西骏数据
WEST HORSE DATA

监管背景下的数据库访问管控场景实践与能力提升

北京西骏数据科技股份有限公司

何泽松 CEO

西骏数据——业界领先的数据访问管控平台专业厂商

- 信创会员单位
- 中国网络空间安全协会会员
- 国家高新技术企业
- 北京市创新基金资助企业

ISO20000　ISO9001　ISO27001　证监会备案

CCRC 三级　CIC 三级　CMMI 3　信创会员单位

北京西骏数据科技股份有限公司(WHD)是一家专注于数据访问管控开发的创新型高科技公司，国家“专精特新”企业、瞪羚企业、数字中国高科技高成长企业。

主营业务

- 数据库云客户端
- 数据库云开发
- 数据库云堡垒
- 数据访问云服务(DAMS)

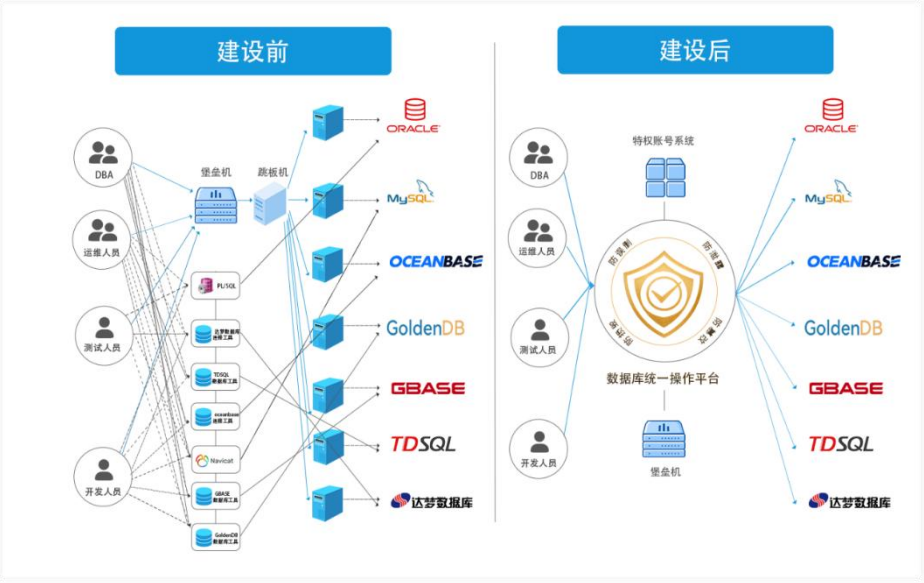
成立日期	注册资金	融资金额
2015年	1020万	数千万
发明专利	软件软著	研发中心
12项	60+个	2个
员工人数	服务网点	服务客户
70+	16个	300+家

西骏数据——国内唯一以数据库访问管控作为主业的专业厂商

西骏数据 WEST HORSE DATA

DataCaptain 数据库访问管控平台

DataCaptain是一款通用的、安全的、开放的、B/S架构的数据库客户端管理工具(UDT)。DataCaptain支持近40多种各类型数据库，包括商业数据库、开源数据库、分析型数据库、国产数据库以及NoSQL数据库。

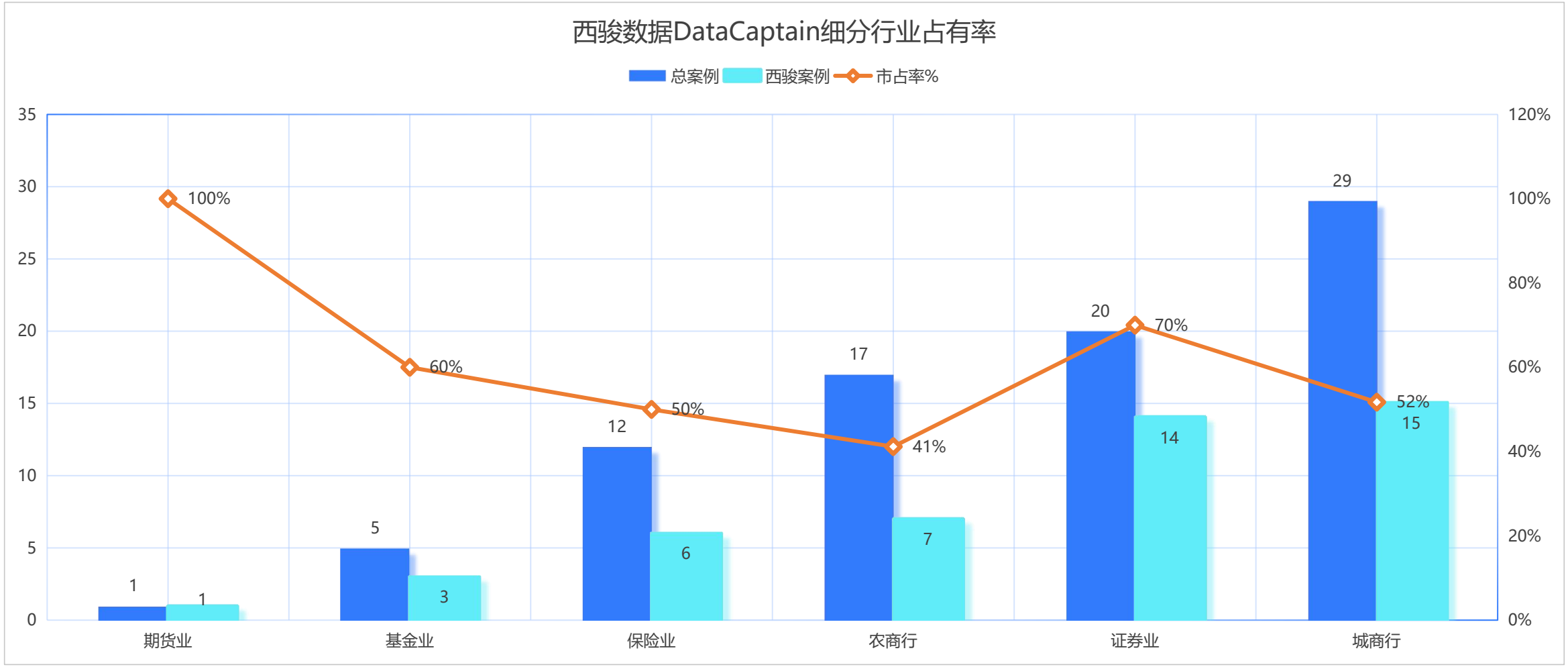


数据库访问管控是指对“**正常**”的数据访问行为进行有效管理，提高数据库操作及访问接口的安全性和便利性，**防范**出现“删库跑路”、数据泄漏、数据篡改、数据窃取、性能影响等事件发生，同时提升应用运维、数据开发的规范性和效率，降低运营管理成本。

数据访问管控平台主要包括如下七部分功能：

- **客户端仿真**：针对不同数据库提供统一的仿真客户端(web)
- **管控精细化**：构建“人-数”二元权限管理，实现精细化的权限管控
- **运维沙箱化**：对所有数据库操作实现沙箱化管理，降低操作风险
- **安全防泄漏**：返回数据通过脱敏、水印、加密等安全措施防止泄漏
- **审计实时化**：提供点对点的高效、实时、场景化、主动式操作审计
- **操作数字化**：所有数据库变更及权限操作支持流程对接与自动执行
- **大模型赋能**：支持与大模型对接，提升运维、开发人员效率

西骏数据在国内主要金融细分行业市场保持占有率领先



根据公开数据统计，截止2025年12月31日

西骏数据
WEST HORSE DATA

目录

金监局发布93号文，推动《银行保险机构数据安全管理办法》落地见效

西骏数据 WEST HORSE DATA

银行保险机构数据安全管理办法

第一章　总　则

第一条　**（立法目的及依据）**

为规范银行业保险业数据处理活动，保障数据安全、金融安全，促进数据合理开发利用，保护个人、组织的合法权益，维护国家安全和社会公共利益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国银行业监督管理法》《中华人民共和国商业银行法》《中华人民共和国保险法》等法律法规，制定本办法。

金融机构数据安全管理能力提升专项行动工作部署会

国家金融监督管理总局

近日，国家金融监督管理总局办公厅颁发了《**关于开展金融机构数据安全管理能力提升专项行动的通知**》（**金办发〔2025〕93号**），全国众多金融机构都现场或者线上参加了国家金融监管总局组织的数据安全管理能力提升专项行动工作部署会。刘司长做了部署和要求：**监管26年会针对数据安全“发现一批、整改一批、通报一批、处罚一批！”**

黄处长做了《银行保险机构数据安全管理办法》专项解读培训：就《办法》出台的背景、核心要义及监管导向进行深入解读。《办法》作为规范银行业保险业数据处理活动的重要监管文件，立足数据全生命周期管理，明确了数据安全治理、分类分级、风险防控等关键要求，是金融机构落实数据安全主体责任的根本遵循。

金融机构需要重点补足的短板包括：

>>> 1 一是压实数据安全责任体系

数据安全管理能力提升专项行动，是金融行业在数字经济时代必须跨越的一道“龙门”。它既是一面镜子，照出机构在数据治理上的不足；更是一架引擎，为机构系统性地提升数据安全能力提供了强大的外驱力和清晰的时间表。成功的秘诀在于：**以战略眼光看待，以治理思维谋划，以工程方法实施，以坦诚态度迎检，以长效机制收官。** 通过将监管要求无缝嵌入机构的战略规划、业务流程和技术架构，将外部压力转化为内生动力，金融机构不仅能够从容应对此次乃至未来的各项监管检验，更能**真正锻造出与自身业务发展目标相匹配、能够护航数字化转型行稳致远的数据安全核心竞争力。**

6 大模块、22 个大类要点、 117 条细化检查项，30-80项有问题是常见情况

西骏数据 WEST HORSE DATA

01 最常见硬伤

- 问题数量太少，被认为走过场，被退回
- 只有表面问题，如培训不足；不写实质性问题，如“权限管控不到位”
- 前后口径矛盾，如 未分类分级 <-> 实现差异化保护
- 生产 -> 测试，数据没脱敏或者脱敏不完整
- 权限管理，只开通，不回收，僵尸账号
- 第三方合作无协议、无要求、无审计
- 操作，特别是高危操作，没有审批流程
- 只做分类分级，没有把分类分级用起来
- 外包人员管理不达标
- 应急演练只有方案，没有实际操作记录、会议纪要等...

02 技术相关的重点要求

- **分类分级：**监管最关注，检查最严
  - 必须全覆盖：覆盖结构、非结构数据
  - 必须有输出：资产目录，分级结果，打标记录
  - 必须能落地：差异化管控、脱敏、加密...
- **数据脱敏**：生产数据导出无审批，测试数据未脱敏
- **技术保障平台**
  - 不再是静态检查，而是要有实战应用：“部署 + 策略 + 日志 + 效果”
  - 等保测评、数据库审计、脱敏、权限最小化、
  - 传输加密弱算法（MD5）必须整改
  - 终端防泄漏、USB 管控、水印
- **个人信息保护**
  - 涉及敏感信息要走审批，留痕

发现问题，需要“真、准、全、实”模式夯实数据安全基座

西骏数据 WEST HORSE DATA

4 月 23 日 自查表初稿（必须达到的标准）

- 117 项结论完整，无空项
- 问题数量合理、结构均衡无明显口径矛盾
- 高风险问题已识别
- 整改时间不扎堆年底

4 月 30 日终稿（必须补齐的内容）

- 问题清单完整、责任到人
- 佐证材料目录齐全
- 立查立改已完成并附证据
- 整改计划分阶段、可验证、可检查

检查核心：不是有没有制度，不是看是否买了某种安全设备或者系统等**纸面合规**，而是：

制度是否落地、措施是否有效、问题是否真实、整改是否闭环

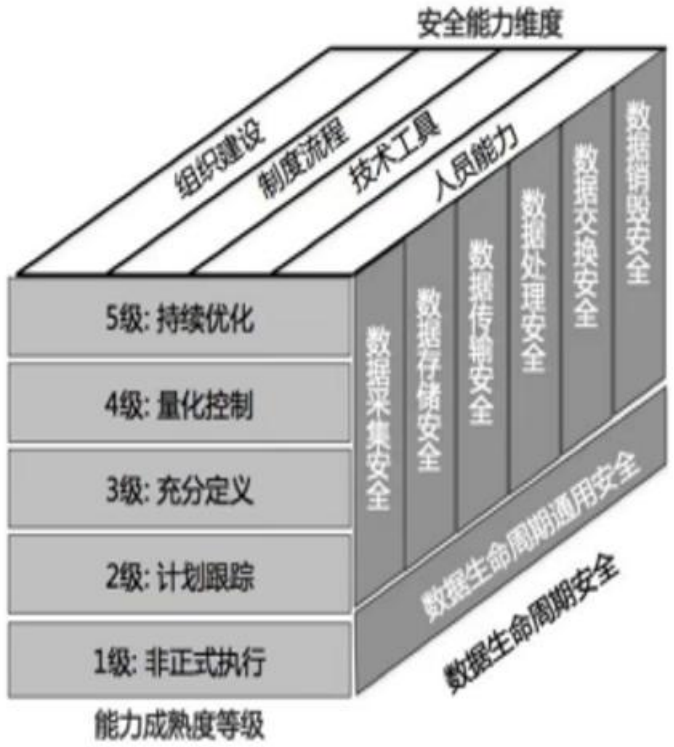
问题整改：有问题不担心，就担心没有落到实处。建议：

- **立查立改**（4 月 30 日前）：制度、发文、权限、流程、培训
- **中期整改**（6–9 月）：梳理、加固、策略优化长期整改
- **长期战略**（2026 年底–2027 中）：系统改造、平台建设、工具上线

西骏数据
WEST HORSE DATA

目录

方法论：从实际出发，拒绝推倒重来，针对性查漏补缺不断增强数据安全保护基线



数据安全能力成熟度模型DSMM（GB/T37988-2019）

♦Step1：业务需求与风险/威胁/合规性之间的平衡

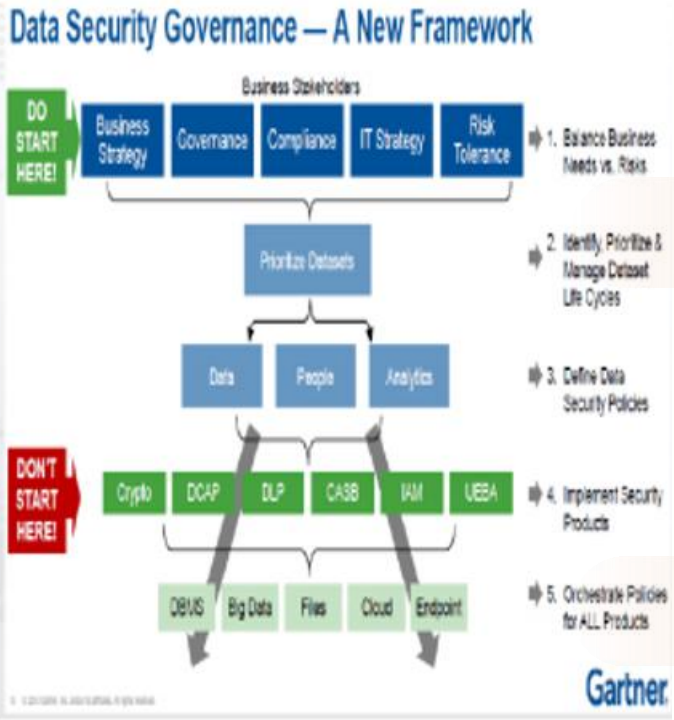
♦Step2：数据分类分级

♦Step3：制定数据安全策略

♦Step4：部署安全控制点

- ✓Crypto（加密）
- ✓DCAP（以数据为中心的审计和保护）
- ✓DLP（数据防泄漏）
- ✓CASB（云访问安全代理）
- ✓IAM（身份识别与访问管理）
- ✓UEBA（用户和实体行为分析）

♦Step5：统一数据安全策略和风险分析



Gartner 关于数据安全治理（DSG）框架

实用性

无需推倒重来。数据安全建设是不断查漏补缺，不断推进的过程

针对性

数据价值的**90%**在数据库，数据安全风险的**90%**在企业内部，重点降低/防范数据访问风险

融合性

新增功能或者产品需要能和现有组件、产品对接，形成一体化、数字化的数据安全治理底座

数据库访问管控是源头：多个数据安全治理场景都涉及数据库管控

西骏数据 WEST HORSE DATA

数据分级分类	数据使用要求	数据集团内部共享	大数据平台安全	第三方数据合作
按照核心数据、重要数据、一般数据进行了划分。不过各单位还需要根据实际情况进行具体落实。	权限管控、数据访问闭环管理、访问行为审计、提取数据审批流程、使用期限管控、密码保护等。	对集团内部数据共享提供集中安全管控；建立数据安全隔离防火墙	建立大数据服务访问授权机制，动态监测与审计大数据访问行为	依据“业务必需、最小权限”原则，采取有效措施对接口设计、开发、服务、运行等进行集中安全保护管理 个人信息防泄露和滥用。
第十八条	第二十八条	第二十九条	第四十九条	第五十三条 第六十一条

访问控制是数据安全的第一道门，很多问题的解决其实是第一道门没有管控住，导致后续问题

数据库访问管控是薄弱环节：最大的短板仍在于数据访问控制

西骏数据 WEST HORSE DATA

结合当前数据安全保护的现状，大部分银保机构数据安全保护基线的关键缺失，还在于数据访问控制部分

信息系统保护

- 将敏感级及以上数据纳入信息系统保护
- 在数据全生命周期内采取有效的访问控制管理措施

数据访问控制

- 制定用户对数据的访问策略，采取有效的用户认证和访问控制技术措施，规范数据操作行为
- 定期对数据操作行为进行审计

数据传输保护

- 参与数据交换的相关机构应当采取有效措施保障信息数据传输和存储的保密性、完整性、准确性、及时性、安全性

数据存储保护

- 防止勒索病毒、木马后门等攻击。个人身份鉴别数据不得明文存储、传输和展示

数据销毁管理

- 终端和移动存储介质内的敏感级及以上数据应当采取技术保护措施，确保受控安全访问
- 存储空间数据应当完全清除并不可恢复

数据访问管控是监测重点：有接近一半的监测内容与访问控制相关

西骏数据 WEST HORSE DATA

实现常态化监测

第六十五条 风险监测

银行保险机构应当对数据安全威胁进行有效监测，实施监督检查，主动评估风险，防止数据篡改、破坏、泄漏、非法利用等安全事件发生。监测内容包括：

（一）**超范围授权或者使用系统特权账号**；

（二）**内部人员异常访问、使用数据**；

（三）对数据集中共享的系统或者平台的网络安全、数据安全威胁；

（四）**敏感级及以上数据在不同区域的异常流动**；

（五）移动存储介质的异常使用；

（六）**外包、第三方合作中的数据处理异常或者数据泄漏、丢失和篡改**；

（七）客户有关数据安全的投诉；

（八）数据泄漏、仿冒欺诈等负面舆情；

（九）其他可能导致数据安全事件发生的情况。

每年开展一次数据安全风险评估

第六十六条 （风险评估与审计）

银行保险机构应当**每年开展一次**数据安全风险评估。审计部门应当每三年至少开展一次数据安全全面审计，发生重大数据安全事件后应当**开展专项审计**

每年1月15日前提供上一年数据安全风险评估报告

第七十四条 （机构报告）

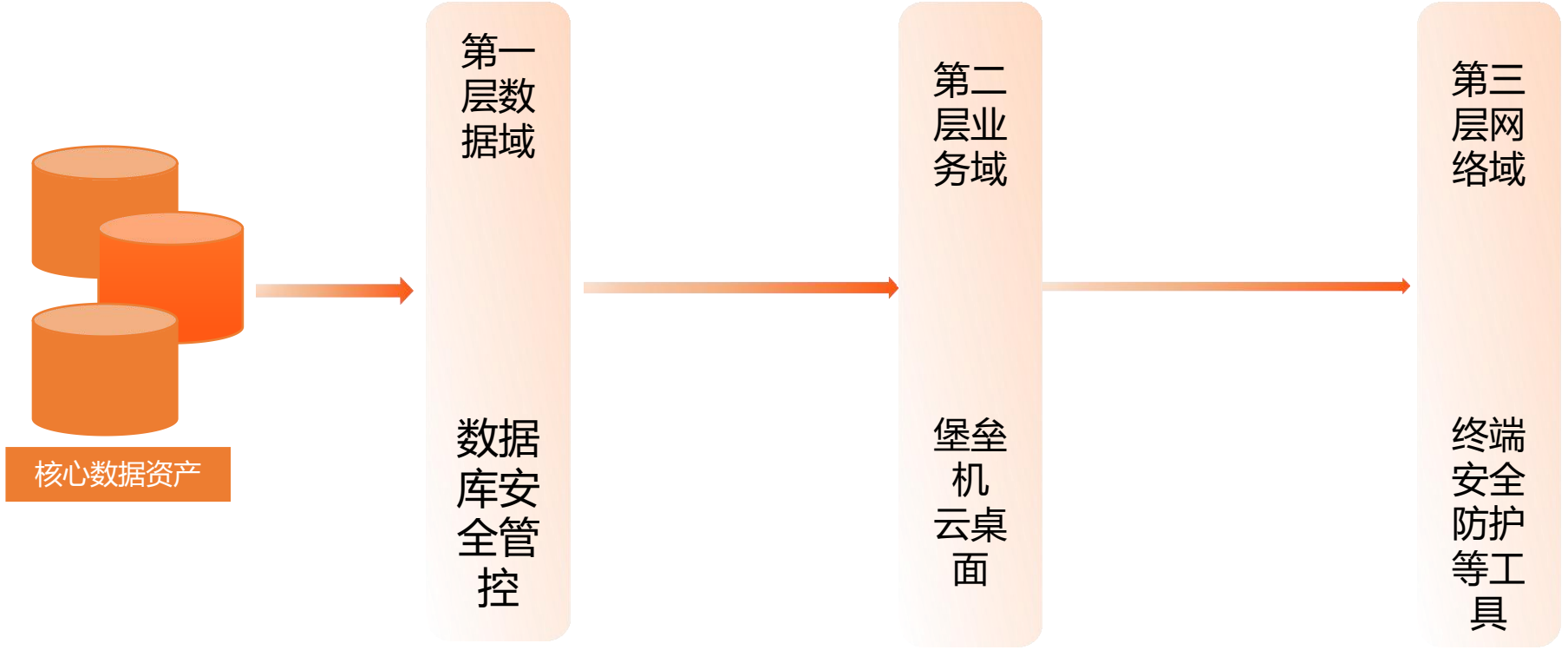
银行保险机构应当于**每年1月15日**前向国家金融监督管理总局或者其派出机构报送上一年度数据安全风险评估报告，报告内容包括**数据安全治理、技术保护、数据安全风险监测及处置措施、数据安全事件及处置情况、委托和共同处理、数据出境、数据安全评估与审查情况...**等

对银保机构及直接责任人等有较为严厉的处罚措施

第七十七条 （监管措施与法律责任）

根据违规情况，...给予纪律处分；银行业金融机构的行为尚不构成犯罪的，对直接负责的董事、高级管理人员和其他直接责任人员给予警告，处五万元以上五十万元以下罚款；取消...终身的任职资格。...依法追究刑事责任

三层数据安全架构，金融机构亟须尽快补齐数据域的安全管控能力



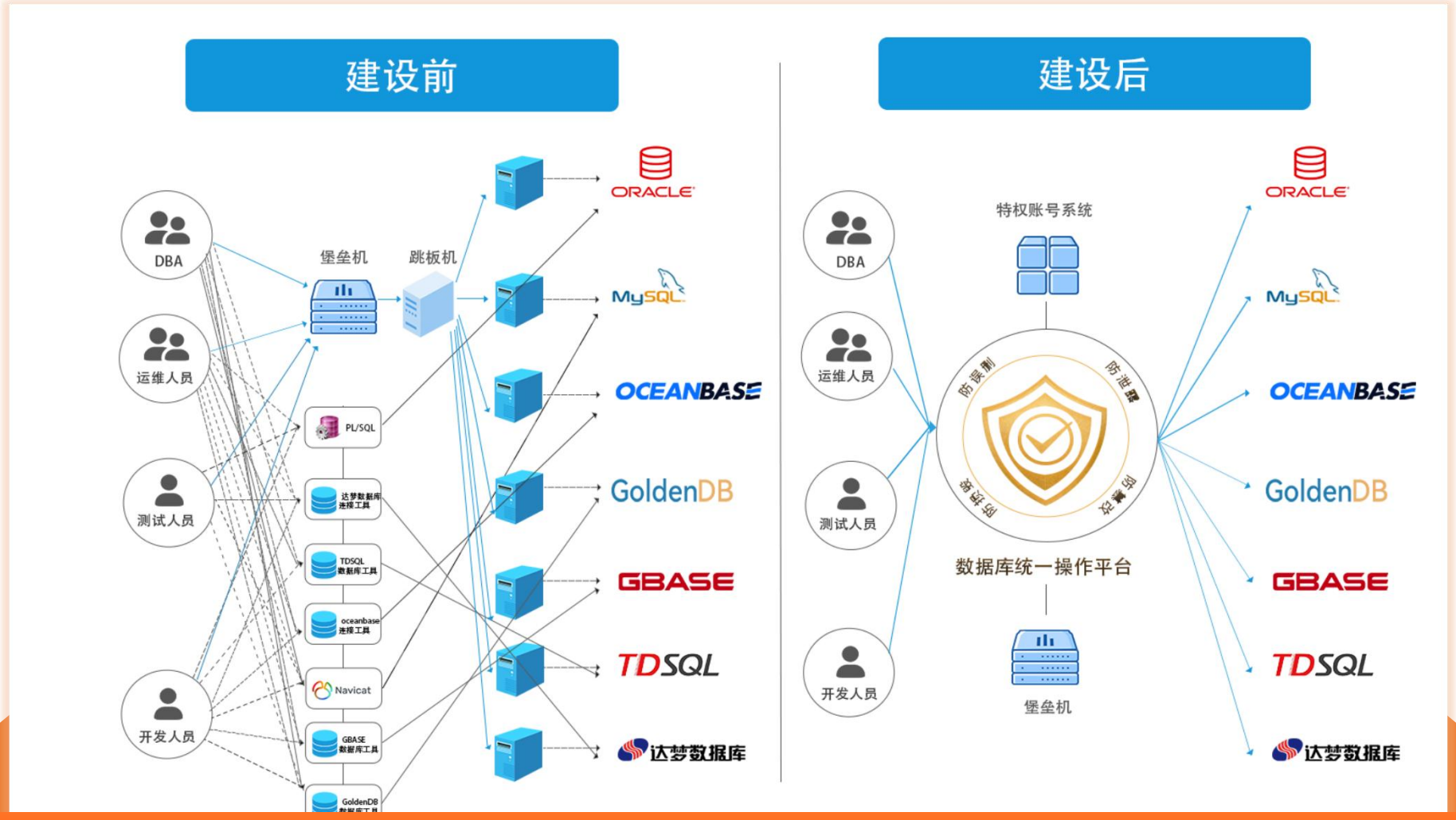
100多家金融机构的实践经验，我们认为存在如下症结：

- **认知错位**：以为数据出不了堡垒机，数据安全就有保障，错把二层当一层。
- **观念偏差**：用网络安全的观念来指导数据安全建设；网络安全靠技术，是被动防御；数据安全靠管理，是主动防御；不能在第三层用设备堆砌来解决第一层的数据泄漏问题。
- **客观限制**：由于信创改造、硬件涨价等客观因素，导致无法快速围绕信创数据库构建新生态

西骏数据
WEST HORSE DATA

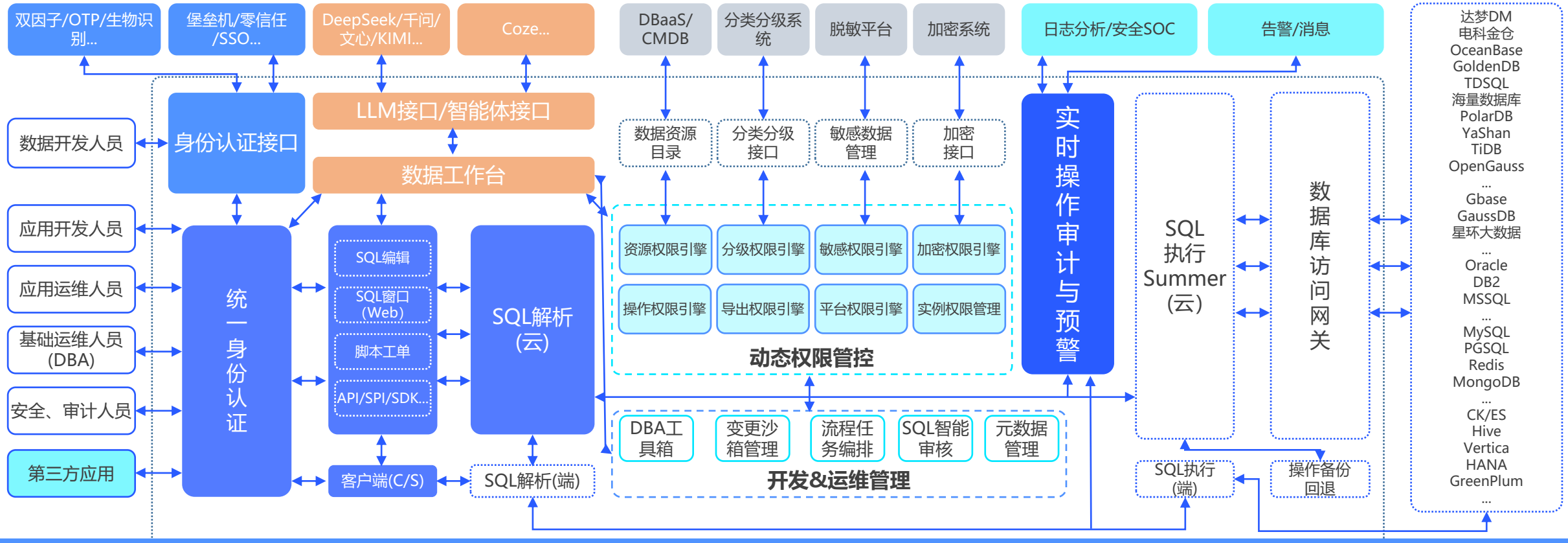
目录

抓手：数据库访问入口的管控是解决大部分问题的抓手



解决数据库访问过程中的难预防、难阻断、难监控、难追踪等实际问题，实现精细化的数据安全管理

西骏数据DataCaptain：看似客户端工具，其实是功能强大的数据库访问管控平台



四 统一

统一入口：统一访问入口消除冒用、私联风险

统一权限：基于岗位和角色细粒度、最小授权

统一操作：多种数据库统一运维、开发操作

统一审计：实现登录、操作、授权、流程、导出等行为全链路审计，无死角

三 安全

操作安全：事前、事中、事后一体化防控

数据安全：分类分级、动态脱敏、水印、导出管控、传输加密

变更安全：SQL预审核、流程变更、异常回环

两 对接

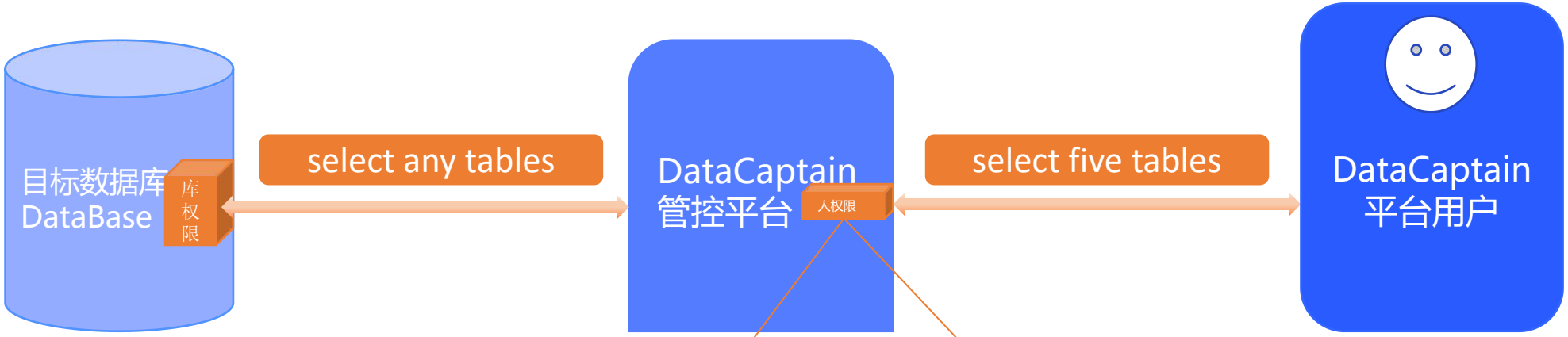
API对接：对外提供统一的数据API、SPI、SDK接入和安全管控、访问限流

大模型对接：支持与大模型、智能体及MCP对接，支持多种AI场景应用

一 替换

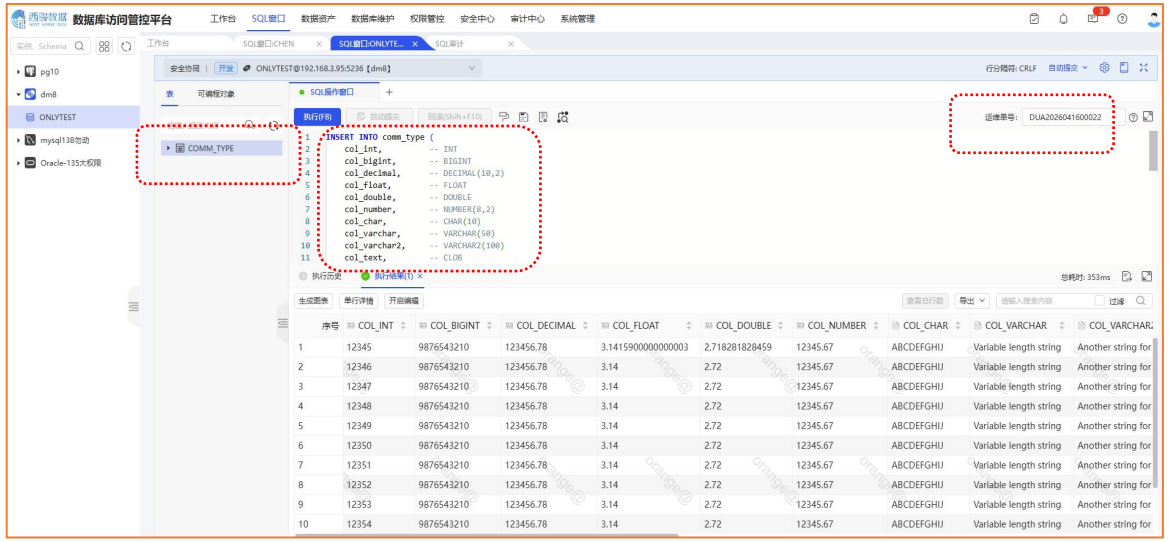
客户端替换：采用B/S SQL窗口整体替换传统 C/S客户端工具，支持40+种各型数据库，实现管理效率提升、信创适配替换率提升

典型场景一：将监管要求的安全原则落地成为每天的操作规范(如“最小必要”)



在DataCaptain平台上实现细粒度权限管控，最小授权

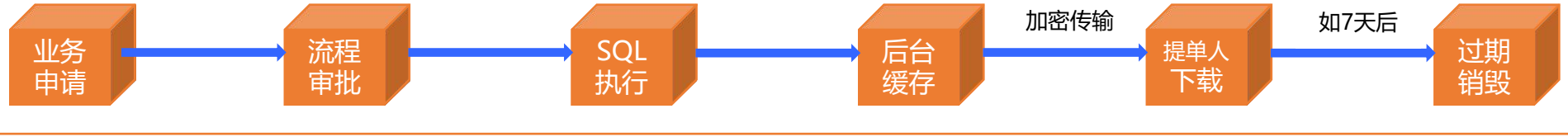
对接流程，通过“一事一议”实现“最小业务必须”授权

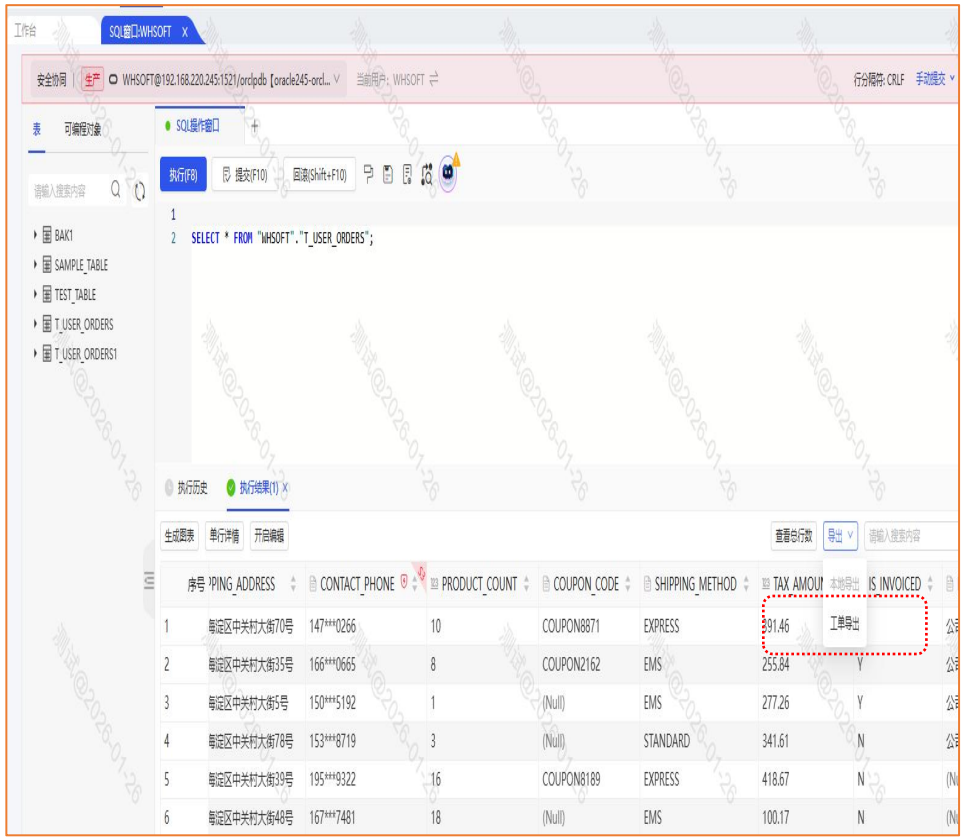


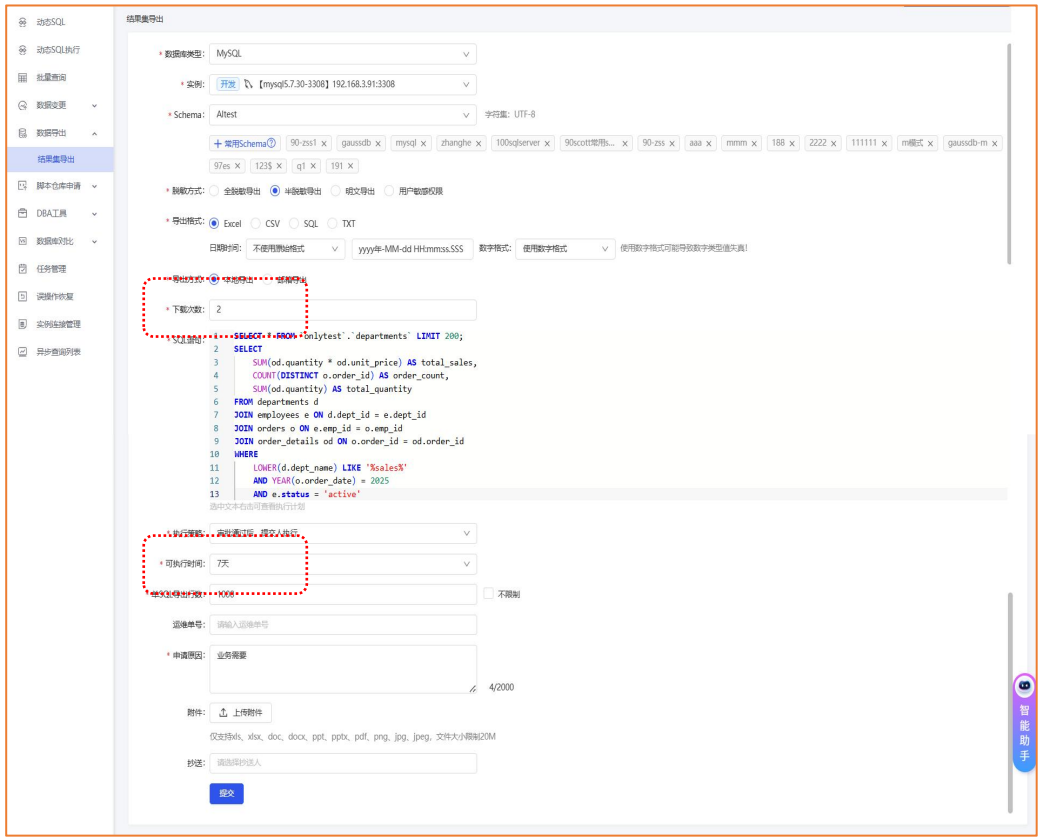
典型场景二：通过体系化模式快速补齐数据安全短板，节省成本与投资

西骏数据 WEST HORSE DATA

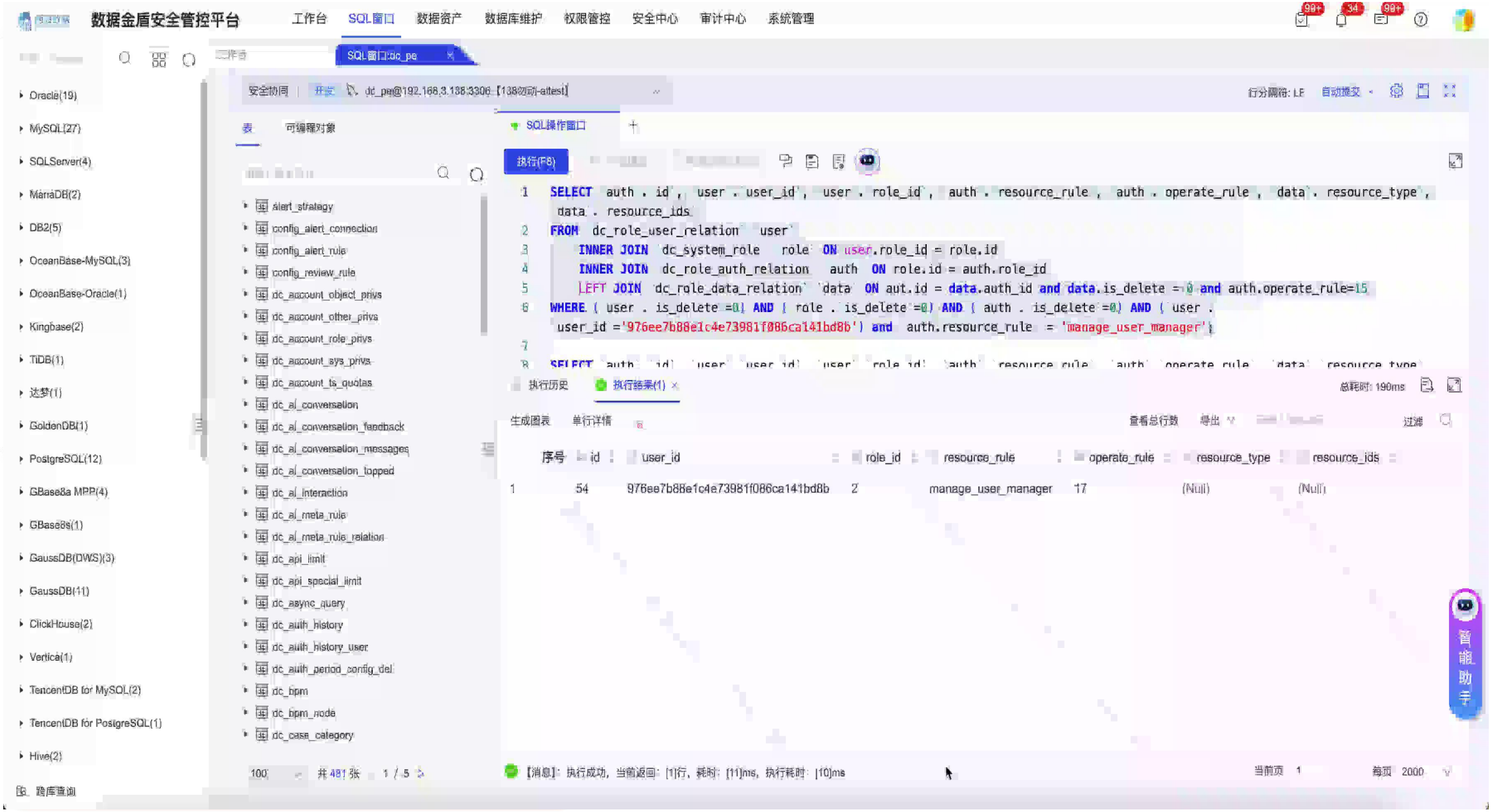
场景举例：数据导出的全过程管理





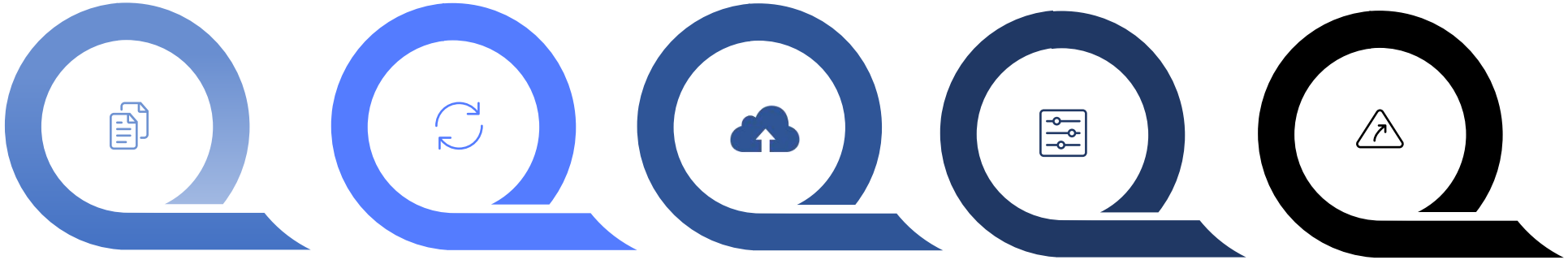


典型场景三：为使用者赋能，实现数据安全与运营效率同步提升，确保持续见效



典型场景N：围绕金监局、人民银行的管理要求，实现十多个数据安全场景

外包人员管理　密码安全管理　数据安全实时监测　大模型数据安全　ECC操作绑定



在线操作复核　僵尸账号回收　敏感数据访问审计　AI辅助审计　AI辅助权限机器人

西骏数据
WEST HORSE DATA

目录

案例|某头部城商行：建设数据库访问控制系统，实现对数据库访问的监控与审计

西骏数据 WEST HORSE DATA

4.79万亿
资产规模

17
支行

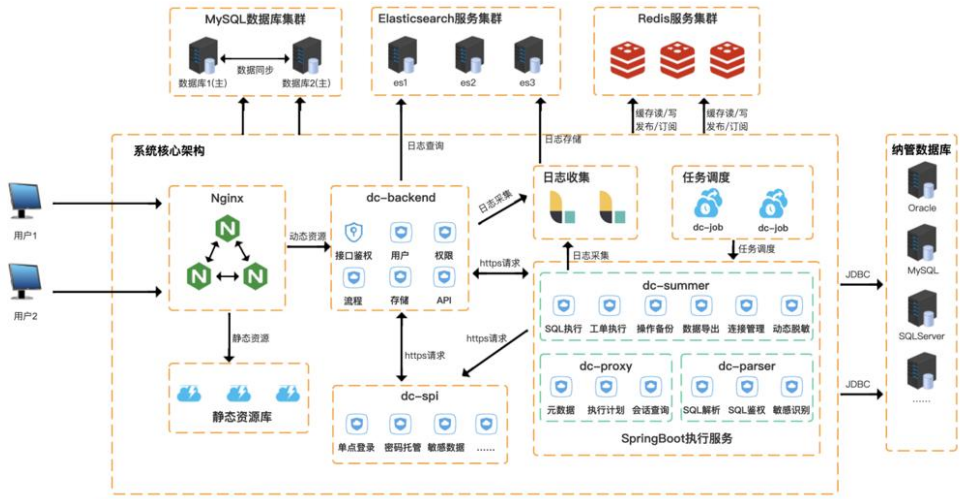
530+
营业网点

8
数据库类型

Oracle、Db2、SQL server、Mysql、Postgresql、达梦、GaussDB、星环hadoop

600+
接入数据库实例数

500+
使用人员



支持所有组件分布式部署，满足高可用及横向扩展需求。

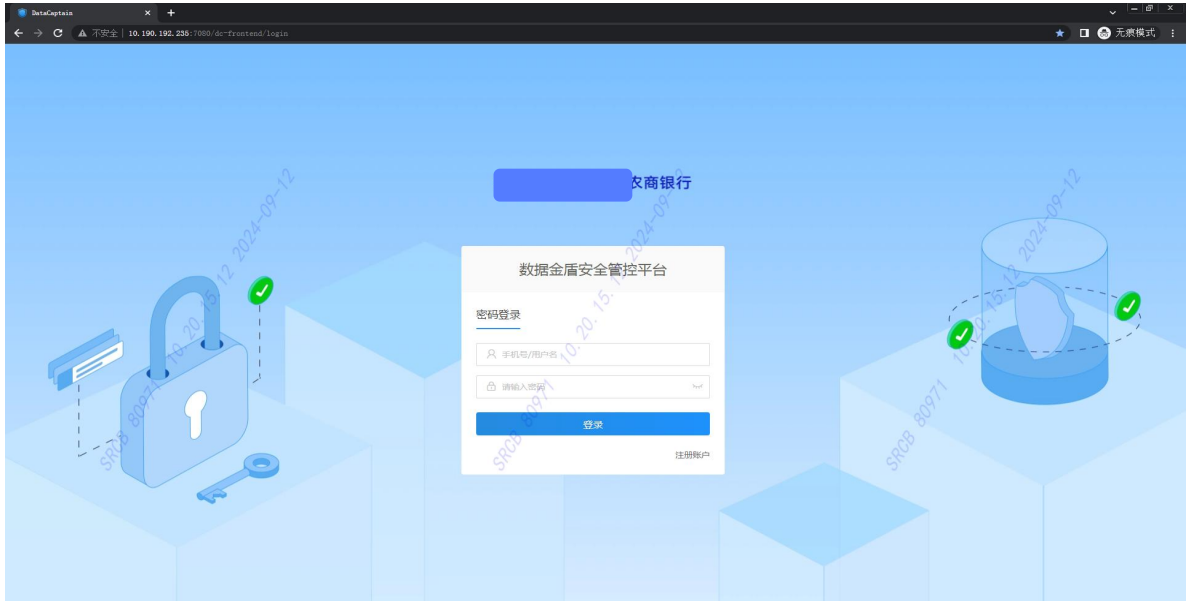
核心需求点

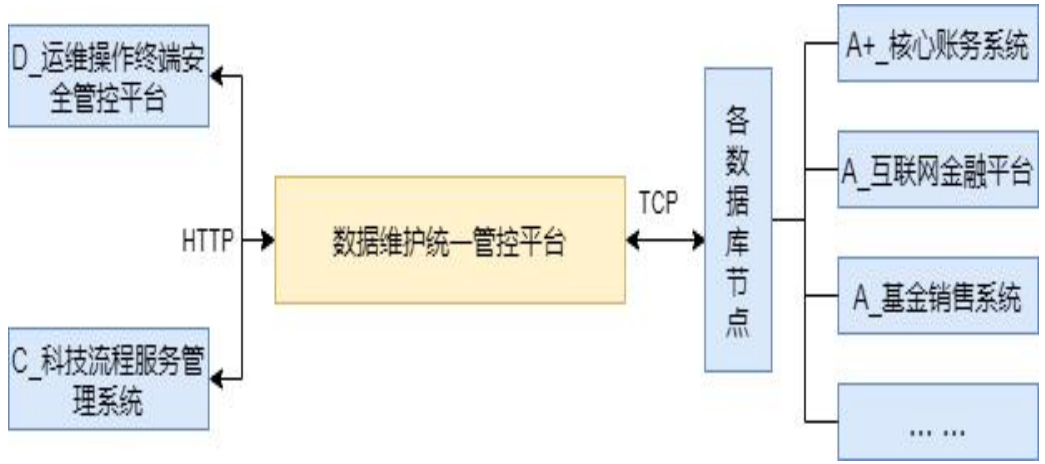
- **运维角色管理**
  -支持数据资源管理、角色权限管理、业务系统管理及员工账号同步
- **数据库操作管控**
  -支持SQL语句级灵活管控，支持高危操作拦截及对象赋权管控
- **数据安全保护**
  -支持水印技术、动态脱敏、自定义脱敏规则、支持与分级分类系统对接，支持行列过滤。
- **数据库操作审计**
  -支持登录登出、SQL操作等的审计，支持SQL操作追溯及授权追溯，支持与工单对接及审计数据输出

实现效果

- **统一访问扎口**，对所有操作进行统一访问管理
- **账号权限重构**，在平台上根据岗位职责重新配置访问权限
- **高危操作拦截**，对高危操作进行拦截，进行细粒度权限管控
- **操作行为审计**，对所有操作行为进行审计，支持场景化审计

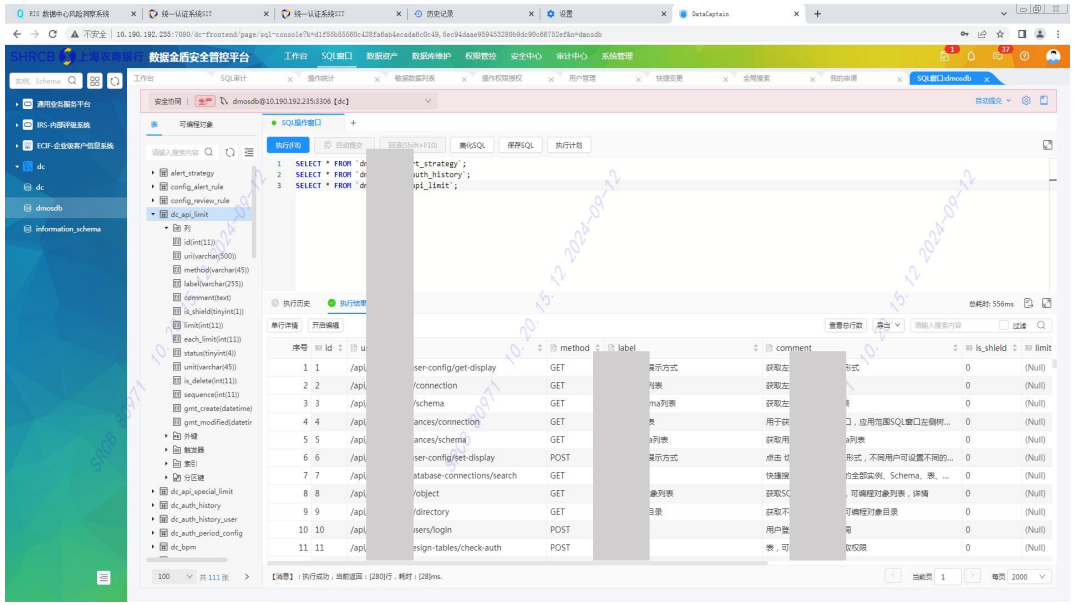
案例|某头部农商行:数据维护统一管控平台项目——有效防范操作风险，大幅提升运维效率





实现效果

- **变更操作流程化**，所有变更操作先审批，再执行，安全提升
- **访问入口固定化**，所有查数、取数操作都通过统一入口执行
- **访问行为全留痕**，所有访问、变更、脚本执行等全部有留痕
- **SQL预审提效率**，启动流程前先调用AI预审脚本，防反复



案例|某省农信联社: 实现数据库统一访问接入及与科管流程对接，提升应用运维安全性

西骏数据 WEST HORSE DATA

1.1万亿
资产规模

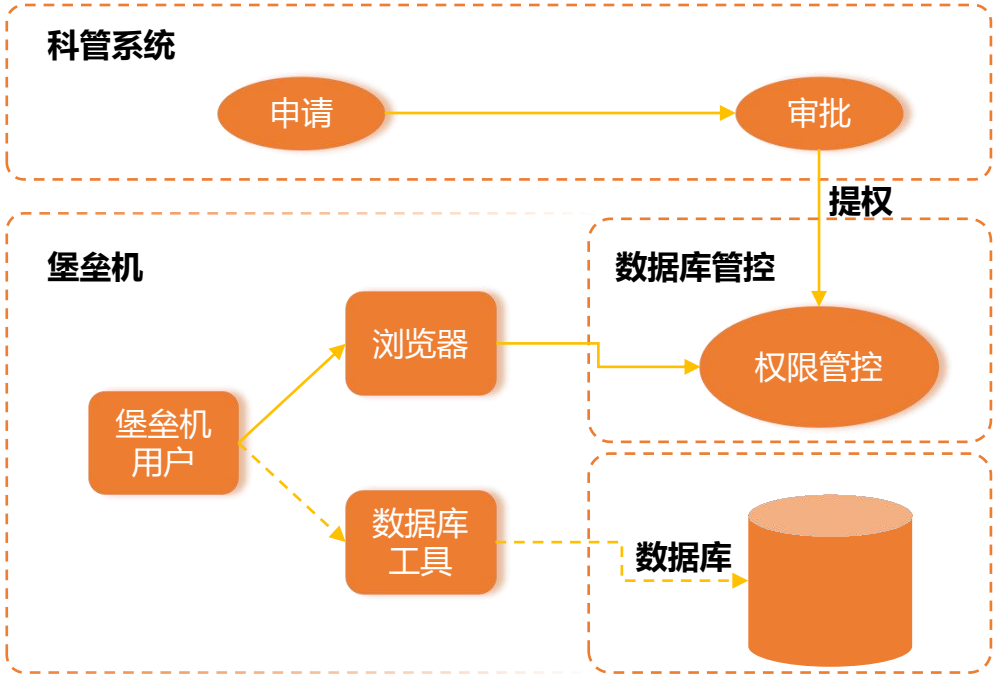
67
下属农商行

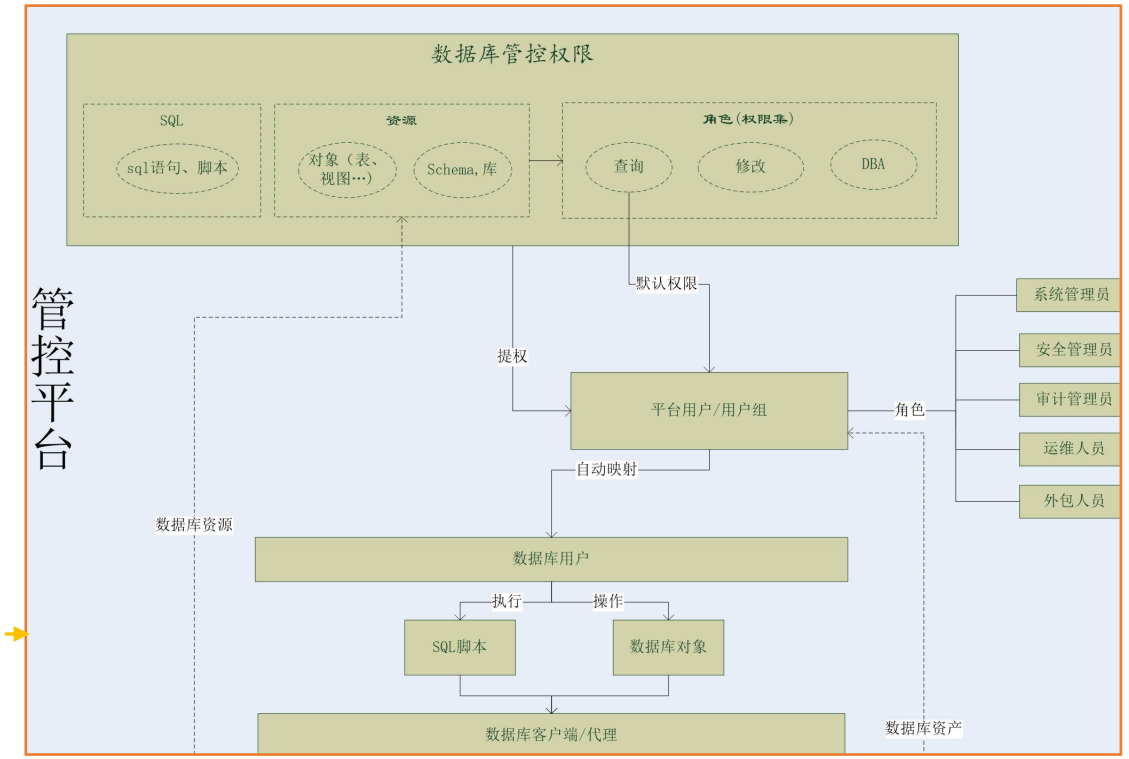
1000+
营业网点

7
数据库类型
Oracle、DB2/OS400、MySQL、Informix、人大金仓、Gbase、SQL Server...

120+
接入数据库实例数

100+
使用人员





实现效果

- **统一访问接入**，可减少7种客户端工具部署
- **动态权限管控**，数据库操作安全性提升90%以上
- **科管流程对接**，所有数据操作行为全部实现闭环管理
- **数据操作审计**，支持对100%数据运维操作及权限操作审计

西骏数据在金融行业数据访问管控领域占据头部地位

西骏数据 WEST HORSE DATA

100+金融客户选用DataCaptain产品及服务

中国平安 PING AN | 中国银行 BANK OF CHINA | 中国人民银行 THE PEOPLE'S BANK OF CHINA | 中国中信金融资产 China CITIC Financial AMC | 招银金租 CMB FINANCIAL LEASING

江苏银行 BANK OF JIANGSU | 上海银行 Bank of Shanghai | 徽商银行 HUISHANG BANK | 齐鲁银行 QILU BANK | 兰州银行 BANK OF LANZHOU

九江银行 BANK OF JIUJIANG | BOTS 唐山银行 | 湖州银行 BANK OF HUZHOU | 赣州银行 BANK OF GANZHOU | MIZUHO 瑞穗银行

河北省农村信用社 RURAL CREDIT COOPERATIVE OF HEBEI | 福建农信 FJRC | 上海农商银行 | SRCB 深圳农商银行 | 顺德农商银行 SHUNDE RURAL COMMERCIAL BANK

华泰保险 Huatai Insurance Group | 申能保险 SHENERGY PROPERTY & CASUALTY INSURANCE | 中英人寿 AVIVA-COFCO | 渤海人寿 BOHAI LIFE | 中意人寿 GENERALI CHINA

国泰海通证券 GUOTAI HAITONG SECURITIES | 广发证券 GF SECURITIES | WESTERN SECURITIES 西部证券 | 山西证券 SHANXI SECURITIES | 中原证券 CENTRAL CHINA SECURITIES

华泰证券 HUATAI SECURITIES | CICC 中金公司 | 国金证券 SINOLINK SECURITIES | 金融街证券 FINANCIAL STREET SECURITIES | 渤海证券 Bohai Securities

易方达 | 博时基金 BOSERA FUNDS | 银华基金 YINHUA FUND | 开源证券 | 东莞证券 DONGGUAN SECURITIES

100+
金融客户

80,000+
纳管数据库实例

50万亿+
守护客户资产价值*

*根据客户公布的资产数据统计

西骏数据：欢迎更多银行圈朋友，加入我们的朋友圈

西骏数据
WEST HORSE DATA

专业、认真、值得信赖

感谢聆听