

甲子智库定义者系列报告：

甲子光年
JAZZYEAR

2026

AI原生组织

openLaw 推动组织形态重塑

出品机构：甲子光年智库

发布时间：2026.03

「水木人工智能学堂」

水木AI知识荟 & 交流社群钜

粤每日分享行业报告、行业资讯等！

@链接海量AI行业精英！

圈不定时进行名校名企行活动！

醪足不出门，尽在水木AI知识荟！

鸣扫码添加小编微信，免费进水木AI交流群

交流
社群
去噪
星球



去噪星球 每日仅需0.5元

公众号：水木人工智能学堂

目录

part 01

新趋势

openclaw掀起新一轮 应用热潮

- 1.1 openclaw是什么
- 1.2 openclaw技术架构
- 1.3 openclaw技术优势
- 1.4 openclaw局限性与争议
- 1.5 openclaw影响

part 02

新定义

AI原生组织, 以AI OS为调度中枢的新型组织形态

- 2.1 openclaw催生AI原生组织加速到来
- 2.2 组织新形态: AI原生组织
- 2.3 走向AI原生组织的两条路径
- 2.4 路径一: 从传统企业到流态型企业
- 2.5 路径二: 从传统个体到生态节点
- 2.6 两类AI原生组织共生共长
- 2.7 AI原生组织架构
- 2.8 AI原生组织定义卡片

part 03

新范式

A 原生组织转型路线图

- 3.1 AI原生组织转型路径
- 3.2 路径一: 流态型企业转型路线图
- 3.3 路径二: 生态节点转型路线图

part 04

新实践

AI原生组织的实践案例

- 4.1 B端AI原生组织实践案例
- 4.2 C端AI原生组织实践案例
- 4.3 G端AI原生组织实践案例
- 4.4 AI原生组织产业图谱

目录 >>>>

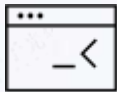
Part 01 新趋势 OpenClaw掀起新一轮AI应用热潮

- 1.1 openclaw是什么
- 1.2 openclaw技术架构
- 1.3 openclaw技术优势
- 1.4 openclaw局限性与争议
- 1.5 openclaw影响

从极客脚本到全球现象级AI开源神话, openclaw4个月走完行业十年路

2026年初席卷全网的“养虾”，并非一次简单的软件部署热潮，而是标志着Agent真正迈入生产力变革阶段。过去大模型受限于对话框形态，难以充分释放价值，openclaw则突破该交互边界，成为可接管系统底层权限、跨应用自主执行任务的“数字员工”

clawHub技能库破
1.3万个, NPM每周
下载量达220万次



Git Hub star数突
破33万+, 登顶全
球软件项目榜首



受“养虾”热潮影
响, 全球GPU租金
环比上涨15%-30%



破圈拐点引爆 (2026.1)

- 遭Anthropic侵权警告, 经历多次改名后, 正式定名openclaw



生态萌芽

- openclaw引爆MacMini抢购潮, 导致多平台断货
- 阿里、京东、华为、腾讯云等推出一键部署服务

初代原型诞生 (2025.11.24)

2025.11.24

初代原型诞生



- peter steinberger仅耗时1小时发布极客脚本whats APP Relay
- 开发者跑通“全自动抢单”等插件, clawBot雏形上线即引爆全网搜索热度
- 开发者为抗议大厂高昂API抽成, 转向本地零成本部署的clawBot

生态指数级爆发 (2026.2-至今)

国内大厂布局类claw产品与生态

- 生态市场卡位: 月之暗面与智谱等厂商推出百万Tokens补贴, 抢占市场生态
- Pc桌面端: 腾讯推出workBuddy/Qclaw/skillHub、阿里推出copaw/HiclawTeam版、网易有道推出Lobster AI, 抢占pc端办公入口
- 云端部署: 火山引擎推出Arkclaw、月之暗面推出kimicla、百度推出Duclaw, 实现开箱即用云端部署
- 移动端渗透: 小米推出xiaomimiclaw、百度推出红手指operator, 接入手机os底层, 并实现跨APP接管
- 硬件实体: 联想与小米推出原生支持openclaw的电脑底层系统、Nano Labs发行专属运行设备(一体机), 实现硬件实体落地

全民代安装狂欢

- 腾讯工程师线下助千人排队装虾
- 代安装、卸载服务炒至500元次



地方政策支持

- 深圳龙岗推出“龙虾十条”, OPC最高可获得1000万元股权投资
- 苏州常熟出台“龙虾十三条”, 人才项目综合支持最高600万元

海外新兴业态与传统巨头布局

- Matt schlicht发布Moltbook, 打造首个Agent专属交互平台
- 英伟达推出Nemocl原因架构维持硬件护城河
- cloudflare推出Moltorker, 实现通过云端与边缘节点收取流量过路费

openclaw爆火背后的核心逻辑：AI第一次以“数字员工”形态接管 workflows

openclaw的爆发标志着AI从“对话框”向“操作系统”的权力接管。通过一键部署抹平技术壁垒，将复杂的Agent配置降维为高参与感的“社交养成”，并以全天候的自动化运行重构数字员工的生产力边界



一人公司

通过“数字员工”形态重构人机协作与任务执行逻辑，降低个体创业门槛，支撑轻量化商业模式落地



独特养成属性

语料投喂与调教产生的具备高度个性化的“养成”特征，消解大众认知壁垒并建立情感联系



大厂平台卡位

头部企业以“一键部署”方案抹平技术门槛，争夺开发者入口与模型调用增量，借Agent放大后端推理需求



自主执行力

突破纯文本交互限制，依托统一网关与运行时直接调度文件系统、底层进程及异构应用，实现端到端的自动化任务闭环



直观视觉展示

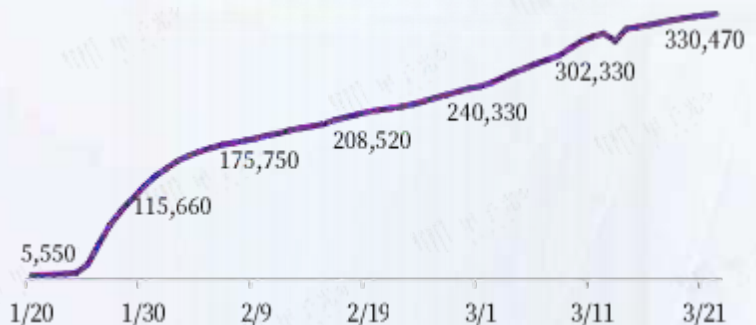


将底层系统调度转化为直观的自动化操作，大幅降低非技术人群的认知门槛，迅速引爆全网传播

开发者的广泛应用

2026年1月20日更名openclaw后，GitHub星标数仅用57天从0.55万增长至33万，证实开发者正大规模基于此构建应用，脱离短期热点范畴，进入场景应用阶段

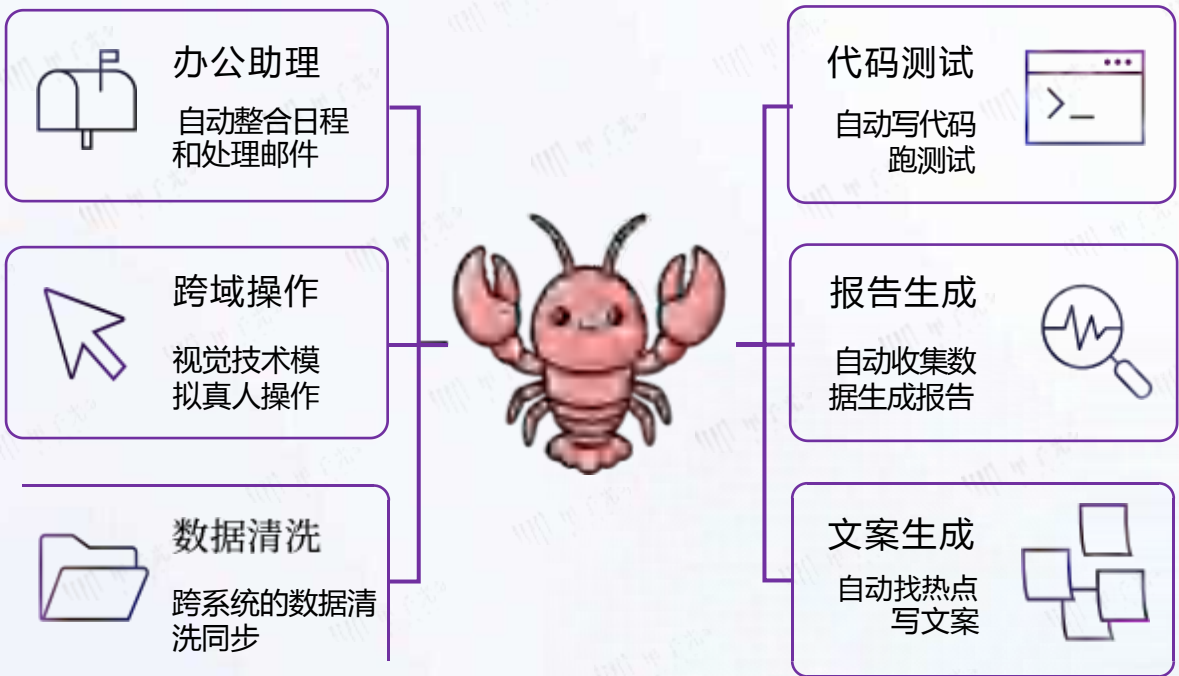
openclaw2026年累计GitHub星标数



openclaw是开源Agent框架，早期定位个人AI助手，目前正向B端场景延展

open claw (前身为clawbot/Moltbot) 是一个开源的, 支持本地或云端部署的AI Agent框架。它通过Gateway作为接入与控制层, 连接外部通信渠道与大模型, 并在用户授权、工具接入和运行环境配置完成的前提下, 调用浏览器、文件系统、脚本及部分外部服务能力, 执行跨工具、跨系统的自动化任务

openclaw应用场景



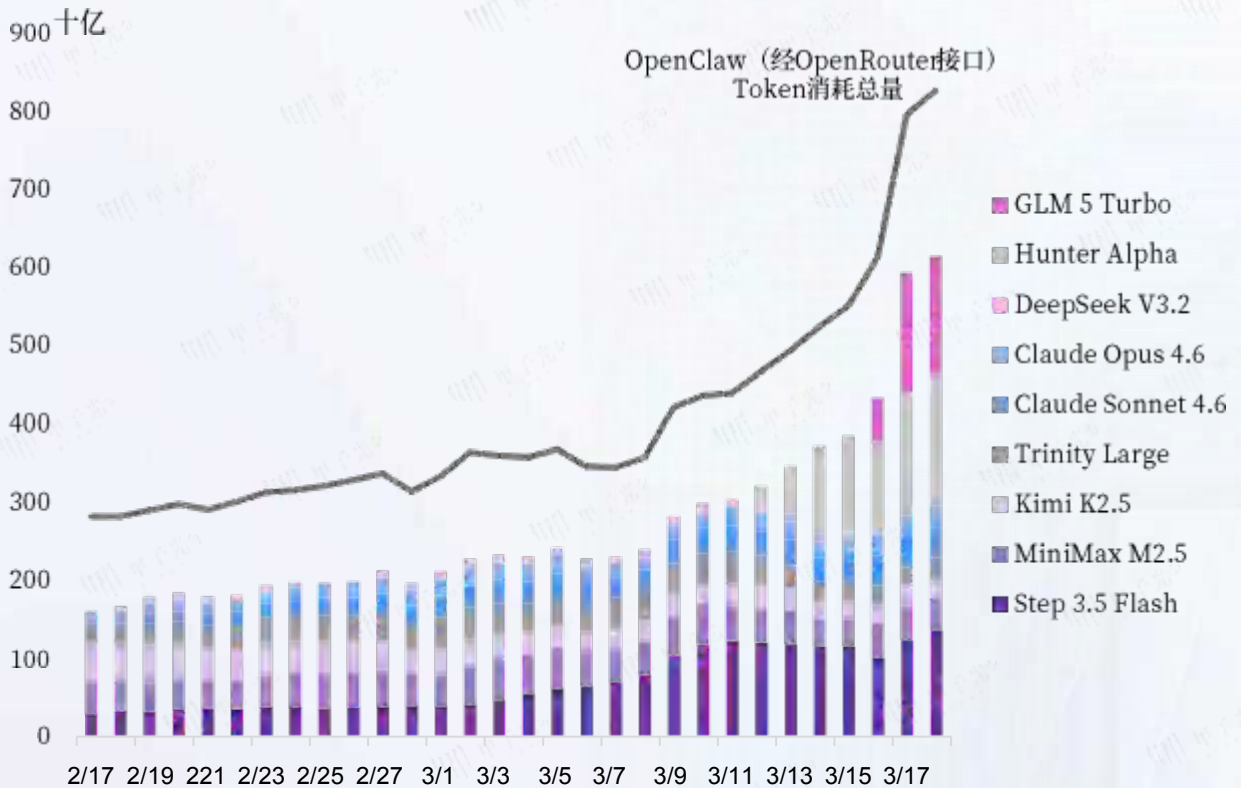
尽管openclaw的官方定位首先是个人AI助手, 但其能力组合--环境执行、界面自动化、任务编排--已展现出向团队协作和组织流程外溢的潜力与意义

- 环境执行能力: 可在授权范围内调用命令行、脚本、文件读写等底层能力, 与宿主环境形成协同
- 界面自动化能力: 借助浏览器控制完成网页访问、界面交互、信息提取等操作
- 任务编排能力: 可将消息入口、系统级工具与外部服务连接为连续工作流, 实现监测、触发、执行与反馈的闭环自动化

openclaw高频调用机制推高Token消耗基数, 改变大模型算力性价比格局

- 机制导致Token消耗激增: openclaw的循环推演与记忆回溯机制, 导致上下文消耗激增。openRouter数据显示: 从2月17日至3月17日, 单日Tokens消耗量由约2800亿快速攀升至8280亿, 实现近3倍增长
- 算力成本导致的流量迁徙: Agent的高频调用放大API成本边际效应。为规避旗舰模型高价 (如claude4.6sonnet输出单价约\$25/M Tokens), 模型调用向高性价比平替 (如MiniMaxM2.5输出单价约\$1.2/MTokens) 倾斜
- 中国大模型的生态卡位: 凭借性价比优势, 中国大模型已在openRouter的openclaw链路中实现局部替代, 3月第二周单周调用总量达4.69万亿Tokens, 连续两周超越美国模型。从市场演进看: 存量方面, 2月数据显示MiniMaxM2.5与kimi K2.5一度在该链路前五大模型中合计占比达67%; 增量方面, 3月中旬后的新增需求由HunterAlpha (小米MiMO团队早期内测版本) 与GLM 5Turbo承接

openclaw在openRouter平台调用的主要模型Token消耗分布和总量 (近30天)



注: 本页所有数据仅限于通过openRouter平台接口产生的openClaw模型调用记录。统计范围不涵盖OpenClaw通过其他分发平台、聚合API或厂商直连API产生的消耗, 不代表openclaw全网及全渠道的总量数据

从个人助手到生态破圈, openclaw快速完成多轮技术迭代

阶段 1

2025年11月——项目立项与原型

- 本地持久化状态: 确立JSONL格式本地磁盘文件集, 实现对话历史与上下文的本地持久化存储, 大幅减少对上下文窗口的依赖
- Heartbeat (心跳机制) : 引入后台心跳调度器, Agent实现由 "被动问答" 向 "定时自主巡检" 转型
- 端侧控制: 实现Tmux终端控制与音视频多模态处理, 构建系统级感知基础

阶段 2

2025年12月——架构重构与多渠道拓展

- 统一Gateway架构: 部署Node.js全局网关, 接入了Telegram、slack等多个主流通讯平台
- 动态模型路由: 建立算力分层机制, 高阶任务分配至旗舰模型, 日常任务下放至本地模型
- 全场景生态: 发布swift原生macosAPP; 推出Browser control技术, 实现底层DOM自动化控制

阶段 3

2026年1月——安全重构与能力解耦

- Docker sandbox (瞬态沙盒隔离) : 引入可选的瞬态隔离机制 (默认关闭) , 支持按需配置跨系统操作的 "用完即毁"安全环境
- plugin架构解耦: 发布clawHub标准规范, 将LLM推理核心与外部API及本地脚本的执行域进行物理剥离

阶段 4

2026年2月——内核级加固与混合基建

- Live canvas实时画布: 引入可编程UI渲染层, 允许Agent在聊天界面外直接生成、控制并更新可视化交互组件, 实现超越纯文本的协作
- 多模态系统穿透: 底层打通Macos、IOS与Android的原生音频/视频接口, 实现 "听、说、看" 全时态感知, 而非单纯的文字指令触发
- 统一控制面板 (Gateway2.0) : 将Gateway重新定义为 "控制面板" , 实现跨设备的助理状态同步与统一权限管控
- pi极简推理内核集成: 深度优化底层调度逻辑, 支持调用极致精简的pi推理模型, 以实现亚秒级的代码生成与任务分发响应

openclaw采用模块化解耦设计，为Agent提供本地/云端执行与编排环境

openclaw采用模块化解耦设计，提供Agent本地/云端执行与编排环境，系统自上而下分四层：

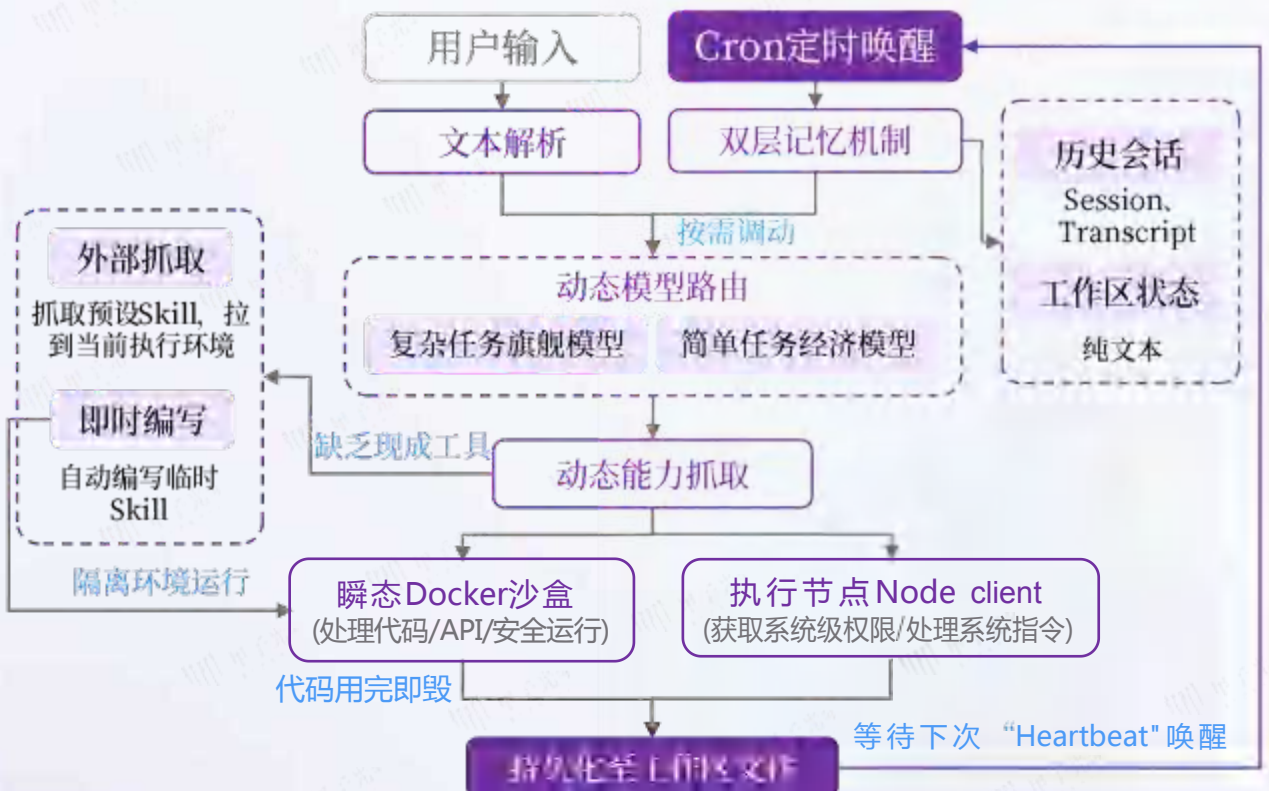
- 交互渠道：接入whatsAPP、Telegram等外部平台
- Agent本地/云端执行环境：作为系统核心物理载体，内部集成Gateway核心网关（负责路由分发、系统通信，内置Node.js及长短期双层记忆）、skills技能插件（提供联网搜索、代码解释等能力）与系统工具（落地文件读写、浏览器自动化等具体操作）
- 模型调度层：实现多模态动态路由与底层模型按需分配
- AI模型层：接入GPT-4o/Claude3.等大模型，支撑指令理解、逻辑推理与决策



openclaw依托自托管网关与动态路由, 驱动大模型跨环境自主完成任务

作为支持本地及云端部署的AIAgent框架, openclaw的核心是可持续运行的自托管网关。其采用控制面与执行面解耦的架构, 通过Gateway统一调度skills、隔离沙盒与执行节点 (Node client), 将大模型推理转化为全域自动化执行:

- Gateway网关层: 作为任务运行时 (Runtime) 的统一编排与路由中枢, 负责接收和处理多渠道输入, 并依据任务复杂度、时延要求与成本约束, 动态选择云端大模型或本地轻量模型执行, 以在性能、响应速度与推理成本之间取得平衡
- 双层记忆机制: 将记忆拆分为彼此独立的两部分: 历史会话 (如 sessions.JSON与Transcript.JSONL) 和工作区状态 (纯文本文件)。二者分离存储, 有助于降低长任务对上下文窗口的持续占用, 缓解上下文遗忘问题, 从而提升复杂任务的连续执行能力
- skills矩阵: 通过加载skill模块, 对文件系统、进程调用、浏览器、API等底层能力进行封装与组合, 使Agent能在受控环境中直接调度操作系统及各类应用, 进而实现跨系统、跨软件的自动化操作



openclaw的文件记忆机制, 打破对大模型对话窗口的路径依赖

openclaw重新定义了AIAgent的运行边界。通过将执行链路与持久化存储引擎深度融合, 它彻底剥离了对前端聊天窗口的依赖, 建立起由后台守护进程和工作区状态文件共同驱动的自动化机制



- "决策-执行" 交互闭环: 以大模型为逻辑核心驱动指令拆解, 直接调用系统底层 shell 代码与外部网络协议, 将自然语言解析转化为端到端的操作, 由 Gateway 统一编排执行
- 文件系统记忆中枢: 创新性地使用一组工作区文本文件, 将动态数据持久化至执行节点, 使其突破模型上下文窗口限制, 让智能体的目标、任务和历史对用户完全透明、可审阅、可手动干预
- cron 后台调度机制: 部署守护进程脱离前端界面依赖, 可通过配置的策略 (如定时触发器、事件监听) 自主唤醒并执行任务, 实现了从需要人工提问的“聊天机器人”到可托管、持续运行的“智能自动化服务”的范式转变

openclaw的技术本质, 不是让AI更聪明, 而是让AI真正开始“干活”

openclaw并非单纯的效率工具, 而是通过赋予AI跨系统执行能力, 实现任务级自动拆解与动态调度, 驱动多Agent高效协同、可控、规模化的执行任务

传统软件技术路径

- 高度依赖异构系统标准集成
- 跨部门数据锁死在封闭系统

企业能力扩张受限于昂贵的集成成本

"静态配置"



转向“全域执行”

OpenClaw技术路径

- 从“雇佣资源”转向“调用资源”
- 企业边界从“资产拥有”转向“能力接口”

企业通过“接口化”降低调度成本, 组织边界将被彻底打破

OpenClaw推动AI应用演进的核心技术优势

01 全域执行能”

突破“只能说, 不能做”瓶颈
跨应用执行·自动操作·多步骤任务闭环

- 从“语言系统”升级为“行动系统”

02 跨工具统一调度

统一工具调用协议
屏蔽系统差异·工具标准化接入·动态工具组合

- 把企业所有系统“API化+Agent化”

03 任务级自动拆解与规划

具备任务编排能力
多步骤拆解·依赖关系构建·执行顺序优化·动态调整路径

- 从“函数调用”升级为“流程自动生成”

04 状态感知与闭环执行

持续执行与状态跟踪
结果校验·自动重试·完整执行闭环

- 让Agent具备“工程化可靠性”

05 多Agent协同机制

多Agent分工与协同
并行执行·角色分工·任务流转

- 从“单体智能”走向“群体智能”

06 人机混合控制

支持人工介入与风险控制
审批节点·可控可审计·可中断可修正

- 让AI系统“可用、可控、可落地”

openclaw与模型/Agent的耦合, 消除业务意图与实际执行的偏差

openclaw与模型/Agent相互补位高度耦合, 二者缝合了从“业务意图”到“实际执行”之间的台阶式断裂, 共同构成了完整的智能闭环系统

传统模型/Agent在缺乏执行环境时存在“意图-执行”断层

模型 Agent

- 具备基于语言模型的决策与规划能力
- 执行能力仍需外部工具或执行环境

open claw

- 具备系统级执行能力的运行环境
- 不具备完整的任务理解与规划能力 (需与模型协同)

模型/Agent与OpenClaw耦合驱动的“意图-执行”闭环

模型/Agent负责 智能编排

- 基于openclaw返回的界面状态与工具结果进行环境感知与智能调度
- 推演复杂任务的最优路径



openclaw负责 能力调用与执行

- 接收并转译模型/Agent意图为系统调用指令, 完成实际执行
- 通过可控执行环境完成页面操作、文件处理、跨应用联动等任务

人类负责判断与最终目标下达

极低TER揭示“算力黑洞”真相：约九成Tokens消耗于系统维持而非实际输出

openclaw的底层上下文管理机制导致极低的Token能效比 (TER, Token EfficiencyRate), 其指数级激增的隐性算力消耗, 成了阻碍企业级规模化部署的核心商业壁垒

图1:按照TER测算, 在典型任务场景中, openclaw的Token能效比普遍处于c级

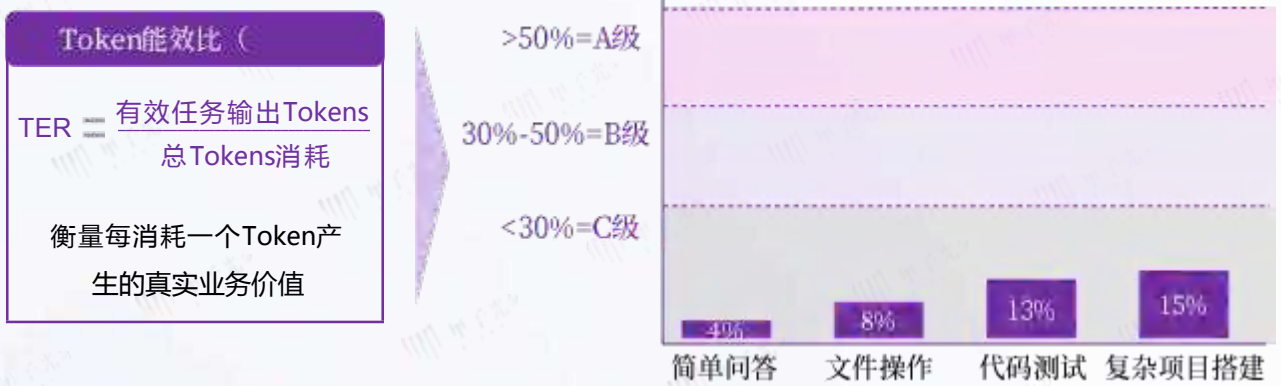


图2: openclaw隐藏的消耗机制

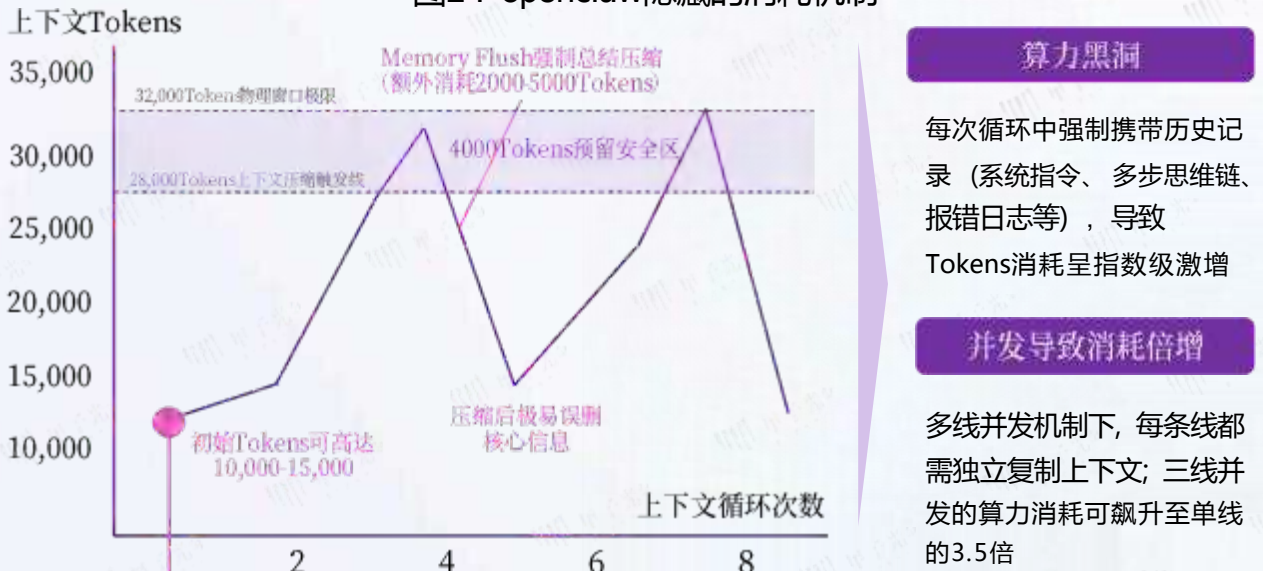
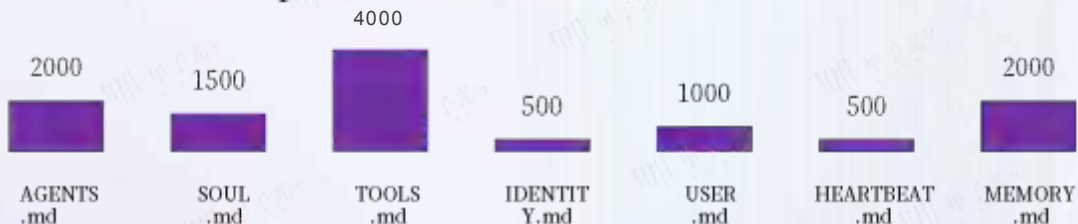


图3: OpenClaw每次对话携带文件的默认Tokens消耗数



openclaw过度权限与架构缺陷导致系统级的安全风险

为追求极致的自动化效率, openclaw通常需要较高的系统权限与持续运行能力。在真实高并发业务流中, 极易因外部暴露或内部失控导致安全约束失效

外部风险：从防盗门失效到工具箱投毒

暴露面层面

securityscorecard统计数据显示, 截至2026年3月11日, 公网上可被探测到的openclaw暴露实例累计超46.9万个(活跃数量20.3万个)。其中, 通过版本匹配检测发现, 27.2%的实例存在高危漏洞, 面临被利用攻击风险

生态层面

openclaw官方复盘称, 2026年2月24日至3月2日, claw Hub (openclaw插件平台) 中约20%的插件 (skills) 为恶意或可疑插件, clawHub成为植入恶意代码的重要渠道

内部失控：源于底层架构的系统性弱点

组件/层	占比/暴露面	主要风险
src/tools (执行层)	35%	命令注入、路径遍历
src/gateway (网关层)	26%	权限控制、认证授权
src/auth (权限层)	12%	认证绕过、CSRF
src/sandbox (隔离层)	10%	路径遍历、SSRF
src/hooks (生命周期层)	8%	prompt注入、信息泄露

- 通过对openclaw自身代码仓库的审计揭示了项目本身在高频修复安全问题。通过基于Git历史与commit message的安全语义分析, 可以量化一段时间内与安全相关的代码变更规模与分布, 从而判断攻击面集中在哪些层次
- 对openclaw近期commits进行筛选与分类, 可发现风险高度集中在执行层与网关层

"淘金者迷失, 卖水人盈利", 商业闭环尚未形成

openclaw的早期商业生态正陷入 "淘金者迷失, 卖水人盈利" 的结构性的陷阱: 技术杠杆尚未能在应用层创造实质性的业务增量与ROI闭环, 部分盛况停留在贩卖认知焦虑、部署服务, 真正实现盈利的是提供底层算力与API的基建层

信息差套利的畸形现状

社交平台上涌现的50-500元不等的 "代装龙虾" 服务, 本质上是利用openclaw早期复杂部署门槛收割技术焦虑的短期流量生意, 不具备长期商业复用价值

内容变现的伪神话

大量宣称用Agent实现 "一人公司" 的个人, 实际上并未通过内容获得实质性的广告分成或带货利润, 而是在通过兜售教学课程进行次级变现

未形成商业
闭环

真正实现规模化盈利的是提供底层算力与API的云服务与大模型厂商



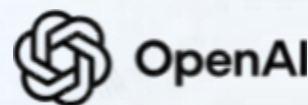
2025全年营收7903.8万美元

2026年2月
1.5亿美元



2025全年营收1.15亿美元

2026年K2.5上线后20天
1.2亿美元



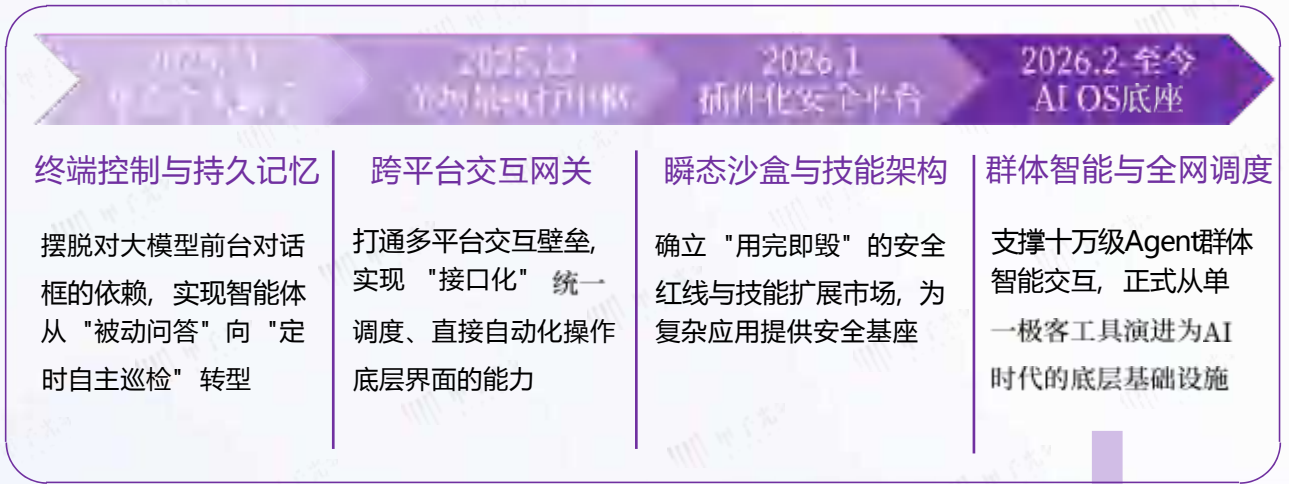
2025全年营收131亿美元

2026年1-2月
250亿美元

openclaw开启以AI OS为核心的代理执行时代

人工智能的发展已正式进入“代理执行”阶段。openclaw的出现，让AI跳出了传统的聊天对话框，转变为能够直接跨软件、自主完成复杂任务的系统执行者

openclaw从单点工具走向全局调度的AI OS



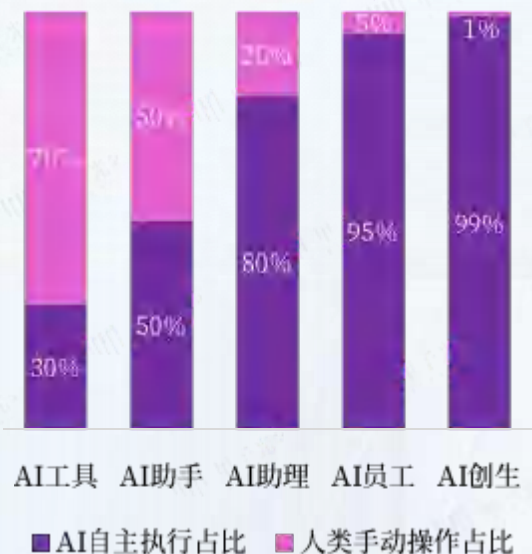
底层OS化调度让AI从“被动对答”转向“主动执行”，驱动Agent应用从单点工具进化为数字员工

代理式AI的应用演进阶段：从“AI助手”向“AI员工”演进

代理式AI阶段，根据人与AI的协同程度不同，可以分为五个阶段：

- AI工具：AI作为单点工具，大部分工作由人主导规划
- AI助手：AI作为可交互的助手，人与AI各承担半数执行
- AI助理：AI作为高度智能化助理，一多半工作可以交给AI完成
- AI员工：AI作为数字同事，自主完成所有内容
- AI创生：AI突破数字世界，通过协作对现实世界产生影响

代理式AI应用的五个阶段



目录

Part 02 新定义 AI原生组织，以AI OS为调度中枢的新型组织形态

2.1 openclaw催生AI原生组织加速到来

2.2 组织新形态：AI原生组织

2.3 走向AI原生组织的两条路径

2.4 路径一：从传统企业到流态型企业

2.5 路径二：从传统个体到生态节点

2.6 两类AI原生组织共生共长

2.7 AI原生组织架构

2.8 AI原生组织定义卡片

openclaw推动组织形态出现关键跃迁

openclaw所体现的不只是AI能力增强，更是AI从对话系统走向执行系统的重要一步，使AI原生组织从概念推演走向现实预演，并提供了一个具象的实践样本

对话到执行

- 不只是能力增强，更是角色进化
- 对话系统→执行系统
- 被动应答→主动执行


概念到现实


- 概念推演→现实预演
- 理论框架→具象实践
- 提供可验证的实践样本


openclaw催化传统组织跃迁至新组织形态




openclaw对组织形态演进的核心价值

 验证可行性
提供首个完整实践样本

 降低尝试门槛
具象化实施路径

 明确演进方向
定义AI原生组织标准

 加速产业采纳
从概念到可复制解决方案

AI原生组织：以AI OS为中枢、Agent为执行单元的动态协同网络

AI原生组织定义

AI原生组织是以AIOS为调度中枢、以Agent为执行单元、以动态协同网络为运行机制的新型组织形态。其典型形态既包括由传统企业演进而来的流态型企业，也包括由传统个体演进而来的生态节点

AI原生组织的“五化”特征

系统接口化

依托统一调用协议，将企业异构系统与各类应用转化为Agent可直接调度的标准接口

经验资产化

将隐性经验固化为工作流资产（Workflow Asset），使经验变成可复用的按次计费数字资产

交互意图化

通过自然语言下发意图，系统自主完成工作流的拆解与跨应用的执行

协同流态化

打破组织与个人边界，由AI OS实时编排Agent与节点，实现按需聚散的动态协作



接入凭证化

为Agent签发专属身份，在跨系统交互前强制核验身份，预防恶意攻击与机密泄露

走向AI原生组织有两条路径：企业重构与个体外扩

AI原生组织主要有两大演进路径。路径一是传统企业组织演进路径：传统实体组织通过削减管理层级与开放业务边界，由固化的科层结构最终转化为依托AI OS全局调度的流态型企业。路径二是新兴超级个体演进路径：个体通过调用外部资源与AI Agent，实现生产力杠杆放大，最终演变为具备企业级运作能力的生态节点

传统企业组织形态演进路径

传统企业不是直接变AI原生组织，而是通常先经历信息化、数字化，再进一步被Agent、自动执行和动态编排改造，走向流态型企业

存量形态被AI重构



新兴超级个体演进路径

超级个体借助AI获得过去只有组织才有的生产能力，先形成“一人公司”，再进一步嵌入协作网络，成为生态节点

增量个体被AI放大



AI原生组织

以意图为中心，以AI OS为全局调度主体的无边生态网络

- AI原生组织有两种典型形态：流态型企业与生态节点
- 流态企业（任务需求方）与生态节点（弹性供给方）不再是割裂的实体，而是共同构成了依托AI OS动态编排的生态网络

单点工具堆砌的传统数字化模式，已经无法满足AI时代自主执行需求

组织形态由工业化时代的科层型结构，演进至数字化时代的平台型、生态型形态，其底层逻辑是通过不断叠加单点工具来实现局部效率优化。然而，这种“工具层叠式”路径在推动数字化的同时，也导致了信息孤岛与界面断层问题，造成系统间割裂，难以满足AI时代对端到端自主执行的要求

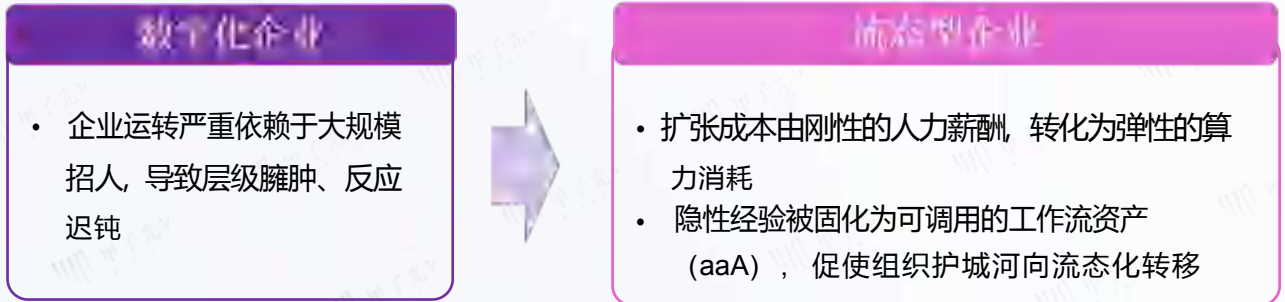


组织形态向数字化演进虽搭建了平台生态，但单点工具的扩张与组织架构的固化产生割裂，导致传统依赖系统堆砌的线性路径反而将企业推入结构性困境：

- saas反噬：员工沦为跨系统的“人肉API”，界面切换占据近10%工时
- 线性加人失效：面对繁琐的系统操作，企业已经无法靠单纯增加人手来解决业务缺口
- 系统孤岛：缺乏底层意图统一调度，单点工具各自为战，难以实现端到端自主执行
- 组织架构僵化：静态资源配置引发人才错配，难以适应复合型业务需求

构建以意图为中心的无边界立体流态型企业

随着系统复杂化与时间碎片化，人类从调度者成为最大瓶颈。企业必须将执行主导权全面移交Agent，人退居战略层面，迈入流态型企业



流态型企业：无边界的立体流态结构



从“固态科层制”到“无定形网络”

- 打破传统物理办公与长期雇佣边界，消除固定部门
- 人转变为“超级个体”，与海量Agent构成节点，组织边界彻底消融为随需聚散的流态生产网络

从“静态分配”到“随需聚散”

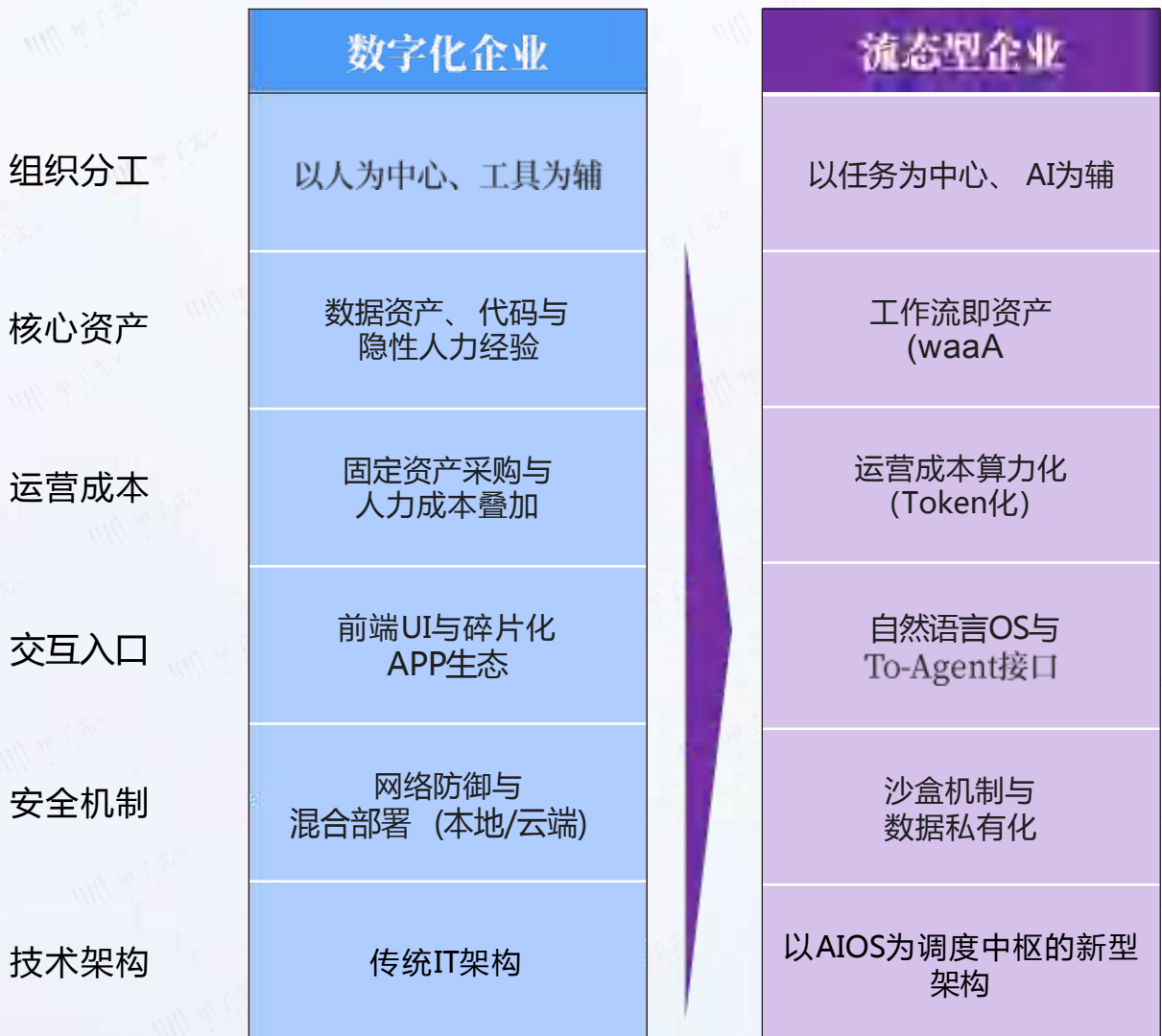
- 决策下放至Agent，以基于数据的系统级决策，取代基于局部经验的人工判断
- AI OS中枢自主分发任务并匹配算力，实现组织资源的随需汇聚，交付即解散

从“指令下达”到“意图识别”

- 人只需要下发意图与验收，Agent接收后自主拆解任务并调度资源
- 剥离对刚性SOP的依赖，确立基于“意图下发+自动路由+随需结网”的全自动交付模式

数字化企业与流态型企业的边界厘清

企业向AI原生组织的跨越，并非简单的工具升级，而是底层运行逻辑与商业范式的全面重构。传统金字塔式的固化科层制，本质是为了弥补人力在跨系统执行、信息流转与部门协同中的物理局限。当底层系统操作与数据流转被AI接管，传统协作摩擦被清零，组织形态将打破原有边界，由“管理驱动的集合体”彻底演进为“算力驱动的AI原生组织”



个体生产力的局限性, 已无法支撑AI时代对个体能力提升的需求

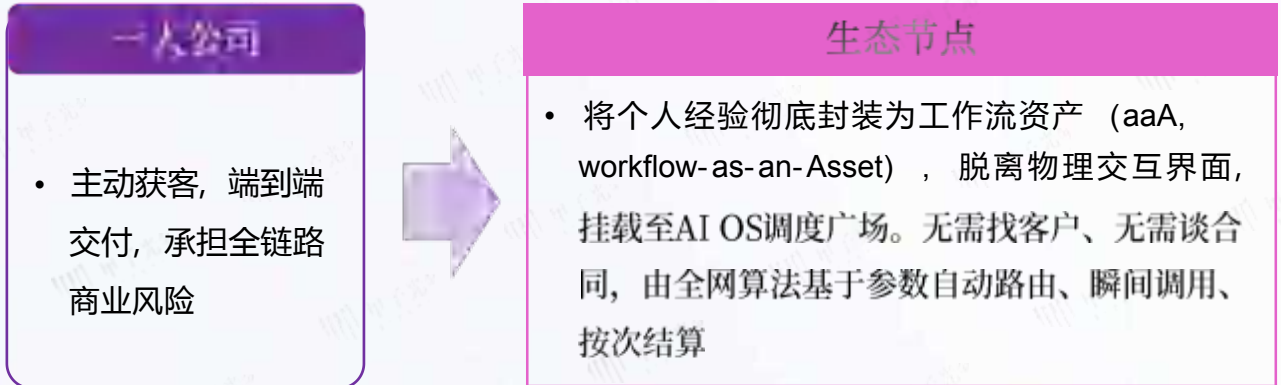
传统个体形态向超级个体演进, 本质是叠加AI工具以实现单点生产力的放大。然而, 以个体为核心的微型商业模式, 极易触及时间、精力与认知盲区的边界。这种对单点的依赖与线性增长路径, 难以适配AI原生组织的协同需求。其局限性主要表现在三个方面:

- 物理时间枷锁: 最终交付仍高度依赖人工进行质量审核与兜底。收入模型 (客单价 \times 时间) 永远无法突破人类每天24小时的生理极限
- 商业内耗: 被迫承担销售与运营角色。高昂的获客成本与繁琐的非标沟通, 严重反噬了AI带来的产能红利
- 缺乏容错单性: 一旦生病、精力枯竭或遇到知识盲区, 整个微型商业系统将停摆
因此, 个体需要借助Agent与外部资源突破以上局限性, 完成自动化商业闭环



将个人经验封装为waaA，成为流态型企业生态中的关键交付节点

传统个体演进的终局并非无休止地维持“一人公司”的运转，而是褪去繁重的商业外壳，降维成A调度网络中即插即用的生态节点



Ai原生组织：生态节点

经验资产化：将个人决策与经验封装为工作流资产（WaaA），作为可订阅的系统服务

算法杠杆化：通过优化WaaA提高服务性价比，以最少的Token消耗获得最高的产出

调度无感化：通过标准化协议实现任务的自动认领与执行

供给矩阵化：通过并行挂载多个WaaA，突破个人时间精力限制

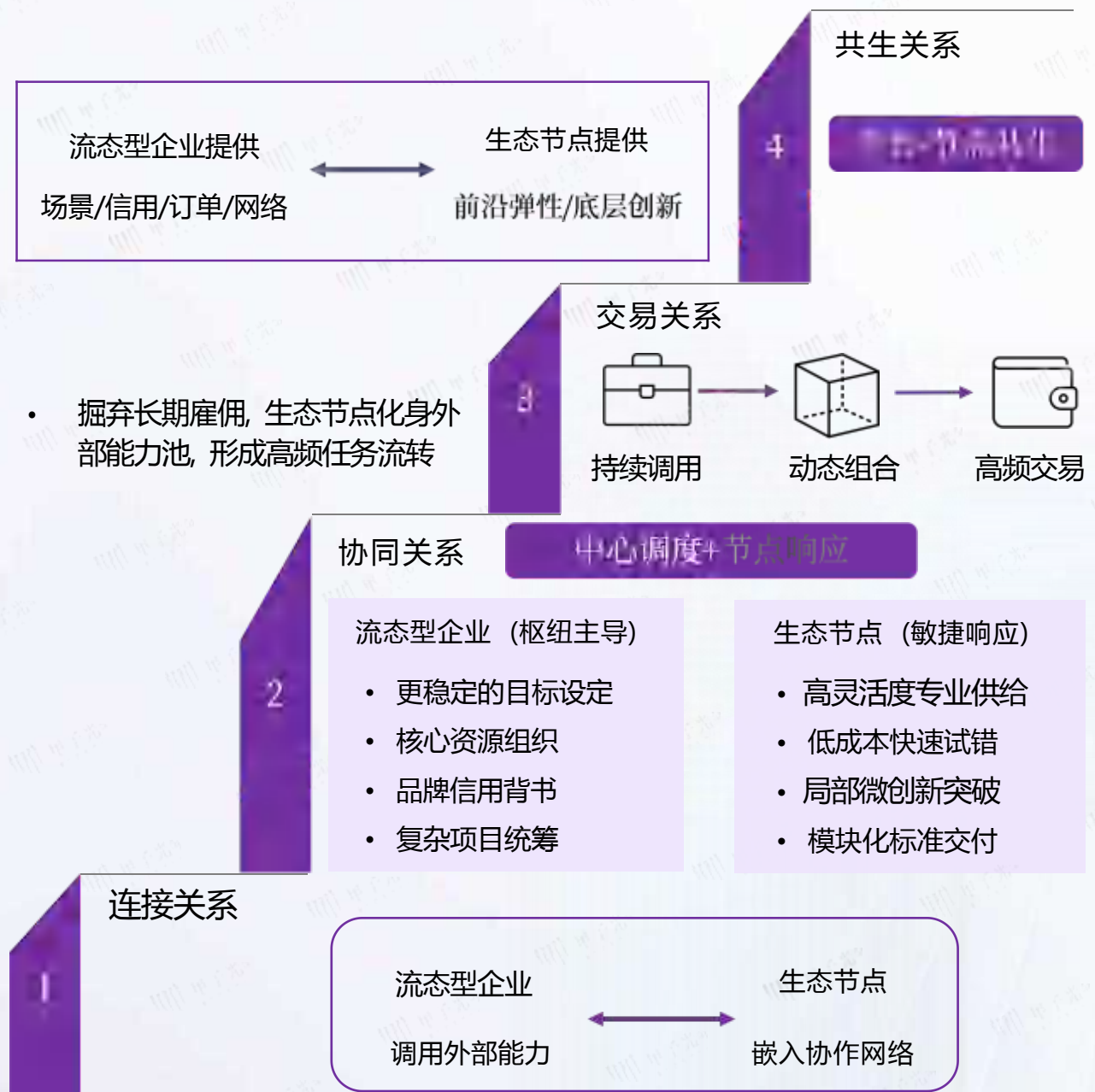
流态型企业

生态节点

生态节点

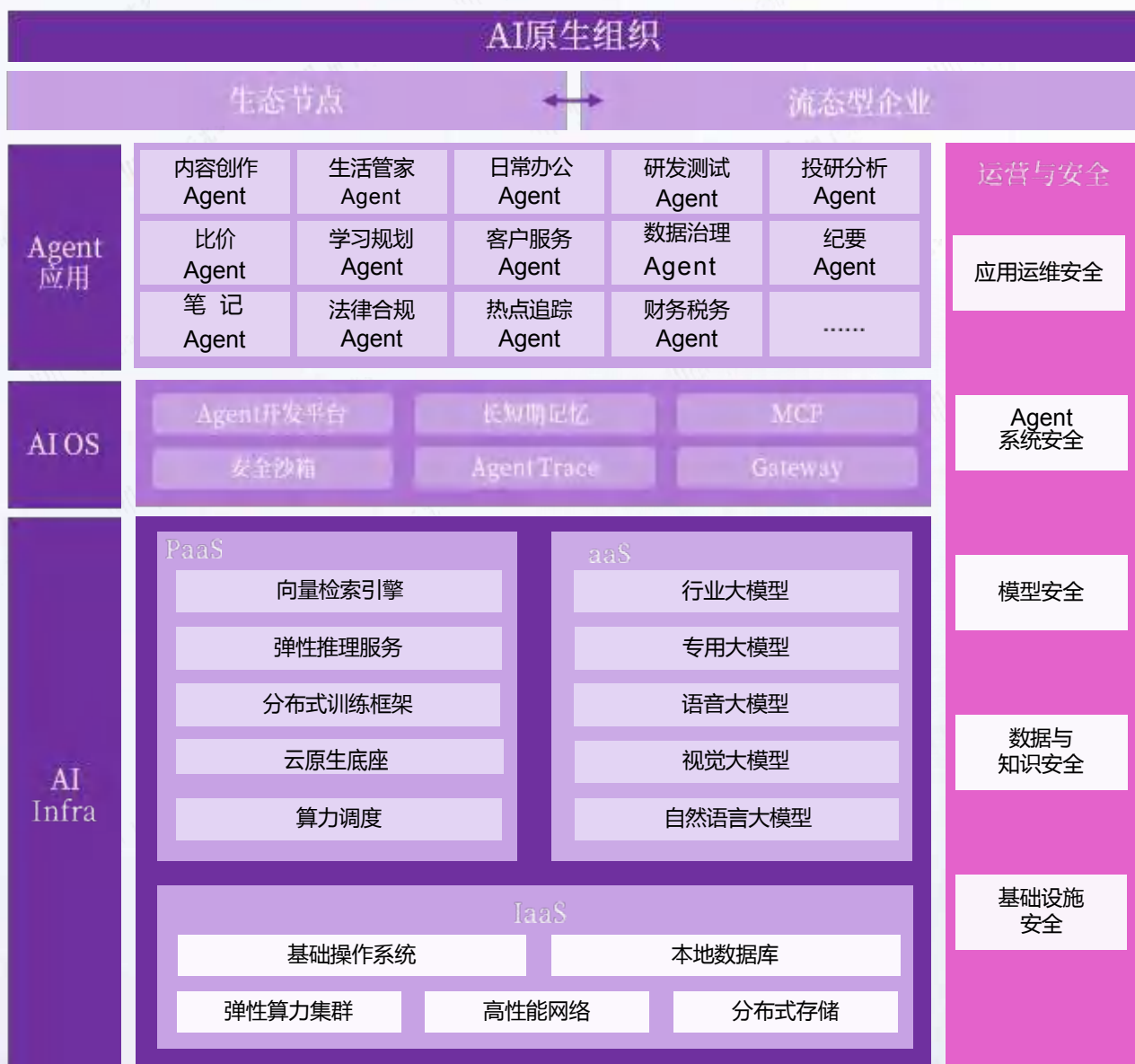
流态型企业调度与生态节点供给深度耦合，构成AI原生架构下的网络化共生体

最终，流态型企业成为经济枢纽，生态节点成为高弹性供给单元。流态型企业与生态节点将形成一种以动态调用、协同编排和价值共创为特征的网络化共生关系。流态型企业与生态节点不会彼此替代，而会共同构成AI原生组织时代的“枢纽-节点”网络：前者负责调度与整合，后者负责供给与创新



依托AI OS，企业与个人成为“随需聚散”的流态生产网络

AI原生组织架构模型由三个核心层级及一项垂直支撑构成。底层AI Infra层整合IaaS、PaaS及MaaS，提供软硬件算力与大模型基础服务；AI OS层集成开发平台与安全沙箱等核心系统组件，成为调度中枢；Agent应用层广泛覆盖办公、投研、内容创作、生活管家等各类工作与生活场景；同时，运营与安全模块作为垂直支撑，在全局层面观测运行、把控成本、防御安全风险。AI原生组织依托上述能力，演化出“生态节点”与“流态型企业”两种新组织形态



AI原生组织依托能力接口化与资产化将企业与个体重塑为动态协同网络

定义

- AI原生组织，是以AIOS为调度中枢、以Agent为执行单元、以动态协同网络为运行机制的新型组织形态。其典型形态既包括由传统企业演进而来的流态型企业，也包括由传统个体演进而来的生态节点

关键特征

- 系统接口化: 依托统一网关打通异构系统，将其转化为Agent调用的标准接口
- 经验资产化: 将隐性经验固化为可即插即用的工作流资产 (aaA)，按调用次数计费
- 接入凭证化: 为每个Agent签发身份凭证，强制执行身份核验，预防恶意攻击与信息泄露
- 交互意图化: 自然语言下发意图，系统自主完成工作流的拆解与跨应用的执行
- 协同流态化: 由AIOS编排Agent与节点，实现按需聚散的动态协作

典型架构



目录

Part 03 新范式 AI原生组织转型路线图

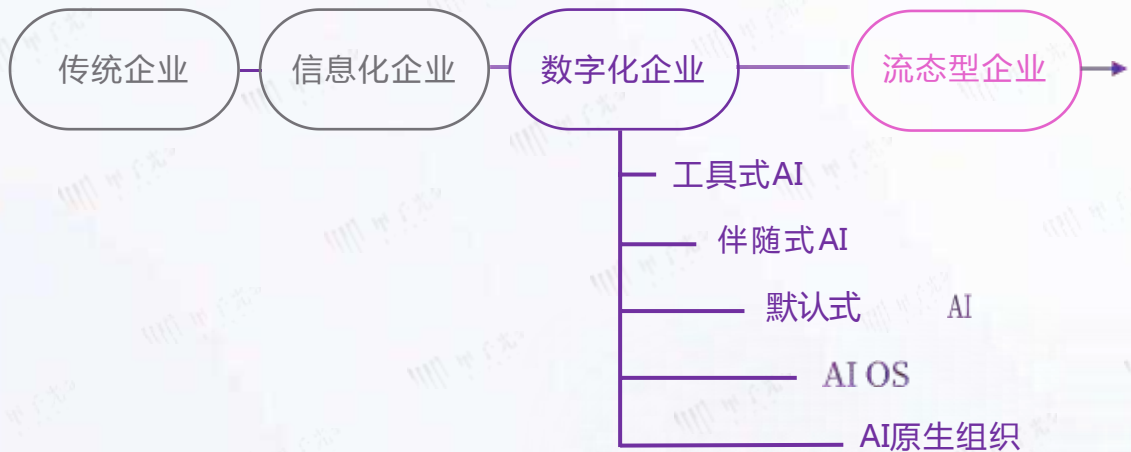
- 3.1 AI原生组织转型路径
- 3.2 路径一：流态型企业转型路线图
- 3.3 路径二：生态节点转型路线图

AI原生组织两大转型路径：传统组织流态化以及超级个体节点化

AI原生组织的转型不再是单一的企业自上而下的改良，而是“传统企业架构流态化”与“超级个体节点化”的双向奔赴，最终形成无边的AI原生组织，重塑组织架构的运转逻辑

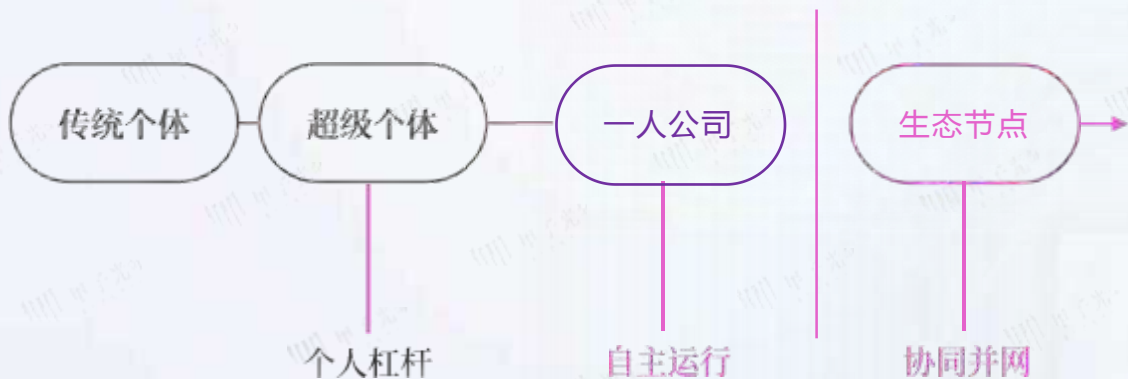
路径一

传统企业向流态型企业的转型路线

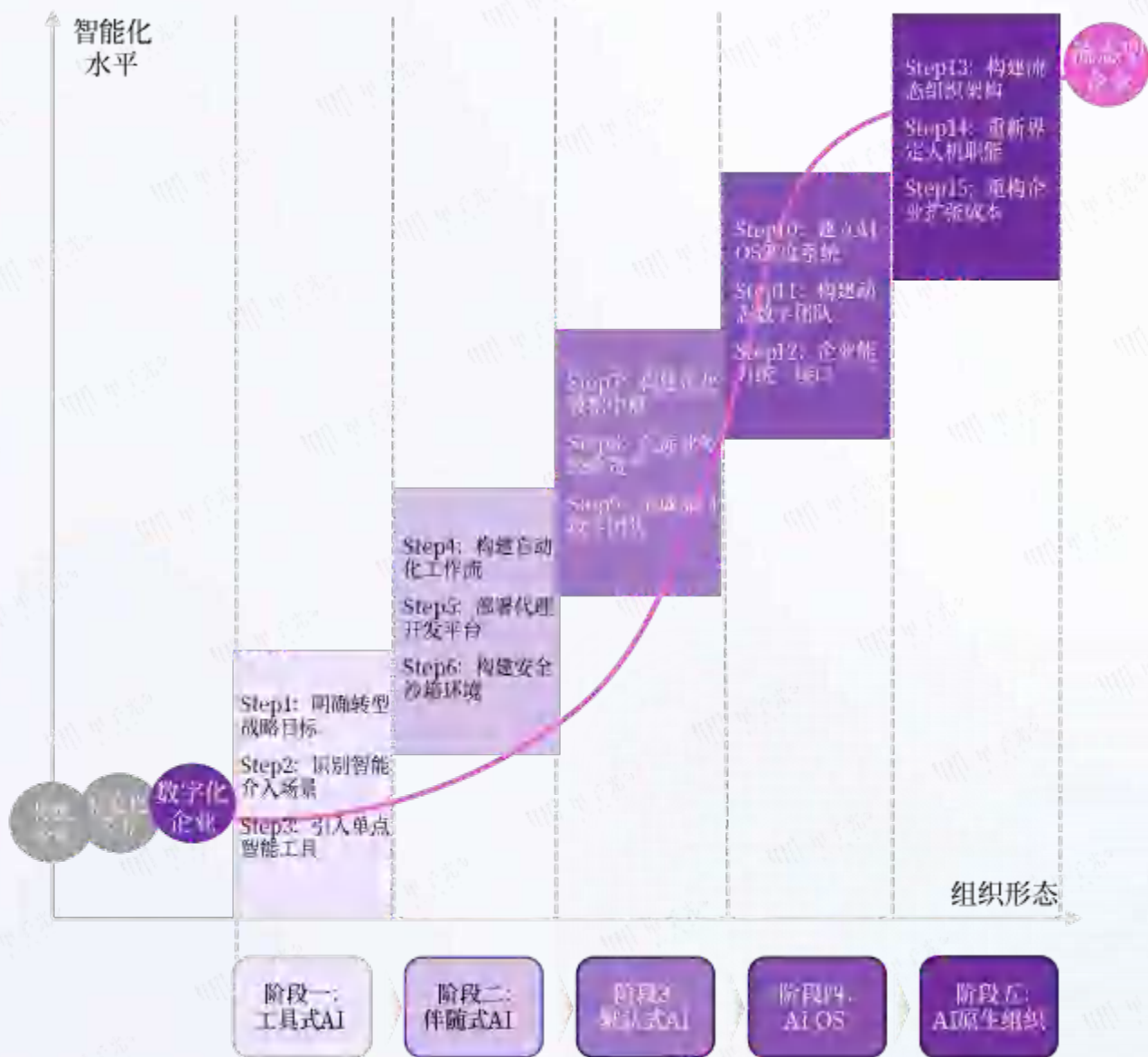


路径二

传统个体向生态节点的转型路线



AI原生组织转型路线图：从传统企业到流态型企业



传统企业向流态型企业的演进，必须以完成“传统企业→信息化企业→数字化企业”的演进为前置条件。在具备数字化底座后，转型根据五个阶段展开：首先通过明确战略目标与引入单点智能工具提效起步；随后依托代理开发平台与安全沙箱构建自动化工作流；继而经由沉淀数据中枢与业务经验资产，组合形成垂直数字团队；进而建立AI OS全局调度系统与动态协同机制；最终通过重新界定人机职能与重构企业扩张成本，完成按需聚散的流态型架构重构

从数字化企业向流态型企业转型的具体实施步骤

阶段一：工具式AI

step1: 在组织内明确以降低内部协作成本与减少跨系统操作为转型核心目标

step2: 对内部流程进行扫描, 锚定高频、规则明确且需跨系统操作的机会点

step3: 在识别AI介入场景的基础之上, 引入适合该场景转型赋能的AI工具, 验证ROI并培养员工使用习惯

阶段二：伴随式AI

step4: 将初步验证的单点AI工具串联成完整的AI工作流

step5: 引入具备多模态视觉与DOM解析的系统级Agent (如openclaw), 用机器视觉和前端解析替代人工的跨系统界面点击

step6: 部署Docker沙盒物理隔离与熔断机制, 构建企业内部的Agent开发平台

阶段三：默认式AI

step7: 企业须建立统一的数据认知层, 部署DataAgent作为全局知识中枢, 以驱动数据与知识的体系化治理

step8: 将员工的隐性经验与决策逻辑, 转化为可复用的工作流资产 (aaA), 建立企业自己的数字员工库

step9: 将单功能的数字员工拼接, 组合成具备独立交付能力的垂直数字团队

阶段四：AI OS

step10: 将AI升格为组织的调度中心, 运行逻辑演进为“意图驱动”, 由AI OS解析自然语言意图, 自主完成任务拆解、任务分配

step11: 依托AI OS按需动态编排跨界Agent, 瞬间组建临时数字团队

step12: 企业将所有系统能力统一接口化, 将其转化为Agent可调用的标准化接口 (B2A)

阶段五：AI原生组织

step13: 打破实体部门界限, 以任务为目标, 建立按需组建Agent的流态型组织

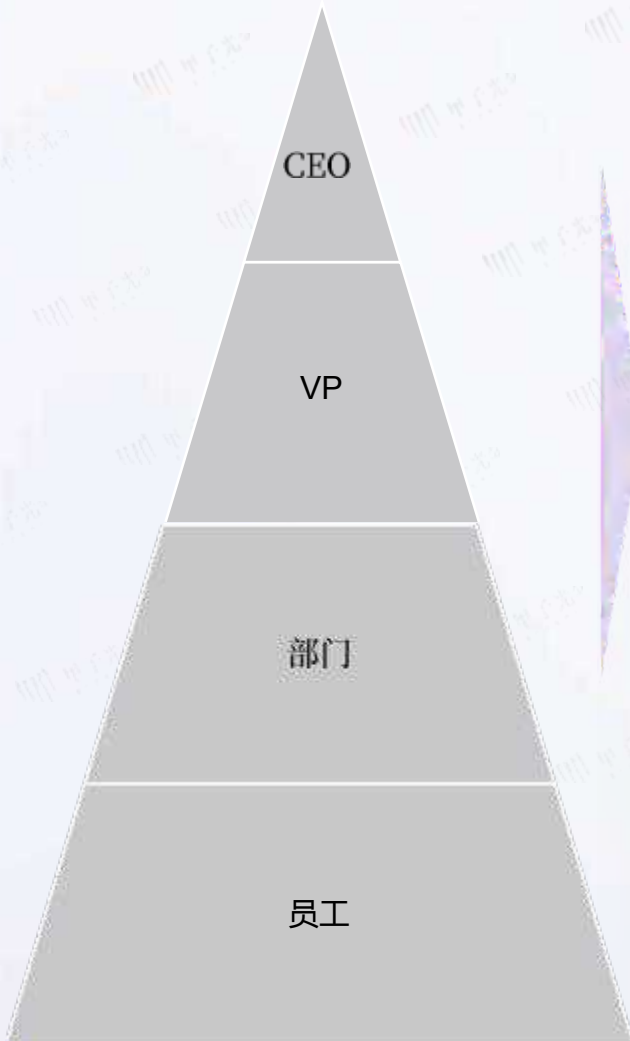
step14: 明确人员与系统的分工界限, 人负责“定方向、提需求、验结果”, AI OS负责复杂的系统调用与资源编排

step15: 企业的扩张不再依赖招募新员工和增加薪酬, 转变为增加Agent的数量与算力规模

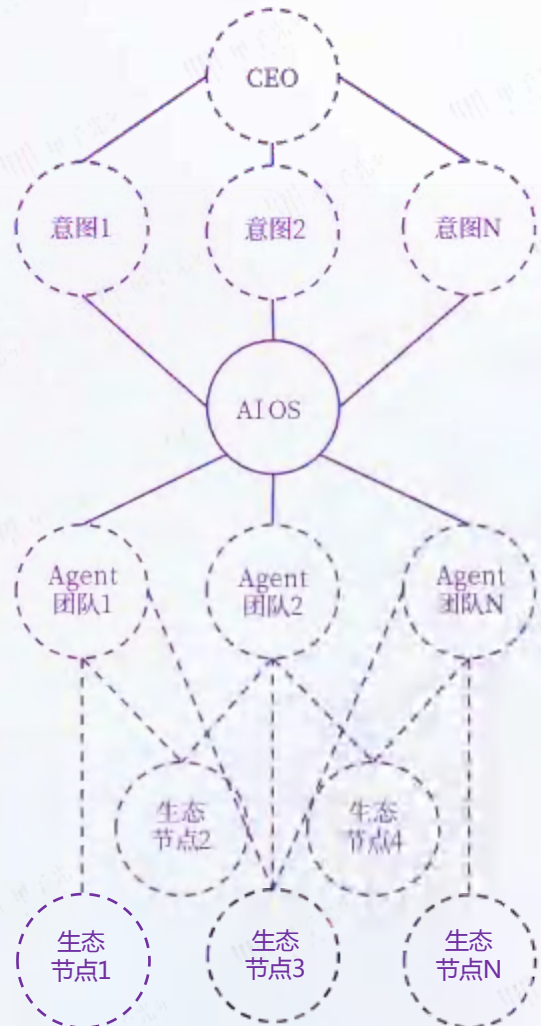
流态型企业的本质是AI调度的生产网络

- 传统企业的物理边界是一座僵化的科层金字塔，业务指令必须依托 "CEO、VP、实体部门到员工" 的链条进行自上而下的传导，会产生极高的信息损耗和管理成本
- 在AI原生组织形态下，科层金字塔将被重构为意图驱动的流程协同网络：管理者仅需下发意图任务，作为全局中枢的AI OS会瞬间拆解任务，动态组建Agent团队，并以生态节点作为高弹性供给单元，独立完成特定业务流的端到端闭环交付

组织经济模式



调度经济模式



AI原生组织转型路线图：从传统个体到生态节点



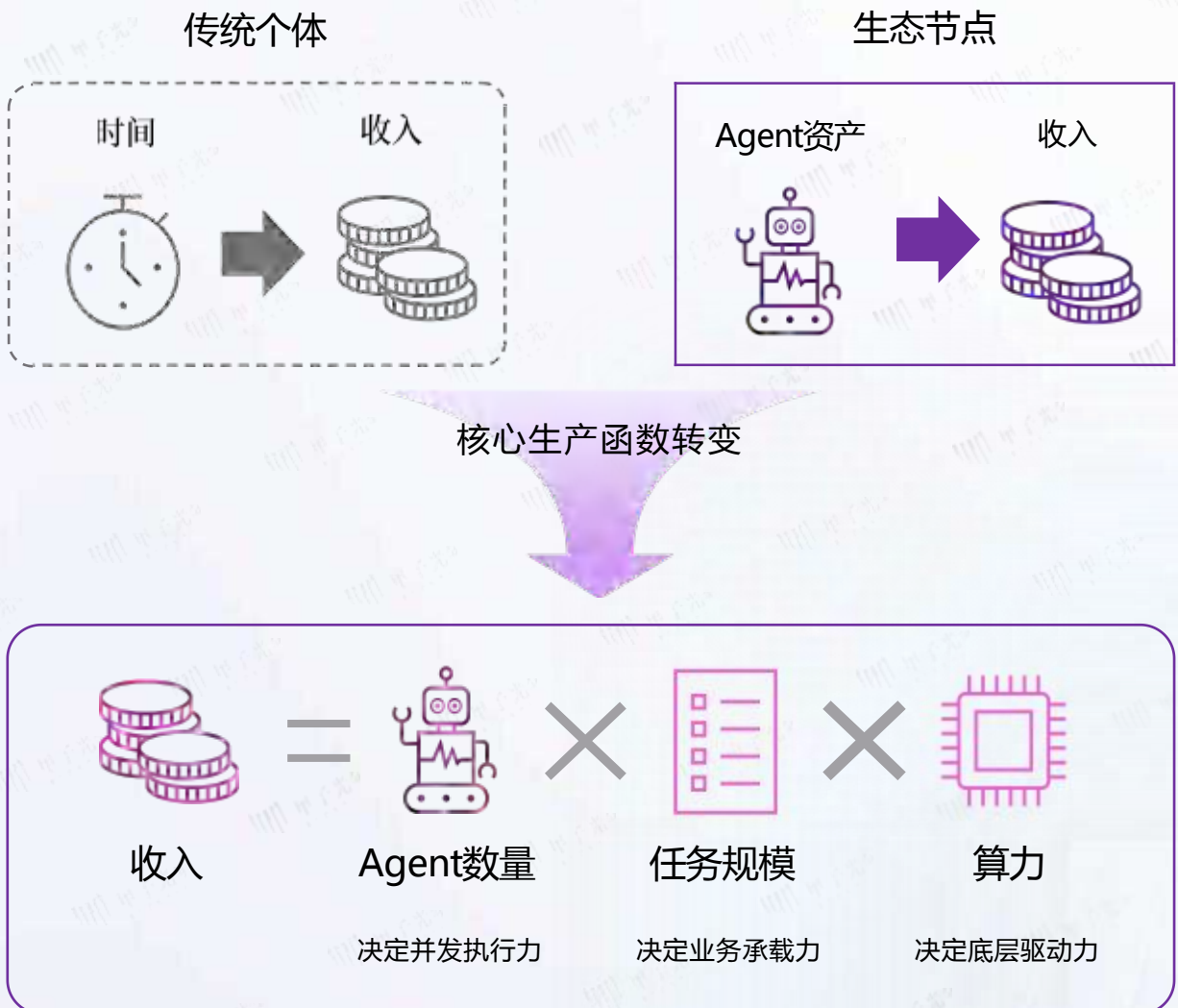
从超级个体向生态节点演进的路线，从盘点工作流程与验证智能工具效能起步，经由部署系统代理框架、构建意图调度中枢等步骤，最终通过封装标准服务接口并对接全网调度引擎，使个体成为高弹性供给单元，嵌入流态企业生态网络，完成向生态节点的跃迁

从传统个体向生态节点转型的具体实施步骤



生产函数转变，个体收益天花板被打开

传统个体的收入逻辑被困在用时间换取收入的线性模型中，物理时间的上限限制了产能与价值的边界。而“生态节点”突破这一瓶颈，将底层逻辑转为“Agent资产驱动收益”。核心生产函数变为“Agent数量×任务规模×算力”，将个体扩张的边际成本从刚性的人力投入转为弹性的Token算力消耗，将个体收益的天花板彻底打开



目录

Part 04 新实践 AI原生组织的实践案例

- 4.1 B端AI原生组织实践案例
- 4.2 C端AI原生组织实践案例
- 4.3 G端AI原生组织实践案例
- 4.4 AI原生组织产业图谱

英伟达Nemoclax: 基于硬件级隔离的企业Agent部署实践

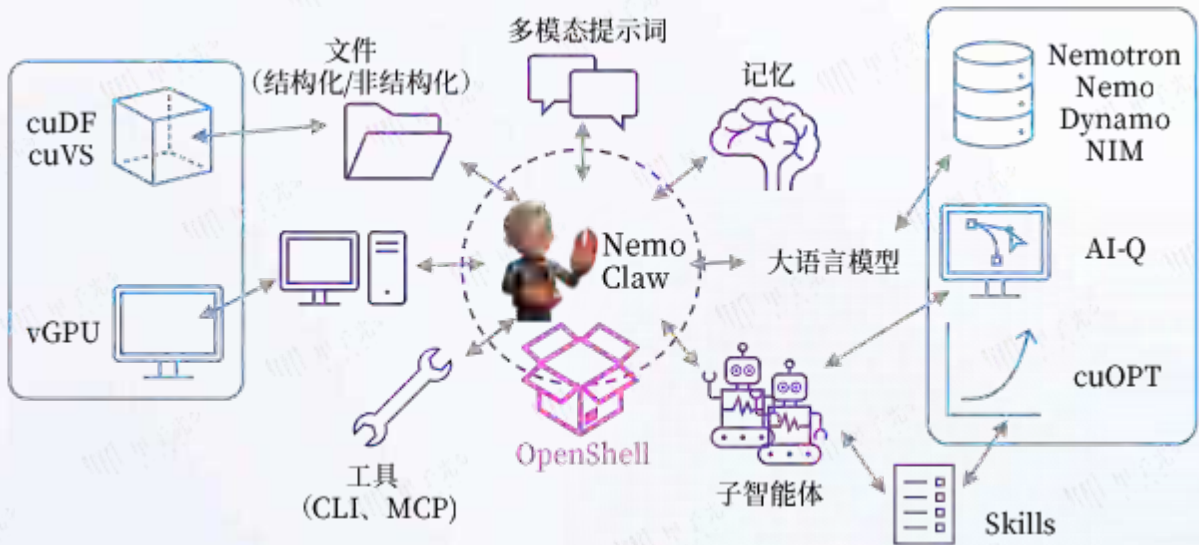
目标与背景

openclaw的爆发凸显了B端在全权限模式下，因缺乏行为观测与边界约束，面临严重的渗透风险，难以满足生产级部署要求。英伟达推出Nemoclax，

旨在通过硬件级隔离与实时审计，将非受控Agent重构为工业“数字员工”底座，破解企业“不敢用、难管理”的部署痛点



实施路径



- 通过openshell构建硬件级沙箱限制Agent底层权限，阻断越权与数据泄露风险
- 结合多模态视觉模型实现非侵入式跨系统操作，并引入成本感知调度器动态分配算力以优化集群部署ROI

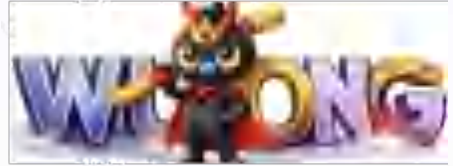
落地效果

戴尔利用Nemoclax在受限内网环境部署了上千个“合规审计Agent”。在保持7x24小时无人值守运行的同时，Nemoclax将平均Token消耗降低了40%

阿里悟空：基于六层防御与底层重构的企业级Agent实践

目标与背景

针对openclaw等通用开源Agent在企业生产环境面临的““权限失控、数据泄露、行为不可观测”等风险，阿里巴巴成立了ATH (Alibaba Token



Hub) 事业群，由钉钉团队打造了企业级AI原生工作平台“悟空”。其目标是通过钉钉底层架构，将Agent关进安全沙箱，实现向确定性生产力的质变

实施路径

底层架构全面CLI化

- 将GUI操作转向命令行界面 (CLI) 驱动，AI不再模拟人类的鼠标点击，而是通过原生接口直连系统能力，确保了指令执行的极高确定性与秒级响应速度

六层递进安全体系

- 构建从“双层规则体系”、“统一身份认证”到“容器级沙箱”、“policy引擎”、“专属模型”及“网络代理”的防御架构。确保AI权限严格限制在用户授权交集内，实现“不是悟空有安全功能，而是悟空架构在安全之上”

AI原生文件系统

- 集成“快照管理”与“命令引擎”的文件系统。AI的每一步操作均产生实时快照，支持秒级任务回退与全链路审计，解决了企业对Agent误操作、乱操作的后顾之忧

落地效果

覆盖10大行业的。PT方案，通过封装淘宝、1688等skill模块实现业务全自动串联，将数周流程缩短至数小时；依托ATH体系，计费模式由“买软件”转向“买结果”，显著提升了经营人效与Toke"利用率

猎豹移动龙虾助理三万：无代码AI助理的14天业务验证

目标与背景

2026年春节期间，猎豹移动CEO 傅盛因滑雪意外导致骨折，被迫卧床休养。面对春节员工放假、公司仍需维持运转的现状，他通过探索AI能否实质性替代人类团队完成复杂的企业运营任务，最终选择使用 openclaw 框架进行长达14天的极限测试，自主驱动了多平台内容的创作与分发，触达大量C端用户



实施路径



抛弃了所有代码编写，仅通过22万字的自然语言语音和屏幕截图，生成了一个高度还原其思维模式的“数字分身”

落地效果

8 Agents				
40+ skills				
20+ crons	6+	100万+	30万+	5000+
14 天	公众号	X Threads	短视频	涨粉

香港大学数据科学学院 Nanobot: 引入严苛财务约束的智能体自我优化验证

目标与背景

绝大多数Agent框架在运行复杂任务时缺乏成本约束, 极易因陷入死循环而消耗巨

额的API费用。香港大学数据科学学院 (HKUDS) 的研究团队希望验证: 能否通过引入严苛的财务限制, 迫使openclaw像真实员工一样追求ROI



实施路径



项目组为Nanobot设定了极其苛刻的生存条件, 仅为其注入10美元的初始启动资金。每执行一次外部搜索或调用一次LLM推理, 系统都会实时扣除相应的Token成本, 强迫其进行 "自我优化"

经营数据

在完全无人干预的测试环境下, Nanobot仅耗时11个小时, 便利用这10美元预算创造了折合15,000美元的等效经济产值, 从根本上证明了将 "算力成本" 转化为 "机器经营指标" 的调度经济范式是成立的

图: 10美元初始资本下的各模型经营绩效实测对比

模型	结余	收入	成本	时薪	平均质量
ATIC+Qwen3.5-plus	\$19,915.68	\$19,914.38	\$8.70	\$2,285.31/hr	61.60%
Gemini3.1 pro preview	\$15,661.71	\$15,757.48	\$105.76	\$1,287.47/hr	43.30%
Qwen3.5-plus	\$15,268.13	\$15,264.92	\$6.78	\$1,390.42/hr	41.60%
GLM-4.7	\$11,497.05	\$11,503.49	\$16.44	\$877.80/hr	40.60%
ATIC-DEEPSEEK	\$10,877.01	\$10,870.52	\$3.52	\$2,579.16/hr	66.80%
Qwen3-Max	\$10,782.80	\$10,781.06	\$8.26	\$1,072.14/hr	37.90%
kimi-k2.5	\$10,471.21	\$10,483.20	\$21.99	\$858.62/hr	36.60%

sunlc虚拟量化对冲基金：基于openclaw的“一人公司”极客实践

目标与背景

随着openclaw的诞生，构建复杂Agent组织架构的技术门槛急剧下降。在此背景下，独立开发者sunlc试图验证：能否在极低硬件（仅一台



MacMini) 与资金成本下，利用openclaw全拟真构建一个包含分析、交易、风控与合规等全链路环节的虚拟量化对冲基金公司

实施路径

极简硬件与成本

- 摒弃传统金融机构的重资产机房配置，系统全部部署于一台入门级MacMini本地终端。核心算力开销仅依赖每月的claude模型订阅费，实现零雇佣成本

角色设定机制

- 通过提示词为代理节点配置对立的投资流派（如“木头姐”与“巴菲特”），强制生成差异化策略视角。当子系统发生观点冲突时，调用更高权限的全局调度节点（如“马斯克”人格）进行强制调解与决策收敛

分阶段异步基建

- 规避直接切入交易环节的失控风险，首期实施限定为构建非侵入式的信息处理基础设施（自动化资讯搜集系统），延后高危的实盘决策权限下放

落地效果

耗时两天即完成多角色Agent节点的满编配置与连通，验证了“单人超级公司”低门槛极速部署的工程可行性，但目前系统仅停留在资讯搜集阶段，无实盘数据支撑；同时，多Agent策略分歧受限于同源基座模型而存在同质化，且高频运行面临严重的框架不稳定性及大模型账号反代封禁风险，尚未具备真实的基金公司能力

深圳福田政务龙虾：基于本地隔离与人工监护的政务Agent实践

目标与背景

福田区作为深圳行政中心，基层公务员每日需处理海量民生诉求。但由于政务外网存在严格的物理隔离，历史遗留的异构系统无法通过常规API

打通，只能依赖极度耗时的人工搬运与审核。福田区的目标是利用openclaw穿透系统壁垒，大幅降低基层行政损耗



实施路径

本地化外网部署

- 基于国产DinTal claw架构开发了“政务龙虾”，并将其基于政务外网环境部署，充分复用了政务云各项安全保护能力

非侵入式跨域调度

- 系统利用3000行核心开源代码构建了九大原子工具。Agent直接以“数字员工”的身份登录各个政务后台，跨越业务系统进行界面抓取与表单预审

沙箱隔离

- 为防范合规风险，所有Agent必须在受限账号的沙箱内运行，且强制要求配备一名在编公务员作为“监护人”，对敏感操作进行最终核验

落地效果

“政务龙虾”上线后，日均稳定处理3500件政务工单。在公共场所卫生许可变更业务中，将传统需3个工作日的人工预审压缩至“当天秒批”。将综合审批效率提升了近3倍，还通过深度聚合民意数据，成功让政府工作从“事后灭火”向“事前预警”转型

AI原生组织产业图谱

Agent应用



AI OS



AI Infra

PaaS



MaaS



IaaS



注：
 • 分类及企业数据截至2026年3月，随着AI在多场景、多领域的不断应用，将不断推动更多企业进入AI领域，未来市场概念可能形成不断分化
 • 由于版面所限，仅通过部分示例企业展示市场特点，顺序不分先后
 • 部分企业具备多个领域的解决方案能力，版面所限，不做一一展示

法律声明

版权声明

本报告由甲子光年智库制作完成，报告内容的版权及相关知识产权均归北京甲子光年科技服务有限公司所有。任何单位或个人在引用本报告内容时，须保持内容的原始性，不得进行歪曲、删改或误导性引用，并须注明报告出处为“甲子光年智库”。否则，由此引发的一切后果由引用方自行承担，甲子光年保留追责权利。

免责条款

本报告中的行业数据、市场预测和相关分析主要来源于甲子光年研究团队通过桌面研究、专家访谈、问卷调查、公开数据整理及甲子光年产品数据等方式获得，部分数据通过甲子光年自主统计预测模型进行估算。我们已尽合理努力确保数据的准确性、完整性与可靠性，但甲子光年不对其作出任何明示或暗示的保证。在任何情况下，本报告中包含的内容、数据或观点均不构成对任何单位或个人的投资建议、法律建议或其他形式的专业意见，相关决策应由读者自行判断并承担风险。由于调研方法和样本范围的限制，报告中发布的数据结果仅反映特定时间段、特定对象的调研情况，具有一定的局限性，仅供读者作参考用途。甲子光年对因使用本报告内容而产生的任何直接或间接损失不承担任何法律责任。

THANKS

谢谢观看

北京甲子光年科技服务有限公司是一家科技智库，包含智库、媒体、社群、企业服务版块，立足于中国科技创新前沿阵地，动态跟踪头部科技企业发展和传统产业技术升级案例，致力于推动人工智能、大数据、物联网、云计算、AR/VR交互技术、信息安全、金融科技、大健康等科技创新在产业之中的应用与落地



扫码关注甲子光年公众号



扫码关注甲子智库公众号

分析师

沈郁翔：微信 (syxkris)

智库院长

宋涛：微信 (stgg_6406)

商务合作

郑爽：18600502376 (微信同号)