏规则，自动对数据库中的数据进行脱敏。同时，也支持自动查找数据库中的敏感数据，用户可以设置敏感数据进行分级分类设置，满足不同访问级别下的敏感数据控制。满足分级分类的安全法规制度需要，避免敏感数据泄露。

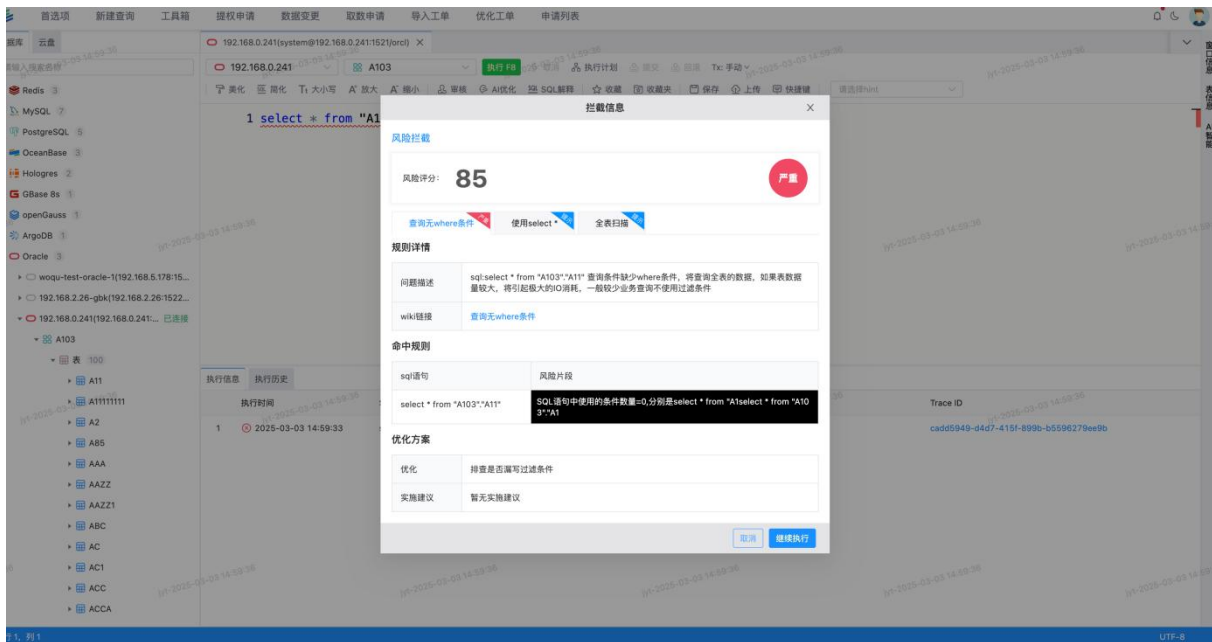


5、高危行为拦截

管理员可设置高危行为规则，对用户**在 SQL 编辑器、SQL 命令行、SHELL 终端执行的 SQL 与命令进行拦截**。

司南在拦截高危行为的同时，也向操作用户进行风险提示，清晰阐述该操作的风险与详情，比如“**无 where 条件**”、“**全表操作**”、“**使用 select ***”等 风险。用户可通过问题简述、代码片段、知识库链接查看风险详情，优化代码。

在提醒操作用户的同时，司南也可以通过邮件、短信、办公工具等多种方式 方式向管理员发出告警。

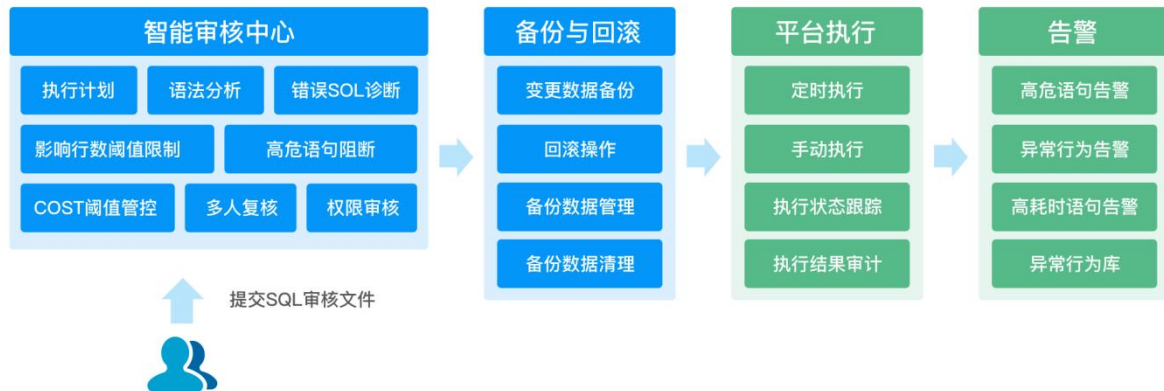


6、上线审核发布

司南提供 SQL 上线流程的闭环管理。支持 SQL 发布的自动审核、人工审核、无锁变更、变更数据备份、定时与手动发布、发布任务跟踪。

平台内置 1200 条审核规则库, 审核规则来自于数据库原厂以及行业最佳实践库, 可以对发布到测试库、生产库等多种环境的 SQL 进行自动审核, 并向管理员提供评分与审核报告。

同时, 发布的 SQL, 可以通过定时或手动发布模式被发布到数据库中。在发布前, 司南对变更数据进行自动备份; 在发布中, 司南对发布任务进行状态跟中; 在发布后, 司南对发布任务完成情况进行通知与告警。实现上线流程的闭环管控给, 避免有风险或者未经审核的 SQL 发布上线; 避免流程绕过, 紧急临时发布; 避免变更数据无备份等多种影响数据库稳定运行的情况。



7、监控审计

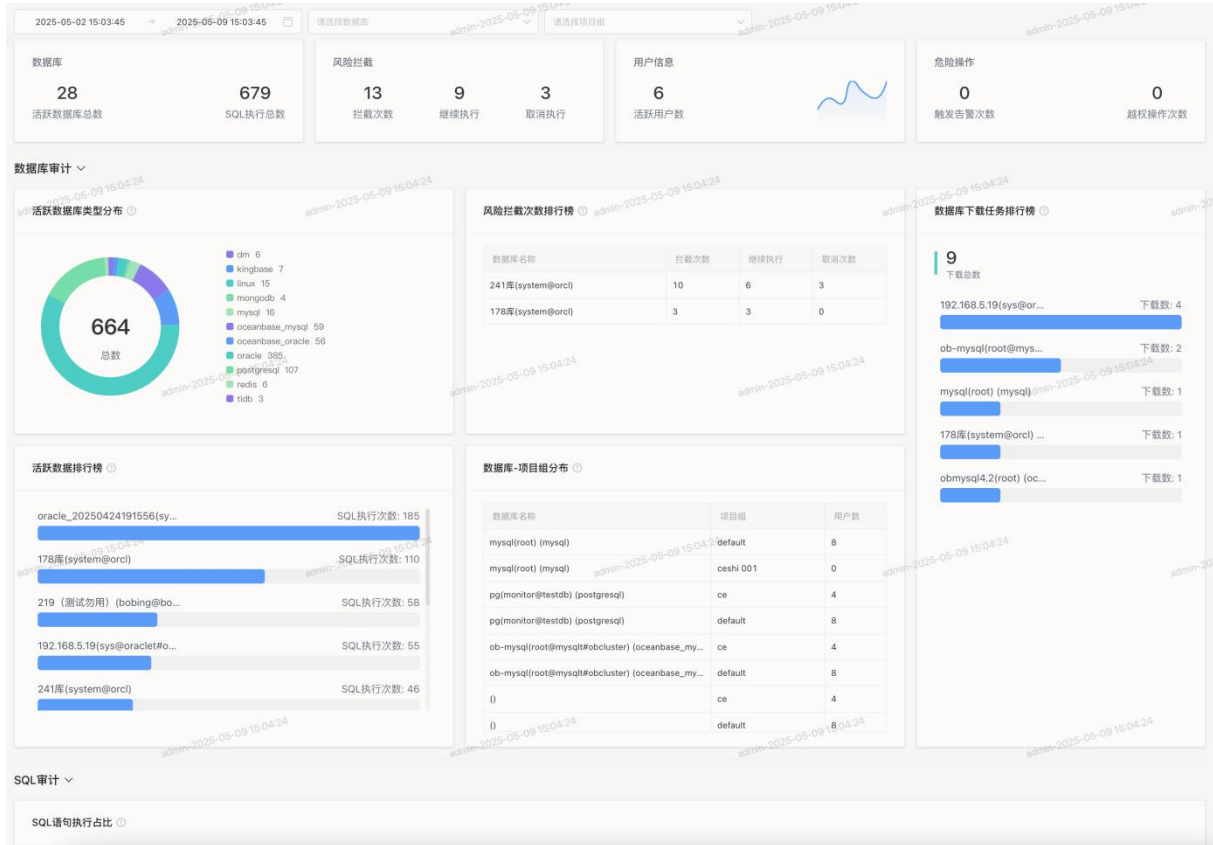
司南对用户通过平台操作数据库的行为，进行全方面审计，并留存日志和记录。能够记录操作人账号、IP、SQL 语句、操作对象、执行结果、耗时、影响行数、错误提示等信息。

同时，提供多维度的查询检索能力，满足操作行为追溯、授权路径跟踪、慢 SQL 查找等同种业务场景。防止溯源困难、定责模糊的情况，导致二次侵害事件 的发生。

操作人	SQL文本	纳管资源	database/schema	影响行数	执行类型	执行信息	执行结果	操作
zy(u)	select /*+ monitor */ * ...	241库(system@orcl)		0	DQL	执行时间: 2025-05-09 15:02:54 执行耗时: - SQL耗时: - 客户端: 192.168.3.84	已完成	回执行日志
zy(u)	select /*+ monitor */ * ...	241库(system@orcl)	A103	0	DQL	执行时间: 2025-05-09 15:02:54 执行耗时: 6ms SQL耗时: - 客户端: 192.168.3.84	已完成	回执行日志
admin(超级管理员)	select * from "A103"...	241库(system@orcl)	A103	0	DQL	执行时间: 2025-05-09 15:02:54 执行耗时: 7ms SQL耗时: - 客户端: 192.168.2.66	已完成	回执行日志
zy(u)	select /*+ monitor */ * ...	241库(system@orcl)		0	DQL	执行时间: 2025-05-09 15:02:54 执行耗时: - SQL耗时: - 客户端: 192.168.3.84	已完成	回执行日志
zfq(赵延之)	select /*+ gather_plan...	241库(system@orcl)	A103	1	DQL	执行时间: 2025-05-09 15:01:54 执行耗时: 5ms SQL耗时: - 客户端: 192.168.5.49	已完成	回执行日志

8、可视化数据报表

记录用户所有操作，并生成分析报告。



9、云客户端接入 AI

司南云客户端集成 AI 智能引擎，可高效实现 SQL 语句优化，生成对比报告，提升查询效率；智能分析 A/B 两库执行同一 SQL 语句的性能差异根源，并精准定位 SQL 报错原因。据需求自动生成高质量 SQL 语句，降低对 DBA 的依赖，让运维更轻松。

04

应用场景

Application Scenarios

■ ■ ■ ■

1、构建统一的数据安全访问平台

- **人员管理混乱：**用户直连数据库；账户管理复杂；有密码即可登录；使用业务账户；存在账户共享；无法独立授权。
- **数据访问工具繁杂：**多种软件维护成本高，授权不可控；账户密码自动记忆；登录无超时设置。
- **权限管控粗犷：**用户账户标识不唯一；个人与业务账户无法分离；应用系统修改密码代价大；存在密码泄漏风险。
- **敏感数据泄露风险：**数据明文存储；数据查询明文展示；数据导出无管控；敏感数据无法发现。
- **缺少审计与监控：**用户操作数据库无法有效地审计与监控。审计线索不足，追溯困难。
- **满足合规性要求：**满足行业标准规范及等保对数据库系统的安全要求。

2、保障业务稳定性，避免数据库抖动

- **SQL 审核发布流程混乱：**研发、测试、运维、DBA 等人员跨部门沟通频繁，需线下反复沟通、沟通效率低、流程进度不可见、不可控。
- **SQL 审核成本高：**无法准确评估批量 SQL 性能与数据影响范围，失误率高，审核人员负担大。
- **数据库误操作风险高：**对核心业务数据库的数据删除、变更操作，没有安全管控机制。
- **高危操作无法拦截：**高危语句与越权语句等危险行为无法阻断与告警，经常需事后救火。

05

关于我们

About us

■ ■ ■ ■ ■

公司简介

浙江薄冰网络科技有限公司是一家专业的数据库综合服务提供商。团队通过在数据库领域多年的积累，自主研发了数据库安全管控、智能运维、SQL 代码审核、数据变更管理等多款企业级产品，同时提供数据库咨询、设计、实施、运维管理等一站式专业服务。

薄冰科技坚持面向数据库管理者日常工作场景的产品研发理念，探索数据库管理的最佳实践。



公司使命

让数据使用高效而安全



公司战略

保障数据安全，挖掘数据潜能

联系我们

- 0574-27911286
- 400-8780-309
- 浙江省宁波高新区创苑路 750 号 A 栋 2 楼 205 室



扫一扫 关注公众号



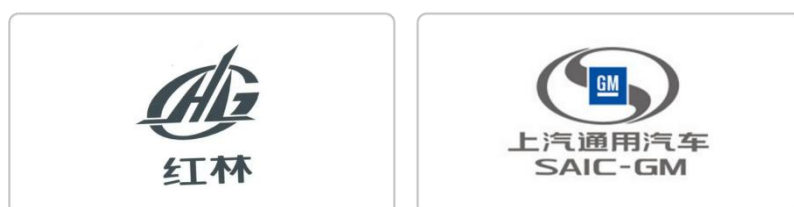
扫一扫 关注小程序

我们的客户

- 金融行业



- 制造业



- 政府机关



- 运营商



- 公共交通

