白皮书

数达安全数据库安全运维系统

V4R0

重庆数达信息安全技术有限公司

2023 年 1 月

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更新，恕不另行通知。

数达安全在编写本文档的时候已尽最大努力保证其内容准确可靠，但数达安全不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

目录

前 言

近年来，以 5G 技术、数字化、智能化为主要特征的新工业革命蓬勃兴起，推动我国产业结构深刻变革。数据作为创新发展的基石，已成为国家基础性战略资源和驱动行业转型发展的重要引擎。随着全球数据呈现爆发增长和海量集聚，为人类带来无限发展机遇的同时也带来了新的安全风险和挑战，严重影响国家安全、经济发展、社会稳定和个人权益。

在此背景下，数据安全的重要性被提到了前所未有的高度。我国积极加强数据安全管理布局，《网络安全法》、《数据安全法》、《个人信息保护法》与《关键信息基础设施安全保护条例》的相继出台，全面构筑了中国数据安全领域的基础法律框架。继上述四个国家级法律之后，各行业陆续出台了本行业配套的法规、标准、指南。为我国企业落实数据活动主体义务与责任提供了法律依据。

为解决数据安全领域中数据运维场景中的突出问题，数达安全在国家政策、法律法规、行业监管等基础上，针对当前组织普遍面临的数据安全风险现状、治理困境等，研发了数据库安全运维系统，以完善数据安全管控体系，为关键信息基础设施保驾护航。

1 概述/背景

1.1 数据资源成全球博弈主赛道

在数字经济时代，信息和知识普遍以数字化的形式产生、保存、传播和利用，通过对数据资源的探索利用，可以推动更多新兴技术、新兴模式、新兴产业诞生和发展，推动传统产业转型升级。数据也因此成为新的生产要素和国家基础性的战略资源。

2022 年 4 月 10 日发布的《中共中央国务院关于加快建设全国统一大市场的意见》中提出，加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。

数据网络空间成为了国家间博弈的新角力场，国与国竞争日趋多元化和白热化，正在重塑全球政治经济格局。在数据技术的加持下，政治博弈、经济角力、安全渗透都已是不容忽视的新的战争形式。

1.2 全球重大数据泄露事件频发

大数据、互联网、5G 的迅速发展，为人类带来无限发展机遇的同时也催生了大量的数据泄露事件，严重影响国家安全、经济发展、社会稳定和个人权益。数据泄漏事件几乎覆盖国内外所有行业，全球各地深受数据泄露事件困扰的同时也造成了重大损失。

如：国外安全团队 Cyble 在一次日常安全监控中发现了多个帖子正在出售个人数据，与中国公民有关的记录总数超过 2 亿；被媒体称为“史上最大规模的数据窃取案”涉及 30 亿条用户数据，波及范围包括 BAT 在内的全国 96 家互联网公司；乌克兰媒体《乌克兰真理报》3 月 1 日在其网站发布了在乌克兰作战的 12 万俄罗斯军人的个人信息，详细记录了 12 万俄军的名字、注册编号、服役地点、职务等信息，页数多达 6616 页；《纽约时报》从 1200 多万人的电话记录中获得了超过 500 亿个位置的数据集，研究人员仅用了几分钟就对位置数据完成了反匿名处理，并获得特朗普一天的行踪记录。

2021 年 7 月 2 日，国家网信办发布公告称，为防范国家数据安全风险，维护国家安全，保障公共利益，网络安全审查办公室按照《网络安全审查办法》，对“滴滴 出行”实施网络安全审查。7 月 4 日晚，国家网信办发布通报称，根据举报，经检测核实，“滴滴出行”App 存在严重违法违规收集使用个人信息问题，通知应用商店下架“滴滴出行”App。2022 年 7 月，滴滴因此被罚款 80 亿元。

1.3 数据安全面临的主要风险

数据全生命周期涵盖采集、传输、存储、使用、共享、销毁等多个阶段，其全生命周期都存在数据安全风险隐患的问题，针对数据全生命周期的技术防护是企业开展数据安全的核心和难点工作。

数据采集阶段：存在管理制度不规范、采集策略不合理、缺乏采集监控等，导致未授权采集、过度采集、数据倒流等风险。

数据传输阶段：存在敏感数据未加密传输、缺乏数据流动监测、缺乏溯源手

段等问题，导致数据泄露和非法篡改等风险。

数据存储阶段：存在敏感数据明文存储、数据备份与恢复能力欠缺等问题，导致数据泄露、篡改破坏、丢失、无法复原的风险。

数据使用阶段：存在未建立数据访问控制机制和数据风险检测机制等问题，导致数据使用不当或被恶意盗取、篡改破坏的风险。

数据共享阶段：存在数据共享接口安全管控能力不足、数据脱敏能力缺失、数据溯源能力缺失等问题，导致数据未授权提供、超范围公开、再共享等风险。

数据销毁阶段：存在销毁技术手段不完善、缺乏销毁管理措施等问题，导致残余数据利用和残余介质利用的风险。

共性风险：除上述各个阶段之外，组织因缺乏数据梳理和数据分类分级能力造成敏感数据的失管和泄露、缺乏整体数据安全态势感知和数据安全监测评估能力导致企业无法进行整体的数据安全监测预警和风险评估。同时，因误操作、权限滥用、恶意窃取以及内外部联合攻击等因素造成的数据安全事件等风险广泛存在数据的全生命周期各个阶段中，属于**共性风险。**

1.4 相关法律法规

《网络安全法》对数据安全保护提出了新规定和新要求，特别是其中涉及的个人信息保护、跨境数据传输评估等方面，明确提出了网络运营者（包括关键信息基础设施的运营者）的安全保护义务之一是防止网络数据泄露或者被窃取、篡改。

《数据安全法》中规定开展数据处理活动应当建立健全全流程数据安全管理制度、组织开展数据安全培训、采取相应的技术措施、加强风险监测等。发生数据安全事件时，应当立即采取补救措施并按照规定及时告知用户并向有关主管部门报告。

《个人信息保护法》中规定，个人信息处理者应履行必要的数据安全保障义务以及其他基本法定义务。如发生个人信息泄露、篡改、丢失的，数据处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。

《网络安全等级保护条例》（等保 2.0）的相关规定中，数据安全是核心内容之一。在原有等保 1.0 对数据安全的要求基本不变的情况下，根据新计算环境和业务场景对数据安全保护能力做出了更贴合实际情况的明确要求。数据安全的测评指标主要来自于通用要求的“安全计算环境”部分，其中对数据访问的审计、访问控制、加密都有要求明确要求，并且在附录部分大数据应用场景说明中对脱敏和溯源也进行了相关规定。

《关键信息基础设施安全保护条例》要求运营者在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

《民法典》人格权编第 1038 条规定，信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供个人信息，但是经过加工无法识别特定个人且不能复原的除外。

1.5 数据库安全运维需求

1.5.1 运维场景敏感信息泄露事件频发

当敏感数据直接用于第三方公司进行开发、测试、培训、运维等环节时，必将导致敏感信息泄露，大量敏感信息流入黑色产业链。将敏感数据外发的企业将面临难以估量的经济损失和问责风险。

盘点已发生的敏感信息泄露，有大量第三方人员作案的事件：

- 2020 年贵州某银行运维主管修改数据，牟利 596 万元；
- 2019 年前后，国内银行接连爆出数据泄露事件，上海、浦发、兴业等 6 家银保机构“数据泄露门”风波未平，北京银行、建设银行紧随其后，涉案人有临时工也有行长；
- 医院系统普发运维人员非法统方，与医药代表勾结，通过泄漏处方信息；
- 外包公司泄露某游戏公司 300 多张原画加音频，导致版本上线时间推迟，造成一点六亿损失；
- 2018 年 12 月 24 日，郑大一附院 HIS 系统突发故障，造成郑大一附院系统全部无法工作，大量患者积压在门诊无法就诊，医院测算损失超过 800 万元。导致该事件的原因是第三方运维人员夏某某，在未经授权或许可的情况下，私自编写了“数据库性能观测程序”和锁表语句，并利用私自记录的账号密码将该程序私自连接郑大一附院“HIS 数据库”，导致该锁表语句在“HIS 数据库”运行。
- 2012 年 10 月，上海市公安局经侦总队侦破两起特大个人信息外泄案，抓获犯罪嫌疑人 50 余名，查获各类公民个人信息近 2 亿条。其中，泄露数十万婴儿信息的竟然是上海市卫生局数据库的第三方维护人员。据介绍，犯罪嫌疑人张某是帮助卫生局维护数据库的某公司技术部经理，他每个月都从家里访问卫生局新生儿数据库，从中下载私密信息。

1.5.2 针对运维场景的数据安全合规要求

《网络安全法》第二十一条规定：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。同时，第四十二条规定：网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

《网络安全等级保护条例》（等保 2.0）中对个人信息保护以及脱敏也做出了明确要求，在**安全计算环境和大数据应用场景中**要求：应禁止未授权访问和非法使用用户个人信息；大数据平台应提供脱敏和去标识化的工具或服务组件技术。

《个人信息保护法》第五十一条规定：个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

（一）制定内部管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训。

《信息安全技术个人信息安全规范》（由信安标委 2020 年 3 月发布）中也

明确建议，个人信息要求去标识化管理。

1.5.3 数据运维业务需求

随着人工智能、5G、物联网、大数据等技术的广泛应用，企事业单位或机构数据运营者的运维环境变得越来越复杂，尤其是数据的安全运维形势不容乐观。特别是数据运营者由于自身运维人员较少，大部分运维工作外包给了第三方代维公司或者数据库、应用系统原厂商，就会出现运维风险不透明、不可控等问题。

数据运维场景中的安全风险与业务痛点如下：

- 数据库账号多人共享，无法确认真实身份。多个运维人员同时使用同一数据库账号访问数据，无法准确定位具体是谁在执行运维操作；
- 密码泄露，容易导致黑客攻击。将运维账号密码告知第三方运维人员，容易导致账号秘密的传播，泄露的几率高，容易遭到黑客攻击；
- 敏感数据直接暴露，存在巨大风险。对运维查询到的数据未脱敏，会将高敏感级别的数据向低敏感级别的人员展示，从而导致数据泄露，风险极大；
- 操作授权粒度过大，容易造成越权访问。运维授权粒度大，不能精细到具体的操作语句和数量级授权，从而无法按照最小权限原则分配权限，导致运维人员有机会恶意盗取敏感信息；
- 脚本无审核机制，易出事故。执行脚本时没有经过审核和预执行，容易出现 SQL 纰漏或误操作，造成严重事故。
- 越来越多的业务系统和数据库实体，有大量的账户和密码信息需要管理，同时不同的数据库的访问客户端又是形形色色，数据运维管理的效率亟待提升。

为应对上述风险状况，亟需针对运维场景的数据安全系统，以减少运维场景的数据安全事件和提升工作效率。具体的，需要如下的功能和特性：

1）针对数据运维的账号和权限管理

- 需要对运维人员账号进行统一管理，防止账号共用、滥用；
- 需要对高权限账号进行细粒度的权限控制，避免越权访问；
- 需要对第三方及运维人员进行访问权限控制，防止危险访问行为。

2）针对运维的交互式动态脱敏

- 需要对敏感数据进行动态脱敏，减少敏感数据泄露的可能。

3）针对运维的脚本管理

- 对脚本的历史、权限进行管理；
- 有脚本审核机制，保证高危操作和敏感操作必须经过批准才可执行。

4）统一的数据运维操作台

- 具有强大的兼容性，支持各种各样的数据库；
- 提供专业易用且功能丰富的操作界面

2 产品概述

数达安全数据库安全运维系统（简称 DS-DSOM），是一款专业的数据库安全运维产品，由数达安全公司**独立**开发，并拥有**完整的自主知识产权**。通过独立和

统一的身份认证、权限控制、脚本审核和管理、交互式脱敏、以及数据运维操作台，构建安全的数据运维环境。

2.1.1 技术目标

数达安全公司基于多年数据安全产品研发经验，凭借自有研发力量，针对现阶段国内数据保护市场的需求特征，在原有数据库动态脱敏产品的基础上推出了数达安全数据库安全运维系统 V4.0。

DS-DSOM 整体技术目标为提升运营场景数据安全管控能力，由以下三个具体技术目标实现：

1）提升数据运维权限管控能力

对各类运维人员提供统一的权限管理，细化权限授权粒度，从而实现最小化授权。

2）为运维场景提供交互式脱敏能力

通过 SQL 改写技术，对敏感数据的运维提供必要的交互式实时脱敏功能，防止敏感信息向运维人员直接暴露。

3）提升运维脚本管理能力

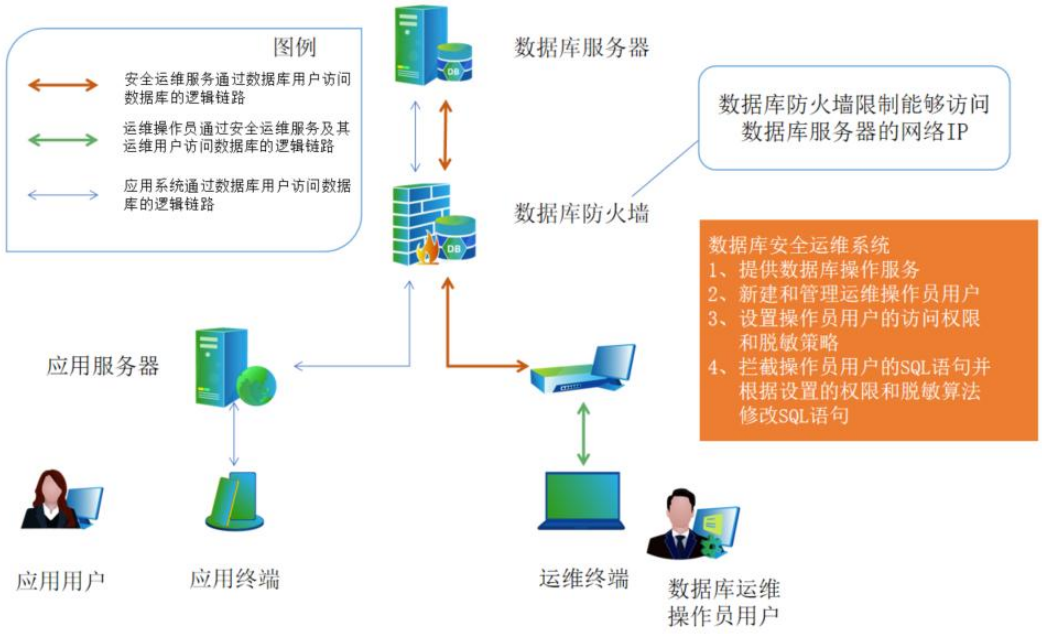
对运营场景提供脚本管理能力，可以方便的管理历史脚本，并对脚本提供审核机制，减少误操作和恶意操作的可能。

4）统一的数据运维操作台

能够给运维人员提供专业易用且功能丰富的运维操作台界面，同时具有强大的兼容性，能够支持各种各样的数据库。

2.1.2 产品原理

DS-DSOM 的原理如下图所示。



DS-DSOM 以逻辑串联的方式部署于运维终端和数据库服务器中间，所有的运维操作都必须经过 DS-DSOM 过滤或改写后才发送给数据库。

该系统的安全管理员可以通过预置统一的数据库用户来连接目标数据库，并

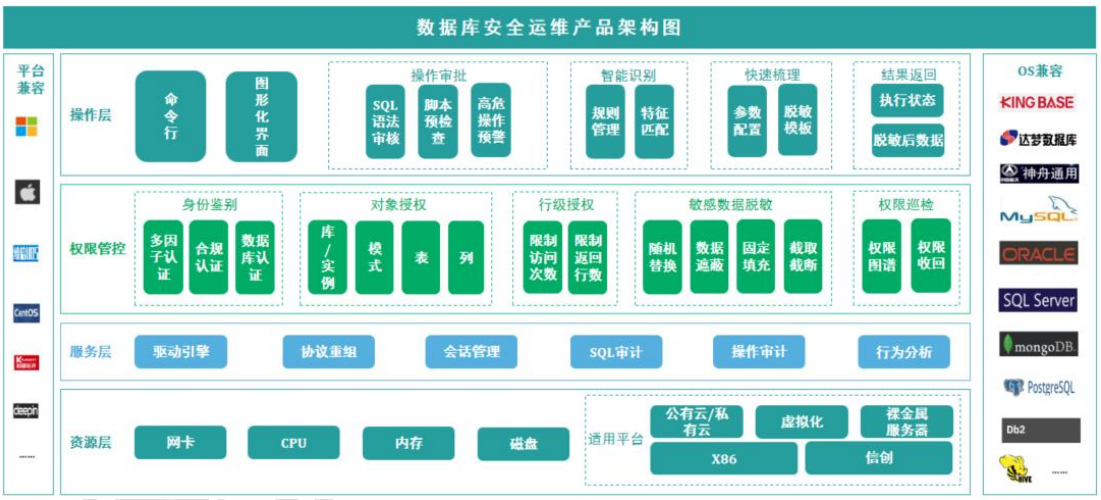
且在系统中新建和管理数据运维操作员用户，同时分别设置这些数据库操作员对目标数据库的访问权限和脱敏算法。连接数据库的数据库用户权限是这些运维操作员用户的上限，即在系统中新建与管理的数据库操作员用户权限不会超过系统连接数据库的数据库用户权限范围。

当数据运维操作员通过系统提供的操作台页面来操作数据库时，系统会拦截该操作员发出的 SQL 语句指令，并且判断该操作员的访问权限，然后根据预置的脱敏算法修改 SQL 语句，从而使得返回的数据满足系统设置的针对该操作员用户的访问权限和脱敏算法要求。

该系统基于 B/S（浏览器-服务端）架构设计，可提供基于网络浏览器页面的数据库操作服务，无需在运维终端安装应用程序，从而实现统一的运维机制。

2.1.3 产品架构

DS-DSOM 从下到上分为资源层、服务层、权限管控层和操作层。采用 B/S 架构实现跨平台部署，面向各个数据库整合了统一的业务操作流程，拥有针对库级、表级、列级多维度的权限访问控制，同时规范了运维人员对隐私数据的运维流程。



资源层：为系统提供适用的硬件资源和系统软件资源；

服务层：为安全运维的提供引擎管理、协议重组、SQL 审计等底层服务；

权限管控层：为安全运维提供身份鉴别、对象授权、数量授权、脱敏等细粒度权限管理功能；

操作层：向运维人员提供主要的交互界面，包括运维命令操作台、权限管理界面、数据梳理识别界面等；

平台兼容：实现不限制运维人员使用的操作系统类型，且无需安装应用程序；

数据库兼容：支持主流的关系型数据库、国产数据库、大数据平台等。

3 产品功能

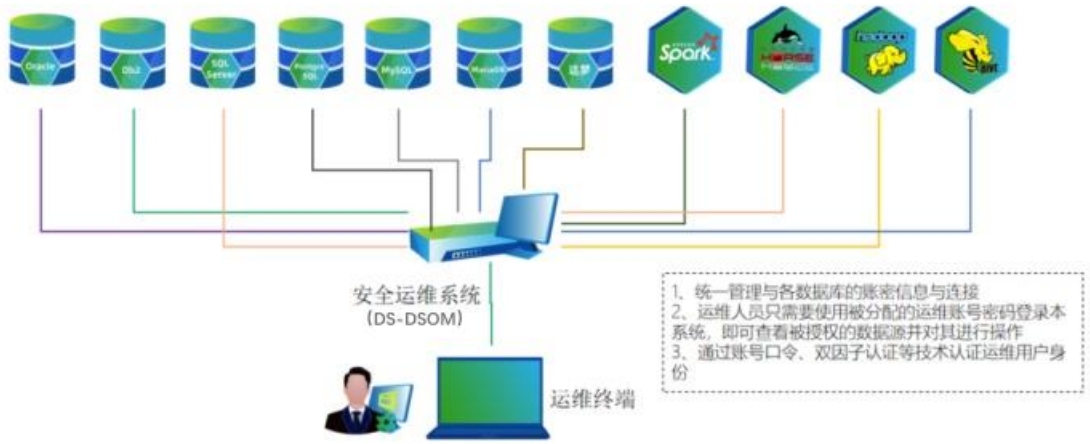
DS-DSOM 的功能主要包括：敏感数据发现、统一身份认证、统一运维操作台、权限管控、动态脱敏、操作审批、多租户管理和行为审计。

3.1 敏感数据发现

敏感发现可以自动扫描数据源，依据内置的 100+种敏感数据识别算法，对数据源的内部数据进行自动随机抽样，识别解析，发现敏感数据，并对敏感数据进行分类标记。敏感发现可以为数据运维策略设置提供有意义的参考，简化策略设置的过程。

3.2 统一身份认证

可以通过账号口令、双因子认证等技术认证运维用户身份，再由 DS-DSOM 管理各个数据库的连接信息，并连接到各个数据库。当运维用户需要登录数据库进行运维操作时，无需记住多个数据库复杂的各类密码，只需要使用被分配的运维账号密码登录 DS-DSOM，即可查看被授权的数据源并对其进行运维操作。使统一身份认证完全替代分散的数据库账号密码，可以简化数据库登录账号管理，同时避免账号共享带来的各种未知风险。



3.3 统一运维操作台

DS-DSOM 针对各种各样不同类型的数据库开发了统一的操作台页面，参考数据运维人员常用的主流数据库客户端功能设计，提供了以下功能：

1）基于树形结构的数据库、模式、表和视图的图形化操作方式，可以通过该图形化的方式对已授权的表和视图进行增删改查、设置主外键、查看索引和触发器等操作。

2）具有执行、停止、提交、回滚、清除和美化等完善功能的 SQL 编辑器，利用该编辑器通过 SQL 语句可以对已授权的表和视图进行增删改查、设置主外键、查看索引和触发器等操作。

3.4 运维权限管控

DS-DSOM 从数据对象、数据访问量等维度提供独立于数据库自身的授权管理机制，可以形成更加细粒度的访问控制，更有利于实现最小权限控制。

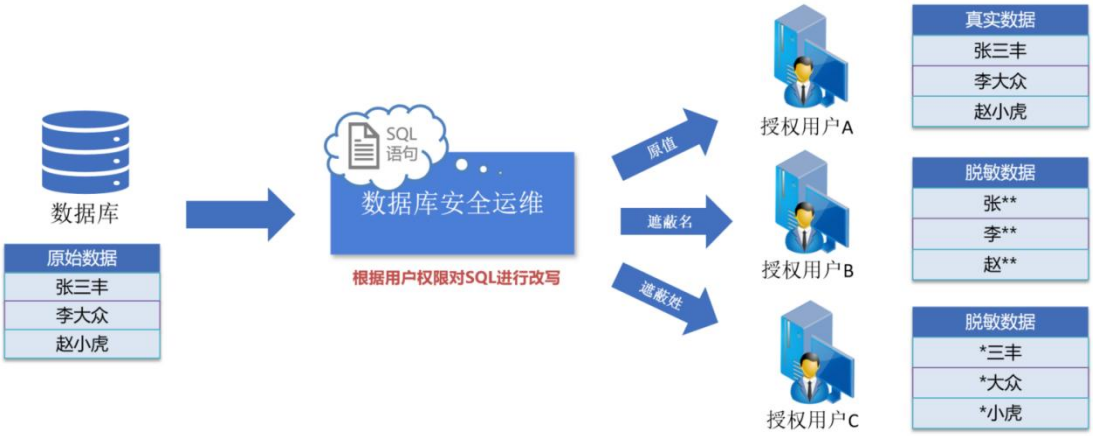
提供对象级的权限控制，粒度主要包括：库/实例、模式、表、列等。针对敏感数据对象的访问，需要经过安全管理员的授权才能执行。如果运维用户不具备访问权限，将明确阻断拒绝，防止人为误操作。

访问方式授权：DML（增、删、改、查）、DDL（Create/Alter/Drop）等。

提供行级授权，主要包括访问频次控制、查询行数控制、更新行数控制、删除行数控制、脱敏模板控制等，全方位保障访问控制体系的安全性。

3.5 交互式脱敏

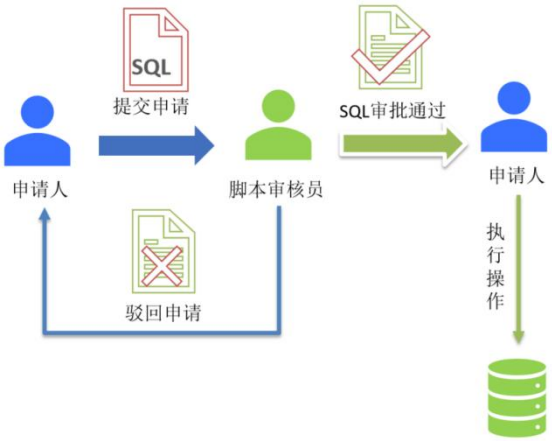
DS-DSOM 基于 SQL 改写技术，将包含敏感字段的查询语句进行改写，对敏感字段采用脱敏函数进行替换，让数据库自行返回不包含敏感数据的改写后的结果，保证对于各类运维语句交互式的进行动态脱敏。确保运维人员以及第三方代维人员严格根据其工作所需和安全等级访问敏感数据，防止敏感数据从从高敏感级别向低敏感级别流动。



DS-DSOM 支持的脱敏规则主要有遮蔽、按位遮蔽、随机字符串、禁止访问、固定值和字符串截取/截断等。

3.6 操作审批

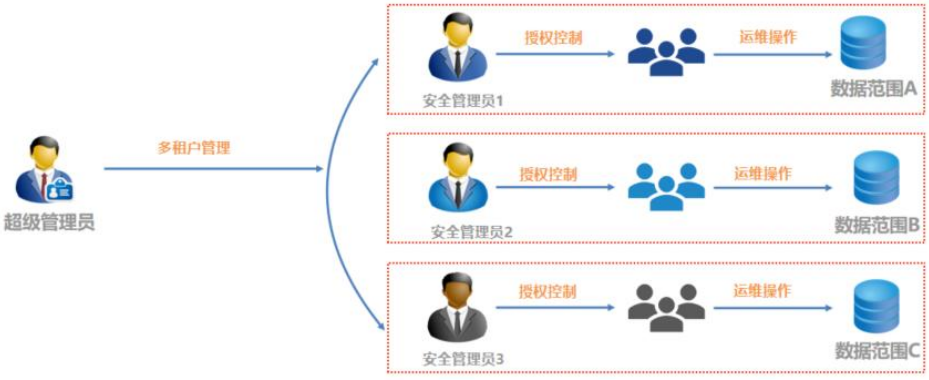
DS-DSOM 提供运维审批功能，支持文本模式和 SQL 脚本模式两种模式的申请。针对提交的脚本能够进行预检查，包括语法、编码、环境、高危语句等自动化校验并标识，协助审核员进行审核。审核通过后，系统授予权限，运维用户才可以执行相关脚本。



DS-DSOM 能够阻断恶意、高风险操作，保障运维命令的安全执行。

3.7 多租户

租户是指云环境下的独立租户，或大型组织的部门，系统和数据相对独立。DS-DSOM 的多租户模式能够满足这种场景下的安全运维需求，而无需为每个租户部署单独的产品。多租户模式为每个租户提供独立的管理空间，实现多租户统一管理，每个租户保证运维合规，租户间数据隔离，从而使运维管理界限清晰。

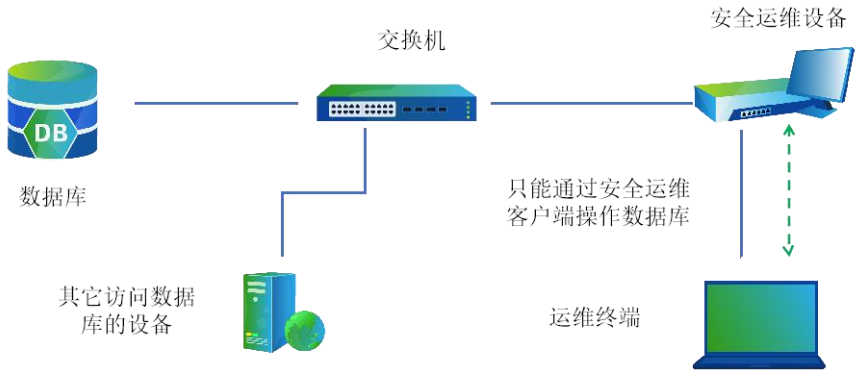


3.8 行为审计

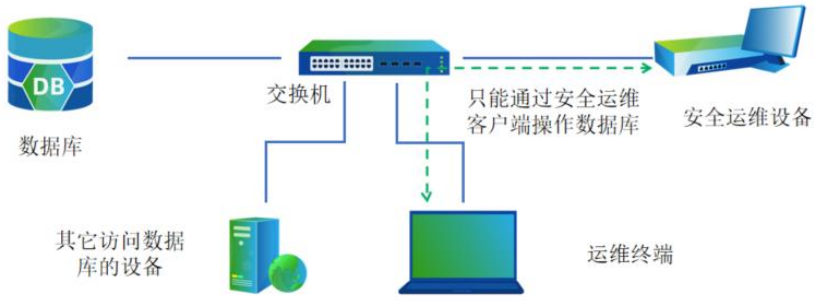
DS-DSOM 能够对所有用户的登录日志、系统操作日志和运维操作自动留痕并进行智能审计。包括：登录退出、权限授予、SQL 操作、脚本执行等。日志内容包括：运维用户、操作 IP、授权项、动作、操作类型、操作时间、原始 SQL、语句执行时间、执行结果等。并可根据审计内容生成报表。也可以将审计日志发送给其他审计系统进行统一分析和展示。

4 产品部署方式

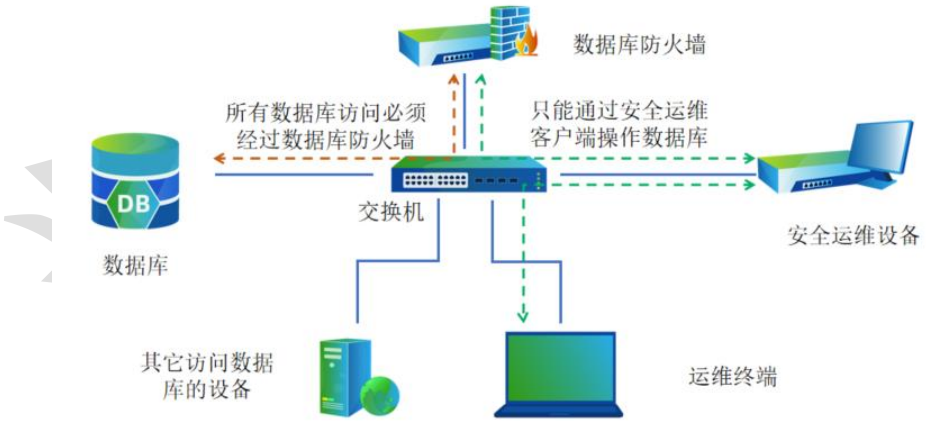
DS-DSOM 可以采用物理串联的方式部署于数据库访问运维侧与数据库服务器之间，所有数据运维的访问均需要经过 DS-DSOM。



也可以采用逻辑串联的方式接入。安全运维系统单臂接入网络，以代理的方式接收所有的运维流量，分析和处理后转发到数据库。



也可以与数据库防火墙联合部署，进一步提升运维场景的安全防护能力。



数据库设置为只接收防火墙的访问，数据库防火墙成为数据库的唯一入口。通过防火墙设置，所有的运维操作必行经过安全运维系统，通过防火墙提供额外的攻击保护功能。

5 特性和优势

系统具有高安全性、高易用性以及强大的兼容性等特性和优势。

5.1 高安全性

通过独立的系列安全能力，打造安全的运维环境：

- 通过统一身份认证，运维人员访问数据库时，不再需要数据库账号密码，转而使用运维用户在 DS-DSOM 上的账号登录，从而防止密码泄露以及轻松实现账号的锁定；
- 通过细粒度的运维权限控制，对运维用户操作进行数据对象、表、列、访问频次、行数等多维度控制，保证访问者依据其工作所需和安全等级，最小权限的访问敏感数据；
- 通过敏感数据动态脱敏保证针对不同授权的用户可返回不同的数据，包括真实数据、部分遮蔽、全部遮蔽以及其他脱敏算法得到的结果，实现敏感数据的交互式动态遮蔽，防止运维人员泄露敏感数据；
- 通过运维操作审批，针对提交的 SQL 与脚本能够进行预执行和预检查，必须经过审核员审核通过后，才可以上线执行，避免 SQL 纰漏或者操作失误，造成事故；
- 精确的运维行为审计，记录详细的运维行为信息，快速定位操作人员、操作对象、操作类型、操作时间等内容，实现事后溯源。

5.2 高易用性

- 提供统一的账号管理方式，能够批量的管理各类运维账号；
- 采用 B/S 架构，客户端无需安装任何程序，直接使用网页操作数据库，避免安装各种程序，避免记忆多个数据库的众多密码；
- 内置了丰富的**敏感数据识别规则**，能够自动发现数据库中存在的各类敏感数据，增加了策略设置的便利性；
- 多租户模式能够满足云场景和多部门场景下的安全运维需求，使运维管理界限清晰，简化了设备需求量，减少了管理工作量。

5.3 强大的兼容性

DS-DSOM 具有强大的兼容性，支持主流的进口、国产数据库，以及各种大数据、NOSQL 数据库的安全运维：

- 支持关系型数据库，包括：ORACLE、DB2、SQLSERVER、MYSQL、MARIADB、SYBASE、POSTGRESQL、GREENPLUM、INFORMIX、TERADATA、CACHE 等；
- 支持国产数据库厂家：GBASE8A、GBASE8T、GBASE8S、达梦、人大金仓、神州通用；
- 支持大数据平台及其组件：HIVE、HBASE、星环 TDH 等；
- 支持 NOSQL 数据库：REDIS、MONGODB、MAX-COMPUTE；
- 支持内存数据库：IMPALA。

6 产品价值

6.1 提升合规满足度

《数据安全法》、《个人信息保护法》、《网络安全等级保护条例》、《关键信息基础设施安全保护条例》、《民法典》以及诸多行业监管政策中，都要求

数据运营者提供合理数据安全保护措施，并具备对高权限账户的审批、监控、权限分立等安全管理能力。

多维度的账号管理、安全访问控制、脱敏和审计等安全特性，很好的解决运维过程中账户共享、临时账号、账号管理混乱、运维操作不透明、数据从高敏感级流向低敏感级等数据安全风险问题，使得组织的合规满足度更高。

6.2 提升数据运维安全性

采用独立的身份认证和访问权限控制，能够在库、对象、字段及具体操作、访问量等项上设置权限，实现细粒度的访问控制；操作审批机制可以防止误操作发生的可能；运维审计能力完整准确的记录所有数据库的访问操作行为，提供事后追踪分析的能力。

支持敏感数据实时动态的交互式脱敏，给不同权限的运维用户显示不同的脱敏数据；既不影响正常运维工作，又防止数据泄露。

这些安全特性提高了数据运营者对核心数据的治理和防护能力，提升整体的安全等级，保障业务数据安全。

6.3 提升数据运维效率

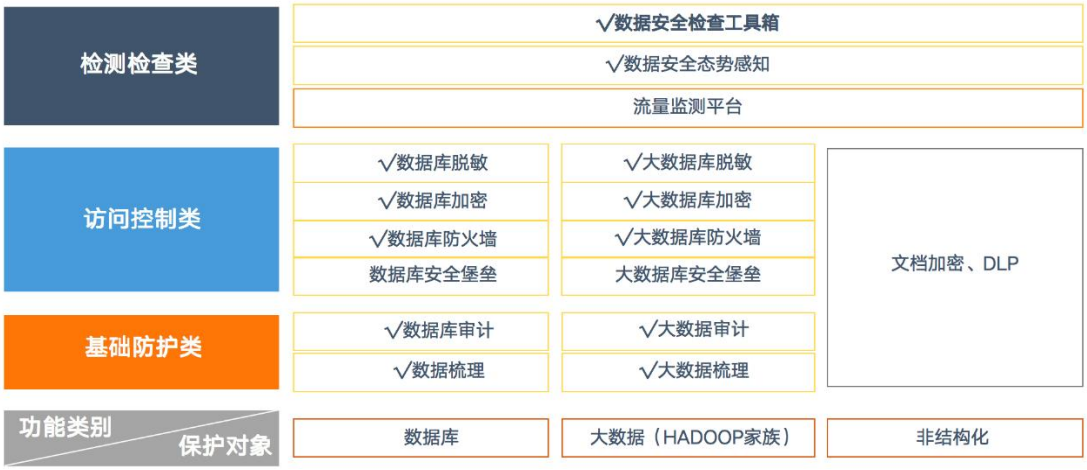
DS-DSOM 能够实现不同数据库的统一身份认证和单点登录，并且支持各种数据库的统一运维管理界面，大大提升了运维的效率，帮助用户更好的运维数据库。而多租户模式则适应了大型组织的组织架构，提升大型组织的数据运维效率。

7 公司简介

重庆数达信息安全技术有限公司是数据安全领域的引领者，核心团队专注数据安全 20 余年。公司的主要目标是对数据库、大数据、文件等数据对象的存管用（存储、管理、使用）全生命周期全场景实现全面的安全防护。

公司成熟产品根据防护能力分为基础防护类、访问控制类以及检查监测和溯源类。公司还将持续推出具有高度 AI 特性的数据安全新产品。得益于深厚的技术积累，公司系列产品的功能和性能在业内处于领先。

产品矩阵如下图所示。



重庆数达信息安全技术有限公司在北京、上海、深圳等全国二十多个省市设

置了办事处，服务全国客户。