AI 智能体平台

AgentWorks

AI 智能体构建与运营平台

在封闭网络中也能运行的无代码 Agentic AI 平台。
自行构建并运营适合机构业务的智能体。



本手册从注重安全的机构 · 企业在引入 AI 时实际遇到的四个顾虑出发。依次介绍 AgentWorks 如何解决每个顾虑，以及实际导入案例和起步方法。



前言

前言 引入 AI 前的四个顾虑 p.03

平台 AgentWorks：机构内部的智能体工厂 p.04

结构 四个层与一个关口 p.05

四个顾虑与解决方案

顾虑 01 网络隔离 · 内部规定导致无法使用商用 AI p.06

顾虑 02 每项业务都外包开发，预算和周期负担太重 p.09

顾虑 03 通用 AI 不了解机构的制度 · 文档 · 数据库 p.12

顾虑 04 无法证明谁向哪个 AI 发送了什么 p.14

案例与导入

导入案例 不同的机构在同一个平台上工作 p.17

导入步骤 从小处开始、逐步扩展的导入步骤 p.19

咨询 试点建议 · 咨询导入 p.20

常听到的顾虑

注重安全的机构在引入 AI 时遇到的四个顾虑

大家都认同需要 AI。
卡住的是之后的事：制度、人力、资料，以及责任。

请从您最在意的顾虑开始点击。
即可直接跳转到 AgentWorks 如何解决它。



顾虑 01 “因为网络隔离和内部规定，无法使用商用 AI。” 本地部署 · 自有模型 →

顾虑 02 “每项业务都要外包开发，预算和周期都很吃紧。” 无代码构建器 →

顾虑 03 “通用 AI 不了解我们的内部制度 · 文档 · 数据库。” 连接资料与数据 →

顾虑 04 “无法确认谁把哪些资料发给了哪个 AI。” 双重关口 →

机构内部的智能体工厂

让 AI 不止于回答，而是在机构内部工作。

AI 智能体构建与运营平台 在封闭网络中也能运行的无代码 Agentic AI 平台。不是一个聊天机器人，而是持续打造智能体的基础。

01 · 构建 · 运营

业务人员自己构建和运营

用一句话下达指示，AI 即设计任务，并通过定时 · 队列在无人值守时执行。



02 · 连接

用机构自己的资料工作

从内部文档 · 数据库中找到依据，并借助系统和工具直接产出成果。



03 · 治理 · 安全

管控并留痕

设定模型 · 权限 · 额度，把用量和审计记录留在机构内部。



持续改进 根据使用记录和质量检查结果修正任务，并按业务不断增加智能体。

4种	10种	15种	9种	2重	GS认证
构建智能体的方式	内置工具	办公工具	数据连接器	AI 调用关口	可通过韩国公共采购购买

平台结构

由四个层和一个关口组成的平台

User Environment
使用之处 · 员工与系统的入口

- **网页对话** 员工直接下达指示
- **现有业务系统** Open API · 定时执行
- **新服务** 在专用应用中嵌入 AI

Agent Runtime
工作之处 · 执行引擎

- **执行引擎** 计划 → 执行 → 确认
- **子智能体** 拆分处理复杂任务
- **定时 · 队列** 无人值守执行
- **安全机制** 重复 · 时间 · 预算 · 个人信息

顾虑 04

Agent Builder
构建之处 · 无代码

- **AI 设计任务** 一句话生成步骤
- **技能** 打包业务规则复用
- **文档模板** 登记机构模板
- **质量检查** 按标准答案评分

顾虑 02

Enterprise Connection
连接之处 · 依据与工具

- **资料库** HWP 等文档知识
- **数据集** 查询数据库 · Excel
- **数据连接器** 自动同步原始数据
- **外部工具** 通过 MCP 执行实际业务

顾虑 03

安全 · 管控 机构隔离 · 角色权限 · 共享 · 委派 · 审计记录 · 登录锁定

部署 本地部署（封闭网络） · 混合 · 云端

AI Gateway · 模型 · 密钥 · 用量管理

- 部门网关
- 模型 · 密钥管理
- 用量 · 成本记录
- 积分额度

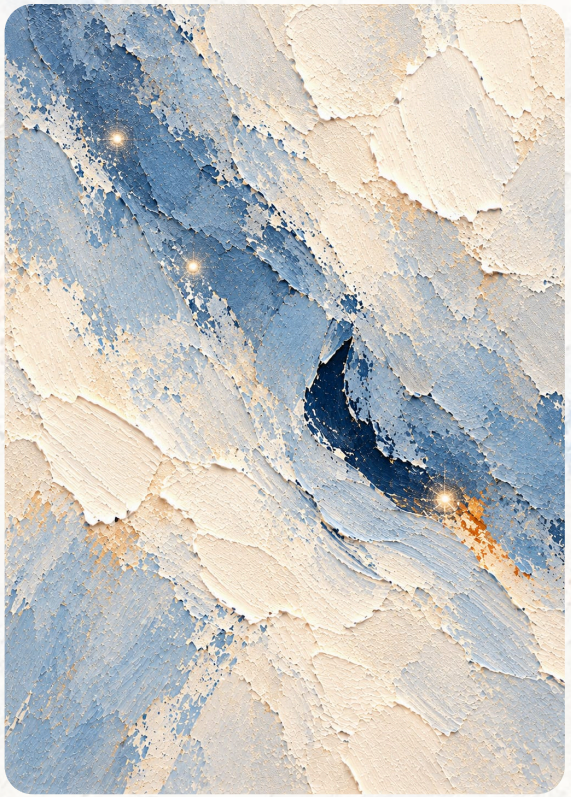
Egress Gateway
对外连接的唯一通道 · 仅连接并记录允许的地址 · 可配置为封闭网络

- **自有小型模型** 机构内部 GPU 服务器
- **商用 AI** 仅在允许时经由 Egress

顾虑 01 顾虑 04

点击“顾虑”按钮，即可跳转至该层所解决的顾虑。

顾虑 01 · 外部 AI 使用受限



因为网络隔离和内部规定，无法使用商用 AI。

这是注重安全的公共 · 金融机构最先提到的情况。

现场常见的情况

需要 AI，路却被堵住了

由于网络隔离和安全规定，业务资料无法发送给互联网另一端的商用 AI。

一禁止就会有人绕道

紧急工作被转到个人设备和个人账号上处理，反而跑到了机构的管控之外。

自行搭建太沉重

要在机构内部引入 AI，就得从零准备模型 · 基础设施 · 运营体系。

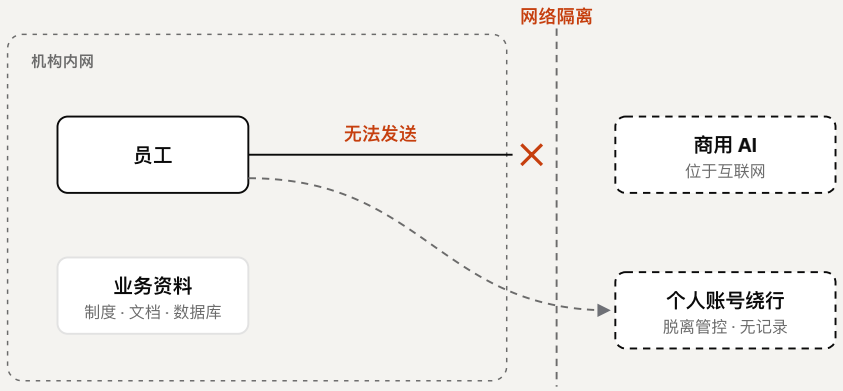
深层顾虑 “因为安全问题，AI 引入一拖再拖。”

查看 AgentWorks 的解决方式 →

解决 01 · 本地部署 + 自有 AI 模型

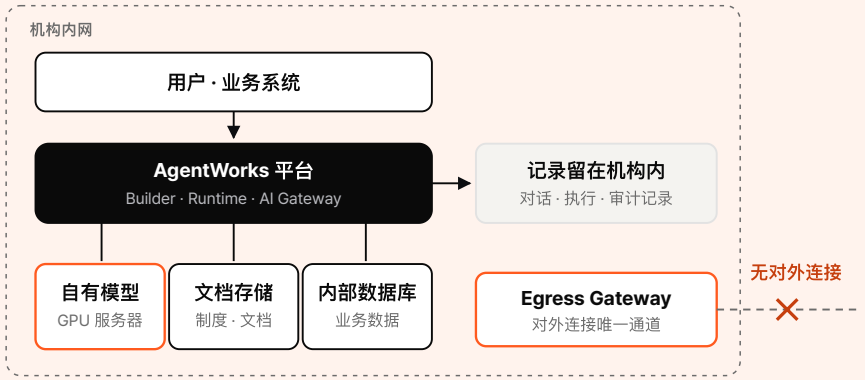
无需互联网，在机构内部全程运行。

现在



内网之外的 AI 无法使用，部分工作在管控之外绕行处理。

引入 AgentWorks 后



对话 · 文档分析 · 任务执行由机构 GPU 服务器上的自有模型处理，资料和记录也留在机构内部。

全程使用自有模型

对话 · 文档分析 · 任务执行均由机构 GPU 服务器上的自有模型处理。兼容 OpenAI 接口，公开模型可直接接入。

资料与记录留在机构内

文档索引 · 对话 · 执行记录和审计记录保存在内部存储中，并按机构（组织）隔离数据。

在内网中连接内部系统

数据库 · 共享文件夹 · SFTP 通过数据连接器同步，现有业务系统通过 Open API 调用智能体。

对外连接只走一条通道

对外连接全部汇集到 Egress Gateway。清空允许列表，即可在无对外连接的状态下运行。

客户收获

- ✓ 在遵守安全规定的同时把 AI 用于业务
- ✓ 封闭网络配置下，资料和记录不会离开机构
- ✓ 即使模型更换，平台照样使用

解决 01 · 适配机构环境的部署

按照安全要求选择部署方式。

本地部署（封闭网络）

公共 · 金融

- 无需互联网，用 **自有模型** 运行
- 资料 · 记录全部在机构内部
- 清空允许列表，阻断外部



适用对象
必须网络隔离的公共 · 金融机构

AI 模型	**机构 GPU 服务器**
资料 · 记录	**机构内部**
对外连接	**无**

混合部署

按敏感程度划分

- 本地部署 + **部分商用 AI**
- 敏感业务使用内部模型
- 商用 AI 经 Egress，仅限允许地址



适用对象
敏感业务与一般业务并存的机构 · 企业

AI 模型	**自有 + 允许的商用 AI**
资料 · 记录	**机构内部**
对外连接	**Egress 唯一通道**

云端（SaaS）

快速试点

- 注册后 **即可使用**
- 试点后转为本地部署
- 适合一般企业业务



适用对象
希望先快速看到效果的机构 · 企业

AI 模型	**商用 AI**
资料 · 记录	**云端**
对外连接	**互联网**

客户收获

- ✓ 选择符合机构安全要求的方式
- ✓ 敏感业务与一般业务分开运营
- ✓ 先在云端试点，再转为本地部署

顾虑 02 · 开发人力有限

每项业务都要外包开发，预算和周期都很吃紧。

这是想把 AI 引入业务的业务部门和信息化部门共同面临的问题。



现场常见的情况

需求越积越多，开发跟不上

各部门都有想交给 AI 的工作，但开发人力和预算有限，只能排队等待。

做好时业务已经变了

在用文档传达需求、等待结果的过程中，工作方式已经改变，只好重新外包。

懂业务的人改不了

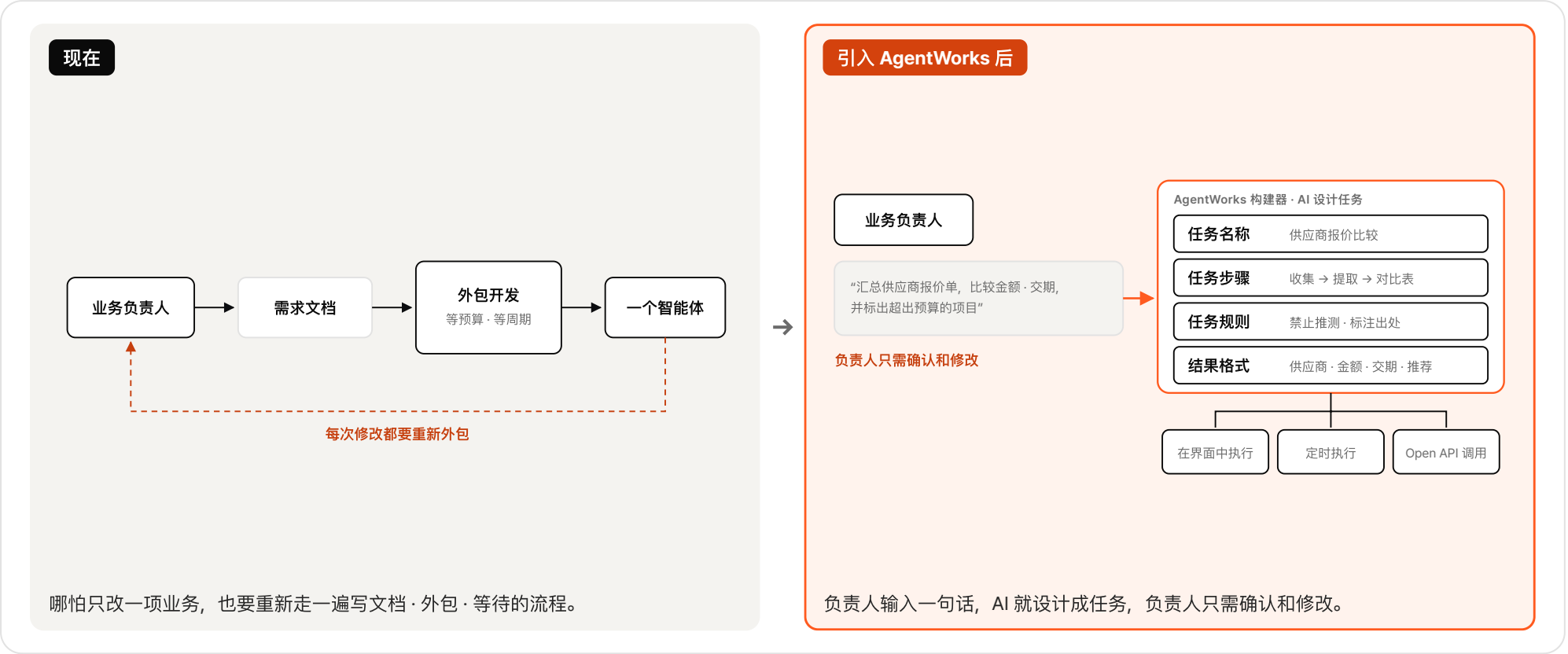
最了解业务的负责人不懂代码，没有办法自己修改或改进。

深层顾虑 “AI 引入又变成一个开发项目。”

查看 AgentWorks 的解决方式 →

解决 02 · 业务人员自己构建的无代码构建器

输入一句话，就成为每周工作的智能体。



任何人 · 直接对话

指定资料库后提问，即成为一个规程指引智能体。

业务负责人 · 用语言设计

用一句话输入要做的事，AI 设计步骤并完成定时设置。

业务专家 · 打包为技能

把撰写规则和格式打包成技能，让整个部门以同样的质量使用。

系统负责人 · Open API

在专用应用或其他系统中通过 API 调用任务。

客户收获

- ✓ 无需单独提开发需求或外包即可开始
- ✓ 业务一变，负责人马上就能修改
- ✓ 整个部门按同一标准和质量使用

解决 02 · 构建过程示例

投诉处理情况报告智能体，这样构建。

负责人输入的指示

“按类型和部门汇总上周受理的投诉，整理处理延迟和重复投诉，做成周报”

第1步
输入指示
用一句话写下想要的结果

第2步
AI 设计计划
查询 → 汇总 → 提取延迟 · 重复 → 报告

第3步
连接资料
投诉受理数据集 + 投诉处理规程资料库

第4步
定时
每周一 09:00 自动执行

第5步
结果
报告（摘要 · 表格 · 图表） · Word · PDF · 邮件通知

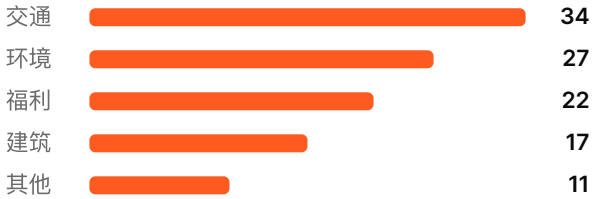
AI 设计的执行计划 · 示例

1. 从投诉受理数据集中查询上周记录
2. 按类型 · 部门统计件数
3. 提取超期件 · 同一投诉人的重复件
4. 在投诉处理规程中确认相关标准
5. 撰写周报 → 邮件通知负责人

投诉处理周报 10 月第 3 周 · 自动生成 　邮件已发送

受理	已办结	处理延迟	平均处理	重复投诉
128 件	112 件	9 件	2.4 天	4 件

按类型受理



需确认

超过处理期限	9 件
同一投诉人重复	4 件
疑似违反规程	0 件

出处 · 投诉受理数据集 · 投诉处理规程

还可以构建这些智能体 注明条款依据的制度咨询 · 招标需求书分析 · HWP 文档摘要 · 用语言查询统计 · 定期报告自动生成 · 故障受理 · 原因分析 · 技术咨询一线答复 · 语音生成会议纪要 · 个人信息遮盖

画面中的计划和报告为便于理解的示例。

顾虑 03 · 机构资料难以利用



通用 AI 不了解我们机构的内部制度 · 文档 · 数据库。

这是在业务中试用过 AI 的负责人最先感受到的局限。

现场常见的情况

无法以机构文档为依据作答

机构的制度和规程以 HWP · PDF 形式积累，但通用 AI 无法以这些文档为依据作答。

不知道答案从何而来

看不出答案依据的是哪项制度 · 哪一条款，无法直接用于业务。

数据被困在系统里

要查看业务数据库和 Excel 中的数字，负责人只能自己导出整理。

深层顾虑 “到头来，AI 的回答还得人再确认、再修改。”

查看 AgentWorks 的解决方式 →

解决 03 · 连接知识 · 数据 · 系统

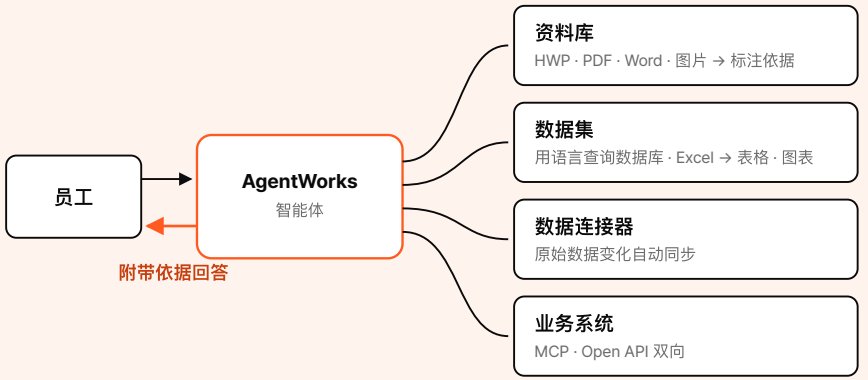
机构的文档 · 数据库 · 系统，成为智能体的依据和手脚。

现在



通用 AI 无法参考机构资料，最终还要负责人重新查找确认。

引入 AgentWorks 后



智能体从机构的文档 · 数据 · 系统中找到依据，并借助工具直接产出成果。

资料库 · 把文档变成知识

把 PDF · Word · HWP · 图片（OCR）文档变成可检索的知识，每个回答都标注依据文档。

数据集 · 用语言查询数据库

无需 SQL 即可向内部数据库 · Excel · CSV 提问，以表格和图表作答。

数据连接器 · 自动同步

定期同步 S3 · SFTP · 共享文件夹 · 数据库 · Redmine 等 9 种存储。

外部工具 · 执行实际业务

借助 10 种内置工具和通过 MCP 连接的机构内部工具，完成查询 · 撰写 · 发送。

客户收获

- ✓ 每个回答都能立刻查看依据文档
- ✓ 不懂 SQL 也能拿到表格 · 图表
- ✓ 原始数据变化会自动同步

顾虑 04 · 管控与留证的负担



无法确认谁把哪些资料发给了哪个 AI。

这是安全 · 审计负责人和管理者在决定导入前会问的问题。

现场常见的情况

使用记录分散

各部门使用不同的 AI · 不同的密钥，无法在一处看到全部使用记录。

个人信息被原样传出

投诉人姓名 · 联系方式等个人信息，可能未经确认就直接进入 AI。

成本和额度难以设定

不清楚哪个部门用了多少，预算难以制定和遵守。

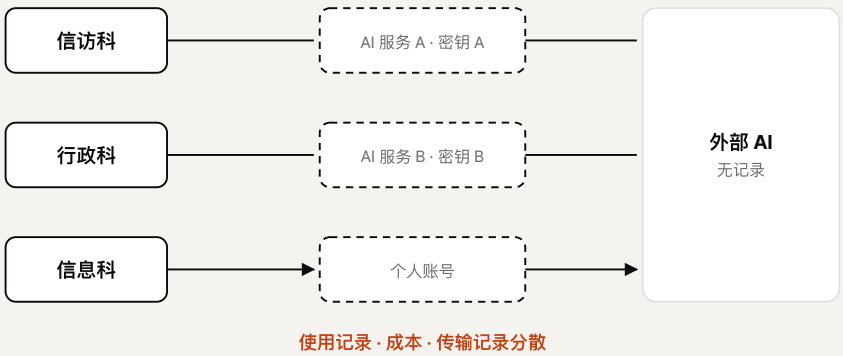
深层顾虑 **“审计时拿不出证据。”**

查看 AgentWorks 的解决方式 →

解决 04 · 用 AI Gateway 统一管理

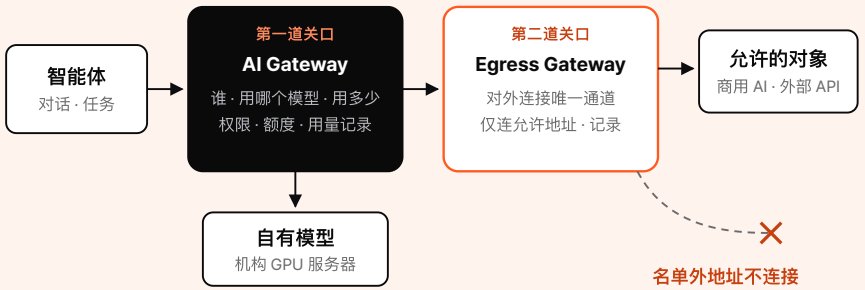
AI 调用通过双重关口管控并记录。

现在



各部门使用不同的 AI 和密钥，无法在一处看到谁发送了什么。

引入 AgentWorks 后



所有调用都经过同样的两道关口，用量和对外连接都留有记录。

拦截什么

阻止向未经允许的 AI 服务发送、无权限部门使用模型以及超出额度的使用。

记录什么

按模型 · 用户统计的用量、对外连接，以及登录和主要操作的审计记录。

部门网关

为每个组指定模型和密钥，停用即刻生效。可按合同 · 期间 · 用户设定积分额度。

只需配置的安全功能

默认提供机构级数据隔离、按角色的权限 · 共享 · 委派、连续 5 次登录失败锁定和会话过期。

客户收获

- ✓ 用记录证明谁发送了什么
- ✓ 在一处查看各部门的用量和成本
- ✓ 无需开发，只需配置即可具备管控与留证

解决 04 · 交给它也能放心

智能体独自工作时，三项安全机制也同时运行。

执行安全机制

防止过度执行



同一动作重复、超出步骤数上限或执行时间上限时，会**自动停止**。

预算 · 额度

成本上限



超出单项任务的 Token 预算或合同 · 期间 · 用户额度时，**阻止新的执行**。

执行前检查

个人信息保护



在输入阶段检测个人信息，**拦截或遮盖后**再执行。

用数字确认质量

登记标准答案
把常见问题和必需 · 禁止条件做成用例

组合执行
更换模型 · 推理强度，一次跑完同样的用例

评分
规则评分 · AI 评分判定是否通过

对比 · 改进
通过率 · 分数 · 响应时间 · 成本，按轮次对比修改前后

不可撤销操作的负责人审批，以及界面切换后仍能继续的自动恢复功能正在开发中。

导入案例

不同的机构在同一个平台上工作。

使用中

A 公司

面向公共部门的 AI 咨询

招标需求书分析 · 方案撰写

资料库 · 画布 · 文档模板

云端

使用中

B 公司

集团 IT 服务子公司

公司通用业务 AI

对话 · 资料库 · 办公工具

云端

建设中

C 机构

公共 · 教育

教育信息网故障受理 · 分析

Open API · 任务 · 连接器

本地部署

试点

D 公司

网络设备制造

技术支持中心自动化

资料库 · 任务 · 个人信息遮盖

混合部署

设计 · 计划建设

E 机构

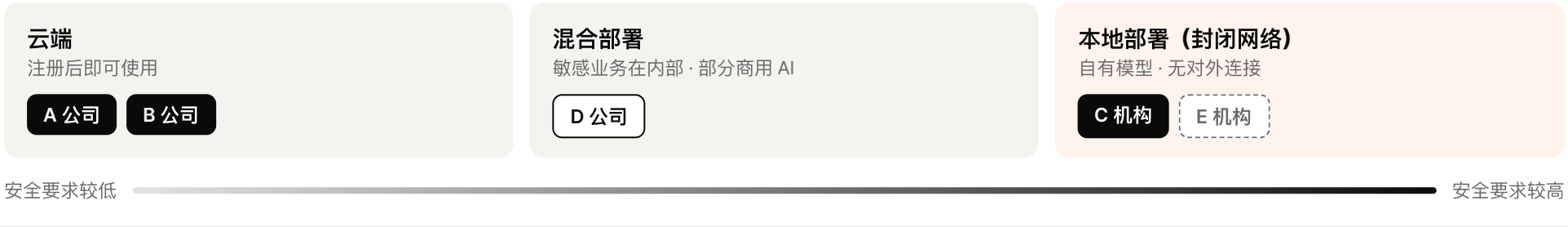
公共 · 能源

大规模数据提取 · 分析

数据集 · 自有模型

本地部署（封闭网络）

部署形态图 · 安全要求越高，越倾向本地部署



共同点 **业务不同、安全环境不同，但都在同一个平台上构建和运营智能体。**

应客户要求，机构名称均匿名表示。状态截至 2026 年 10 月。

案例详情

从案例看构建 · 连接 · 安全的实际情况

C 机构 · 公共 · 教育 建设中 · 本地部署

教育信息网故障受理 · 分析

1,600+ 件 作为依据的 4 年故障记录

1. 教职员工无需登录，用对话报修
2. 专用受理应用通过 Open API 调用任务
3. 检索相似案例 → 原因候选 · 排查指南
4. 运维人员查看分析后判定 · 结案
5. 处理记录成为下次分析的参考资料

以机构记录代替经验
根据相似案例给出原因候选和排查方法

处理期限管理
按工作时间计算期限 · 临近提醒

越用越丰富的知识
办结后立即加入参考资料

构建 · 运营	专用应用通过 Open API 调用任务
连接	以 4 年故障记录为依据
治理 · 安全	5 种角色 · 按地区授权 · 遮盖 IP · 电话 · 密码

D 公司 · 网络设备制造 试点 · 混合部署

技术支持中心自动化

20 万件 由 AI 检索 · 分析的历史问题

1. 受理即按类型 · 严重程度分类并通知负责人
2. 以最相似的 3 个问题为依据给出一线处置方案
3. 读取日志并整理原因候选
4. 经工程师审核后再采用
5. 把处理结果整理成报告和 FAQ

最终由人判断
AI 结果经工程师审核后再采用

沿用现有环境
保持原有门户和账号体系

无需开发即开启的功能
相似问题检索 · 用量控制 · 个人信息遮盖

构建 · 运营	一线处置方案 · 自动分类任务
连接	检索 20 万件历史问题
治理 · 安全	角色权限 · 审计记录 · 个人信息遮盖 · 沿用现有门户与账号

E 机构 · 公共 · 能源 设计案例 · 计划建设

大规模封闭网络数据分析

2 万余种

目标数据表 · 数百 TB · 每年数万件请求

1. 分析需求方用自然语言提问
2. 利用元数据只挑选需要的表并生成 SQL
3. 通过语法 · 执行计划预检拦截危险查询
4. 以只读方式直接查询原始数据
5. 同时给出表格 · 图表和执行的 SQL · 出处

原则 1
数据不搬移

原则 2
用元数据提高准确度

原则 3
负载 · 安全管控优先

构建 · 运营	把自然语言请求变成 SQL 分析任务
连接	不搬移数据，直接查询原始数据
治理 · 安全	封闭网络 · 自有模型 · 时间 · 行数限制 · 审计

导入步骤

导入从小处开始，逐步扩展。

1 咨询
确认业务与安全要求。

2 试点
用 1~2 项代表性业务确认效果。
也可在封闭网络中进行试点。

3 业务选定 · 设计
整理要做成智能体的业务和资料。

4 部署 · 培训
进行本地部署和负责人培训。

5 推广
按部门增加智能体。

第1阶段 · 试点

一个部门 · 1~2 项代表性业务

信访科

从效果立竿见影的业务开始，先验证成果和运营方式。

第2阶段 · 推广

各部门增加智能体

信访科 行政科 信息化

其他部门直接沿用已验证的任务 · 技能，无需开发即可增加本部门的智能体。

第3阶段 · 全机构

机构内部的智能体工厂

信访 行政 信息化 审计 规划 +

各部门打造的智能体按同样的权限 · 额度 · 审计标准运营，管理者在 AI Gateway 一处统一管理。

部门和智能体数量仅为示例。

一并提供
培训 · 手册 · 技术支持

计费方式
按部署方式 · 规模协商

采购咨询
VICS Technology

公共采购（韩国）
GS 认证 · 可通过采购购买

下一步

我们建议用贵公司的实际业务进行试点。

从效果立竿见影的 1~2 项业务开始，用自有模型在机构内部验证，再根据结果一起制定推广计划。

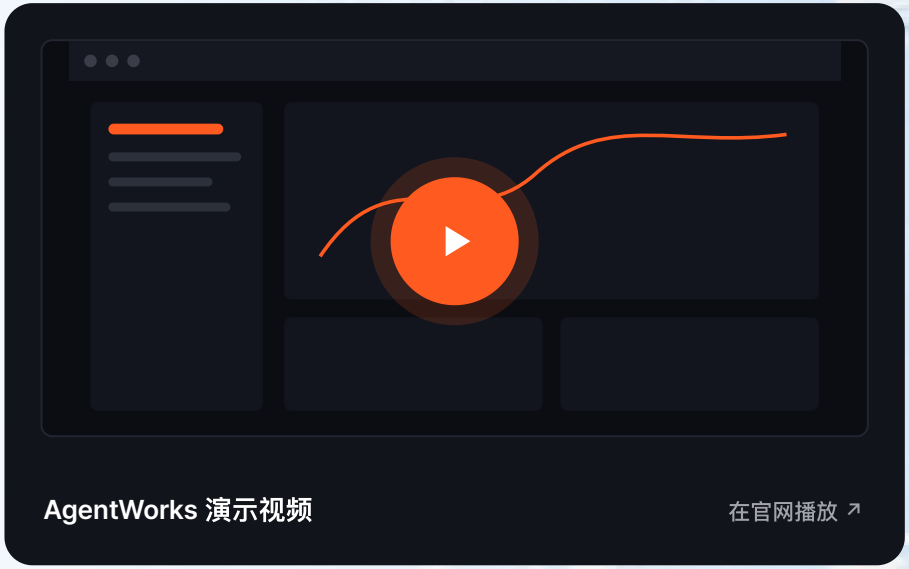
选定代表性业务
效果立竿见影的 1~2 项业务

封闭网络试点
用自有模型在机构内部验证

结果报告
整理效果与推广计划

咨询导入 →

▶ 观看演示视频



邮箱
sales@vicsnc.com

网站
vicsnc.com