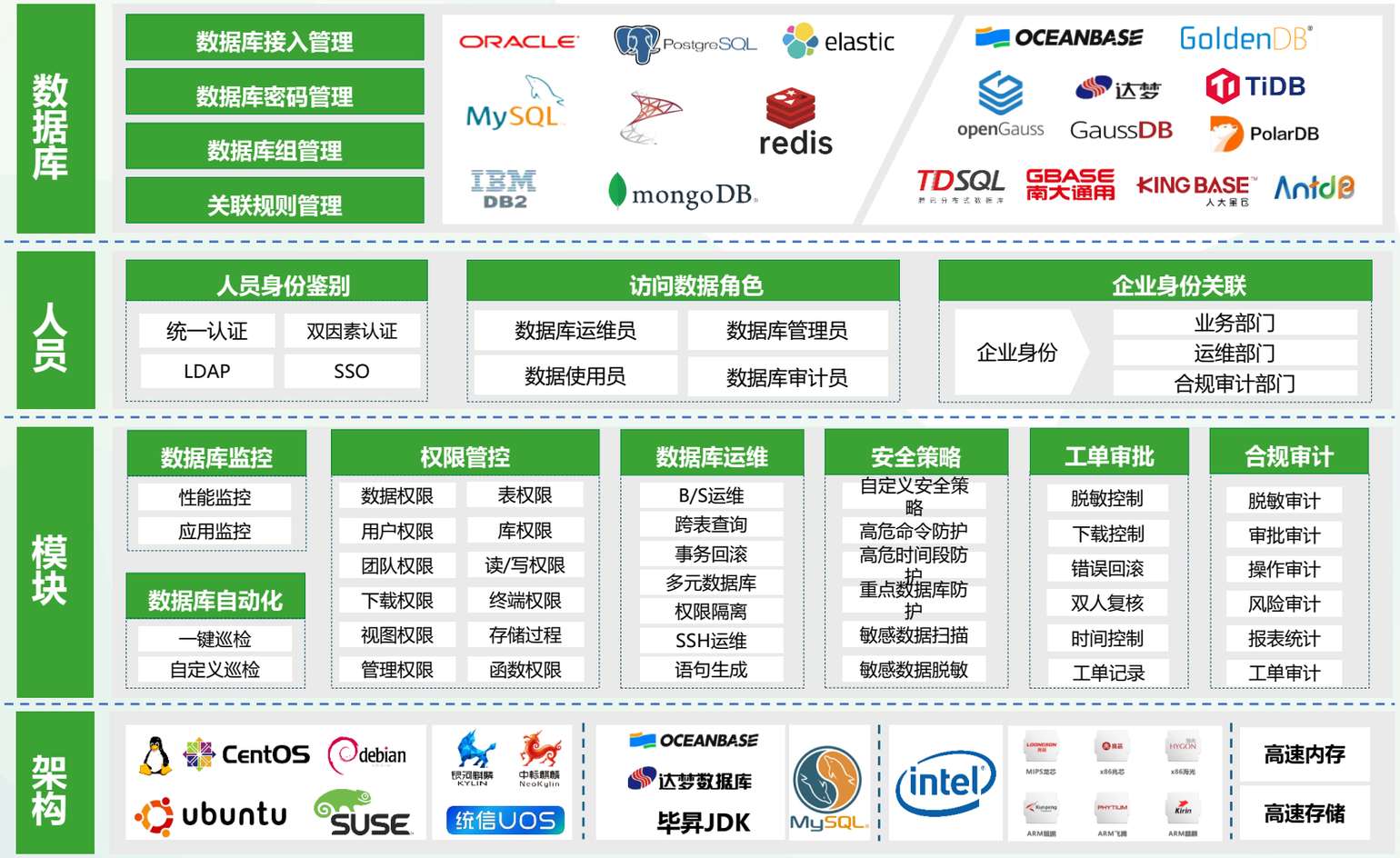
EntroDB数据库风险控制平台

不要成为下一个数据丢失的主角

您是否正在为数据库权限控制、敏感数据保护或 AI 数据使用边界发愁呢？您是否听到或者经历过数据库被删库、越权访问或数据泄露的安全事件呢？现今，越来越多企业因数据库管理不善、权限失控和数据外发缺乏约束而面临安全与合规风险。

EntroDB数据库风险控制平台旨在为企业提供数据库访问控制、透明代理接入、数据安全矩阵、动态脱敏、操作审计及 AI 数据服务。平台支持旁路代理部署、大数据权限控制，以及 AI 问数、AI 取数、AI 推理、AI 分析，帮助企业在安全可控前提下释放数据价值。



法律法规

《中国人民银行业务领域数据安全管理办法（征求意见稿）》

第十六条（人员管理要求）

数据处理者应当按照最小必要和职责分离原则，严格管理信息系统各类业务处理账号、数据库管理员等特权账号的设立和权限，人员变动时应当及调整权限或者收回账号。

第三十条（账号权限保护技术措施要求）

数据处理者应当采取有效技术措施，从严管控业务处理账号的数据使用权限，鼓励建设技术平台，采取统一认证、统一授权策略进一步加强管控。

数据处理者应当统一明确特权账号的使用场景，并通过内部审批授权，严格限定其使用。

《工业和信息化领域数据安全管理办法（试行）》

第十六条

工业和信息化领域数据处理者利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制。

第二十五条

工业和信息化领域数据处理者应当在数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志。日志留存时间不少于六个月。

《自然资源领域数据安全管理办法》

第十五条

数据处理者开展数据加工使用处理活动，应当采取访问控制、数据防泄露、操作审计等管控措施，确保过程安全、合规、可控、可溯源，防范数据关联挖掘、分析过程中有价值信息和个人隐私泄露的安全风险，明确数据使用加工过程中的相关责任，保证数据的正当加工使用。加工使用过程中，应当按照数据级别采取相应的措施保护数据的安全性，所使用的数据必须是真实可靠的，数据来源、收集过程须经过审查和核实。涉及利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。加工使用重要数据和核心数据，还应当实施严格的访问控制，建立数据可信可控、日志留存审计、风险监测评估、实时监控、应急处置、数据溯源等相关技术和管理机制。

产品简介

核心功能：

权限控制

支持依据不同角色、不同人员进行数据库访问授权，授权颗粒度可到实例、库、表、字段及数据库操作 DML、DDL、DQL、DCL；

支持高危风险命令识别与控制，并支持大数据权限边界管理；

代理接入

支持透明代理、旁路代理两种部署模式，在业务系统与数据库之间建立统一访问入口；

支持浏览器访问，无需安装客户端；

工单审批

支持高危命令、数据库特殊语句或者跨权限访问的工单审核；

支持工单审批双人复核；

安全脱敏

支持自动发现隐私与敏感数据，依据行业特征制定脱敏规则；

支持字段内容自定义脱敏规则；

支持查询、下载、报表、接口等场景的动态脱敏；

数据使用

支持以数据安全矩阵统一管理角色、数据源与共享边界，满足跨部门、跨系统数据使用需求；

支持数据库之间的跨库查询、跨表查询；

支持 AI 问数、AI 取数、AI 推理、AI 分析，并执行权限与脱敏策略；

合规审计

支持所有数据库操作的审计，审计规则可以自定义，审计参数包括用户、时间、IP、操作、语句、影响行、响应时间等；

支持系统、消息、告警及 AI 调用日志记录；

产品优势

- ■ 开箱即用
- ■ 部署简单
- ■ 信创适配
- ■ 安全可靠
- ■ 单点登录
- ■ 合规审计

支持的平台

- ■ 操作系统
  - Linux
  - Centos
  - SUSE
  - Ubuntu
  - FreeBSD
  - 麒麟系统
  - 统信UOS
- ■ 硬件平台
  - X86 服务器
  - 海光平台
  - 兆芯平台
  - 鲲鹏平台

数据库支持

- ■ 通用数据库
  - Mysql
  - Mssql
  - Oracle
  - MongoDB
  - PostgreSQL
  - DB2
  - HANA
  - .....
- ■ 国产数据库
  - 达梦
  - Oceanbase
  - Tidb
  - 人大金仓
  - 南大通用
  - GaussDB

上海数跃信息技术有限公司
上海市浦东新区祥科路58号2栋615