亚马逊云科技

中国峰会

2026年6月23日-24日　　上海　·　世博中心

亚马逊云科技
中国峰会

Agentic AI 的数据之道——
Agent 自己找数据、记数据、管数据，你准备好了吗?

曾蕾

首席数据工程师

亚马逊云科技

马丽丽

资深数据库解决方案架构师

亚马逊云科技

议程

- AI 创新步伐
- Agentic AI 基础架构
- Agentic AI 的数据底座
- 行动倡议

亚马逊云科技
中国峰会

Agentic AI 的创新步伐, 基础架构

AI 格局不断演变

抄□权峭桄淆阃峄俦矍俣尘寿萄

选择合适的向量数据库

具备高级上下文能力的聊天机器人

上下文工程设计、混合搜索、GraphRAG

自主 AI Agent

推理、规划、任务执行

2026 年的 AI 呢?

付诸实践

Terry：我要申请车祸理赔

AI：欢迎使用 AnyCompany Insurance。请描述事故经过并上传证明材料

➡ *人工对接……*

Terry：今早出了一场小车祸。

AI：别难过 Terry。下面就让我来协助您申请事故理赔吧

➡ *自主执行任务……*

Agentic AI 基础架构

推理

通过调用**大语言模型**来理解
用户请求，制定实施计划，
并确定下一步操作

Agentic AI 基础架构

推理

通过调用**大语言模型**来理解
用户请求，制定实施计划，
并确定下一步操作

实施

根据大语言模型的响应，
使用**杨抄**
实施操作，
并保存结果

Agentic AI 基础架构

推理

通过调用**大语言模型**来理解
用户请求，制定实施计划，
并确定下一步操作

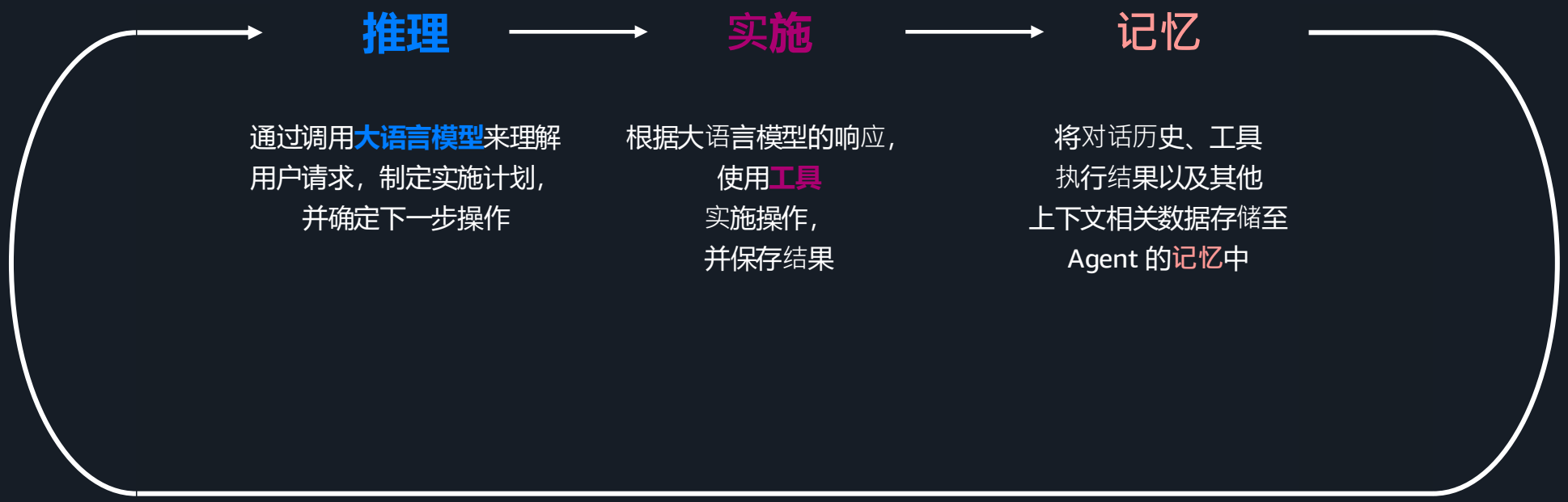
实施

根据大语言模型的响应，
使用**工具**
实施操作，
并保存结果

记忆

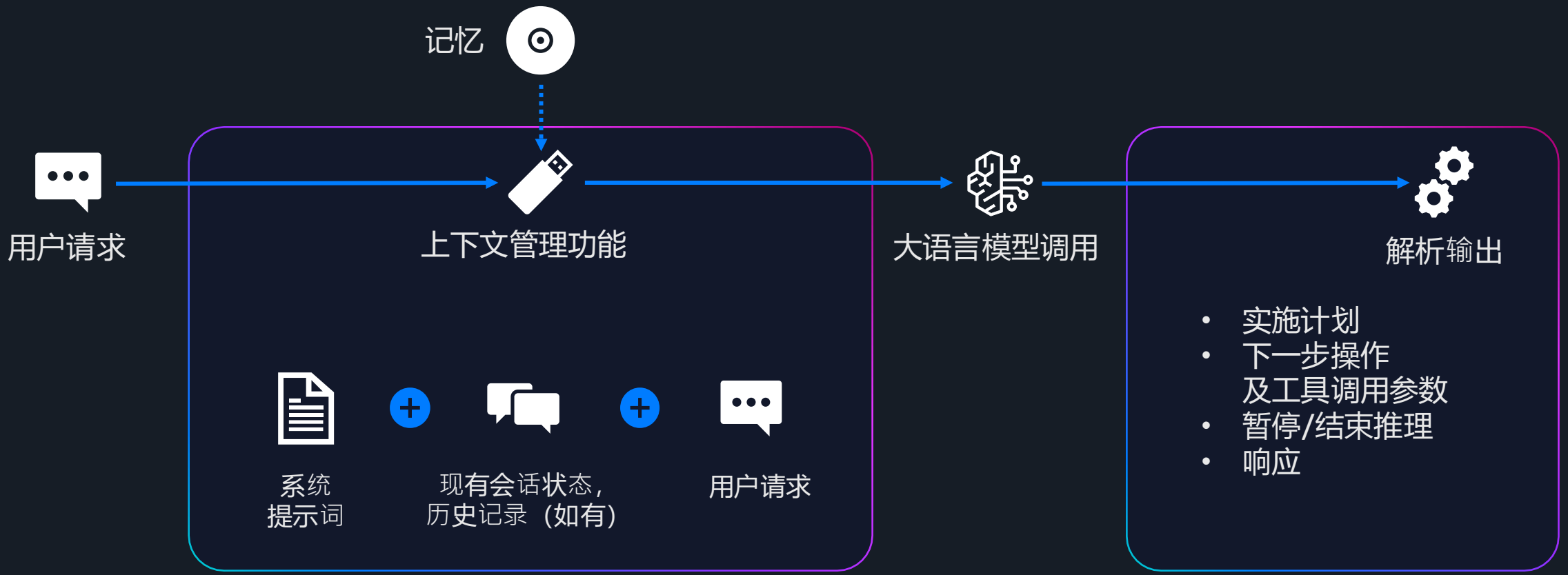
将对话历史　工具
执行结果以及其他
上下文相关数据存储至
Agent 的记忆中

ReAct 循环

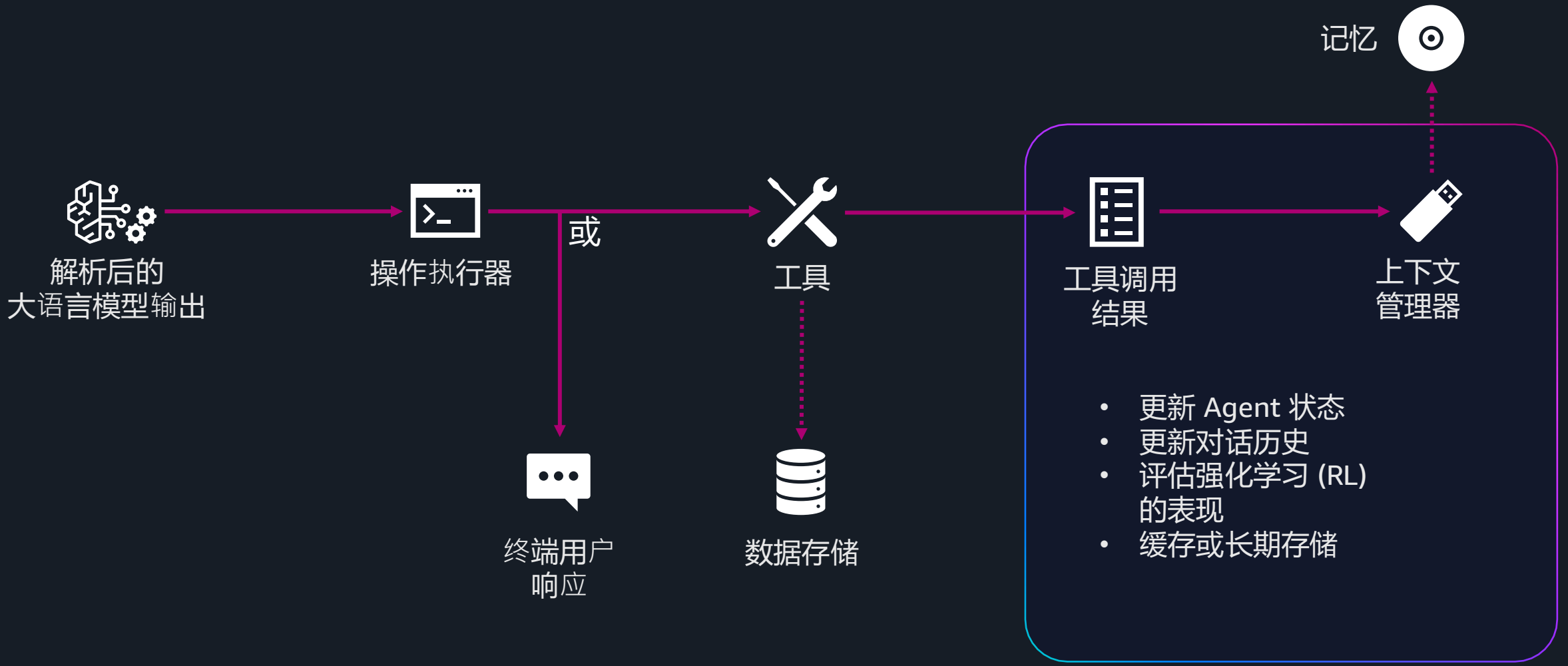


ReAct 循环

推理与规划



实施操作与管理上下文



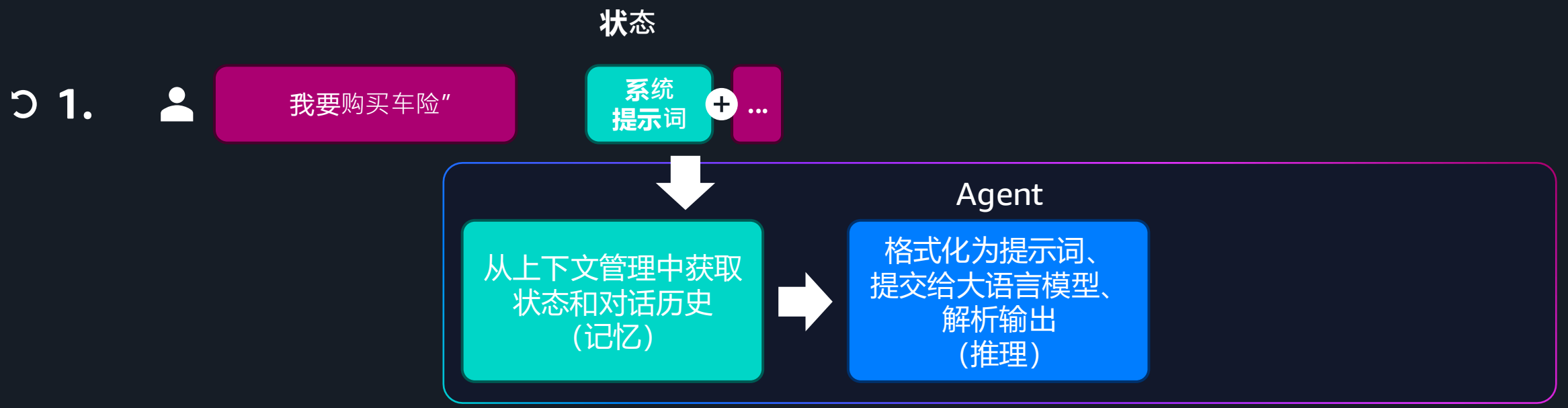
*前述特定亚马逊云科技生成式人工智能相关的服务目前在亚马逊云科技海外区域可用。亚马逊云科技中国区域相关云服务由西云数据和光环新网运营，具体信息以中国区域官网为准。

通过 ReAct 循环获取报价

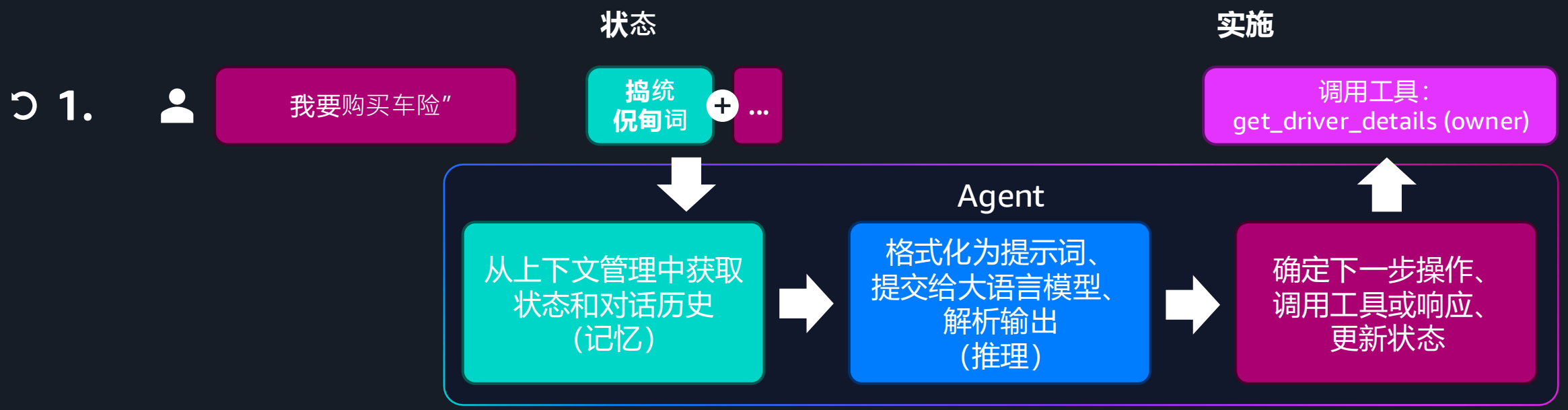
1. “我要购买车险”

通过 ReAct 循环获取报价

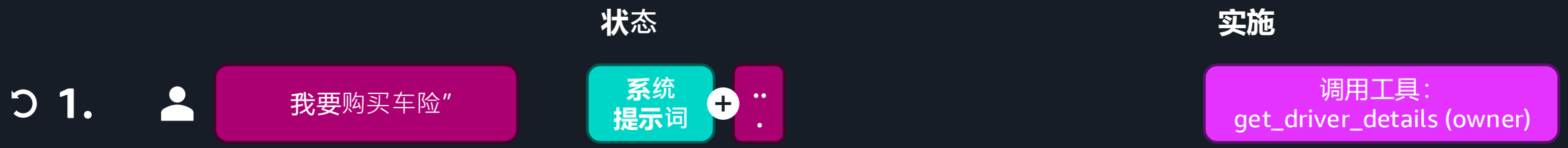
通过 ReAct 循环获取报价



通过 ReAct 循环获取报价



通过 ReAct 循环获取报价



通过 ReAct 循环获取报价

通过 ReAct 循环获取报价

通过 ReAct 循环获取报价

通过 ReAct 循环获取报价

通过 ReAct 循环获取报价

记忆组件

短期

当前任务或当前会话（线程）

长期

当前用户或应用全局持久存在

Agent 状态

实施计划、循环之间共享的数据、草稿内容

核心信息

对话历史、消息序列

通常使用
依赖 Agentic 框架
的后端数据存储

构建者缺乏控制

记忆组件

短期

当前任务或当前会话（线程）

长期

当前用户或应用全局持久存在

Agent 状态	核心信息	语义	档案	情节
实施计划　循环之间共享的数据　草稿内容	对话历史、消息序列	与请求任务相关的语义上下文	用户画像及类似数据	历史交互和输出 (RL)

通常使用
依赖 Agentic 框架
的后端数据存储

构建者缺乏控制

通常**使用工具**在向量
数据存储库和企业数据库中
进行检索

数据可访问性和质量

记忆组件

短期

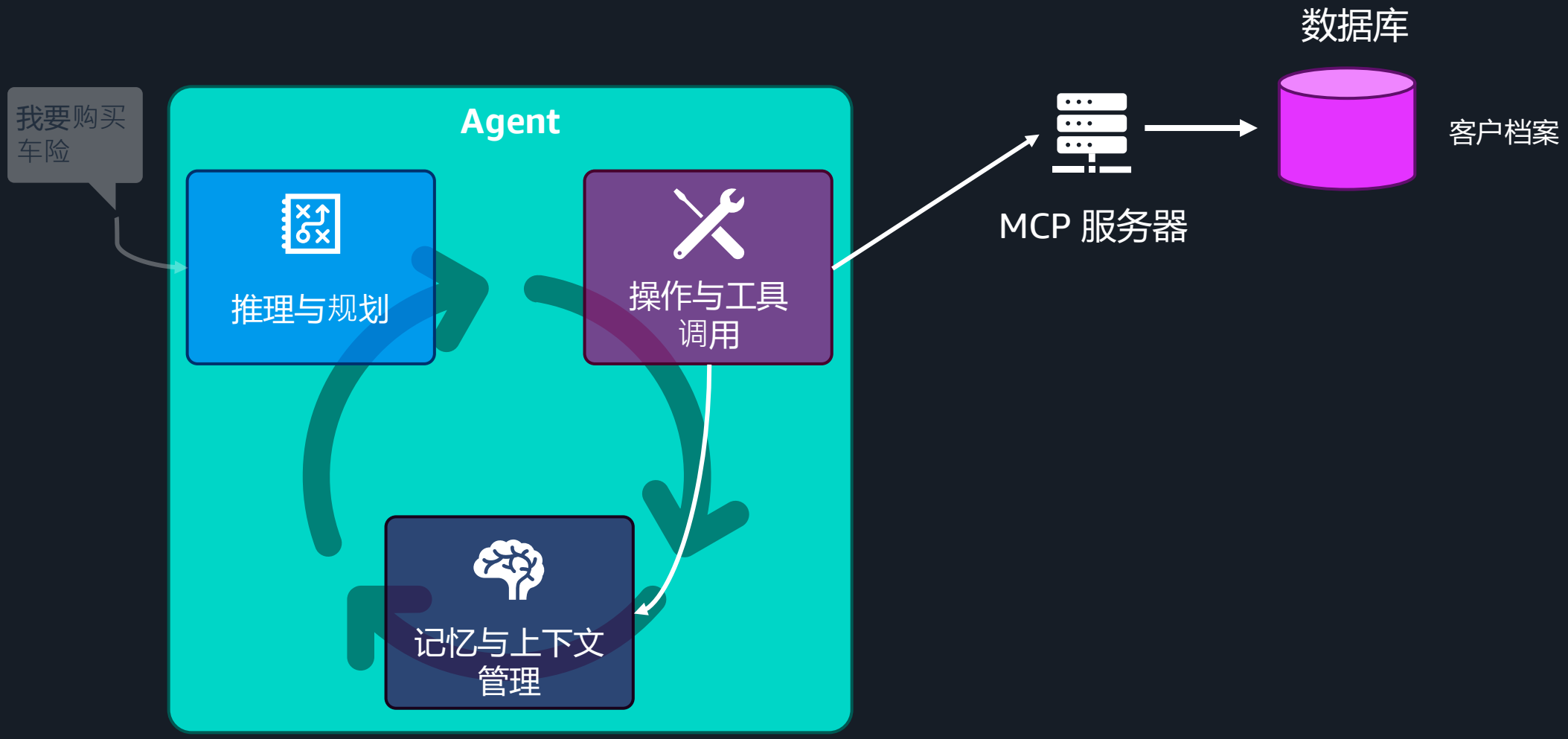
当前任务或当前会话（线程）

长期

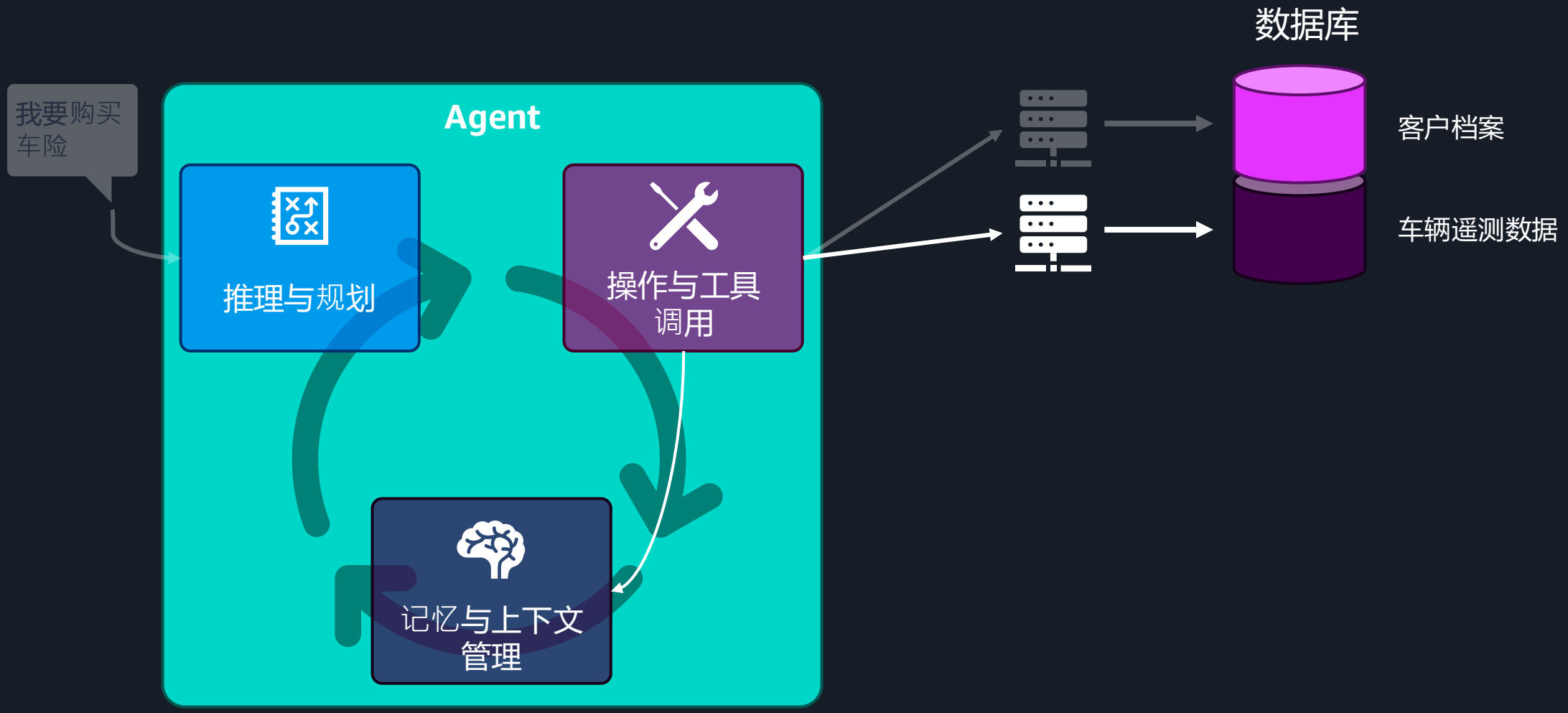
当前用户或应用全局持久存在

Agent 状态	核心信息	语义	档案	情节	提示词
实施计划、循环之间共享的数据、草稿内容	对话历史、消息序列	与请求任务相关的语义上下文	用户画像及类似数据	历史交互和输出 (RL)	系统提示词、指令
通常使用 俯□ Agentic 殰另 的后端数据存储		通常**使用工具**在向量数据存储库和企业数据库中进行检索			根据应用代码、文件或键值存储进行版本控制
构建者缺乏控制		数据可访问性和质量			提示词调参

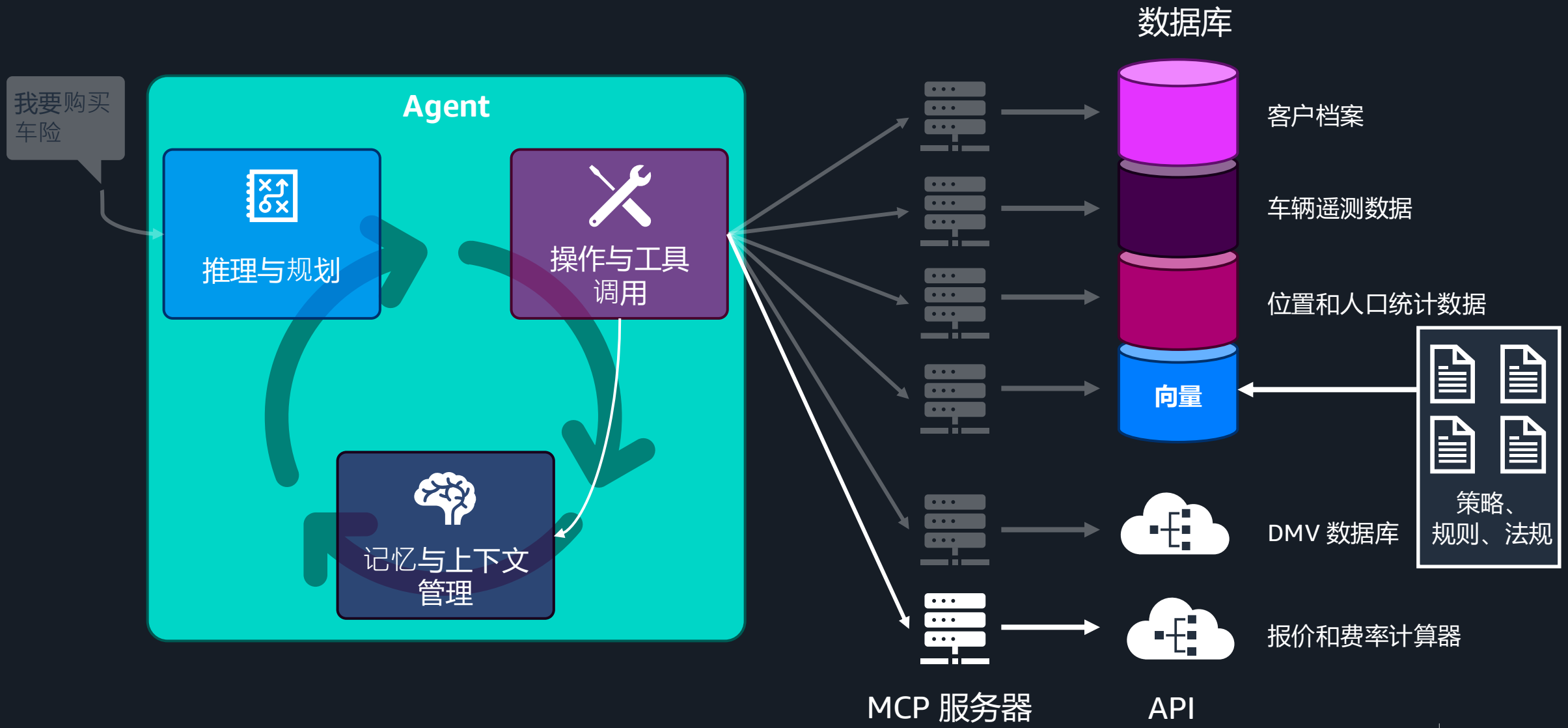
连接 Agent 与数据



□谈 Agent 寘补衷



连接 Agent 与数据



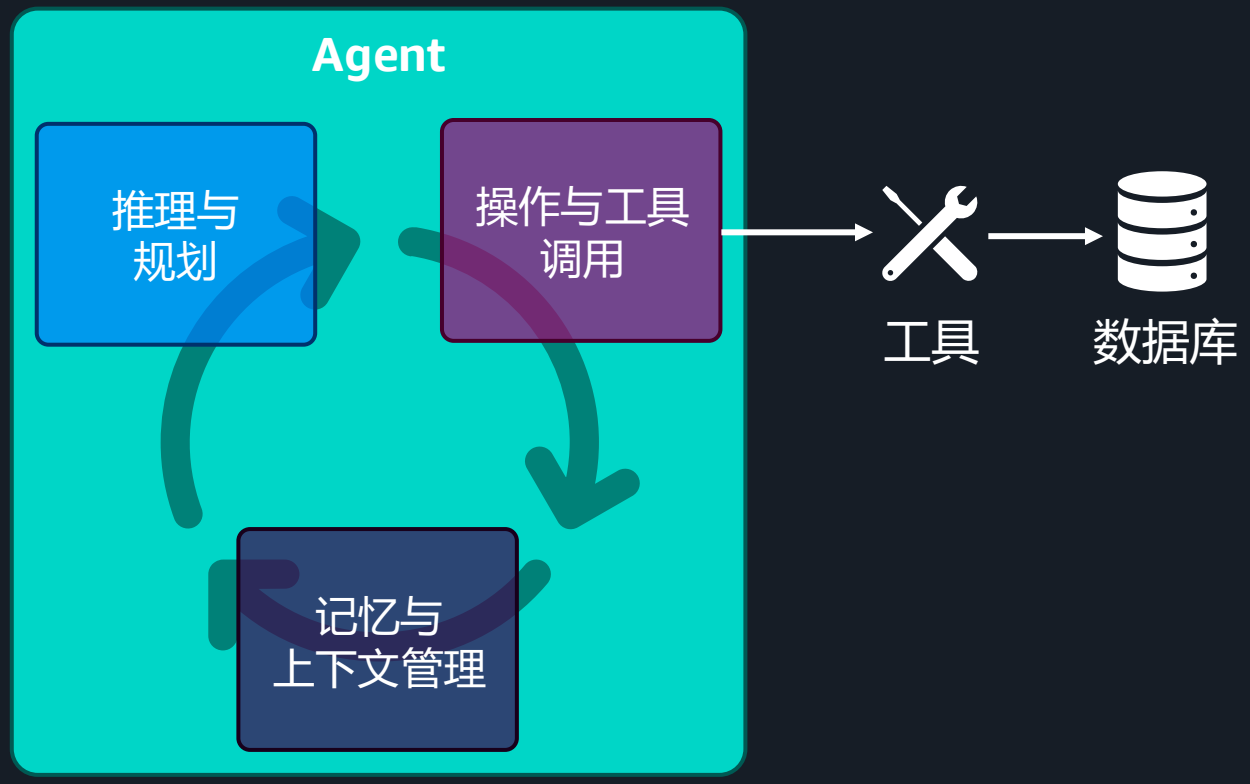
Agentic AI 应用程序中的缓存

减少响应延迟

避免调用大语言模型（降低成本）

减轻后端系统负载

集成强化学习 (RL) 反馈回路



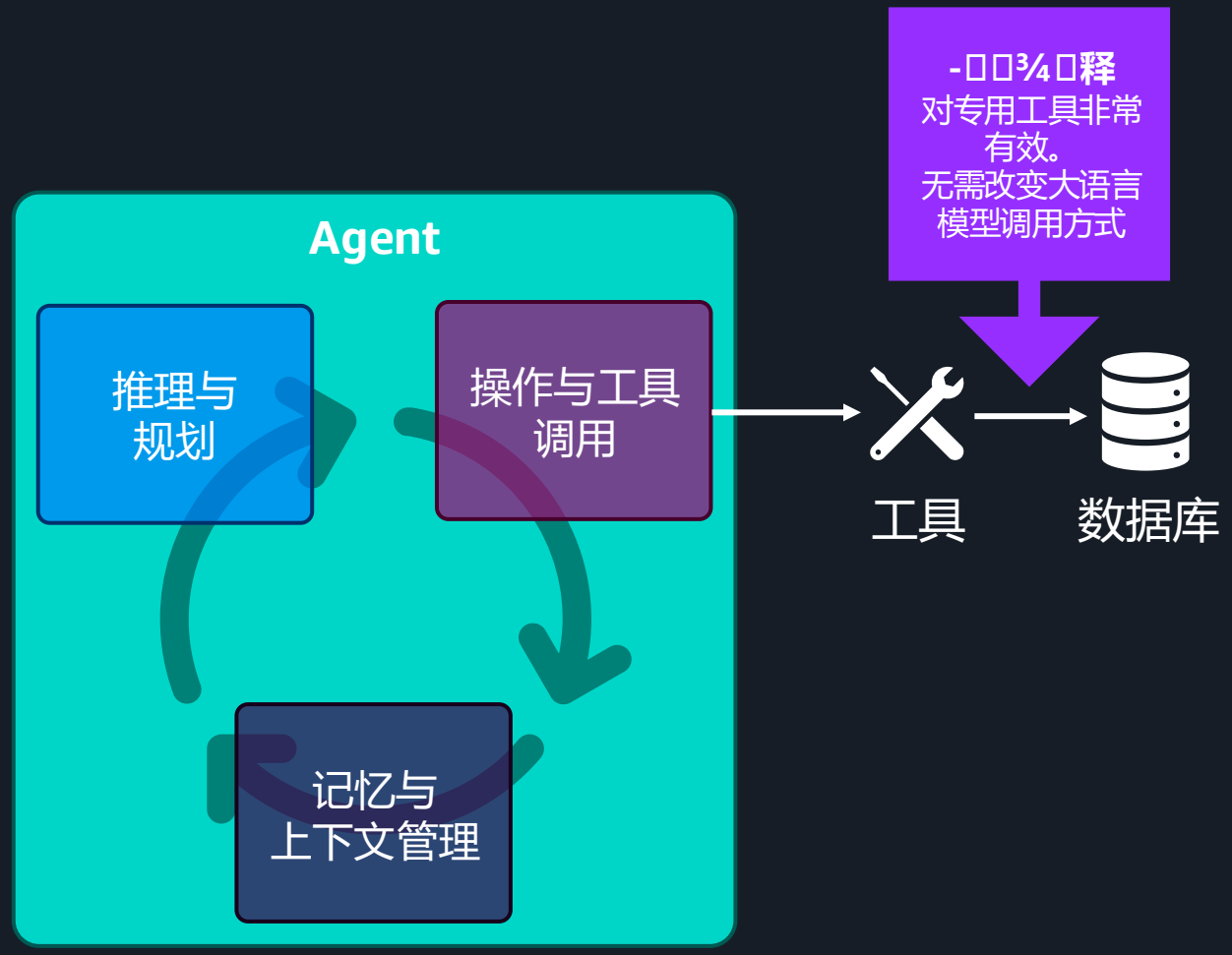
Agentic AI 应用程序中的缓存

减少响应延迟

避免调用大语言模型（降低成本）

减轻后端系统负载

集成强化学习 (RL) 反馈回路



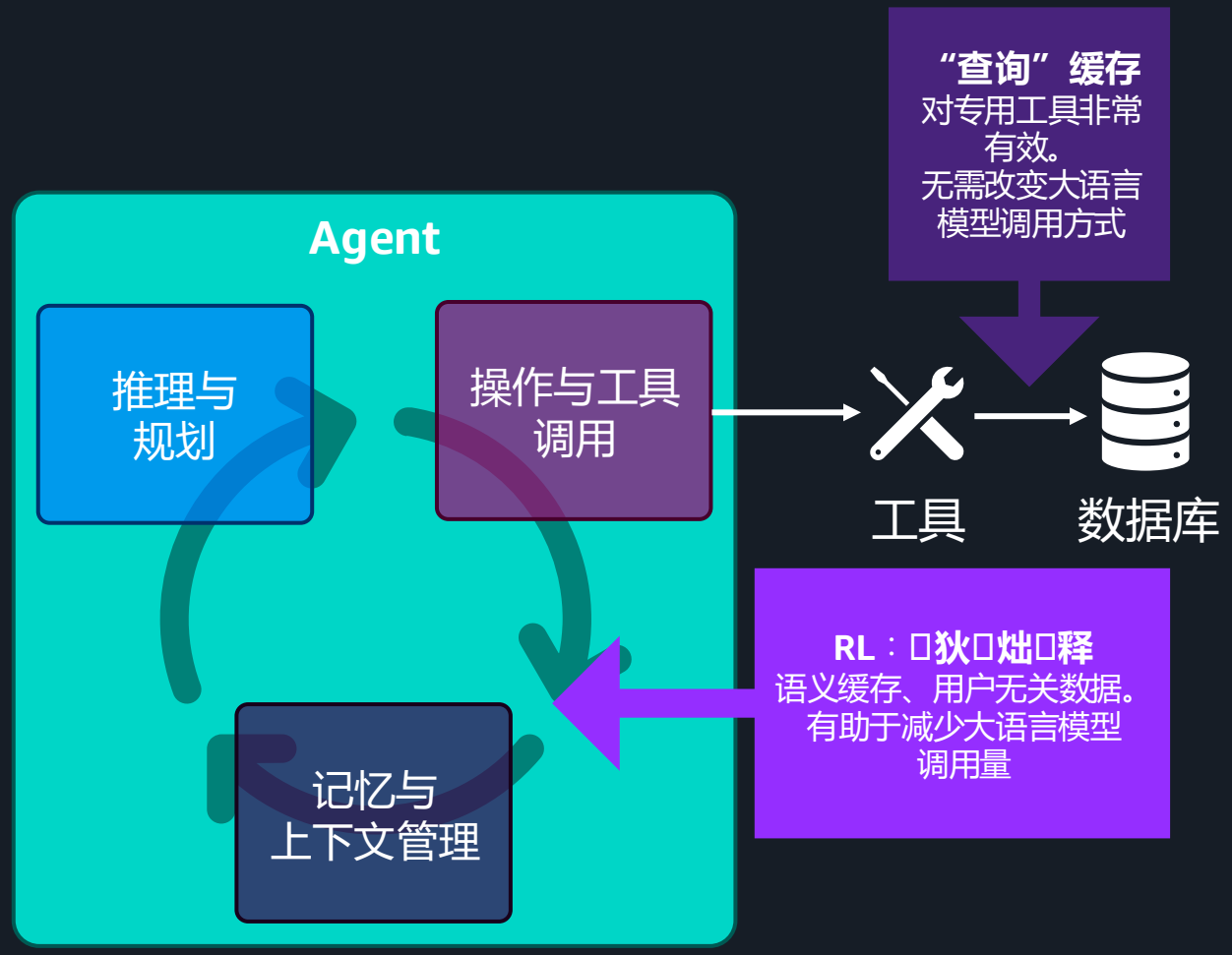
Agentic AI 应用程序中的缓存

减少响应延迟

避免调用大语言模型（降低成本）

减轻后端系统负载

集成强化学习 (RL) 反馈回路



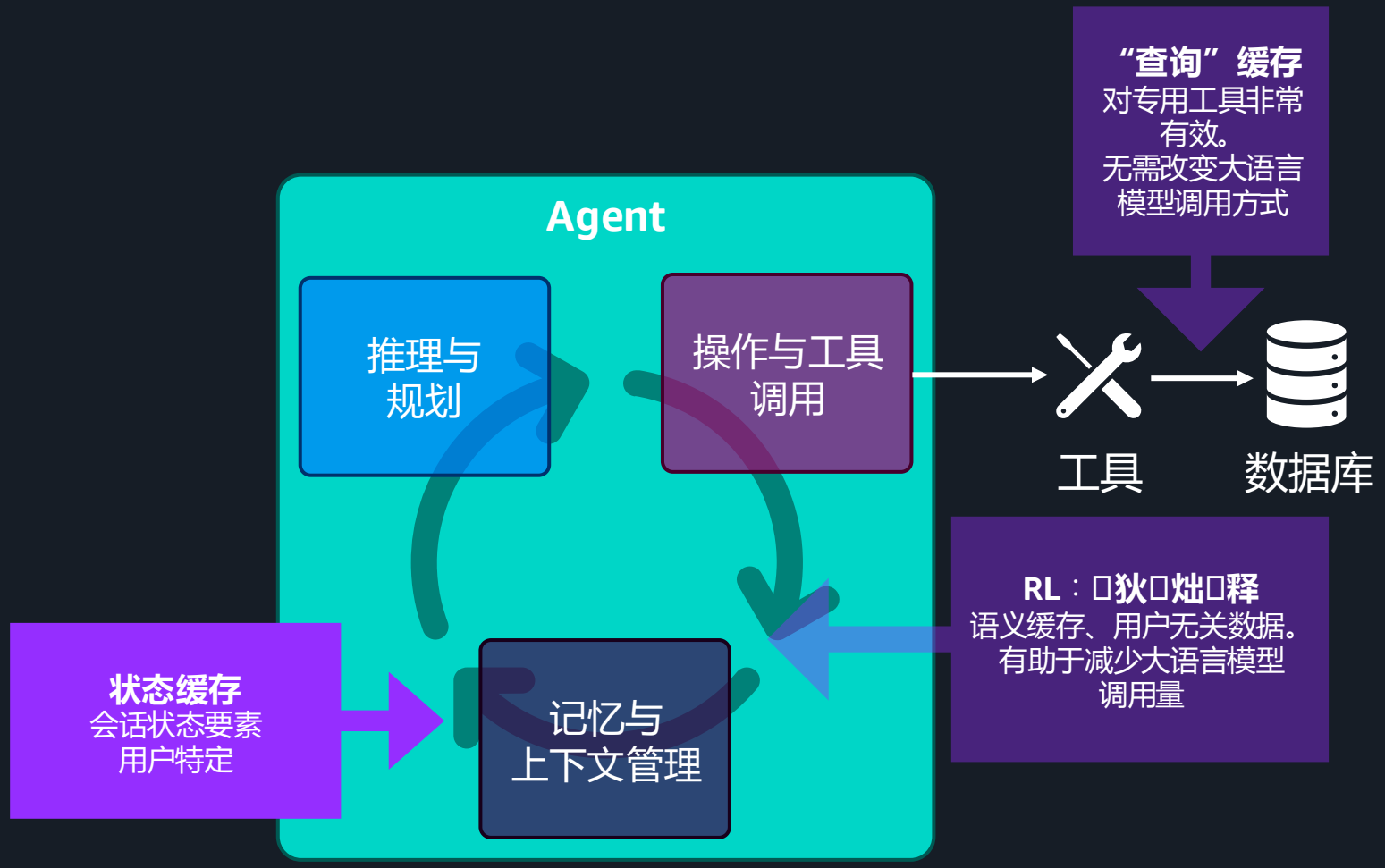
Agentic AI 应用程序中的缓存

减少响应延迟

避免调用大语言模型（降低成本）

减轻后端系统负载

集成强化学习 (RL) 反馈回路



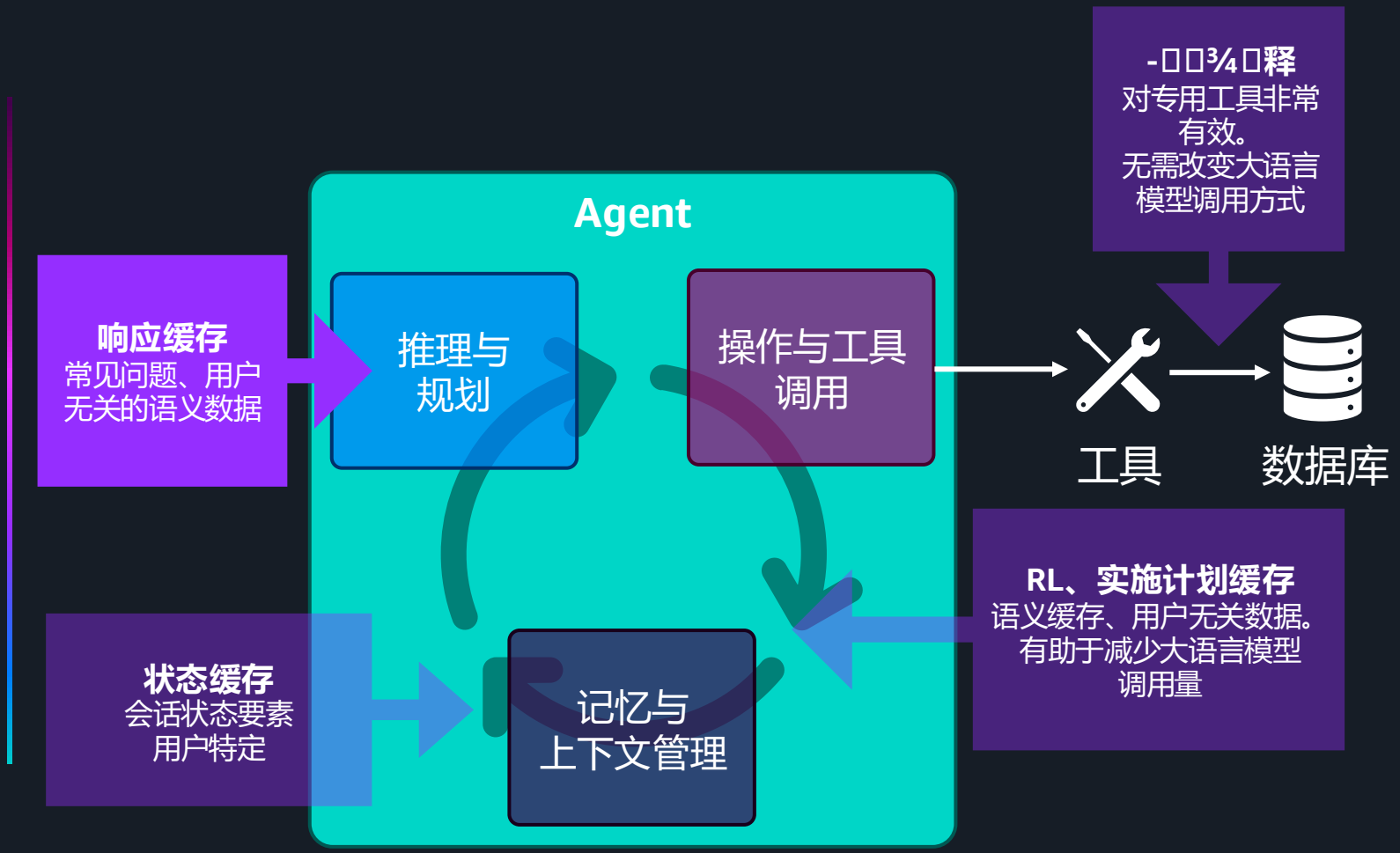
Agentic AI 应用程序中的缓存

减少响应延迟

避免调用大语言模型（降低成本）

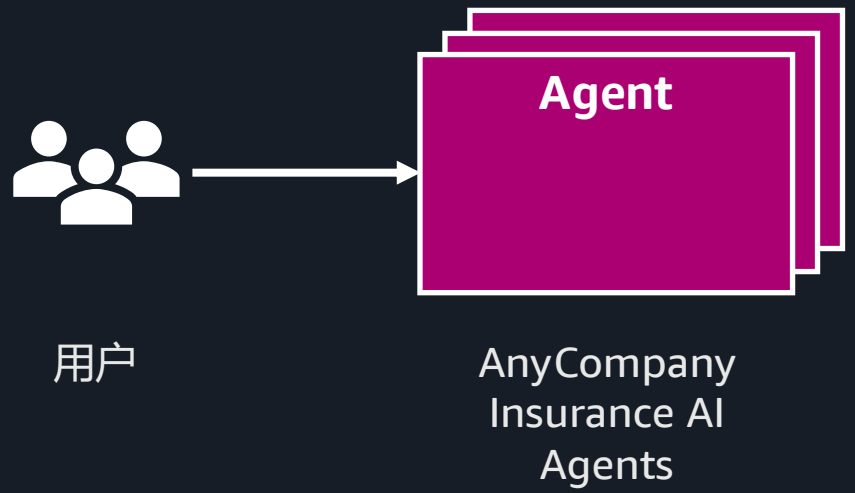
减轻后端系统负载

集成强化学习 (RL) 反馈回路



模型上下文协议 (MCP)

标准化 Agent 与数据源的交互

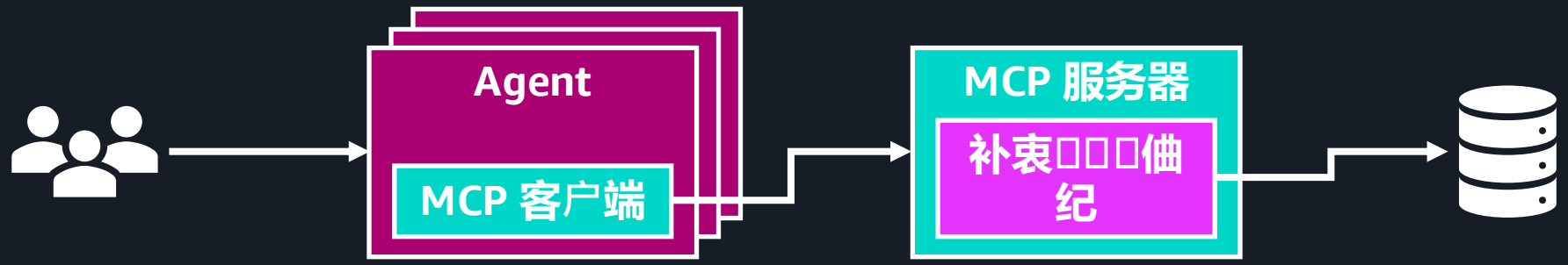


模型上下文协议 (MCP)

标准化 Agent 与数据源的交互

模型上下文协议 (MCP)

标准化 Agent 与数据源的交互



用户

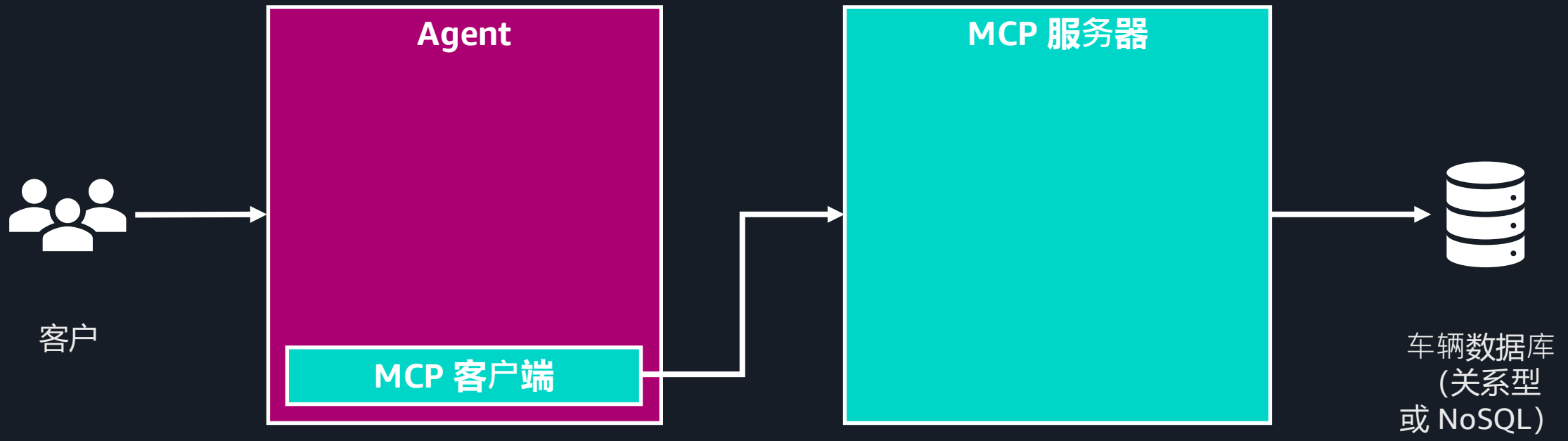
AnyCompany Insurance AI Agents

车辆数据 MCP 服务器工具：

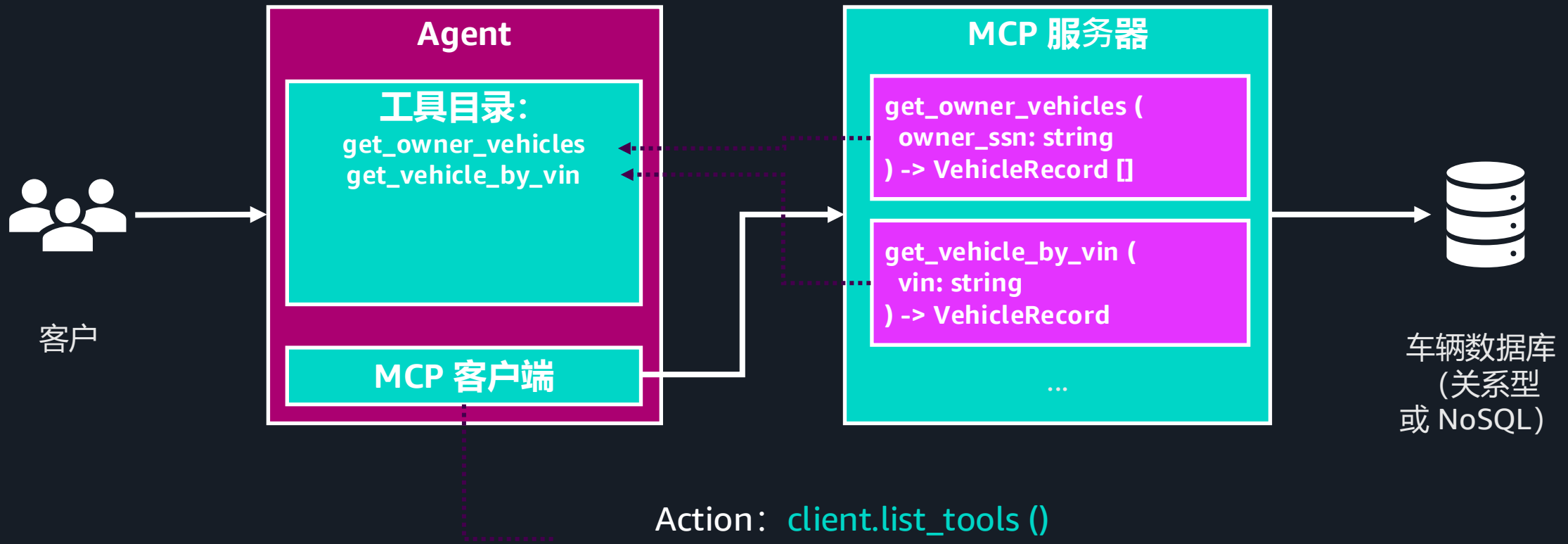
get_owner_vehicles (ssn)
get_vehicle_by_vin (vin)
get_vehicle_telemetry (vin)
...

车辆数据库（关系型或 NoSQL）

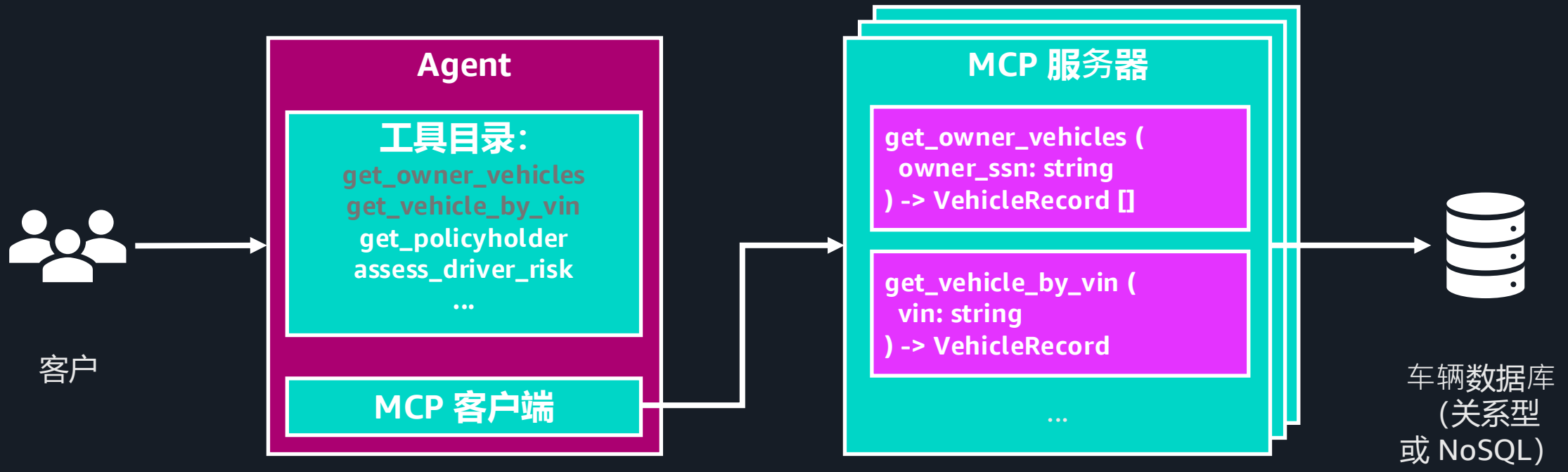
MCP 和工具



MCP 和工具



MCP 和工具



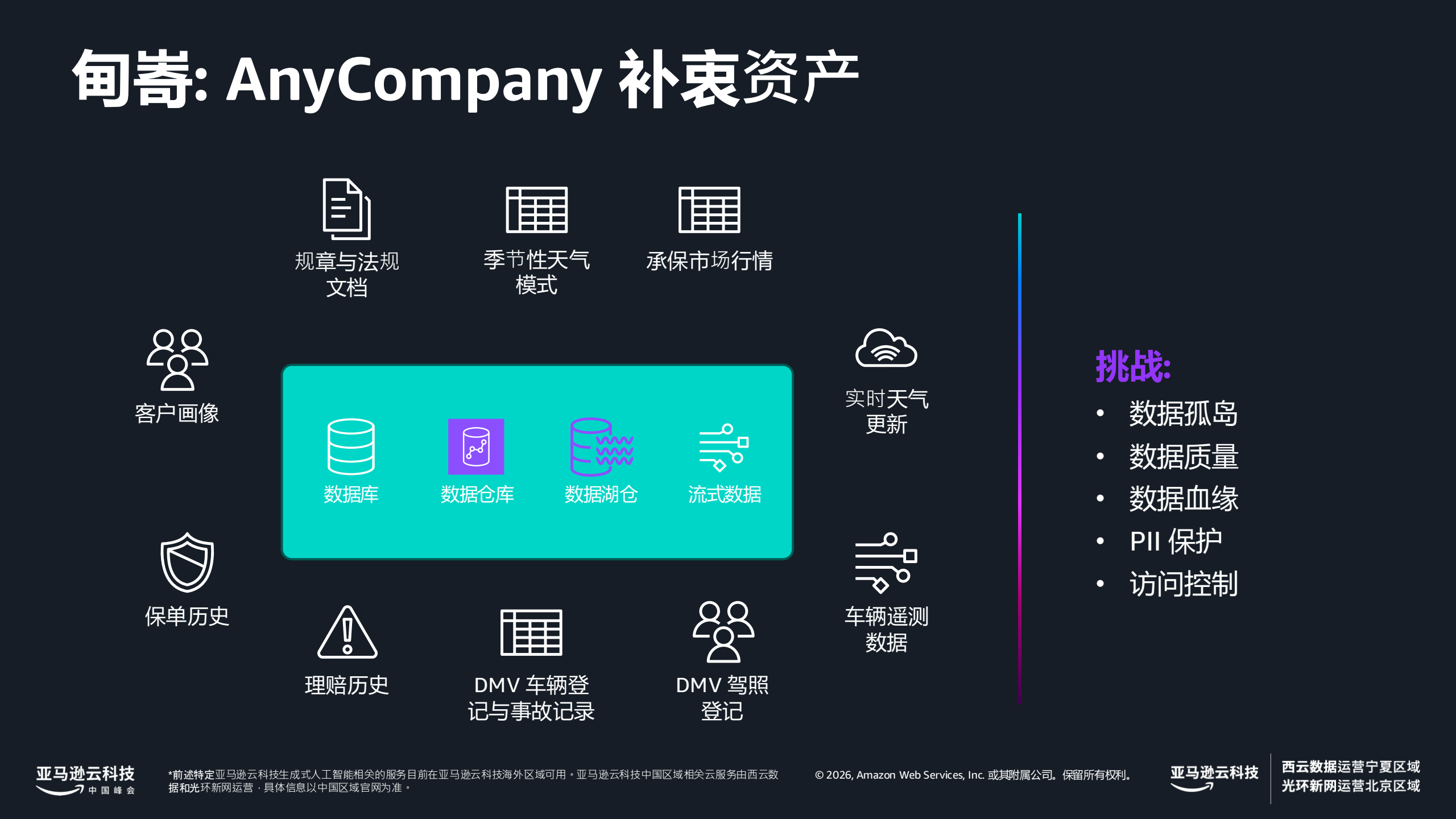
亚马逊云科技
中国峰会

Agentic AI 的数据底座

补衷尴界確岑?

*前述特定亚马逊云科技生成式人工智能相关的服务目前在亚马逊云科技海外区域可用。亚马逊云科技中国区域相关云服务由西云数据和光环新网运营，具体信息以中国区域官网为准。

甸嵩: AnyCompany 补衷资产



挑战:

- 数据孤岛
- 数据质量
- 数据血缘
- PII 保护
- 访问控制

数据市场 Data Marketplace

数据消费方

发现
订阅
衍生数据集
构建 API 与工具

数据产品、工具市场

数据生产方

发布
血缘
质量控制
分类
访问控制

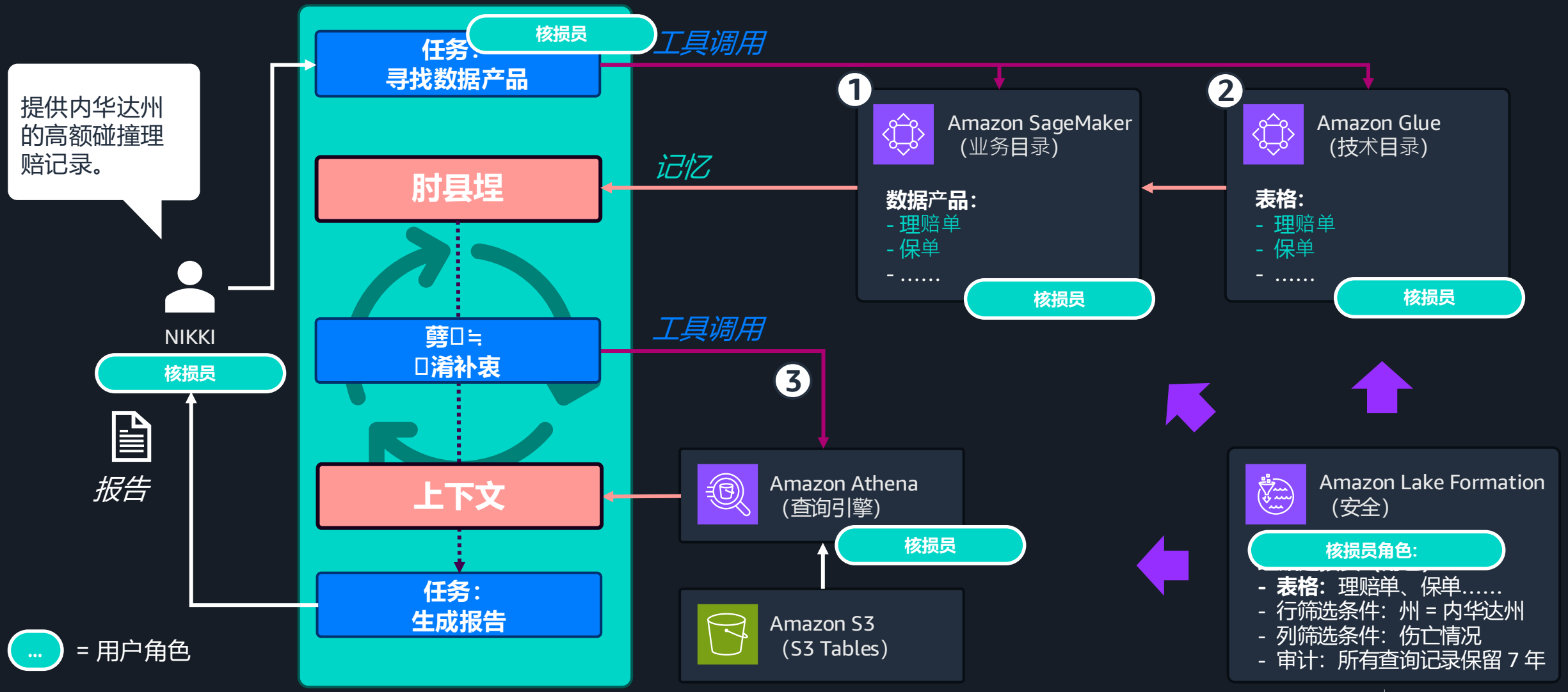
Step1: 构建数据产品市场

Step 2: 封装数据 API

Step 3: 将 API 暴露成 MCP 工具 / Skills

Agent 自主选择工具 / Skills

Agentic AI 数据消费方体验

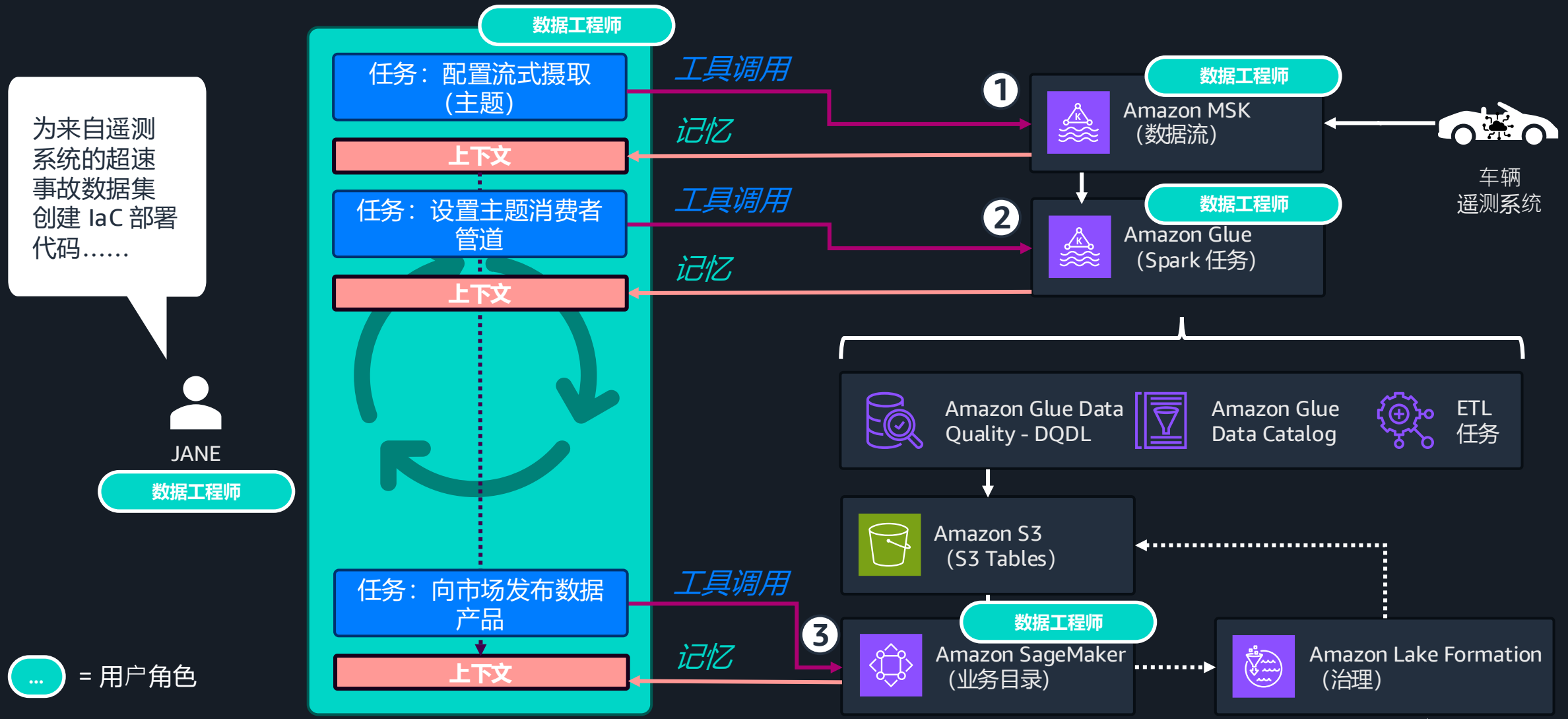


Agentic AI 数据消费方关注重点

数据产品的信任、安全与性能

1. **数据质量**：在 SageMaker Catalog 中查看数据质量和血缘关系
2. **补衷发□□觉**：根据 SageMaker Catalog 中的元数据和业务术语表搜索数据
3. **数据访问**：使用可信身份传播，基于用户身份定义访问策略
4. **安全**：利用 Lake Formation 中的细粒度访问控制移除敏感数据
5. **低延迟数据访问**：使用 Glue Materialized Views 基于访问模式预计算数据

Agentic AI 数据生产方体验



Agentic AI 数据生产方关注重点

数据控制和准确性

1. **准确性**：利用 SageMaker Data Agent 辅助构建管道，并保留最终验证环节
2. **数据质量**：使用 Glue Data Quality 在管道中嵌入数据质量规则
3. **有意义的数据**：在 SageMaker Catalog 中通过定制化列级元数据和标签为数据增加上下文
4. □□：跟踪并监控使用情况，利用目录元数据验证用途是否符合预期

确保 AI Agent 交互安全

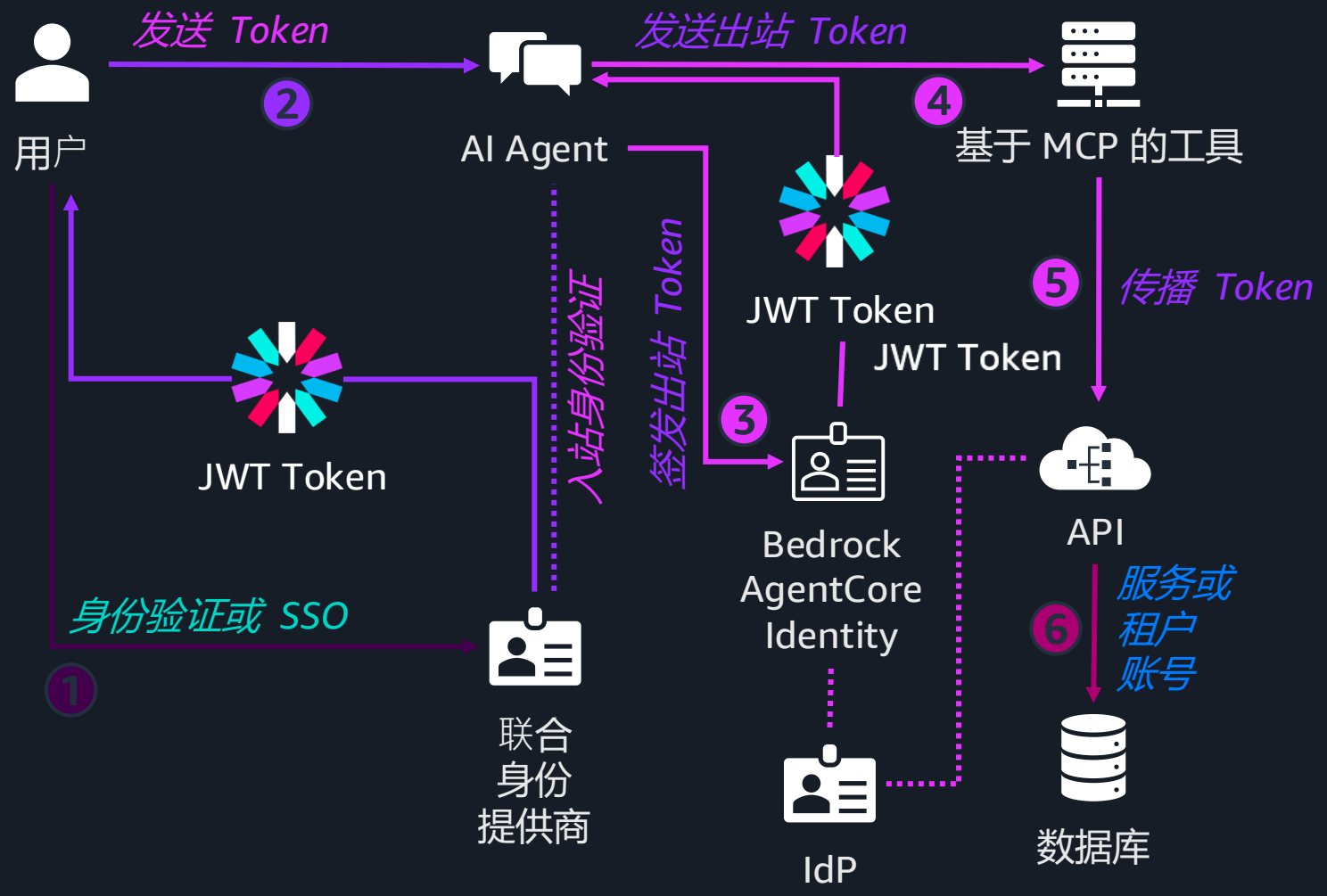
Amazon Identity and Access Management (IAM)

授权访问托管在亚马逊云科技托管服务上的工具、Agent 和数据（如 Bedrock AgentCore、LakeFormation）

OpenID Connect 和 OAuth2

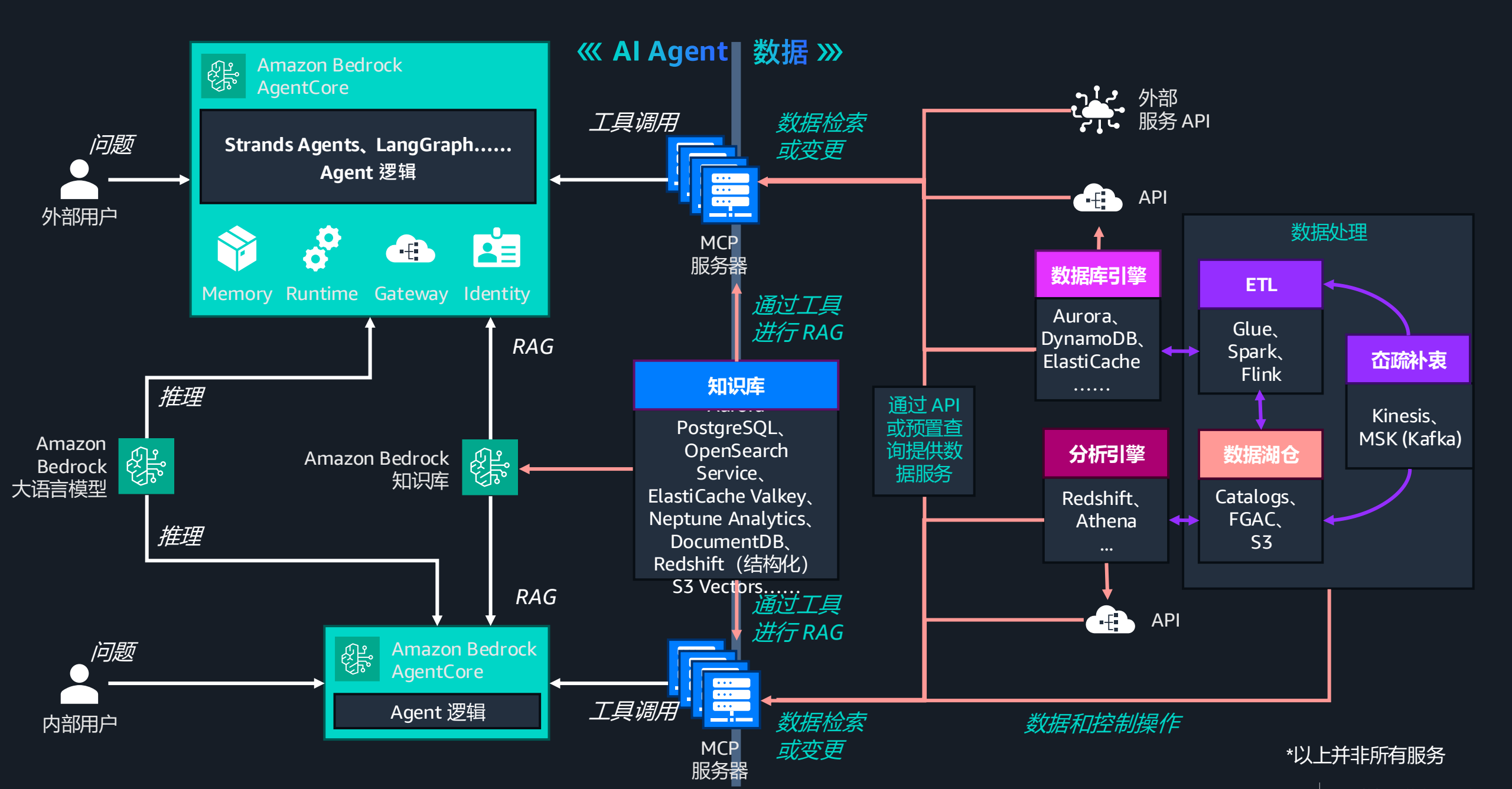
式渚 Y 窟嘗环葛对 MCP 慌务蓋　Agent 快慌务进請窓ъ验证快访问倦洪 ぜJWT 访问快 ID Tokenそ

确保 Agent 和工具调用安全



单个逻辑应用程序，
同一身份提供商

多个应用程序，
多个身份提供商



行动倡议

使用 API
封装数据

使用 MCP
连接 API 与 Agent

补衷田屣
寞震糪震
依跳覆笑馆勰笑

利用
亚马逊云科技服务
简化运维

亚马逊云科技
中国峰会

Thank you