

玄武 Agent 中台： 企业级 AI 智能体从 Demo 到生产系统

——
安全可控、算力可运营、场景可复制的企业级 Agent 中台实践

演讲人：姚航

公司：清昂智能

职位：联合创始人兼COO



安全可控

权限完备可审计
数据不出域



算力可运营

资源统一纳营
成本可视可控



场景可复制

组件化 + 模板化
快速可用落地



价值可度量

效果可驱动
持续优化迭代



清昂智能：打造自主可控的 Agent Infra (AaaS)

让企业级 AI Agent 从“单点实验”走向“规模化生产”



成立于2022年
深耕自主可控 Agent 基础设施



全链路产品矩阵
玄武智算云 | MLGuider | Harness | Token工厂



顶尖复合团队
核心团队源自清华大学计算机系
成员来自交大、斯坦福、新国立、华为、阿里等



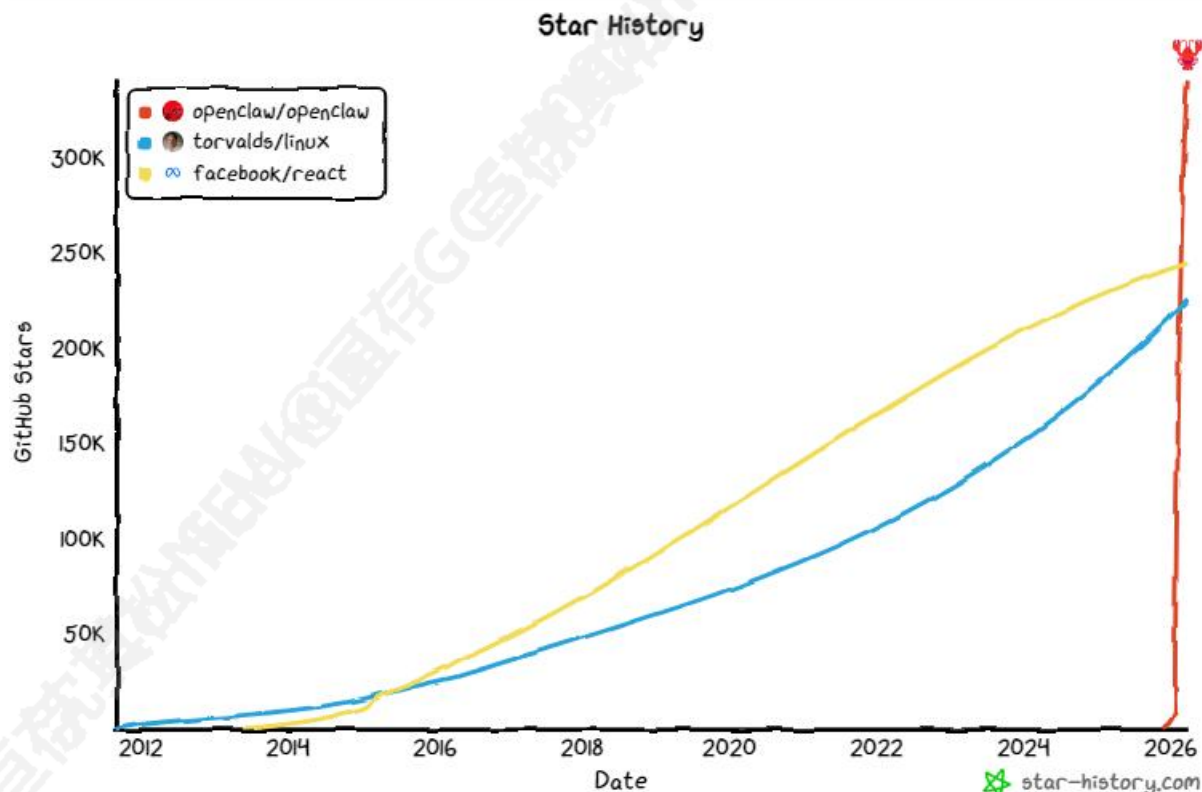
资本与产业认可
获得多家国内头部投资机构亿元级联合注资



让 **AGI** 触达世界每个角落

Agent成为新技术基座，能力拐点×形式拐点

核心判断：Agent 正从「单一应用」上升为软件与计算的新基座——类比移动时代的 OS 与应用生态，载体变为可执行任务的 Agent



共识：OpenClaw 与开发者

- ✓ 左图可见：相较 Linux、React 等长周期累积，OpenClaw 曲线在近端陡升，反映关注度与传播强度
- ✓ 共识：Agent 被视作新一代入口与执行载体，而非又一个 App

拐点：基座模型

- ✓ 约 2025 年末起：任务从「单步建议」走向规划—执行—校验—纠错的稳定闭环。
- ✓ 本质：从语言模型走向决策与行动（agency），且可规模化复用。

能力 × 形式 → 基座



当执行框架与基座智能同时跨过阈值，Agent 不再是功能模块，而是

颠覆以人为中心的工作范式

基座

Agent 上升为技术与交付层面的底层载体

AI Agent正在成为企业智能化的新型操作系统

AI正在从“被动响应工具”，走向承载任务、流程与系统协同的智能执行层。

辅助工具

智能执行层

企业智能操作系统



Agent不再只是功能插件，而是企业任务执行、系统协同与知识流转的**新型基础设施**。

未来，所有企业的底层逻辑都将走向 Agent 原生

这次 Agent 变革不是功能增强，而是对执行框架、工作方式与组织协作方式的重构。



当执行框架与基础智能同时跨过阈值，Agent 不再是功能模块，而是组织应用与工作方式的载体



Agent 爆发，推动 Token 消耗快速增长



任务从单轮问答升级为持续执行后，单任务 Token 消耗被系统性放大。



结论： Agent 重塑组织执行方式，也将持续拉动底层推理与 Token 需求的长期增长。

从“可用”到“可生产”：企业Agent进入生产级落地分水岭

企业级Agent的评价标准，正在从单点演示效果，转向长期、稳定、可控、可复制的生产运行能力。

企业关注点迁移：能不能用 → 能不能稳定运行 → 能不能规模复制 → 能不能纳入生产体系



真正进入生产阶段，Agent不再只是“能跑”，而是要能被**监控、被审计、被治理、被运营**。

企业Agent落地，卡在四个生产级断层



 **结论：**企业级Agent要从Demo走向**生产**，必须同时解决**Agent治理、模型服务、算力运营和场景沉淀**。

清昂Solution：构建企业自主可控的Agent Infra

以 AaaS 为核心，贯通算力、模型服务与 Agent 运行体系，支撑企业级智能体从单点实验走向规模化生产



各行各业的 Agent



...



Token —— Agent 的原料

- ✓ Agent 特化的 MaaS 服务
- ✓ 极致性能、多端使能



清昂 AaaS



Harness —— Agent 的载体

- ✓ 通往自主智能、AGI 的底层机制
- ✓ 管理、协作、鉴权



底层算力基础设施 / Agent Infra Base

英伟达 / 华为 / 沐曦 / 燧原 / ... 公有云 / 私有云



清昂 Solution: 以玄武AI中台构建企业自主可控的 Agent Infra

从算力到模型服务，再到Agent运行与业务执行，构建企业级可运营、可治理、可持续优化的智能体生产系统

清昂 Solution (抽象逻辑)

玄武AI中台 (具体实现)



MLGuider: 让Agent在国产异构算力上高效运行



性能提升

更高吞吐, 更低延迟



推理成本降低

更高资源利用率, 更优性价比



国产算力适配

深度适配国产异构芯片, 稳定高效运行

玄武平台：让模型服务可调用、可计量、可运营

统一的模型服务底座，打通算力、模型、计量与成本，支撑企业级 Agent 场景的规模化落地与持续运营。



企业 Agent 的持续运行，必须建立在可运营模型服务底座上。

xwclaw: 企业级治理闭环的Agentic AI产品

构建闭环治理体系，让每个 Agent 都在企业边界内安全运行、可追溯、可复制，支撑规模化落地。



安全可控

协作可编排

执行可约束

全程可审计

资产可沉淀复用



安全治理闭环，支撑生产级规模化落地

场景一：从人工审核到可追溯的政务Agent流程

以政务办事为例，通过 Agent 流程辅助初审，提高效率与一致性，实现可追溯、可审计，可持续优化的治理闭环。



场景痛点

- 材料格式多
- 政策规则多
- 人工审核慢
- 过程需留痕

规范高效
提升办事效率

合规可控
确保政策一致

可追溯
全程留痕可审计

中台能力

- xwclaw 编排任务
- 玄武平台提供模型服务
- MLGuider 支撑本地算力运行

验收指标

初审耗时 平均耗时下降	缺失项识别率 识别准确率提升	政策引用准确率 引用准确率提升	人工复核通过率 一次通过率提升	审计完整性 留痕完整率提升
----------------	-------------------	--------------------	--------------------	------------------

场景二：从研发提效到基础设施自动化，Agent可以进入复杂工程流程

Coding Agent



关键优势



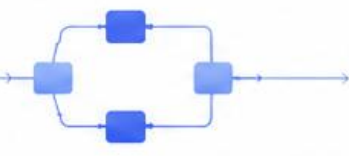
私有化



高保密



研发流程提效



案例标签

某芯片设计厂商

- 私有化 Coding Agent 落地
- 接入研发流程与工具链
- 大幅提升研发效率与质量

Infra Agent



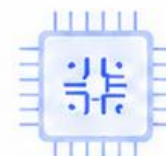
关键优势



专家经验沉淀为 Skills



降低适配成本



某芯片厂商

- Infra Agent 自动化适配
- 模型/算子优化与验证闭环
- 显著降低适配成本与周期



企业级 Agent 不只适合办公问答，也可以进入研发、运维和 AI 基础设施流程。

场景三：从华为算力集群到 MaaS 平台，青引 Claw 支撑区域级 Agent 场景落地

以青白江“青引 Claw”为例，基于华为算力集群与清昂玄武 AI 中台，构建面向办公、物流、工业与一人公司的区域级智能体应用底座。



结论：青引 Claw 将区域算力、MaaS 服务与 Agent 场景编排打通，支撑办公、物流、工业与一人公司等场景从试点走向可复制落地。

后Agent时代方案：既有底层能力，也有平台交付和Agent场景探索

三类能力证据链

01



MLGuider

模型优化引擎



- ✓ 模型优化
- ✓ 国产适配
- ✓ 多芯片
- ✓ 多模型
- ✓ 性能优化

案例标签



华为昇腾



沐曦



燧原科技

02



玄武平台

智算云 & MaaS 平台



- ✓ 智算云
- ✓ MaaS
- ✓ 算力纳管
- ✓ 模型服务

案例标签



北电数智



京西智谷



武建算网

03



xwclaw

Agent 平台与场景探索



- ✓ 研发 Agent
- ✓ Infra Agent
- ✓ 场景共创
- ✓ 流程沉淀

案例标签



安其威



行业探索



医疗



法律



家纺



AI4S

...



可信度来自三类能力叠加：底层优化、平台交付、场景共创

后Agent时代的趋势：AI正在成倍放大差距，而不是缩小



技术代差

- **根本分野**：技术差距从“线性”变“指数级拉大”，形成不可逆断层。
- **能力天花板**：构建闭环Agent工作流者，将甩开仅调用API者的差距。
- **质的飞跃**：不是效率提升，而是“能做”与“不能做”的生存分野。



市场分化

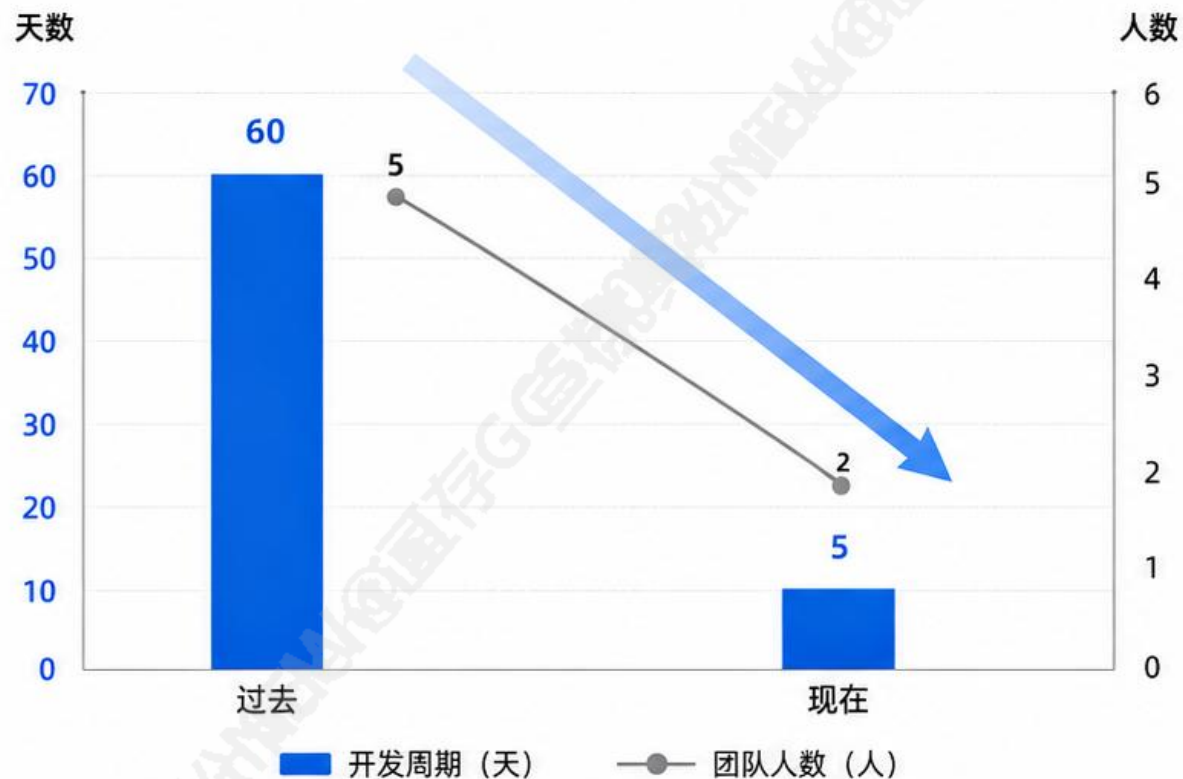
- **先发优势放大**：头部玩家壁垒迅速扩大，资源加速向其集中。
- **赢家通吃**：无法构建有效Agent工作流者将被边缘化甚至淘汰。
- **格局重塑**：旧护城河失效，新领导者基于Agent重新定义规则。



结论： 后Agent时代，真正的差距不再是是否接入AI，而是是否具备将AI转化为闭环执行能力的系统化能力。

后Agent时代的趋势：技术门槛正在逐步降低

智能体等系统开发周期与所需人数在逐渐降低



数据来源：唯快不破，Anthropic 几天搞定智能体生产-36氪
<https://www.36kr.com/p/3759120023007744>

企业间竞争维度在逐渐上移



结论：当技术门槛持续降低，企业竞争将不再主要取决于技术实现本身，而将更多转向任务定义、目标设计、组织验收与价值判断能力。

后Agent时代的趋势：Harness与模型，现在是互补，未来是融合

随着模型能力持续增强，Agent竞争将逐步从单一模型能力竞争，走向模型能力与执行系统能力的协同竞争。

Big Harness vs Big Model

AI价值最终沉淀在模型，还是沉淀在模型外的系统层？



01 Big Harness 一派

越接近真实生产，越需要稳定的工具链、上下文结构化、流程编排与运行时约束。

因此 Harness 并非过渡层，而是承接企业级执行与交付的长期价值层。

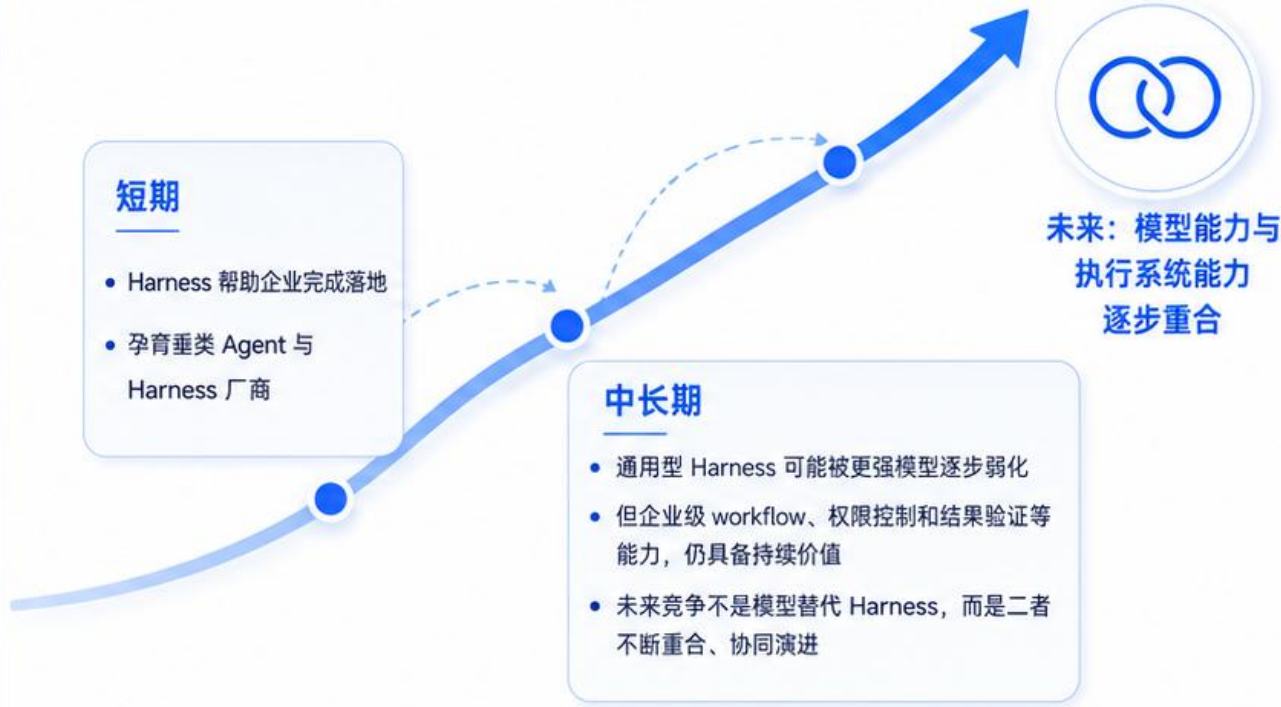


02 Big Model 一派

随着模型持续进步，许多今天看起来复杂的外层编排、流程封装与系统能力，长期可能被更强模型逐步吸收与替代。



Agent竞争本质是 Big Model 与 Big Harness 协同竞争



结论：短期看，Harness 是企业级Agent落地的重要抓手；
中长期看，模型与Harness将从互补走向重合，竞争核心转向协同能力。

后Agent时代的趋势：重新定义企业与个体的核心竞争力

后Agent时代，竞争力不再只不再来自单点技术能力，而来自企业能否把Agent沉淀为可治理、可复用、可规模化的组织能力；
个体能否从“任务执行者”跃迁为“任务定义者、编排者和验收者”。

企业核心竞争力



01



构建Agent原生组织能力

- 重构业务流程，形成“人 + Agent”协同分工
- 将流程、知识和经验沉淀为可复用Agent资产
- 从单点PoC走向跨部门、跨场景复制
- 让组织能力不再完全依赖人力线性扩张

02



建设可控可运营的Agent Infra

- 打通模型、工具、数据、算力与业务系统
- 建立统一权限、审计、安全与成本治理
- 让每一次Agent执行可观测、可追溯、可度量
- 通过持续评估和优化，形成长期运营能力

个体核心竞争力

03



积极学习拥抱新技术

- 主动跟进最前沿的模型能力
- 掌握Agent编排框架与工具调用方法
- 建立自己的“Agent工具箱”
- 不会用Agent的人，将被会用Agent的人替代

04



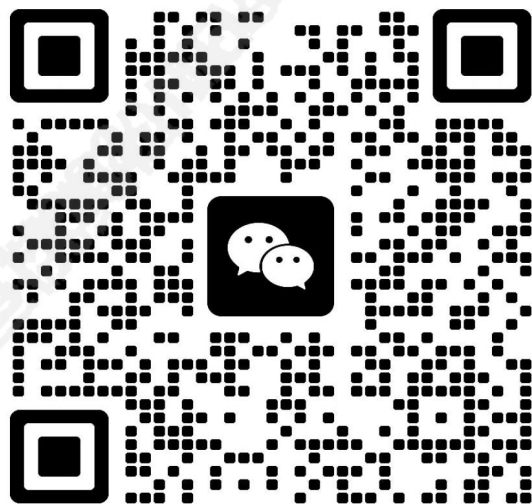
放弃唯技术论，回归高阶判断

- 定义问题、拆解模糊任务
- 设定目标、约束与验收标准
- 组织并带领“人 + Agent”协同团队
- 形成行业深度认知、价值判断与决策能力



后Agent时代，企业要从“工具使用者”跃迁为“Agent原生组织”；
个体要从“任务执行者”跃迁为“任务定义者、编排者和验收者”。

联系我们



清昂智能 COO



公众号