

# 腾讯云企业级智能体解决方案

腾讯云-云产品部

# 智能体时代到来，AI 正从辅助工具走向任务执行与组织协同



当 AI 开始自己干活，自己修复，自己交付结果，人类的工作方式，公司结构，甚至商业模式将会被重构，AI浪潮不是未来，是已经到来！

# 智能体时代，企业转型所面临的痛点分析



## 企业智能体方案建设的痛点是什么？

### 痛点1：无法有效组织Agent完成任务

【痛点】跨角色任务难协同、执行过程易断点、结果难闭环

【需求】能统一承接任务、理解上下文、组织agent完成任务的工作中枢



“谁” 来组织数字员工干活？



Teams

### 痛点2：低代码搭建的智能体难适配生产级任务

【痛点】固定流程难适应生产级任务中的动态变化，能力配置难规模化复制

【需求】需要基于 Harness 构建Agent，并支持Agent快速创建与规模化落地



如何 “构建” 7\*24小时的数字员工？



企业智能体

### 痛点3：企业AI资产难沉淀

【痛点】Skill/专家/知识等经验难复用、能力难传承、资产难沉淀

【需求】需要把分散能力沉淀为可管理、可复用、可分发、可运营的企业AI资产



如何 “沉淀” 企业AI资产？



skills/专家市场

### 痛点4：Agent越多，治理越难

【痛点】配置分散、权限易失控、执行难审计、问题难追溯

【需求】需要统一权限、配置、审计和运营治理的企业管理后台

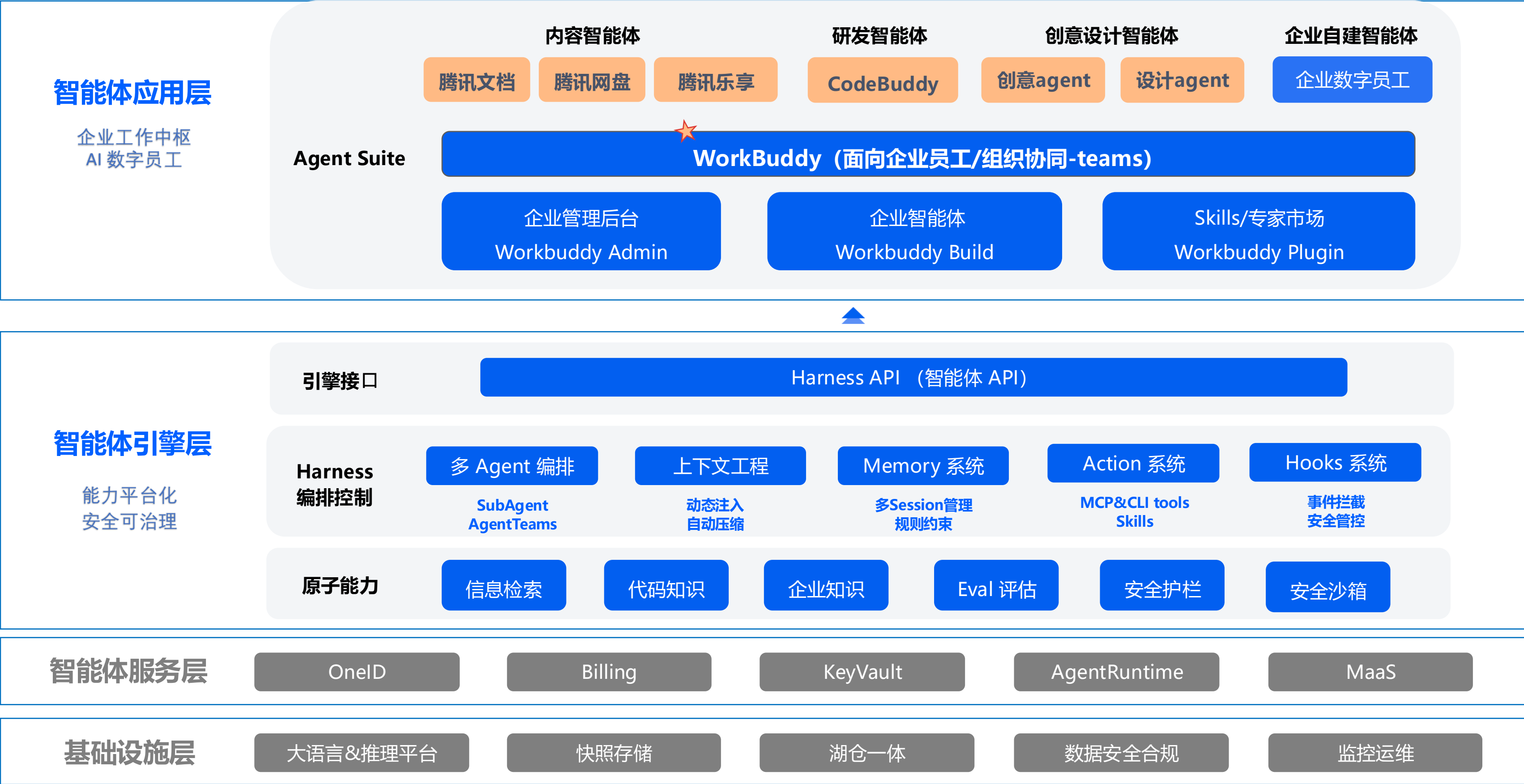


“谁” 来统一管理数字员工和AI资产？



企业管理后台

# 腾讯企业级智能体解决方案分层架构



01

# WorkBuddy: 企业 AI 工作台

# WorkBuddy：从“超级个体” 到 “超级团队”



WorkBuddy 从“超级个体”到“超级团队”，实现从个人能力增强到组织协同生产力的释放，并推动个人 AI 资产沉淀升级为团队 AI 资产沉淀。

# 超级个体：以“一人营销团队”为例说明Wb组织专家团协同完成任务



## ● 任务场景：营销战役策划

SaaS 新版本发布需拉新3000用户，市场只有一个人，需出策划方案。

## ● 营销员工发起任务

"策划一场营销战役 / 为产品发布起草内容 / 审计我们的 SEO"

## ● 任务实现说明

营销总监「增长操盘手」编排 4 位专家（策划/品牌/SEO/内容）并行+串行协作，出一份可落地策划方案



### 营销战役团队

营销增长

3,026次使用

能力介绍

由营销总监领导的 4 人营销专家团队：内容创作者（博客/邮件/社媒/品牌声音）、活动策划师（战役策略/受众/渠道/预算）、SEO 专家（技术审计/内容优化/效果分析）和品牌分析师（竞品定位/品牌审核）。覆盖完整营销生命周期。

擅长领域

营销策划

品牌分析

内容创作

团队成员

增长操盘手 营销总监 主理人

内容创作者 笔达

活动策划师 牟全胜

SEO 专家 优搜

品牌分析师 品析

试试这样问我

“策划一场营销战役 / 为产品发布起草内容 / 审计我们的 SEO”

“制定跨渠道营销传播和预算分配方案”

“设计营销活动全链路执行和复盘流程”

召唤 营销战役团队

腾讯云

# 超级个体：“一人营销团队” 场景demo演示



🏠 + 策划一场营销战役 / 为产品发布起草内容 / 审计我们的 SEO

🔍 ☰ 📄

策划一场营销战役 / 为产品发布起草内容 / 审计我们的 SEO

WorkBuddy

🔍 问答 已回复

你本次想优先启动哪一个工作流？不同工作流会调度不同的团队成员（策略/笔达/优搜/品析）  
营销战役策划  
这次战役/内容/审计的主角是什么？请用 1-2 句描述产品、行业 and 核心卖点（例如：面向中小企业的 AI 客服 SaaS，主打 24/7 自动应答和多渠道接入）  
就用通用示例  
目标受众和主要市场是什么？  
国内 B2B 中小企业  
这次的预算量级和上线时间窗大致是？  
先不设限，出方案再评估

收到。已锁定工作流 1：营销战役策划，主角设为"面向国内中小企业的 AI 客服 SaaS（通用示例）"，受众为企业主/运营负责人，预算按推荐方案出。  
我现在按铁律启动团队协作：先建团队 → 依次调度策略、品析、优搜、笔达 → 主理人中转汇总 → 落盘报告。  

> 工具调用 2 · 过程消息 0

团队已建立。现在我先下发第一阶段任务给 策略（campaign-planner）和 品析（brand-analyst）（它们之间无依赖，可并行启动），同时建立任务清单。  

> ○ 任务列表 · 0/4 已完成 · 制定战役整体策略

现在并行拉起 策略（Camp）和 品析（Brandi）。（优搜与笔达需要等前两者的产出作为输入，暂不启动）  

> 工具调用 2 · 过程消息 0

策略和品析已并行启动。接下来等它们回传产出后，我会中转给优搜做 SEO 关键词策略，再中转给笔达起草内容日历。  
当前进度：

- ✅ 团队 marketing-ai-customer-saas-launch 已建立
- ✅ 任务清单 #1-#4 已创建

@ 📎

输入消息...

🌐 营销战役团队 ▾

🔥 Claude-Opus-4.7 (1M context) ▾

🛡️ 技能

🎤 ⚠️

内容由 AI 生成，请核实重要信息。

# 超级团队：以 “AI为中心” 的组织协作模式的升级



# 超级团队：实现 “AI中心模式” 的四大核心能力

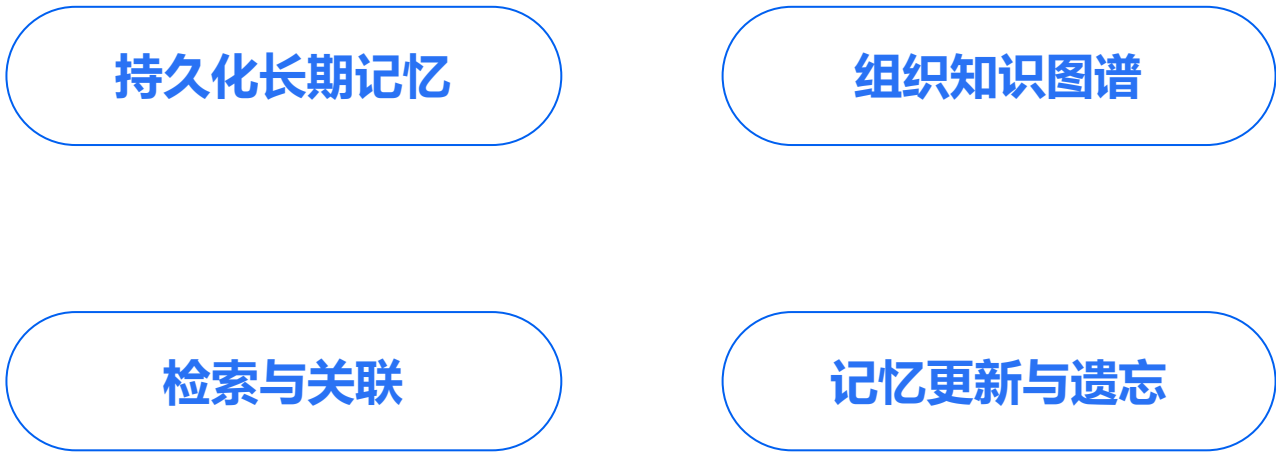


# “AI中心模式” 的核心能力：组织记忆 & 全景感知



## 组织记忆

记得住：没有记忆的AI每次都从零开始，无法积累组织经验



- 这是区分「对话式AI」和「组织级AI」的分水岭。没有组织记忆，AI只能做一次性的工具使用，不能承担持续的协调职能。

## 全景感知

看得见：全局视野，跨全局的协调判断（同时知道5个下属各自的进度和阻塞）



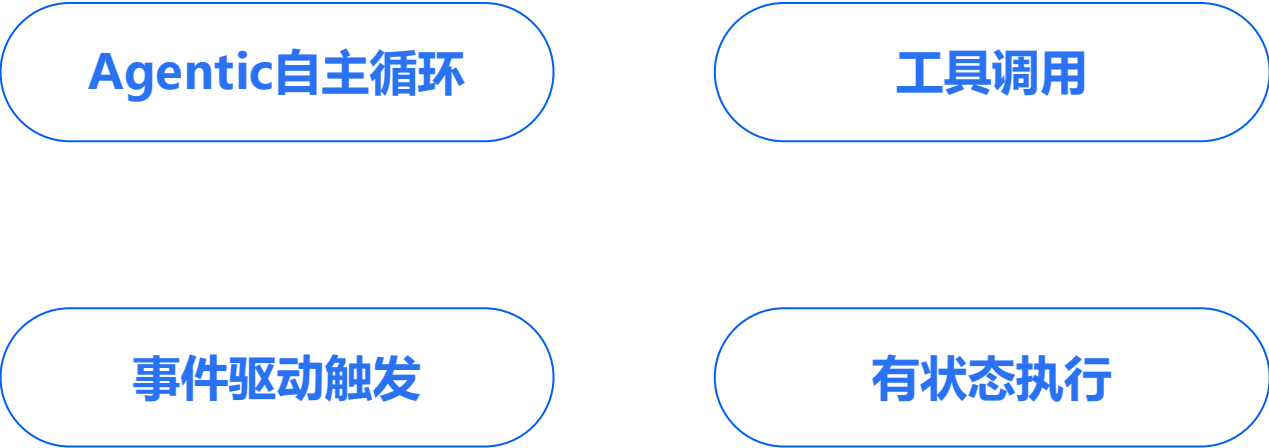
- 这是AI从「被动响应」走向「主动协调」的前提。看不见全景，就无法识别跨团队的冲突和机会。

# “AI中心模式” 的核心能力：自主行动 & 多方协调



## 自主行动

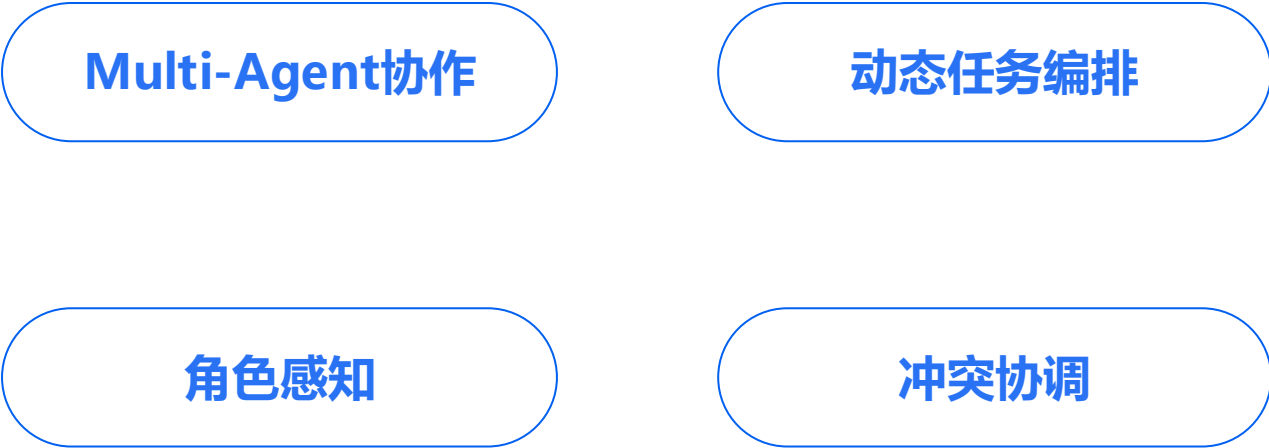
动得了：「推动事情落地」，而不是「等人来问」



- 这是Agent区别于Tool的本质。没有自主行动能力，AI就只是一个被动工具，不能承担「协调者」的角色。

## 多方协调

协调得了：组织协作的本质是多方协调，需理解多方诉求并在其中找到可行解。



- 这是AI从「个人助手」走向「组织协调者」的关键。现实中的协调从来不是一对一的，而是多对多的。

# 超级团队：“人+AI” 组织协作模式的升级



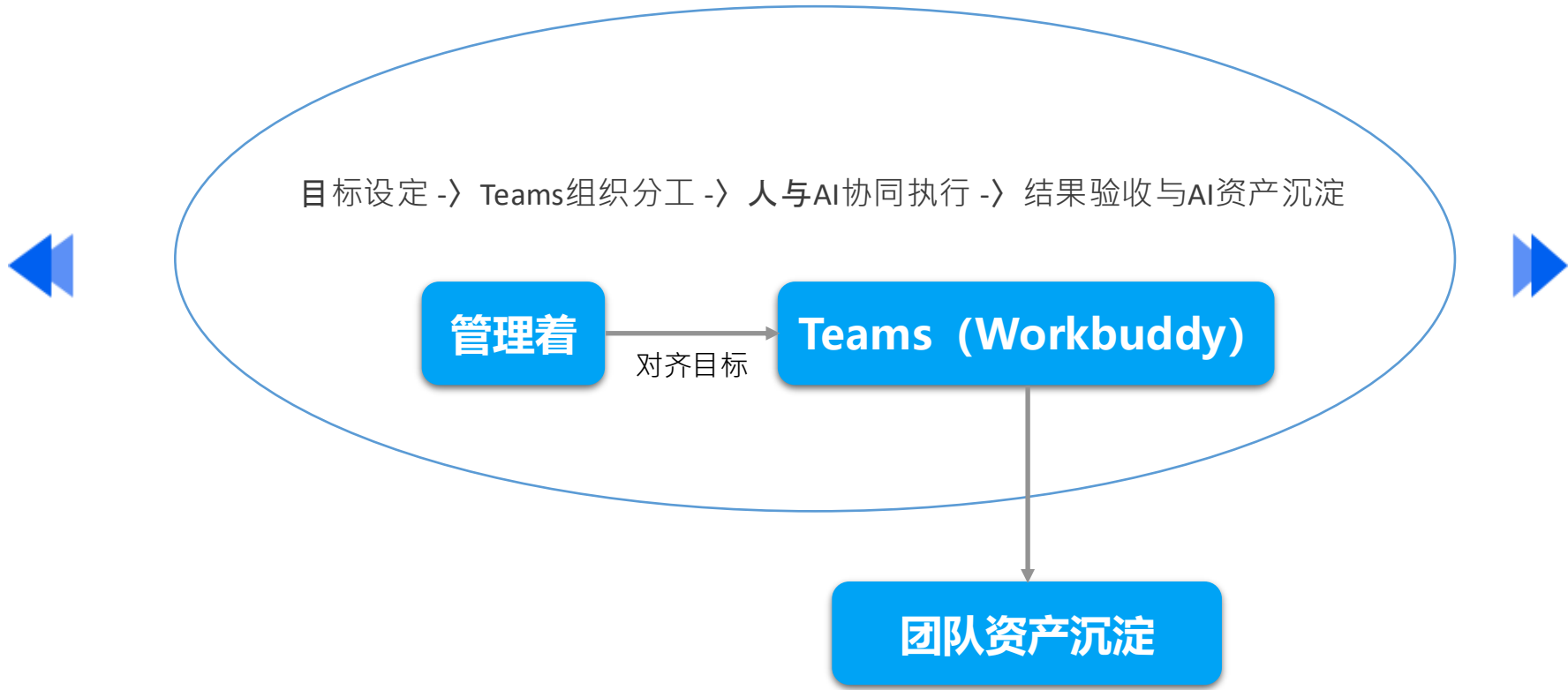
- 管理者和AI对齐目标，Teams 作为协同中枢完成目标理解/任务拆解/角色分工，并组织员工与数字员工协同执行，最终将结果回流并形成闭环。

| 角色    | 核心职责                | 本质定位    |
|-------|---------------------|---------|
| 管理者   | 定方向、做取舍、拍板、验收       | 方向与责任中心 |
| 员工    | 做专业判断、处理复杂问题、完成关键执行 | 专业执行者   |
| Teams | 拆任务、做调度、盯进度、推闭环     | 协同中枢    |
| 数字员工  | 跑标准动作、做高频执行、并行处理任务  | 专业执行单元  |

员工A（如：销售）

员工B（如：客服）

员工C（如：法务）



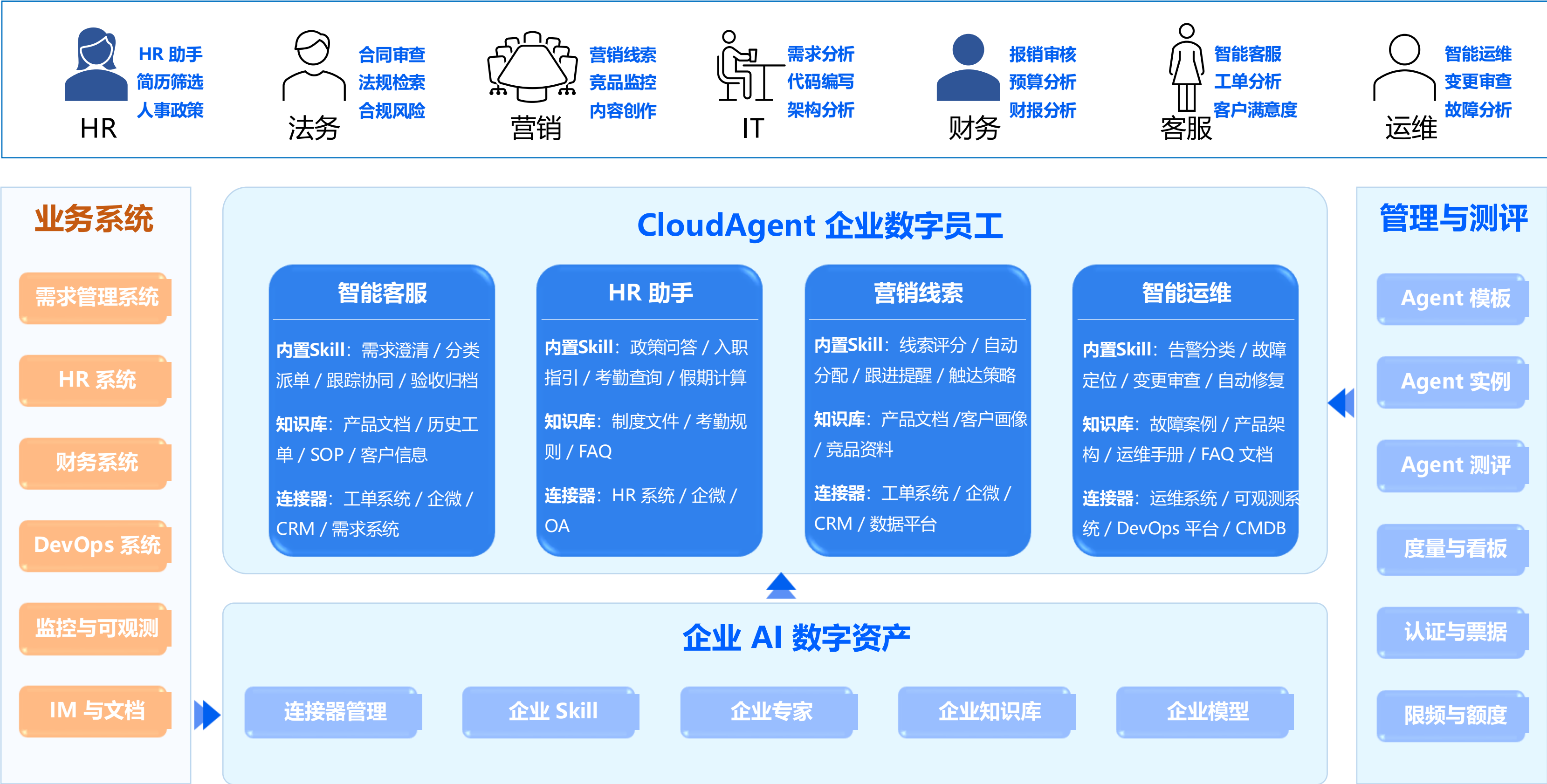
数字员工D（如：财务）

数字员工E（如：运营）

02

# Workbuddy: 数字员工 (打造7\*24小时的数字员工)

# 7\*24 小时可以持续云端运行的数字员工



# 快速创建企业数字员工（智能体）



## 1. 需求描述

自然语言 / 模版 / 文档 描述需求

**自然语言创建：**自然语言描述需求，AI 将自动生成 Agent 配置

**内置模板创建：**内置场景的智能体模板，快速创建

## 2. 构建配置

Prompt / Skill / 专家 / MCP / 知识库

**人工按步骤勾选：**结合企业已有 AI 资产按步骤创建

**manifest 配置创建：**通过配置文件快速创建

## 3. 测评验证

自然语言 / 模版 / 文档 / 描述需求

**Test Run 快速验证：**Agent 发布之前可以快速 Test Run 验证

**Agent 测评集验证：**内针 Agent 场景维护专门的测评集进行验证

## 4. 发布运营

版本发布 / 分享接入 / API调用

**版本发布：**按版本管理 Agent，管理员可迭代 Agent 表现

**分享接入：**分享给团队成员，每个成员一个实例，记忆持久化保存

你想构建什么样的 Agent?

用自然语言描述你的需求，或从下方选择一个模板快速开始

客服支持助手

回答客户问题，查询知识库，必要时自动创建工单升级处理

深度研究员

执行多步骤网络调研，综合多个信息源并生成带引用的研究报告

代码审查助手

审查代码变更，检查潜在问题，提供改进建议和最佳实践

数据分析师

加载数据集，执行分析，生成可视化图表和洞察报告

[查看更多模板 >](#)

描述你想创建的 Agent，例如：帮我创建一个客服助手...

System Prompt

技能 / 专家

高级配置

Manifest

技能

选择 Agent 可以使用的能力

网络搜索

搜索互联网获取实时信息

代码执行

在沙箱环境中运行代码片段

文档解析

解析和提取文档中的内容

数据分析

分析数据集并生成可视化图表

API 调用

向外部 API 发送 HTTP 请求

数据库查询

安全地查询 SQL/NoSQL 数据库

知识库搜索

AI 生成

搜索内部文档、常见问题和历史工单，查找相关答案

专家

指定领域专家增强 Agent 的回复质量

Agent 评测

Agent 评测

通过标准化的评测任务衡量 Agent 的回答质量。选择目标 Agent 和评测数据集，

6 总任务

1 运行中

3 已完成

83 平均得分

评测任务

评测数据

搜索任务名称或 Agent...

状态 全部

评测方式 全部

| 任务名称                       | Agent | 数据集        |
|----------------------------|-------|------------|
| 客服助手 - 常见问题准确率<br>eval_01  | 客服助手  | 客服 FAQ 测试集 |
| 数据分析师 - 多轮对话质量<br>eval_02  | 数据分析师 | 多轮对话质量测试   |
| 代码审查员 - 代码规范检查<br>eval_03  | 代码审查员 | 代码规范检测集    |
| 知识库助手 - 信息检索精准度<br>eval_04 | 知识库助手 | 知识库检索评测集   |

接入 Agent

接入 Agent

通过接入链接或 SDK，将 Agent「周报助手」集成到你的系统中。每个用户打开链接后，系统会自动为其创建专属的独立实例（云端沙箱），对话记录持久保存，实例间完全隔离。

接入链接

需登录

https://tencent.staging-sso.codebuddy.cn/agents/sha...

复制链接

用户需登录 CodeBuddy 账号。首次打开会自动创建专属实例（约需 30 秒），之后再次访问会直接进入已有实例继续工作。

开发集成

API 集成

Go SDK

Java SDK

Node SDK

# 基于模板创建实例

POST /v2/agentos/runtimes

Authorization: Bearer YOUR\_API\_KEY

{

"agentId": "weekly-report-8m42p",

"config": {}

}

# 响应

{

"runtimeId": "rt\_XXXXXX",

}

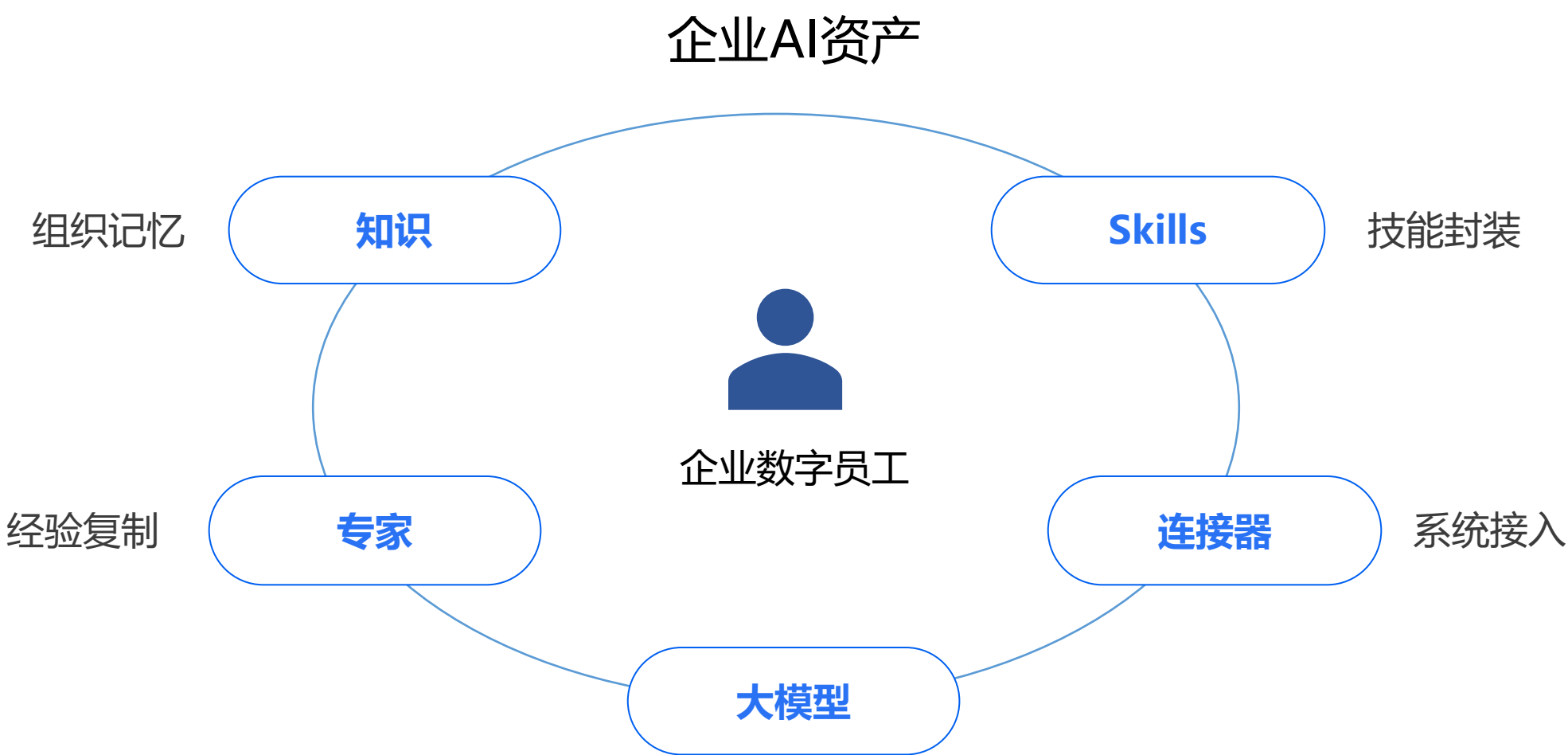
通过企业 API Key 调用，可将 Agent 能力集成到企业自有系统中。

关闭

# 数字员工：让企业沉淀的AI资产成为可复用的生产力



把分散在个人、项目和部门中的模型、Skill、知识、专家经验与系统连接能力，沉淀为企业可管理、可复用、可分发的 AI 资产。



● 企业AI资产核心价值：

- 经验沉淀
- 规模化复制
- 持续迭代
- 统一治理

可视化配置

Test Run 测试验证

发布前验证

持续调优

构建模式Test Run

你想构建什么样的 Agent?

用自然语言描述你的需求，或从下方选择一个模板快速开始

空白 Agent

从零开始自定义，通过对话逐步完善配置

CRM 销售...

客户跟进记录整理、回访邮件起草、销售周报生成

ERP 报表分析

财务数据拉取、异常指标识别、月度经营报告生成

代码评审助手

代码质量检查、安全漏洞扫描、改进建议生成

查看更多模板 >

描述你想创建的 Agent，例如：帮我创建一个客服助手...

↑

System Prompt技能 / 专家高级配置Manifest

发布 Agent

System Prompt

定义 Agent 的角色、行为规范和约束条件

在此输入 System Prompt...

或在左侧对话框中用自然语言描述，AI 将自动生成。

0 字符





### LLM模型评测模版

LLM评测

LLM模型评测模版，用于一键生成LLM评测任务

[LLM评测模版场景示例](#)[LLM评测模板数据集](#)[LLM评测模版提示词](#)[deepseek-v3-0324](#)

[show\\_demo](#)

并发 4 上限 100



### Skill评测模版

Skill评测

Skill评测模版，用于一键生成Skill评测任务

[Skill评测示例](#)[Skill评测模版数据集](#)[Skill评测模版提示词](#)[GLM-5](#)[skill\\_eval](#)

并发 4 上限 100



### Agent评测模版

Agent评测

Agent评测模版，用于一键生成Agent评测任务

[Agent评测示例](#)[Agent评测模版数据集](#)[glm-5-turbo](#)[terminal-bench-2.0](#)

并发 4 上限 100

- 数字员工不是单一模型能力，而是模型、Skill、知识、工具和执行链路的组合体；  
没有评测，就无法判断效果是否达标、版本是否退化、问题出在何处。

# 企业级数字员工从构建到上线全流程示例详解



## System Prompt — 需求对接数字员工人设 & 行为规范(Rules)

角色定义 · 对话风格 · 业务边界 · 澄清策略 · 分类规则 · SLA标准 · 升级路径 · 需求模板 等

### Skills (企业技能扩展)

|                   |                      |                     |                   |
|-------------------|----------------------|---------------------|-------------------|
| 需求澄清<br>需求标准 + 引导 | 分类派单<br>标签规则 + 路由    | 跟踪协同<br>SLA 规则 + 进度 | 分析报表<br>数据洞察 + 台账 |
| 验收归档<br>闭环 + 知识沉淀 | 知识检索<br>Search + RAG | 合规检查<br>信息保护、安全检查   | 流程指南<br>SOP 流程指引  |

### 知识库 (RAG)

- 历史需求案例
- 需求流程模板
- 业务逻辑知识

### MCP / 连接器 (外部系统)

- 需求管理MCP
- 企业微信MCP

### Hooks (事件管控)

- 内容/操作审计  
UserPromptSubmit
- P0/P1需求审批  
PreToolUse

03

## Workbuddy: 企业管理后台

## 管理后台 (admin) : 组织权限管理



## 组织架构管理

## 成员授权控制

## 角色边界隔离

## 统一治理审计

成员与部门

成员、部门数据均来自“腾讯统一身份”平台，如需管理请[前往 腾讯统一身份/通讯录](#)

企业版如何登录?

成员用量

应用用量

用量明细

数据统计

研效看板

明细数据

成员授权

成员与部门

成员审核

用户组管理

管理员角色

企业设置

基础设置

网络设置

开放与集成

组织架构同步

开放平台

北区的头像和名称

北区的名称

东区的名称

南区的名称

西南云原生的名称

develop的名称

客户成功的名称

授权客户端

取消授权

全部授权状态

展示全部成员

输入 ID 或成员姓名

|                          | ID              | 姓名 | 登录账号 | 部门 | 成员来源   | 客户端授权状态 | 操作 |
|--------------------------|-----------------|----|------|----|--------|---------|----|
| <input type="checkbox"/> | 64f43e02-d71b-  |    |      |    |        |         |    |
| <input type="checkbox"/> | 2e9d4bd19901-   |    |      |    |        |         |    |
| <input type="checkbox"/> | 0e0c51c1-1d28-  |    |      |    |        |         |    |
| <input type="checkbox"/> | 32e534ce0d89-   |    |      |    |        |         |    |
| <input type="checkbox"/> | 11989ae9-177a-  |    |      |    |        |         |    |
| <input type="checkbox"/> | 4b6e93b8770d-   |    |      |    |        |         |    |
| <input type="checkbox"/> | dfe7e8b9-1f9d-  |    |      |    |        |         |    |
| <input type="checkbox"/> | 83eed78be76b-   |    |      |    |        |         |    |
| <input type="checkbox"/> | -320210-ae19-   |    |      |    |        |         |    |
| <input type="checkbox"/> | 1d4d5398ca87-   |    |      |    |        |         |    |
| <input type="checkbox"/> | 5-e105000-7711- |    |      |    |        |         |    |
| <input type="checkbox"/> | 249856d70e26-   |    |      |    |        |         |    |
| <input type="checkbox"/> |                 |    |      |    | 腾讯统一身份 | 已授权     |    |

## 管理后台 (admin)：订阅与用量管理



## 订阅统一管理

## 成员用量统计

## 部门归集分析

## 成本持续优化

∞ AI 资源管理

模型管理

知识库

自定义指令

订阅与用量

订阅管理

成员用量

应用用量

用量明细

数据统计

研效看板

明细数据

成员授权

成员与部门

成员审核

用户组管理

管理员角色

企业设置

成员用量

批量调整限量

周期2026-04-23 ~ 2026-05-01

日期范围开始时间 ~ 结束时间

部门 / 成员请选择部门和成员

请输入用户ID

导出

| <input type="checkbox"/> | 用户ID | 成员姓名 | 部门 | 用量消耗 | 周期限量 | 操作 |
|--------------------------|------|------|----|------|------|----|
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |
| <input type="checkbox"/> |      |      |    |      |      |    |

共 36 条数据

10 条/页

1234

跳至1 / 4 页

# 管理后台（admin）：资源管理



模型资源接入

能力配置标准化

权限开放控制

持续运营优化

组织概览

企业智能体 重磅

AI 资源管理

模型管理

知识库

自定义指令

订阅与用量

订阅管理

成员用量

应用用量

用量明细

数据统计

研效看板

明细数据

成员授权

成员与部门

成员审核

模型管理

模型列表 模型策略

搜索模型名称

全部模型 (34)

自定义模型 (1)

内置模型 (33)

+ 新增自定义模型

| 模型名称        | 模型 ID | 模型类型  | 模型供应商         | 模型描述                    | 可见范围 | 可见端       | 模型部署地址     | 操作    |
|-------------|-------|-------|---------------|-------------------------|------|-----------|------------|-------|
| interGLM4.7 | g...  | 自定义模型 | 其他/标准OpenAI协议 | 暂无描述                    | 全部用户 | -         | http://120 | 编辑 删除 |
| Deepseek    | de... | 内置模型  | -             | DeepSeek 旗舰模型，支持 1M ... | 全部用户 |           | https://st | 编辑    |
| Deepseek    | de... | 内置模型  | -             | DeepSeek 旗舰模型，支持 1M ... | 全部用户 | E、Work... | https://st | 编辑    |
| Claude-     | c...  | 内置模型  | -             | 暂无描述                    | 全部用户 | DE        | https://st | 编辑    |
| Claude-     | c...  | 内置模型  | -             | 暂无描述                    | 全部用户 |           | https://st | 编辑    |
| GPT-5       |       | 内置模型  | -             | 暂无描述                    | 全部用户 |           | https://st | 编辑    |
| GPT-5       |       | 内置模型  | -             | 暂无描述                    | 全部用户 |           | https://st | 编辑    |
| GPT-5       | g...  | 内置模型  | -             | 暂无描述                    | 全部用户 |           | https://st | 编辑    |
| GPT-5       | g...  | 内置模型  | -             | 暂无描述                    | 全部用户 |           | https://st | 编辑    |
| GPT-4       |       | 内置模型  | -             | 暂无描述                    | 全部用户 |           | https://st | 编辑    |

## 数据安全

### 输入安全

#### ➤ 内容安全审查

接入腾讯自研内容安全审核引擎，对于用户输入的 prompt 进行实时合规校验，自动拦截违规内容

#### ➤ 提示词注入防护

权限验证、上下文分析、输入清理、命令阻止、隔离窗口、注入检测、失败关闭、层层拦截

### 输出安全

#### ➤ 敏感信息检查

接模型输出内容自动过滤，精准识别并拦截密钥、凭据、个人隐私敏感数据，防止泄漏

### 存储/权限 安全

#### ➤ 企业数据隔离

多级隔离架构，企业数据独立存储，通过 OneID 实现权限精准绑定

## 运行时防护

### 01 Bash 安全沙箱

文件系统/网络/命令 隔离，Agent 操作被限制在安全边界内

### 02 分层权限控制

Allow/Ask/Deny 三级权限体系，默认制度，敏感操作逐一授权

### 03 写入访问控制

文件写入严格控制在项目目录内，禁止修改父目录和系统文件

### 04 MCP 信任验证

外部 MCP 服务器首次连接需信任验证，工具调用遵循权限管控

### 01 Skill 安全扫描

Skill 安装前自动检测恶意脚本与风险行为，保障扩展生态安全

04

# Workbuddy Cloudagent: 云端智能体Api

# 为企业提供完整的 Agent 能力



将 CloudAgent 的 AI Agent 全栈能力通过 API 嵌入到客户自有系统中，客户无需自研 Agent 核心能力，即可获得完整的 Agent 能力扩展



## 基于 Cloudagent 构建“法务数字员工”的实践案例



- ## ● 真实案例：如何基于cloudagent 把合同审查做成可交付的法律数字员工agent



# THANKS

感谢您的聆听!

