

企业级多 Agent 协作与治理平台- AgentTeams

从协作到统一管理与治理，一站式 Agent Harness 落地方案

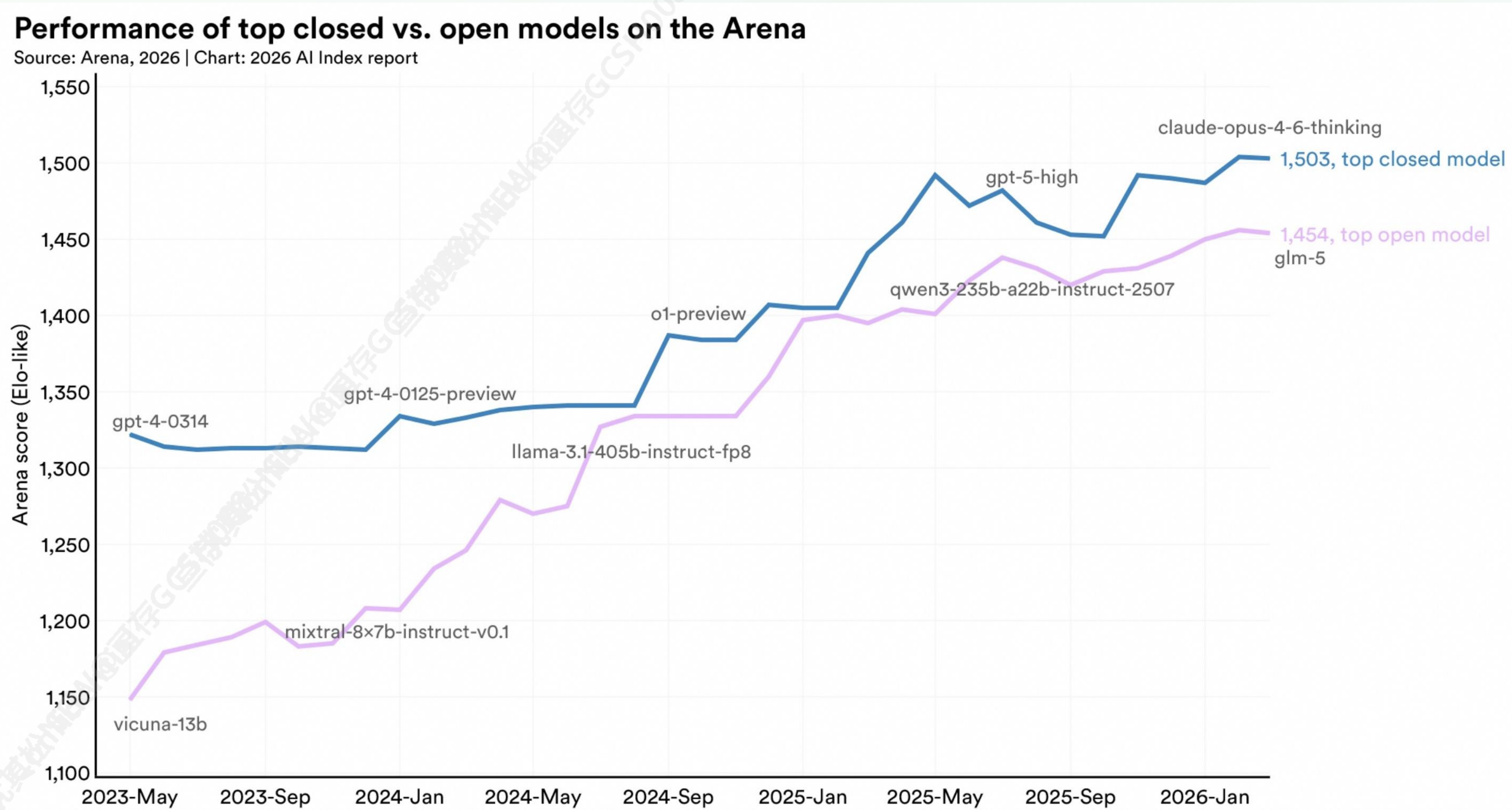
邢学超（于怀）

AgentTeams 负责人，阿里云智能高级技术专家

MODEL CAPABILITIES ARE RAPIDLY IMPROVING

AI 模型能力快速提升

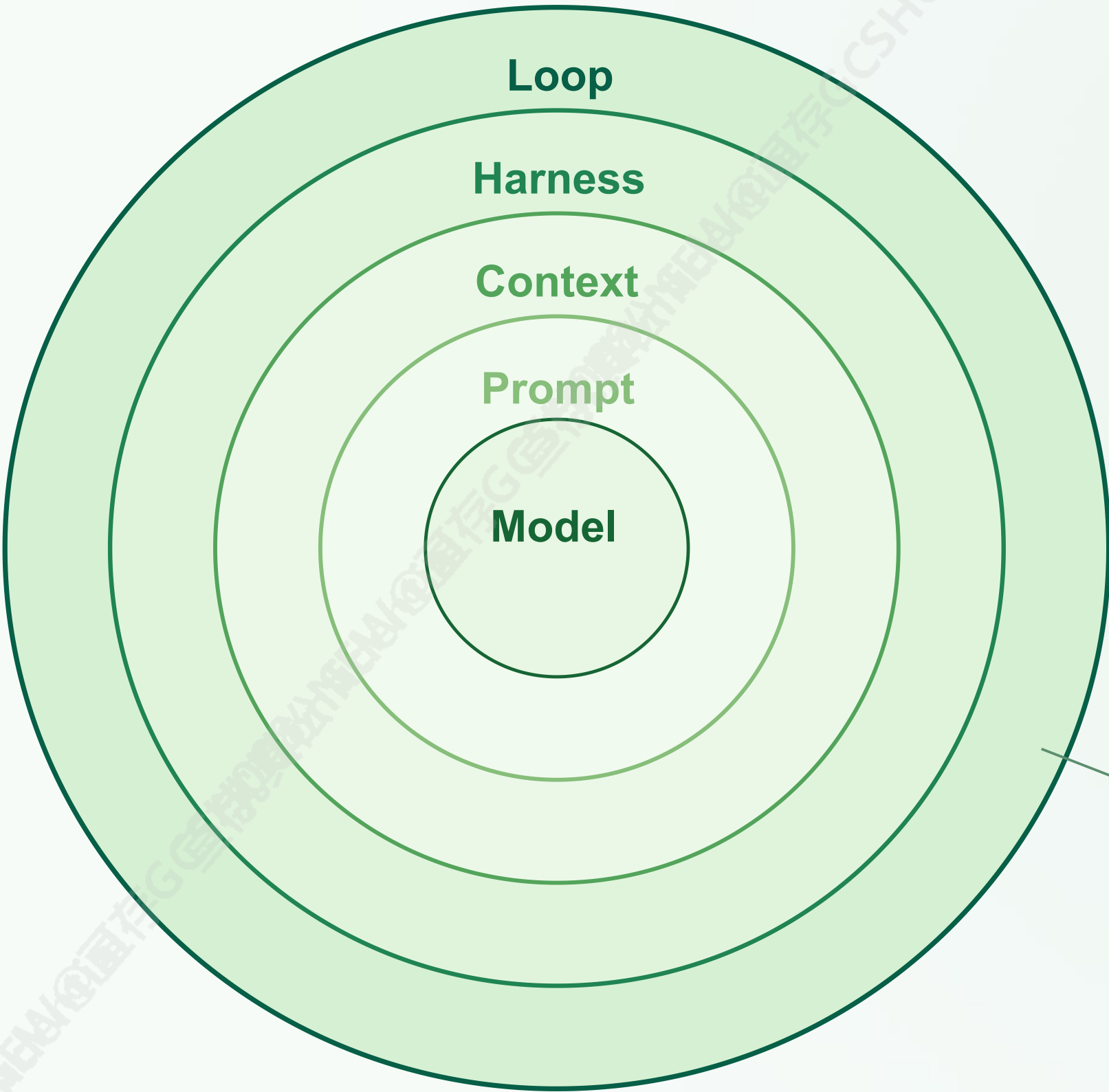
Stanford 2026-ai-index-report



- 大模型军备竞赛-开源、闭源
- 通用模型竞争门槛提升
- 能力效果快速提升
- 业务AI Agent 范式持续迭代

Agent架构快速迭代

The layers that wrap the model



Each layer wraps
the one before it.

Each layer wraps the one before it, so your prompt becomes
one input to a much larger system.

Harness + Loop 面向业务沉淀 Agent 架构

- 模型能力影响 Agent 形态 — 模型改变 Agent 范式
- Agent概念迭代变快 — 从 PE 到 LE 概念越迭代越快
- 持续发展业务视角 — 脚手架建了又删，删了又建
- 业务落地解决问题是核心 — 抓住业务价值，不变实现路径

AI Agent 在企业落地

Gartner Warns: 40% of
Agentic AI Projects to Fail by
2027



主要原因在于治理不足和技术债积累

企业落地 Agent 的瓶颈，不是模型能力本身，能否有能力治理 Agent 和落地业务是关键；

- 零信任治理 — 权限和身份信任治理、资源信任治理、通信信任治理
- 协作治理 — 多人、多Agent 组织在一起，协作如何治理
- Agent 资源治理 — sandbox资源、MCP、Skills 复杂企业级管控
- 业务持续观测进化 — Agent 要能持续进化，怎么积累数据，越用越好用

AgentTeams · 产品简介

AgentTeams · 开源 HiClaw 的企业级商业版

把社区验证的多 Agent 协同内核，补齐 SLA、身份认证与纳管——成为企业级多 Agent 协作 & 统一管理 & 治理平台

开源 HiClaw — 经社区验证的协同内核

- **Matrix 协议** — 人机同构的全透明协作网络
- **Higress AI 网关** — 凭证隔离的零信任治理
- **Manager – Worker** — 高度解耦的分层 Agent 架构
- **AgentScope 社区共建** — 携手 QwenPaw 打造开源生态

商业化

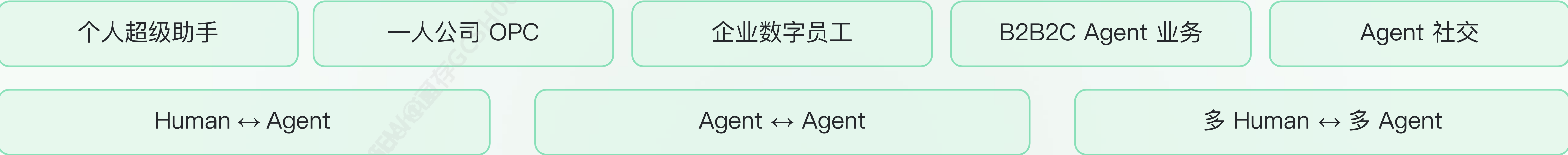


AgentTeams 企业级 — 落地最后一公里

- **BYOK 模型和算力** — Agent 使用的模型和算力用户决定
- **企业 SSO 身份认证** — 接入 Agent Identity 统一身份认证
- **Manager – TL – Worker** — 引入 Team, Team Leader
- **多种 Agent、CLI 纳管** — 纳管 OpenClaw, Claude Code 等

AgentTeams · 多 Agent 协作 · 治理 · 管理统一底座

支持托管 QwenPaw，纳管 OpenClaw、Claude Code 等各类 Agent 与 CLI



AgentTeams · 不是工具 · 而是多 Agent 协作管理底座

不是替代开发工具，而是让企业敢把多 Agent 放上生产

维度	AgentTeams	Claude Code · CMA	通用多 Agent 框架
定位	企业级多 Agent 协作·治理·管理统一底座	开发者编码 / 任务编排	多 Agent 编排库 / SDK
Agent 实现	任意 Agent 与 CLI 纳管 · 跨 Agent 实现 QwenPaw / OpenClaw / Claude Code / 自研	以 Claude 系为主	绑定自身框架
协作模型	Matrix IM 全透明 · A2A+A2H · 跨主机	父子 subagent · 单机为主	进程内函数调用编排
安全治理	零信任 AI 网关 · 凭证隔离 · AI 资产统一管理	应用级权限 + 凭证保管库	基本靠自行实现
可观测	Room 留痕 · SLS 日志&全链路 · Agent Loop下钻	运行日志 / transcript	基本靠自行实现
部署弹性	ACS Sandbox HPA · 单Session单实例	本地会话 / 托管 session	自运维
自进化	集成 AgentLoop · 评估 · 调优	靠 Claude 系黑盒处理	基本靠自行实现
模型类型	每个 Agent 独立模型 · 自行切换模型	Claude 系模型	自行实现切换模型

AgentTeams · 企业级Agent治理和系统实践

四道防线 · 重塑多 Agent 协同的信任边界

从身份、运行时、通信到AI资产管理，构建坚不可摧的「零信任」Agent 管理底座



AI 网关

AI 网关纳管 · Agent 零凭证

Identity & Access

- Agent 零凭证持有
Agent 不再持有任何 API Key 与敏感数据
- 统一鉴权托管
LLM 调用与外部密钥由网关集中加密
- 细粒度风控
Agent 身份认证 + Skill/MCP 指令级拦截



Sandbox 沙箱

Sandbox 安全隔离 · 铜墙铁壁

Runtime Isolation

- 三个维度安全隔离
实例隔离、网络隔离、存储隔离
- 爆炸半径收敛
越权或提示注入破坏 100% 锁死单沙箱
- 保卫企业内网
异常行为不波及核心 IT 环境



Matrix 协议

Matrix E2EE 通信 · 点对点加密

Secure Communication

- 点对点加密
Matrix 原生 E2EE 端到端数据传输
- 防窃听协同
任务派发、上下文与数据流转全程加密
- 审计可溯源
Room 信息透明可追溯



Skill 市场

Skill/MCP 市场管控 · 可信 AI 资产

Trusted Supply Chain

- 上架安全审核
安全扫描审核才注册，杜绝恶意能力
- 按需授权调用
网关 per-consumer ACL · 最小权限
- Skill 分组管理
分组间隔离，Skill Portal 分发逻辑

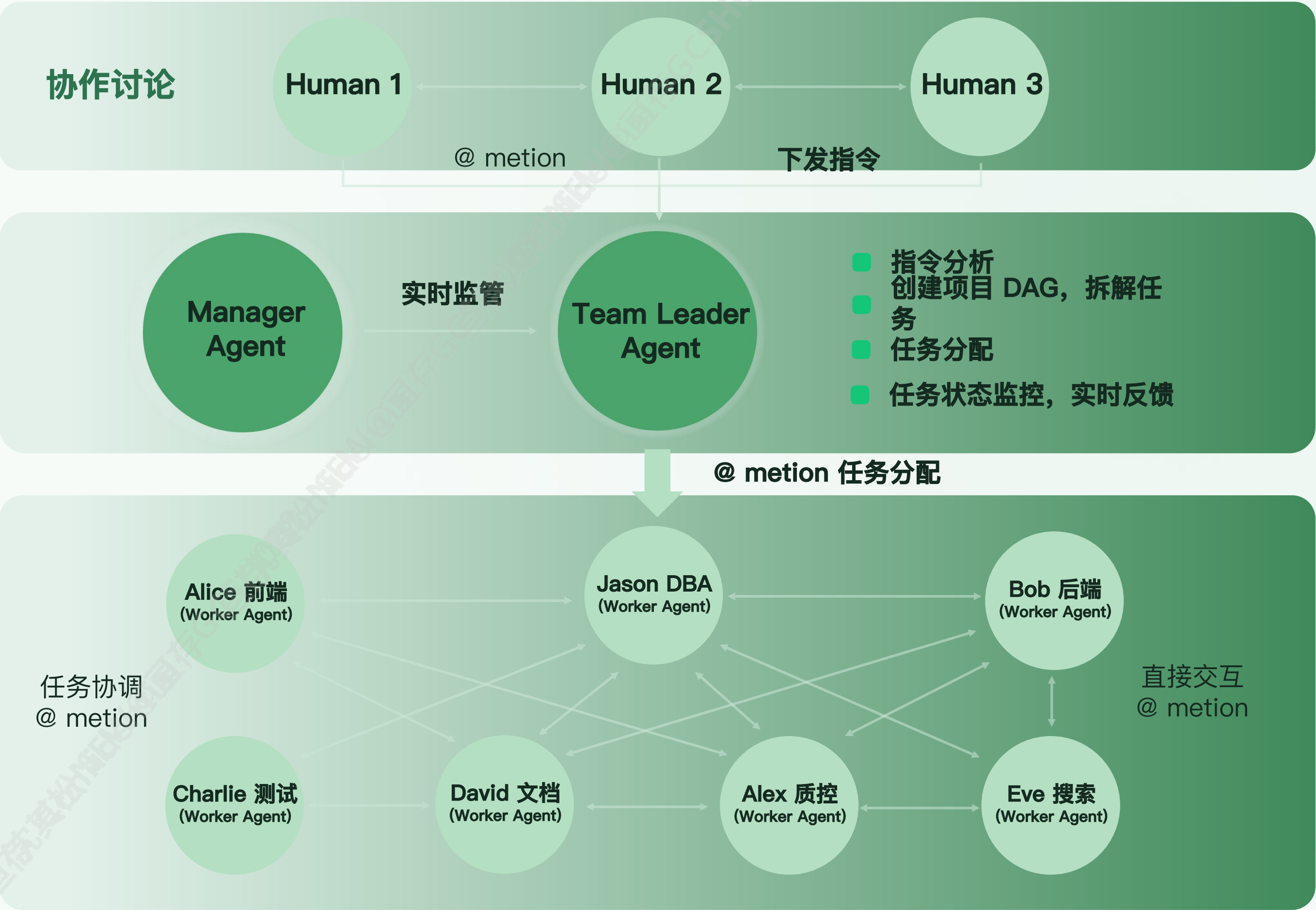
集成 Agent Identity · 统一托管 Agent 身份与凭证

入站认证调用方 · 出站托管凭证 · 细粒度权限授权 —— Agent 零明文凭证持有 · 安全访问内部服务



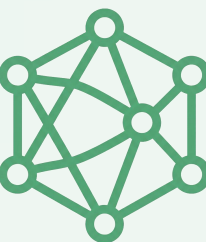
基于 Manager - Team TL - Worker 架构的协同底座

打造透明的、可控的 Agent 团队



Team Leader – Worker 智能调度
各司其职的 Agent

- Team Leader 负责任务分解与分配
- Worker 专注执行



基于 Matrix 的共享上下文
全透明的数字会议室

- 所有对话与状态实时可见
- 人与 Agent 在同一空间协作



Human-in-the-Loop
随时介入的安全感

- 人类可随时 @mention 介入
- 实时观察, 必要时接管控制



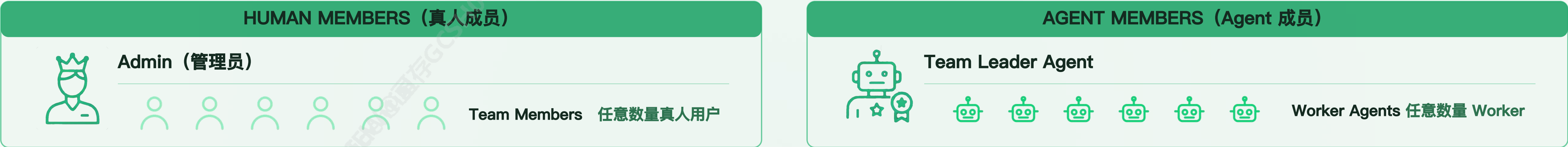
跨群组协作
支撑一人公司与企业级数字员工

- 灵活组建临时团队
- 从个人助手到企业级规模

团队管理 - AgentTeams 的人机协同组织模型

真人成员与 TL / Worker Agent 在团队群中协作：TL 拆解分配、真人随时打断、私聊直达，交互权限严格限定在团队内

LAYER 1 · TEAM COMPOSITION (团队组成)



LAYER 2 · INTERACTION SPACE (交互空间)



LAYER 3 · KEY FEATURES (核心特性)



三种交互方式 · 全场景覆盖 Agent 协作

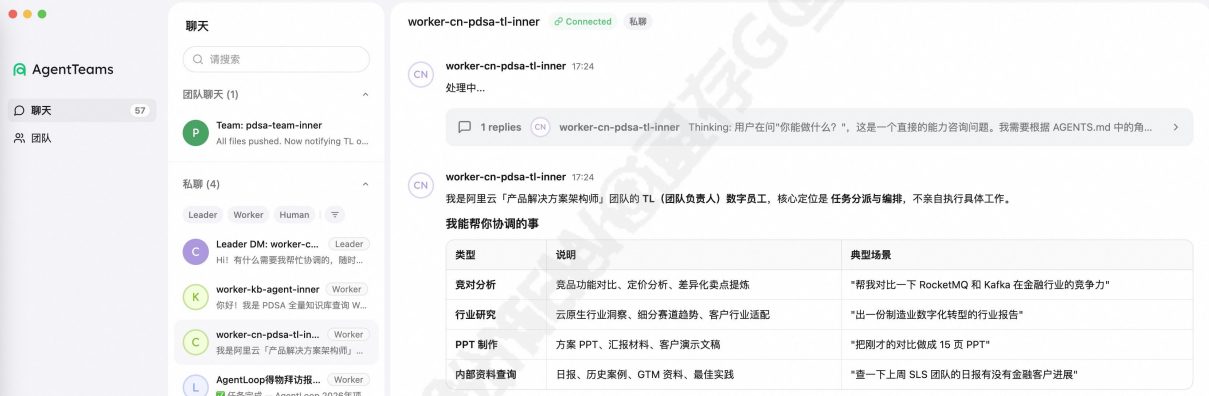
原生 IM · 企业平台集成 · HTTP 服务化 —— 让 Agent 触达每一个工作场景



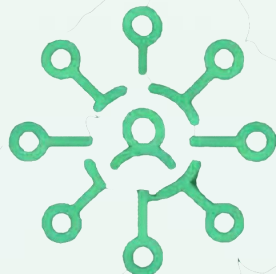
01

AgentTeams 原生客户端

IM 即时通讯交互



- Matrix 协议原生支持
- 多 Agent 协作可视化
- 实时消息与 Agent 对话
- 完整上下文保留



02

企业协作平台集成

钉钉 · 飞书 · 企业微信



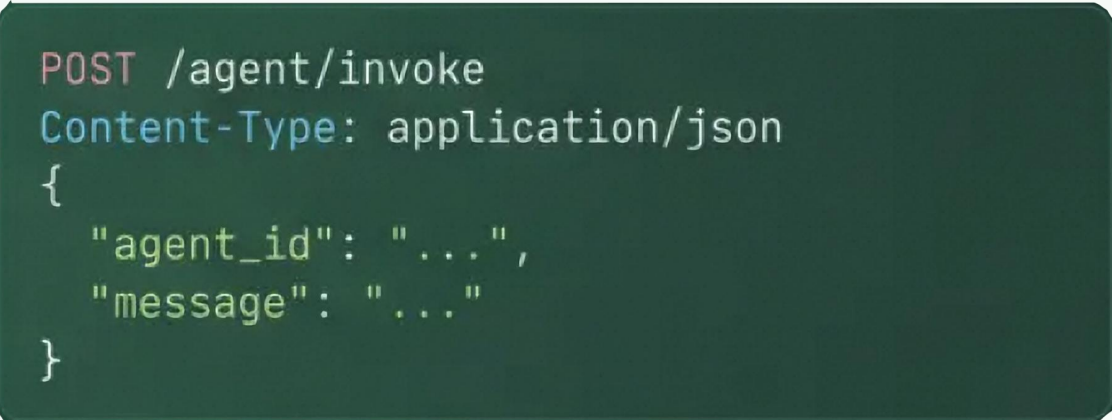
- 无缝对接企业 IM
- 融入现有工作流
- 员工零学习成本
- 统一身份认证



03

Agent 服务化接口

HTTP API 调用

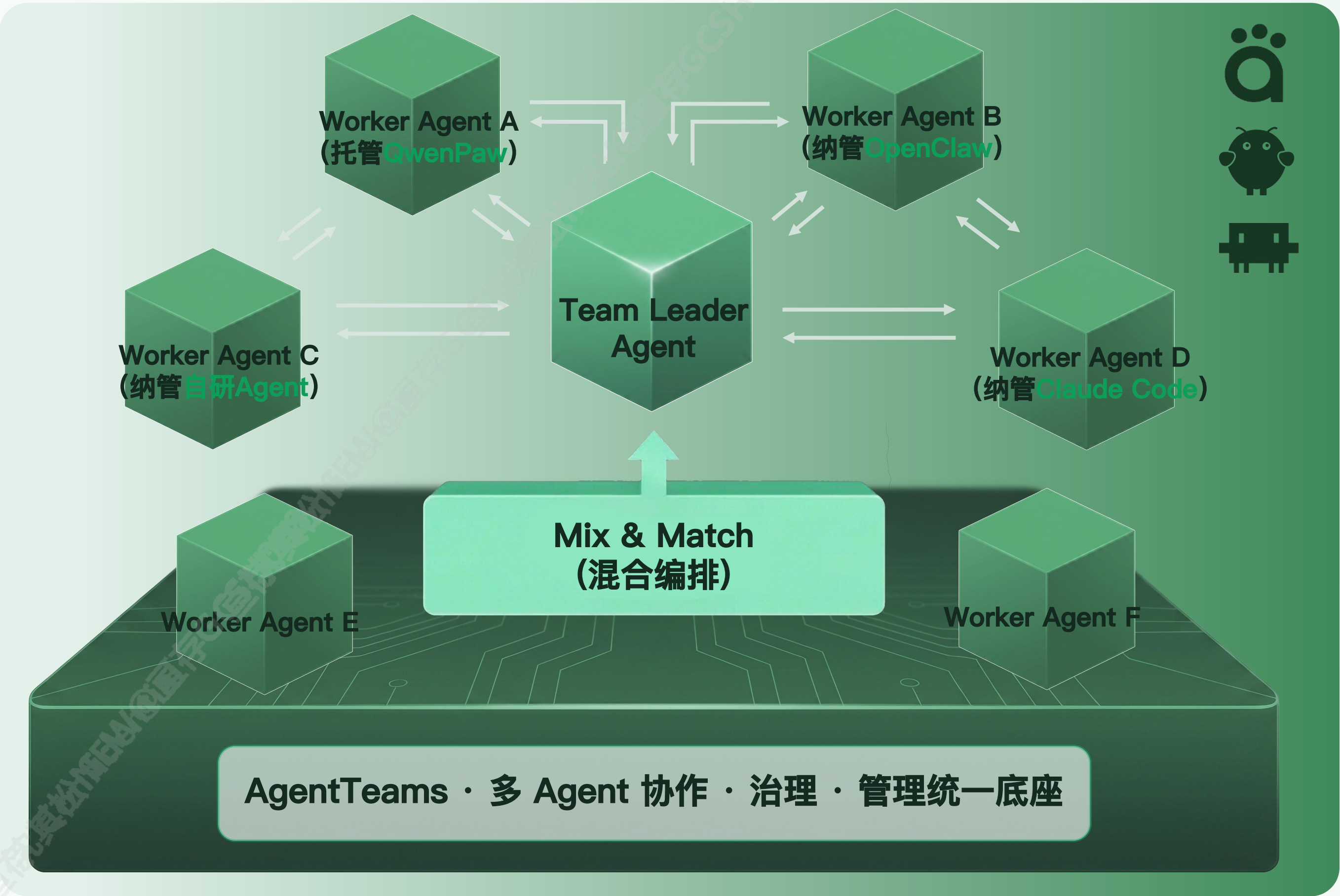


- 标准 HTTP/REST 协议
- 支持同步/异步调用
- 系统间无缝集成
- 完整 API 文档

AgentTeams · 统一底座 · 灵活接入 · 一致体验

AgentTeams 无缝托管和纳管各类 Agent - CLI

托管 QwenPaw, 纳管 OpenClaw, Claude Code, 其他各类 Agent 实现和 CLI



协议级解耦,消除Agent框架绑定

- 所有Agent基于标准Matrix协议沟通
- AgentTeams底层透明,不绑定单一Agent框架,核心资产沉淀在平台层



引擎热插拔,目前完美支持多擎驱动

- QwenPaw: 自研、轻量,特定领域优势
- OpenClaw: 强大任务规划与执行,适合复杂逻辑拆解
- Claude Code: 强大的Coding能力和长程任务能力



“混编团队”: 发挥每个框架的最强战力

- 极致灵活性: QwenPaw可作Team Leader统筹全局,指派 OpenClaw,Claude Code 任务
- 跨引擎协作: 不同底层Agent在同一协作底座内无缝沟通,共享上下文



面向未来的无限扩展能力

- 无缝接入新框架: 通过Channel Plug接入Matrix,可平滑接入 Claude Code、QoderWorker或其他Agent

AgentTeams 客户端

AgentTeams 客户端同时支持Web端、MacOS端、Windows端

AgentTeams

新任务

聊天99+

团队

最近任务

- Element 应用设计
 - 前端开发
 - 产品设计
 - 后端开发
- 团队工时 Skill
 - 团队名单统计
 - 工时计算规则

全部任务

本地 Agent

- U-444MXKVX-233...
- U-555MXKVX-233...
- U-666MXKVX-233...

设置Admin

对话列表

搜索群聊或智能体

群聊 (3)

- Design Team8分钟前
 - Yuanjia: 最新设计方案
- Developer Team8分钟前
 - Yuanjia: 最新设计方案
- Product Team8分钟前
 - Yuanjia: 最新设计方案

私聊 (12)

LeaderWorkerHuman全部团队

- Frontend Developer8分钟前
 - Design Team
- UX Designer8分钟前
 - Design Team
- Product Specialist8分钟前
 - 最近一次聊天内容
- Demo Worker A8分钟前
 - Design Team
- Lisi8分钟前
 - HumanDesign Team
- Zhangsan8分钟前
 - HumanDesign Team

其他 (3)

Front Developer

LeaderDesign Team

你好，帮我写一篇关于 AI Gateway 的报告

Front Developer8分钟前

我将在你撰写一篇关于 AI Gateway 的报告，需要先明确一下，您提到的 AI Gateway 是指阿里云的 AI Gateway 么？

已选择：是

收到你的需求了！为了确保深入理解，我需要先进行详细解析。

了解用户需求完成

导入数据完成

生成执行计划完成

我已经充分了解了 AI Gateway 的相关信息，接下来将开始撰写报告

super_agent_sub_agent Fb

输入

```
1 {
2   "id": "sub-agent-2"
3   "name": "撰写报告",
4   "query": "撰写一篇关于 AI Gateway 的报告。AI Gateway 是阿里云提供的一款智能体开发和运行平台，支持开
```

请输入任务内容，'shift+enter'换行

AI may make mistakes. Please verify important information.

AgentTeams

新任务

聊天99+

团队

最近任务

- Element 应用设计
 - 前端开发
 - 产品设计
 - 后端开发
- 团队工时 Skill
 - 团队名单统计
 - 工时计算规则

全部任务

本地 Agent

- U-444MXKVX-233...
- U-555MXKVX-233...
- U-666MXKVX-233...

设置Admin

团队

搜索

Design Team8分钟前

- Team Leader: PD
- Workers (11)Human (6)
- 任务 (进行中: 8, 已完成: 3)
- Element 应用设计+10

Frontend Team8分钟前

- Team Leader: PD
- Workers (11)Human (6)
- 任务 (进行中: 8, 已完成: 3)
- Element 应用设计+10

Backend Team8分钟前

- Team Leader: PD
- Workers (11)Human (6)
- 任务 (进行中: 8, 已完成: 3)
- Element 应用设计+10

Research Team8分钟前

- Team Leader: PD
- Workers (11)Human (6)
- 任务 (进行中: 8, 已完成: 3)
- Element 应用设计+10

Legal Team8分钟前

- Team Leader: PD
- Workers (11)Human (6)
- 任务 (进行中: 8, 已完成: 3)
- Element 应用设计+10

Branding Team8分钟前

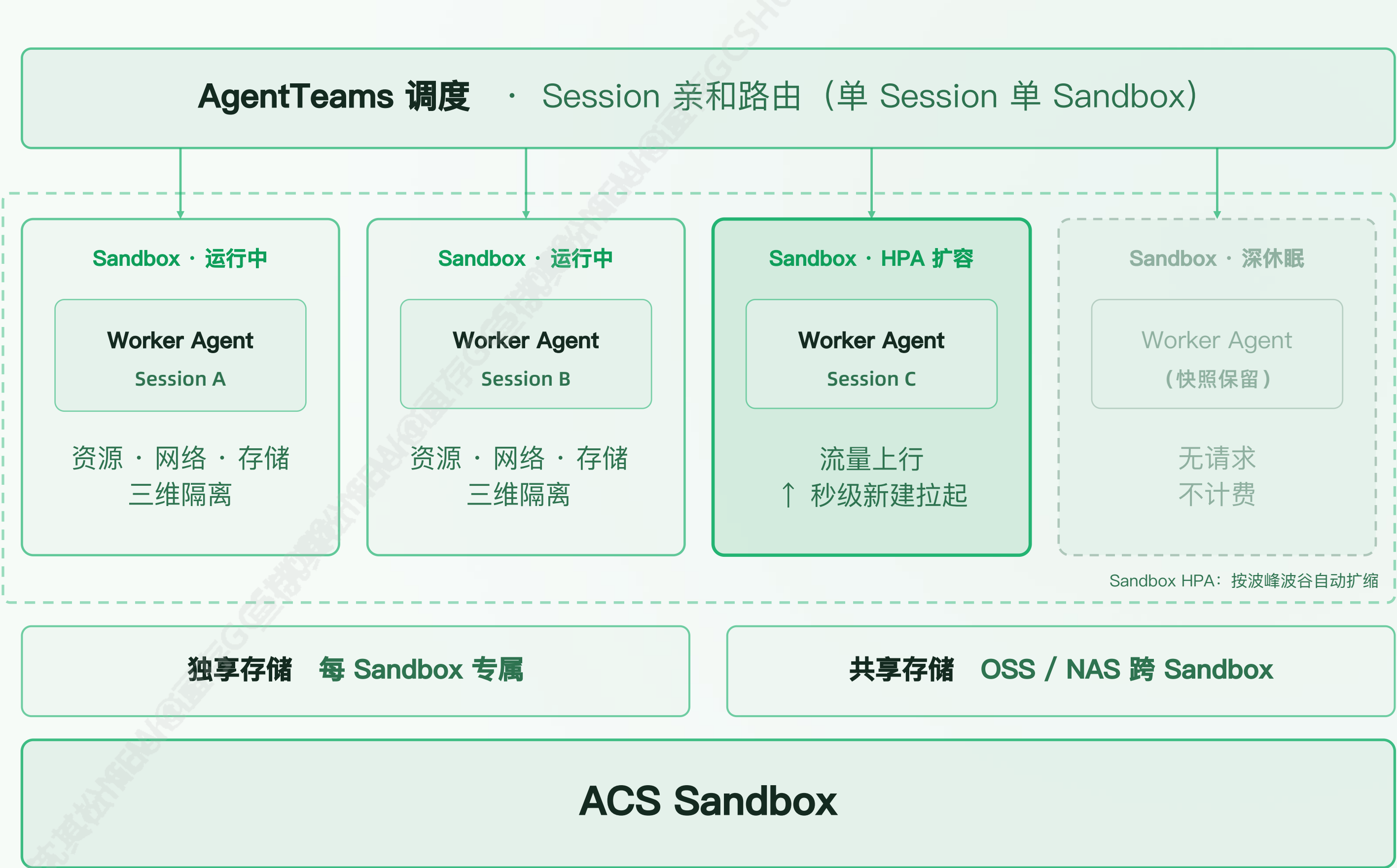
- Team Leader: PD
- Workers (11)Human (6)
- 任务 (进行中: 8, 已完成: 3)
- Element 应用设计+10

共 5 团队

123...共4页，每页显示15

集成 ACS Sandbox · 安全隔离 · 弹性伸缩 · 按需计费

托管 Agent 实现三维物理隔离保障安全 · Session 亲和实现 Sandbox 级 HPA · 深休眠做到无请求不计费



三维安全隔离

- 资源 · 网络 · 存储三重隔离
- Agent 运行环境互不干扰，安全可信



Session 亲和 · Sandbox HPA

- 单 Sandbox 单 Session，会话不串扰
- 按 Session 请求扩缩，稀疏调用不浪费



存储独享或共享

- Worker Agent Sandbox 可独享存储
- 也可挂载共享存储 (OSS / NAS)



深休眠 · 按需计费

- 无请求时 Sandbox 深休眠，不计费
- 有请求秒级拉起整个 Sandbox 快照

扛并发、压时延：Worker Agent 三种伸缩方式

两路扩并发（Session 级隔离 / Team 级分流） · 一路压时延（Subagent 进程内协作）

扩并发 · SESSION 级

单 Session 单 Sandbox

Worker Agent

S1S2S3S4S5

5 人同时交互产生 5 个 Session，Worker Agent 为每个 Session 拉起独立 Sandbox 并行接请求，会话间天然隔离。

→ 并发随 Session 数线性扩展

扩并发 · TEAM 级

多 Teams 副本分流

请求 · 负载分流

Team ATeam BTeam C

在 AgentTeams 中创建多个相同的 Team，以副本为单位分流请求，像多实例负载均衡一样横向扩并发。

→ 并发随 Team 副本数扩展

压时延 · 进程内

Subagent 同进程协作

AgentAgentAgent多跳

Subagent 同一 Sandbox 进程 · 0 网络跳数

SubSubSub0 跳

一个 Worker Agent 内建多个 Subagent，各自独立 SOUL.md / AGENTS.md / Skill / MCP；流程同进程流转，省去跨进程与网络开销。

→ 多 Agent 协作 RT 趋近单进程调用

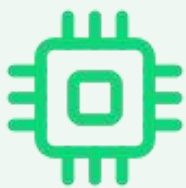
并发 靠加 Sandbox / 加 Team 副本横向扩

时延 靠把 Subagent 收进同一进程压到最低

统一管理 Models · MCP · Skill · Agent 模板 AI 资产

大模型、MCP Server、Skill 集中管理 · 配置即用 · 统一鉴权 · 安全审核 —— AI 资产 BYOK 自主可控

AgentTeams · 统一 AI 资产平面 Unified AI Asset Management



大模型

Models

01

配置代理

- 代理主流大模型厂商（通义 / OpenAI / Claude 等）
- 接入自建 OpenAI 协议模型

细粒度管控 · 对接 AI 网关

- Token 限流
- 灵活的模型路由
- AI 安全护栏



MCP Server

Model Context Protocol

02

配置代理

- 代理原生 MCP Server
- 将 HTTP 服务转换为 MCP Server

统一治理

- 对 MCP Server 统一管理
- 统一鉴权



Skill

技能资产

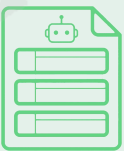
03

安全审核

- 防 Prompt 注毒
- 防敏感信息泄露

分发治理

- 对 Skill 分组管理
- 基于 Portal 统一分发



Agent 模板

Agent Template

将模型 · Skill · MCP 固化封装，沉淀行业经验 —— 快速基于模版构建 Agent，开箱即用、一致可复制

04

任务管理 · 像管理团队一样管理 Agent 的工作

任务全生命周期可管可视 · TL 拆解分配 · 实时进度与阻塞主动上报 · 人机同看板协同，沉淀为可复用 Skill

TASK FLOW · 任务 workflow



任务看板 · Team Room 内实时可视



任务看板 · Team Room 内实时可视



任务管理核心能力 · 每个任务持久化为 tasks/{taskId}/ → meta.json (状态/时间戳) + spec.md (任务描述)



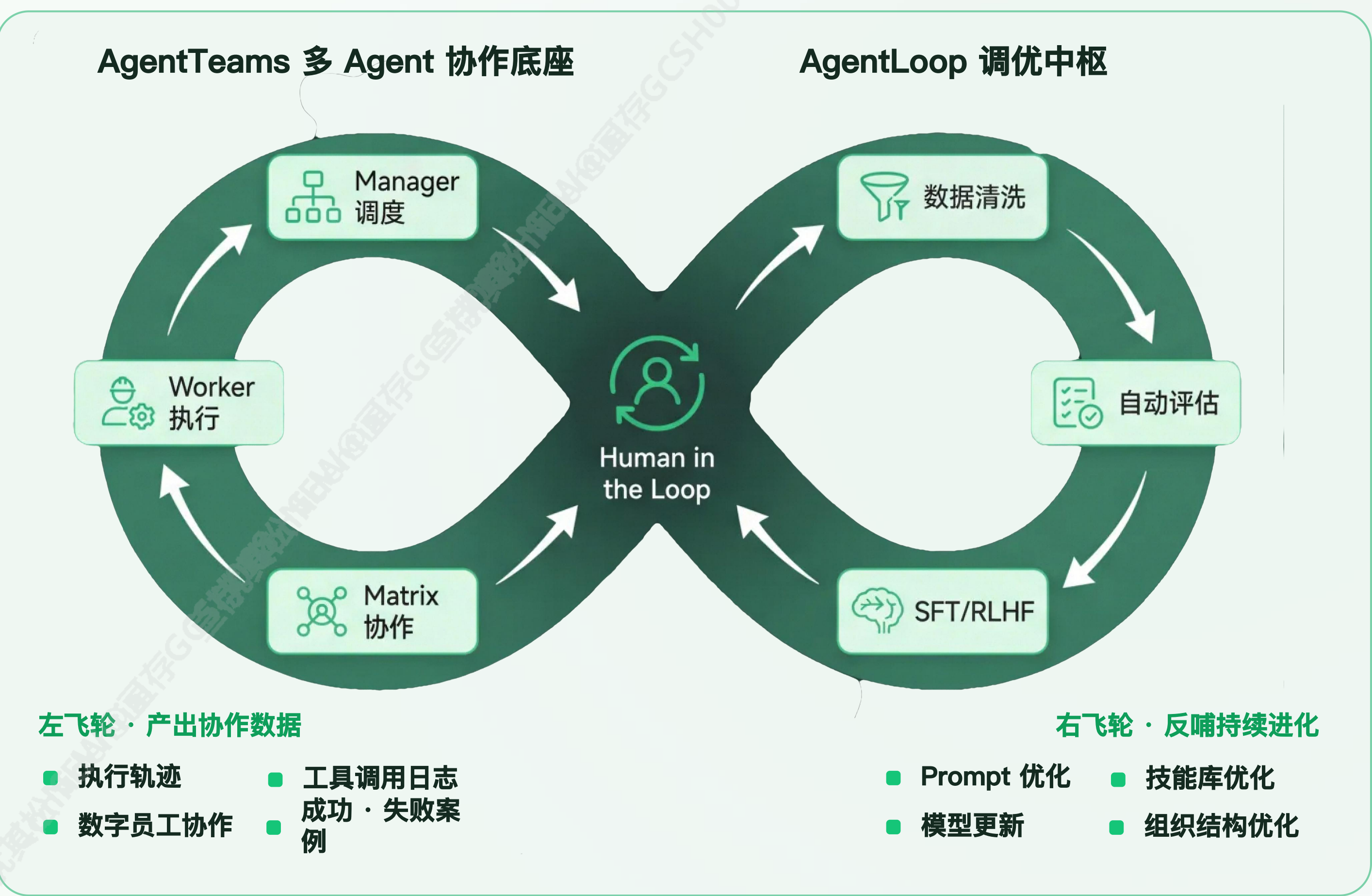
AgentTeams 全栈可观测 · 端到端追踪每一次 Agent 调用

贯穿用户 / Client → AgentTeams Agent → AI 网关 → Skill · MCP · 模型 —— 统一监控 · 全链路诊断 · 结果评估与审计



集成 AgentLoop · 数据驱动的 Agent 持续进化飞轮

AgentTeams 左飞轮产出协作数据，AgentLoop 右飞轮反哺持续进化



理念升级：从「写代码」到科学「养 Agent」

- 打破黑盒：依托 AgentTeams 沉淀的全量协作上下文，用真实业务数据喂养数字员工
- 能力爬坡：让 Worker Agent 在真实报错与人类纠偏中学习企业独有 SOP

无缝对接 AgentLoop 调优引擎

- 数据采集标准化：AgentTeams 提供高质量、结构化的多模态协作日志与工具调用链
- 闭环评估体系：AgentLoop 自动打分与弱点分析，定位是模型、工具还是 Prompt 问题

企业级「数据-智能」飞轮（核心链路）

- 发现 Discover：监控高频失败 Task，沉淀 Bad Case
- 对齐 Align：结合人类偏好数据，构建专属 DPO / RLHF 训练集
- 进化 Evolve：Prompt 自动重构，持续提升效果

沉淀企业核心 AI 资产

- 越用越聪明：Agent Team 从「通用型 AI」进化为契合私有流程的「资深专家集群」，成为不可复制的业务壁垒

AgentTeams · 应用场景

AgentTeams 落地全景

从 IM 入口到职能 Agent Team：身份打通企业用户体系 · 多引擎纳管 · 资产统一 · AI 中台全程观测，让数字员工融入企业组织



企业提效 · 数字员工应用场景示例

Dog Fooding · SRE系统 · 运营系统 · PDSA AI 工作台

SRE AI Native 诊断系统



运营 AI Native 数据分析系统

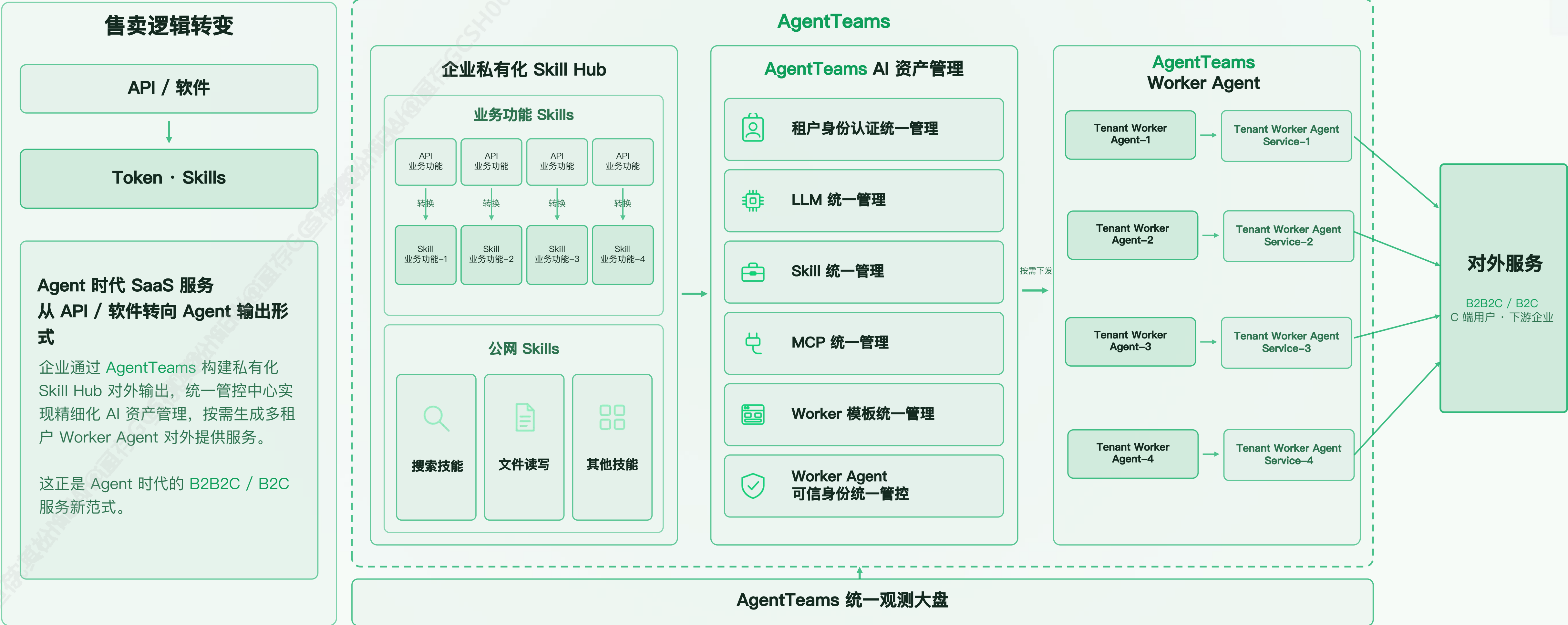


PDSA AI Native 工作台



用 AgentTeams 把企业能力封装为对外 Agent 服务

Agent 时代 SaaS 从 API / 软件转向 Agent 输出：私有化 Skill Hub · 统一 AI 资产管控 · 按需生成多租户 Worker 对外服务



<https://agentteams.console.aliyun.com/>



<https://github.com/agentscope-ai/AgentTeams>



Thank You.