DataFocus OT · 企业本体平台

# 让 AI 进入业务，
# 控制权留在你手里

用业务本体给 AI 一张读得懂的业务地图、一条有边界的通道，以及一套要人批准的动作。

`OT = Ontology` 本体：把企业的业务建成一个模型，人和 AI 都在上面工作

# 老板在催 AI 落地。
# 员工已经在用外面的 AI 工具。
# IT 和法务却不敢把企业数据交出去。

DataFocus OT 让你可以放心地对 AI 说“可以”。

问题

# AI 进企业，缺的不是模型

## 缺上下文

模型不认识你的业务：不知道各系统里的“客户 A”是不是同一家，不知道“交付”怎么算，也不知道哪版规则在生效。

## 缺边界

让 AI 直接连数据，它能看什么、能改什么都不受控；给每个 AI 单独配权限，配不过来，也对不上。

## 缺行动能力

只会回答问题的 AI 价值有限。企业要的是发现问题后能推进处理，每一步都在规则之内、有人把关。

**业务本体补的正是这三样。**

OT = Ontology

# 什么是业务本体

围绕一个业务主题建立的业务模型，由五部分组成

| 组成 | 在 DataFocus OT 中 |
| --- | --- |
| 业务对象与关系 | 把各系统的数据表组织到本体下，写明表与表如何关联及业务含义，在本体图谱中呈现 |
| 规则与知识 | 文档中心存放制度、规则和口径说明，并关联到它们约束的数据 |
| 指标 | 指标中心，按计划推送给相关人员 |
| 动作 | 执行脚本（计算、校验、写回）；控制面板上的业务动作，如生成整改任务 |
| 权限 | 沿用企业的用户、角色和资源权限；按本体逐个授权给 AI Agent |

# 示例：采购审批本体

**对象与关系**

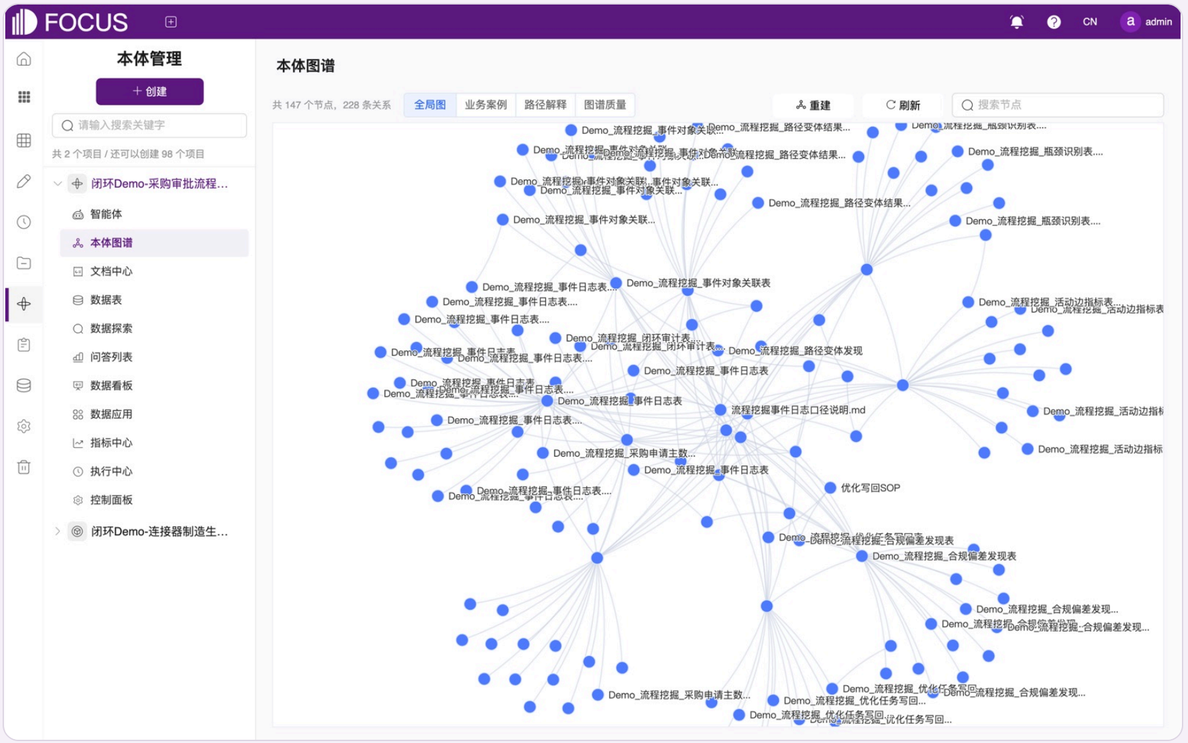
采购申请、审批事件、路径变体、瓶颈、合规偏差、优化任务、审计记录等 9 张表，并写明它们如何关联

**规则与知识**

合规偏差校验规则、SLA 与瓶颈识别规则、事件日志口径说明、任务写回与审计 SOP

**动作与权限**

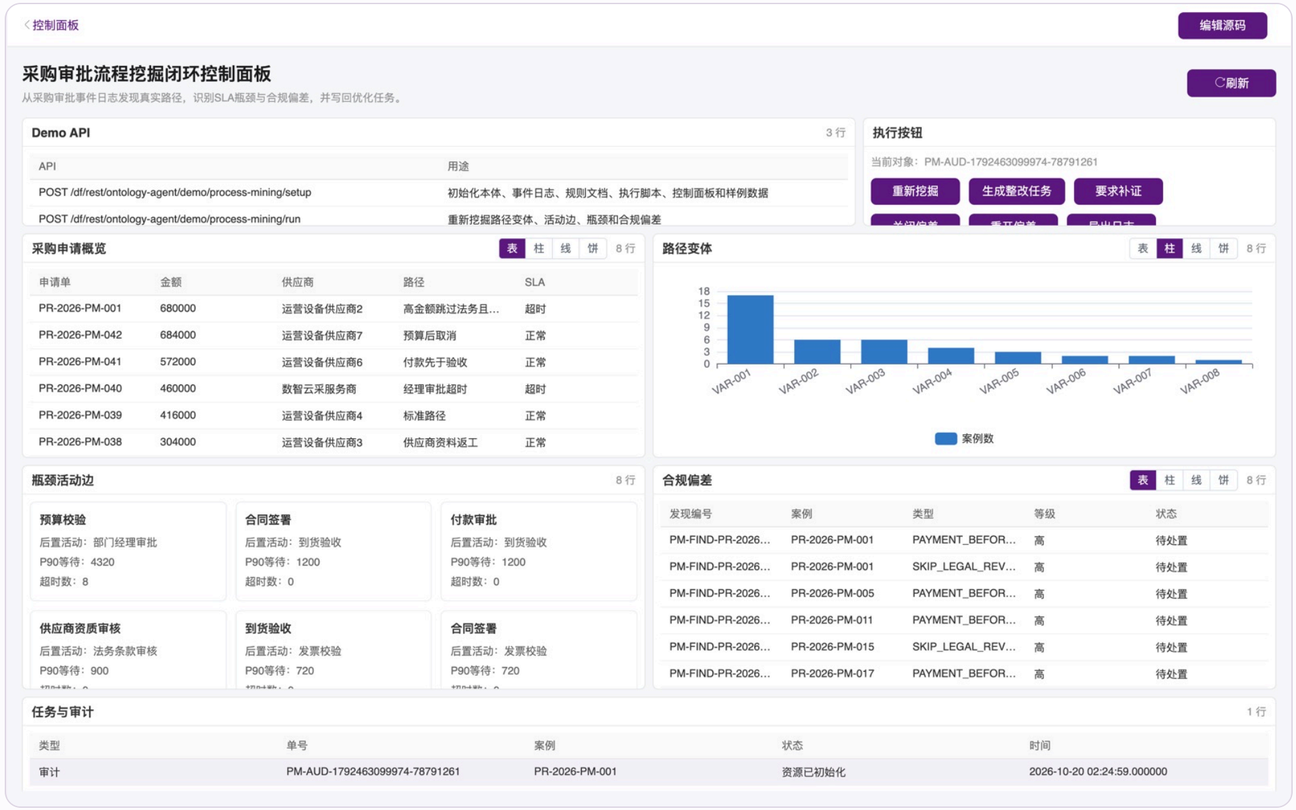
合规偏差检测脚本；生成整改任务、要求补证、关闭偏差。只有被授权的人和 Agent 能看到它




本体图谱：147 个节点、228 条关系

动作

# 从发现问题到解决问题




## 一屏看全

控制面板上同时看到采购申请、路径变体、瓶颈和合规偏差

## 直接处理

选中一条异常记录，就能生成整改任务、要求补证或关闭偏差

## 规则自动校验

执行脚本找出高额申请跳过法务审核、付款早于验收等问题，并写回结果

# 向本体提问，让 AI 帮你搭本体




问采购审批的瓶颈在哪里，本体智能体分析事件日志和规则，给出改进建议。

## 本体智能体

用自然语言提问，它结合本体中的数据和文档给出有依据的回答，还能调用执行项完成分析或写回。

## AI 帮你搭本体

界面上可让 AI 生成执行脚本、生成和修改控制面板草稿；外部 Agent 可起草本体并提出待确认的问题，业务负责人确认后发布。

外部 Agent 起草本体：产品方告知

看得见的证据

# 同一个问题，同一组数字

业务人员 · 数据搜索“申请部门 金额”




AI Agent · Claude Code 通过 MCP

金额合计最高的是**运营保障部**，为 7,842,000 元。

| | |
|---|---|
| 运营保障部 | **7,842,000** |
| 采购部 | **6,966,000** |
| 数字化部 | **5,786,000** |

依据：查询采购申请主数据表，附执行的 SQL 和数据指纹（回答摘录）

**两边的数字逐项相同**

权限

# AI 不越界：权限跟着本体走

### 不超出用户本人的权限

授权 Agent 时只能勾选自己有权访问的本体，默认什么都不开放；普通用户申请不到写入权限。

### 越权请求不泄露

请求授权范围以外的数据会被拒绝，返回结果也不透露这些数据是否存在。

### 收回即生效

管理员收回权限或用户断开连接后，Agent 的下一次调用就被拒，不必等令牌过期。

### 每一步可追溯

每次查询都返回执行的 SQL、所用数据表和数据指纹；Agent 的全部操作还会记入审计日志。

审计日志：产品方告知

变更

# AI 的改动，要经人批准

AI 要新建或修改控制面板等内容时，只能提交草稿

1
**提交草稿**
AI 生成变更内容

→

2
**真实数据预览**
系统校验并预览

→

3
**生成变更计划**
计划不可更改

→

4
**管理员批准**
在后台审阅

→

5
**应用生效**
留有审批记录

未经批准的计划无法应用，伪造的批准凭证会被拒绝；同一次批准重复提交，不会重复执行。

价值

# 功能之外的价值

| | |
|---|---|
| **敢对 AI 说“可以”** | 把“禁止”变成“受控地允许”：有权限、能撤销、改动要批准。AI 用起来了，数据也不再从后门流出去。 |
| **掌握 AI 时代的主动权** | 业务知识留在你自己服务器上的本体里；接入哪个模型、哪个 Agent 由你决定，换了也不用从头再来。 |
| **越用越值钱** | 第二个场景复用已有的对象、规则和权限，每多一个 AI 应用，成本就更低；一次性试点做完就扔了，本体会留下来。 |
| **出了错，能追到责任** | 用了哪份数据、按哪条规则、谁批准的，都查得到。AI 可以追责，管理层才敢放行。 |
| **知识留在公司** | 老员工脑子里的规则和处理办法变成本体；人员流动，知识还在，新的 AI 应用都从这里开始。 |

为什么是 DataFocus

# 都说有“本体”，常见做法有四类

| 做法 | 擅长 | 不足 |
| --- | --- | --- |
| 知识图谱：从文档中抽取实体和关系 | 检索和问答 | 金额、汇总等数字靠模型生成，算不准；没有业务动作 |
| 指标层或语义层：数据平台自带 | 报表数字准确 | 没有规则文档和业务动作；绑定在该平台上 |
| 数据目录 | 说明数据在哪里、是什么 | 只描述数据，不参与业务运行 |
| 重型本体平台 | 功能完整 | 价格高、实施重，依赖驻场团队；AI 多绑定自家产品 |

为什么是 DataFocus

# DataFocus OT 的做法

### 数字算得准

底层是真实计算引擎（Flash 用 Doris，Heavy 用 Trino 等），回答来自实际执行的 SQL，带可核对的回执。

### 数据、规则、动作在同一个本体里

数据告诉你发生了什么，规则告诉你应该怎样，动作让你接着处理。

### 对 AI 开放，但默认受控

标准 MCP 和 OAuth 接入任何支持 MCP 的 Agent；权限继承、实时撤销、变更审批、查询回执都是内建的。

### 轻

私有化部署，Flash 一个引擎就能运行；从一个本体起步，不需要庞大的驻场团队。

### 人和 AI 共用

业务人员的搜索分析、看板和推送用的是同一个本体。投入一次，两边受益。

版本

# 两个版本

| | OT Flash | OT Heavy |
|---|---|---|
| 计算与存储 | Apache Doris，内存计算与数据仓库合一 | Hadoop、Hive、Trino、Iceberg |
| 业务本体 | 支持 | 支持 |
| AI Agent 接入（MCP） | 支持 | 支持（产品方告知） |
| 数据加工 | — | ETL（DataSpring，基于 Flink） |
| AutoML 与 AI 自动建模研究 | — | 支持（产品方告知） |
| 适合 | 想先在一个业务域快速建起本体，数据可以集中到一个分析引擎的团队 | 数据量大、已在使用大数据平台，并需要数据加工和建模的企业 |

产品方告知：产品方说明已有，尚未在正式版本上验证

开始

# 第一步：从一个本体开始

1

选一个有数据、有制度、有负责人的业务问题

2

带上相关的数据表和规则文档，建起第一个本体

3

让业务人员先用起来，再授权一个 AI Agent 接入

4

跑通之后，扩展到下一个业务主题

**带一个业务问题、一张表、一份制度来，我们一起建第一个本体。**

私有化部署，安装在企业自己的服务器上 · 联系我们：datafocus.ai/about