

# AI 技术每日分析：多 Agent 协作、隐私记忆与混合执行

中国高技术产业发展促进会新质生产力工作委员会

博雅云创 & 中科创新驱动

2026 年 9 月 25 日

## 摘要

今天 AI 技术方向最值得关注的，不是单一模型刷新榜单，而是“多智能体协作、隐私记忆、本地 Agent、企业协作入口与数据 workflow”同时成熟。Anthropic 公布 Project Swap，用 201 名员工与 Claude Agent 构建受控交换市场，验证大模型是否能够在真实偏好、信息不完全和多方谈判环境中形成有效协作；Google DeepMind 为 Private AI Compute 加入安全的服务器端长期记忆，在保持密钥由用户个人设备掌控的同时，让跨设备 AI 服务获得连续上下文；Google Antigravity SDK 加入本地模型支持，首次把“云端规划 + 本地执行”做成开发者可直接使用的混合 workflow；新创公司 Ando 获得 2000 万美元融资，试图用“人和 Agent 共享频道、身份、收件箱”的方式重新设计团队沟通；Databricks 则收购 Row Zero，把 AI Agent 与电子表格和企业数据平台进一步连接。AI 正在从“模型即产品”进入“模型 + 记忆 + 本地执行 + 协作界面 + 数据入口”的系统竞争阶段。

## Contents

|                                                         |   |
|---------------------------------------------------------|---|
| 一、Anthropic Project Swap：多智能体协作开始进入真实偏好和交换机制            | 2 |
| 二、Google 给 Private AI Compute 加入“服务器端记忆”：连续上下文与隐私开始同时设计 | 2 |
| 三、Antigravity SDK 支持本地模型：云端规划、本地执行成为可用架构                | 3 |
| 四、Ando 获得 2000 万美元融资：团队协作软件开始为“人和 Agent 共事”重新设计         | 4 |
| 五、Databricks 收购 Row Zero：Agent 开始深入“电子表格 + 企业数据”的最后一公里  | 5 |
| 趋势观察                                                    | 5 |
| 参考文献                                                    | 5 |

## 一、Anthropic Project Swap：多智能体协作开始进入真实偏好和交换机制

9 月 24 日，Anthropic 发布 Project Swap 研究，构建了一个受控的“交换市场”，让 201 名 Anthropic 员工与 Claude Agent 参与书籍交换。每位参与者先用约 5 分钟与 Agent 对话，Agent 据此推断其对书籍的偏好；随后 Agent 代表用户与其他 Agent 持续谈判和交易。

研究显示，仅靠短时间对话得到的偏好排序，Agent 在书籍二选一上与真人选择的一致率约 61%。在交易阶段，Agent 能够形成多轮、多方交换，并在多数运行中提升参与者整体满意度。Anthropic 还发现，模型能力差异对市场效率的影响明显高于单纯 Prompt 差异，能力更强的模型更容易发现复杂交易链。

这项研究把 Agent 从单用户工具带入多主体经济环境。企业未来真正复杂的 Agent 场景，本质上也是资源交换：不同部门争夺预算、算力、排期、库存、销售线索或设备时间。如果 Agent 能够理解个人偏好、组织约束和交易成本，就可能承担部分跨部门协调工作。

但 Project Swap 也暴露了一个关键限制：Agent 缺少完整的参与者状态和外部信息时，无法发现所有潜在交易。多智能体系统的关键瓶颈在于共享状态、权限、身份和可验证信息。

## 二、Google 给 Private AI Compute 加入“服务器端记忆”：连续上下文与隐私开始同时设计

Google DeepMind 近期为 Private AI Compute 加入安全服务器端记忆机制。与普通云端记忆不同，该设计把用户记忆存储在加密数据库中，解密密钥只由用户个人设备掌握；服务器端只能在受硬件保护的安全执行环境中处理已经授权的上下文。

DeepMind 强调，个人设备会与安全 Enclave 建立经过认证的端到端加密通道，服务器软件也通过公开、不可篡改的记录接受验证。其目标是在多设备之间提供连续 AI 体验，同时避免云端服务方直接获得长期记忆明文。

这一方向很重要，因为个人 AI 要提供实用价值，需要保存连续上下文：记得用户长期项目、文档、行程、偏好和工作状态。但记忆越强，隐私风险越高。过去很多产品把“记忆”理解为一个数据库功能，未来则必须把密钥控制、授权、删除、跨设备同步和可审计性一起设计。

这也意味着“隐私 AI”不会简单等同于“所有模型都在本地跑”。更现实的架构可能是：敏感密钥和高价值状态由本地控制，重计算在受保护的云端完成，二者通过可信执行环境和加密协议协作。

### 三、Antigravity SDK 支持本地模型：云端规划、本地执行成为可用架构

Google Developers 为 Antigravity SDK 加入本地 AI 模型支持，首批支持 Gemma 4 26B A4B，并通过 LiteRT 在本地硬件运行。开发者可以让 Agent 在无网络环境下完成代码审阅、补丁生成和其他任务，也可以把云端模型与本地模型组合成混合 Agent。

Google 展示的示例中，云端 Gemini 3.8 Flash 只负责高层规划，且不读取源代码；真正的大量代码分析与修改由本地模型完成。该案例中约 97.2% 的 Token 在本地处理，云端只使用约 95 个 Token 进行规划。SDK 也支持通过 OpenAI 兼容接口连接 Ollama、LM Studio、vLLM 等本地服务。

这种架构对企业意义很大。大量代码、设计文档、客户数据和内部知识不适合直接发送到外部模型，但企业又希望使用更强的云端推理能力。把“规划”与“执行”拆开，就能让云端模型只处理抽象任务描述，本地

模型处理敏感数据。

未来 Agent 很可能不是“选一个模型”，而是根据任务分层路由：云端强模型负责复杂推理，本地模型负责数据密集型操作，小模型负责分类和控制，从而同时优化隐私、成本与延迟。

## 四、Ando 获得 2000 万美元融资：团队协作软件开始为“人和 Agent 共事”重新设计

9 月 24 日，团队消息创业公司 Ando 宣布走出隐身状态，已获得约 2000 万美元 Pre-seed 和 Seed 融资，投资方包括 Accel、Index Ventures 和 Emergence。与给 Slack 增加一个 Bot 不同，Ando 从产品底层就把 Agent 作为“团队成员”设计。

在 Ando 中，Agent 拥有自己的身份、收件箱、频道权限和直接消息，也可以进入实时对话，并在无需每次 @ 的情况下主动理解团队上下文、提醒需要人类处理的问题。公司称已经在软件、房地产和金融等行业拥有来自 15 个国家的客户，当前客户以中小团队为主。

这一设计代表一个值得关注的产品方向：企业 Agent 如果始终被放在聊天窗口的侧边栏里，就很难真正参与组织协作。它需要知道谁负责什么、哪个频道属于哪个项目、什么信息可以主动推送、什么动作需要批准。

未来 Slack、Teams、邮件和项目管理软件的边界可能进一步模糊。协作平台的核心不再只是“人和人沟通”，而会变成“人、Agent 和业务系统共享上下文并协调任务”。

## 五、Databricks 收购 Row Zero: Agent 开始深入“电子表格 + 企业数据”的最后一公里

9 月 24 日, Databricks 收购电子表格创业公司 Row Zero, 交易金额未披露。Row Zero 主打类似 Excel/Google Sheets 的交互体验, 但可以直接连接大规模企业数据平台, 避免财务和业务团队为了分析数据而把敏感数据导出到普通电子表格。

Databricks 称, 一些客户已经将 Row Zero 与 Genie AI Agent 结合使用, 让业务人员在熟悉的表格界面中查询和处理 Databricks 数据。对很多企业而言, 电子表格仍然是预算、运营、销售和财务分析的最终工作界面, 因此“Agent+ 表格”比单纯自然语言问答更接近真实工作流。

这次收购也延续 Databricks 今年围绕 Agent 评测、强化学习和安全领域的并购布局。数据平台的竞争正在从“存储和计算数据”扩大到“Agent 如何理解、操作和解释数据”。

企业 AI 最终是否落地, 往往取决于它能不能进入现有工作工具。表格、邮件、IDE、协作软件和浏览器, 可能比新的独立 AI 应用更重要。

### 趋势观察

今天几条新闻共同说明, Agent 基础设施正快速“分层”。Project Swap 探索多 Agent 协作, Private AI Compute 解决长期记忆隐私, Antigravity 解决本地与云端模型协同, Ando 重构团队入口, Row Zero 则把 Agent 带进企业最常用的数据工具。AI 系统的核心竞争点, 正在从“模型有多聪明”转向“它能否安全地记住、协作、执行并进入真实工作流”。

### 参考文献

- \*\*Anthropic\*\* | 《Project Swap》 | 2026-09-24 | 核验 201 名参与者、多 Agent 交易机制与偏好匹配结果。

<https://www.anthropic.com/research/project-swap>

- **\*\*Google DeepMind\*\*** | 《Advancing Private AI Compute with secure server-side memory》 | 2026-09-23 | 核验加密记忆、设备密钥与安全 Enclave 设计。

<https://deepmind.google/blog/advancing-private-ai-compute-with-secure-server-side-memory/>

- **\*\*Google Developers Blog\*\*** | 《Introducing support for local AI models in the Antigravity SDK》 | 2026-09-23 | 核验本地 Gemma、LiteRT 和云端规划/本地执行模式。

<https://developers.googleblog.com/introducing-support-for-local-ai-models-in-the-antigravity-sdk/>

- **\*\*TechCrunch\*\*** | 《Ando eyes Slack as it builds team messaging platform for humans and agents to work together》 | 2026-09-24 | 核验 Ando 融资、Agent 身份和团队协作设计。

<https://techcrunch.com/2026/09/24/ando-eyes-slack-as-it-builds-team-messaging-platform-for-humans-and-agents-to-work-together/>

- **\*\*TechCrunch\*\*** | 《Databricks buys Row Zero and is scouting for more startups to acquire》 | 2026-09-24 | 核验 Row Zero 收购及与 Genie Agent 的结合。

<https://techcrunch.com/2026/09/24/databricks-buys-row-zero-and-is-scouting-for-more-startups-to-acquire/>

- **\*\*Help Net Security\*\*** | Anthropic 两周性能冲刺使 Claude.ai 速度提升约 3 倍 | 2026-09-24 | 背景资料，观察 AI 辅助软件工程。

<https://www.helpnetsecurity.com/2026/09/24/anthropic-claude-ai-faster/>

- **\*\*Reuters\*\*** | 《AI startup Island valued at \$6.4 billion in latest funding

round》 | 2026-09-24 | 背景资料，观察 AI Agent 安全带动企业安全市场。

<https://www.reuters.com/technology/ai-startup-island-valued-64-billion-latest-funding-round-2026-09-24/>

- **\*\*OpenAI\*\*** | 联合国安理会 AI 治理相关发言 | 2026-09-24 | 背景资料，观察前沿 AI 治理议程。

<https://openai.com/index/sam-altman-un-security-council-remarks/>

- **\*\*Reuters\*\*** | DeepSeek 年化收入运行率相关报道 | 2026-09-24 | 背景资料，观察开源模型商业化。

<https://www.reuters.com/world/china/deepseek-annualized-revenue-run-rate-hits-1-billion-sources-say-2026-09-24/>

- **\*\*Darktrace / 行业媒体 \*\*** | AI Agent 异常行为与安全监测相关研究 | 2026-09-24 | 补充 Agent 安全与运行时治理趋势。

# 联系我们，请扫描二维码



新质生产力工作委员会  
官方公众号



工业智能算网  
gyznsw.cn

## 新质生产力工作委员会：

中国高技术产业发展促进会新质生产力工作委员会，专注于推动工业人工智能、智能制造、数字化转型等前沿技术发展，为企业提供政策解读、技术咨询和产业对接服务。

## 工业智能算网：

专注于工业人工智能、新质生产力、工业软件 CAE、智能制造等前沿技术。提供每日动态分析、技术趋势解读、解决方案分享，推动工业智能化转型。

网站地址：<https://gyznsw.cn>