阿里云

无影AgentBay产品介绍

一站式多模态Agent运行平台

2025/10/25

阿里云

目录

01 市场分析和行业痛点

02 无影AgentBay优势

03 无影AgentBay目标客户

04 体验和购买入口

Agent时代需要创新的云基础设施

Agent 能力进化

从 “工作流” 到 “自主规划”

传统AI应用依赖预设规则和固定流程，如同流水线上的机械臂，只能执行既定任务。而近期主流AI Agent具备强大的推理、学习和适应能力，能够：自主理解复杂场景和目标，动态规划执行路径，灵活调整策略应对变化。它们不仅能执行任务，更能思考为什么、判断怎么做。

从 “问答” 到 “行动”

传统大模型（如ChatGPT）应用主要停留在文本问答和内容生成，通用Agent（如Manus、AutoGLM、Operator等）则具备了“自主规划-多步执行-结果交付”的能力，能够像人一样操作应用、处理文件、自动化办公等。这类能力需要真实的操作环境支撑，远超本地推理或简单API调用。

企业需求快速提升

企业 Agent采用率

IDC预计，2026年中国500强企业中，50%将采用AI Agent进行数据分析和业务自动化，40%将实现AI与数据的统一治理。

效率提升

DeepResearch、Coding等Agent在实际应用中，能将原本需8小时的复杂任务缩短至5-10分钟，极大提升生产力。

Agent 需要什么样的运行环境

安全隔离与合规

- 安全沙箱：Agent在云端隔离环境中运行，避免对用户本地环境造成风险，防止恶意代码、数据泄露等问题。
- 权限与合规：企业级Agent需严格控制数据访问、操作权限，云端环境便于统一管理和审计，满足合规要求（如GDPR、企业内控等）。

弹性&跨OS

- 弹性算力：云端可根据任务量动态分配算力资源，支持大规模并发和高峰期自动扩容，降低企业IT成本。
- 跨 OS：长序列任务常需要跨操作系统环境完成任务，AgentBay 天然支持 Windows/Linux/Android。

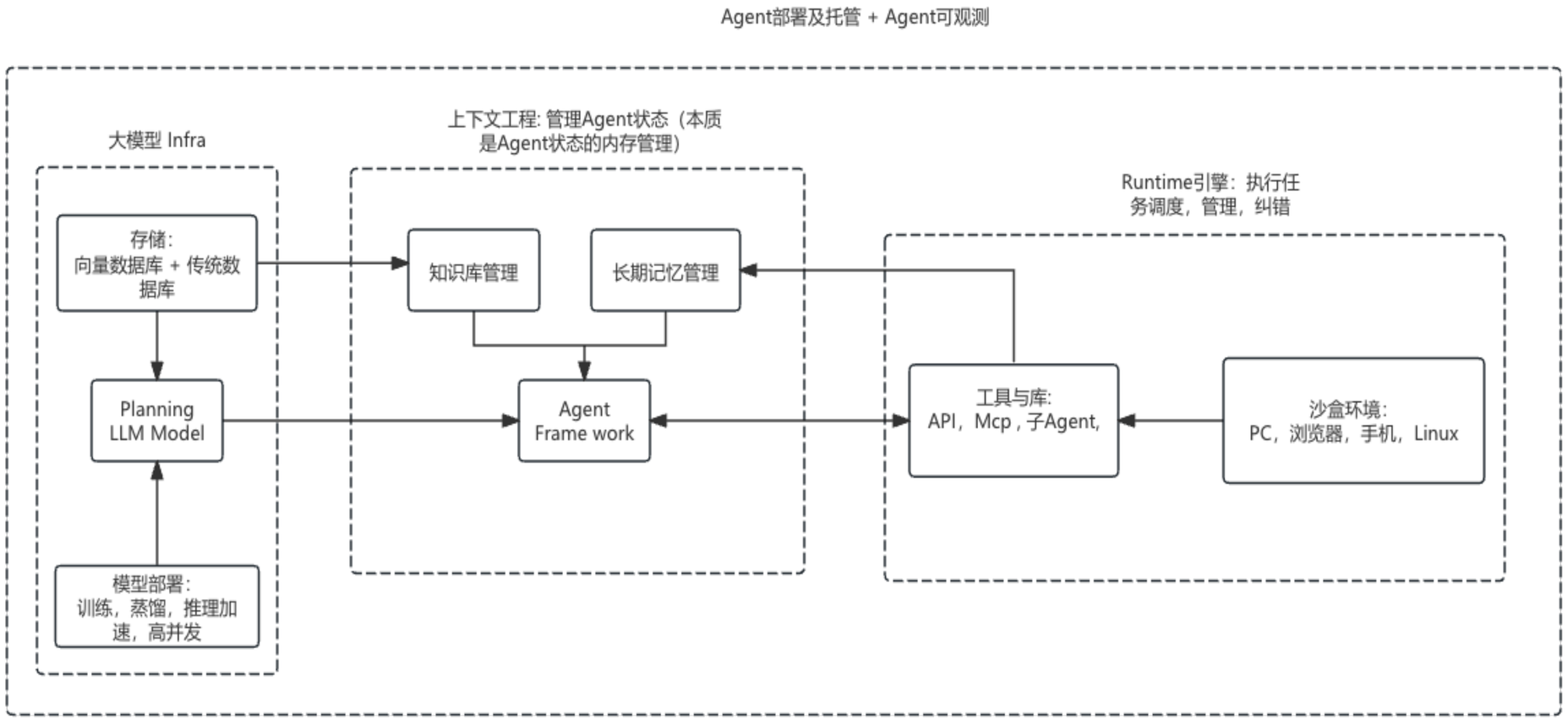
多模态与工具预集成

- 多模态操作：Agent可在云端环境中调用浏览器、Office、开发工具、数据库等多种应用，完成复杂的自动化任务。
- 工具链丰富：云端环境可预装丰富的工具和API，便于Agent按需调用，提升任务完成率和效率。

可观测和自动化运维

- 自动化任务任务日志与回溯：云端环境便于记录Agent的操作日志、任务状态，支持任务失败自动重试、异常报警等自动化运维能力.
- 持续集成与升级：Agent平台可统一升级、维护，快速响应新需求和安全漏洞。

Agent应用开发的生态位



Agent构建的服务逐步向三个核心模块聚合，分别是：

- 大模型（负责意图识别，任务拆解和多模态生成）- 类比人的大脑🧠
- Agent Framework（负责上下文管理，记忆，知识库和Agent的执行任务编排）- 类比人的器官🫀
- 工具集与执行环境（环境服务的业务价值）- 类比人的手脚👋🦶

目前AgentBay所在的是**工具与执行环境**这一层，属于大部分客户比较晚才会接触的模块，客户一般会优先了解到大模型和Framework层，并且会先选择一个适合自身的Framework，比如Dify或者LangChain，然后再会开始考虑选择工具与环境层。

AI Agent 发展历程和展望

长序列复杂任务规划和完成

典型场景

- Deep Research
- 办公PPT生成
- 数据分析
- 智能客服

高并发多Agent协作完成任务

典型场景

- 科学实验
- 自动化测试
- 大规模调研
- APA部署和托管
- 代码调试

自进化智能体建设部署生产系统

典型场景

- 个人网页
- 游戏
- 通信工具
- 电商独立站
- ERP 和 CRM

智能体互联网

典型场景

- 智能家居
- 数字小镇
- 车联网
- 数字分身

- 被动响应 ··· 主动规划 ··· 记忆融合增强规划
- 上下文优化 ··· 长期记忆 ··· 分层记忆架构
- function call ··· mcp ··· computer use

阿里云

Agent开发与应用

Agent开发和应用过程常见的痛点需求

任务规划

- 合理分解
- 逐步完成
- 多智能体协作

长期记忆

- 跨会话存储
- 多工具交互
- 个性化

工具协调与集成

- 工具集丰富度
- 多任务间无缝切换
- 多工具间数据一致性

上下文持续性

- 任务进度可恢复
- 多轮对话连贯
- 实时环境感知

任务沙箱

- 隔离与安全
- 资源管理与性能开销
- 环境一致性

阿里云无影AgentBay：阿里云的Agent Infra核心组件

AgentBay是一款服务于Agent的AI原生产品（Agent Infra），旨在为Agent提供全部类型的执行环境及配套执行工具，同时提供智能化构建工具的能力。

核心能力

以沙箱为核心构建服务

- Browser Use
- Computer Use
- Mobile Use
- CodeSpace

统一持久化系统

集成方式

- SDK
- MCP
- ASP

定制能力

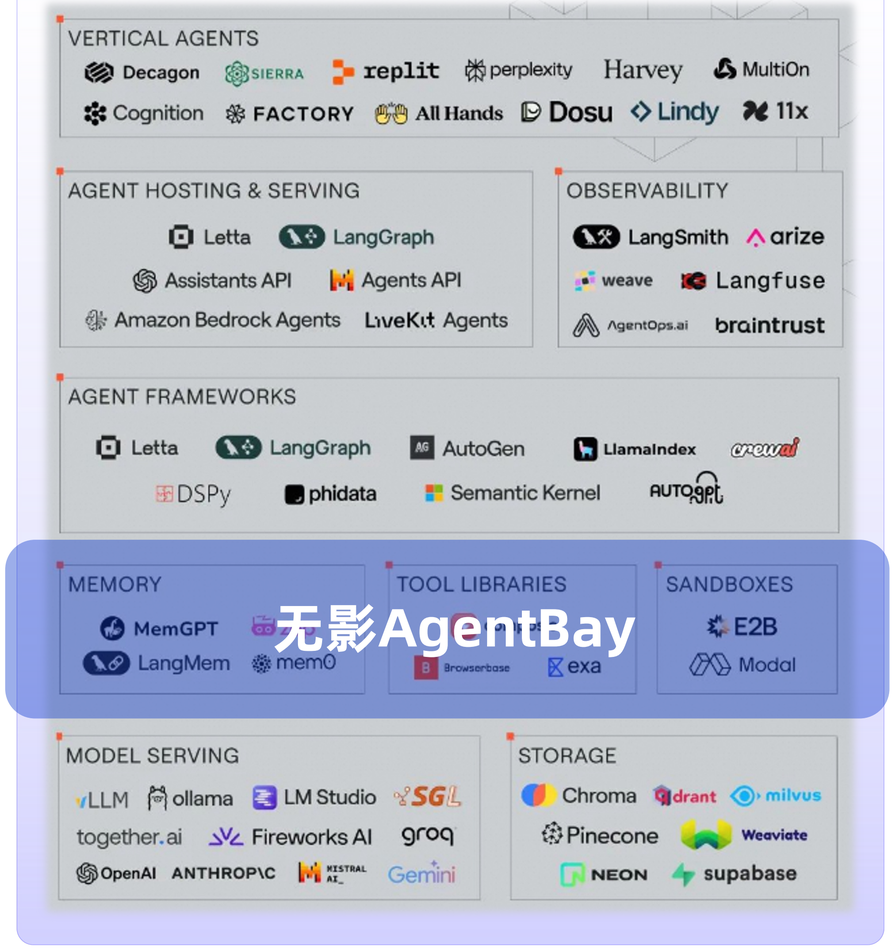
- 开放SDK生态
- 镜像
- 网络出口
- 内置MCP工具
- 兼容主流 Agent开发框架

核心优势

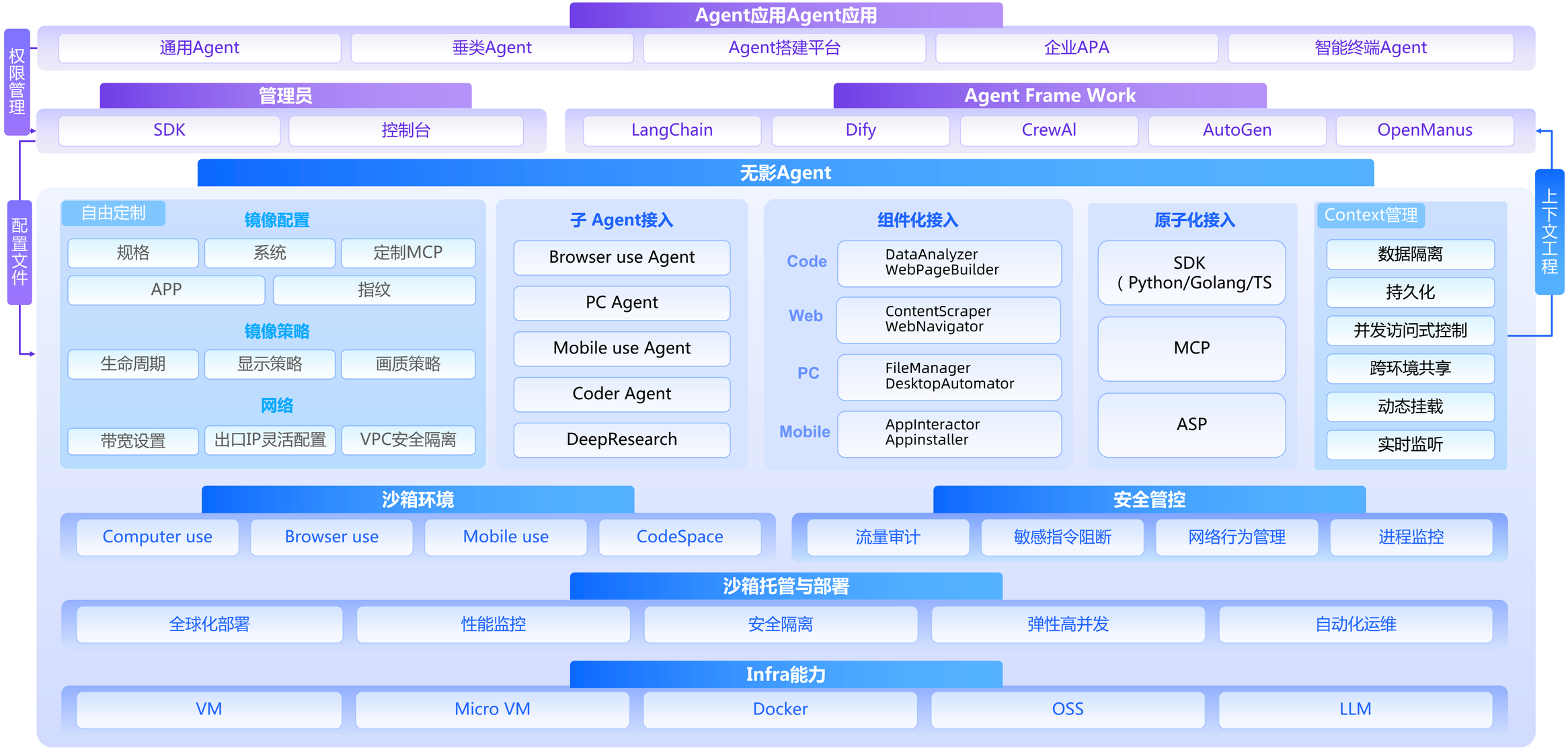
高保真可视化交互（ASP）　全球部署　高并发&高弹性　多平台

统一存储动态挂载　虚机级安全隔离　网络动态可配置

Agent 产业生态



AgentBay产品大图



阿里云

业内最全的智能沙箱：覆盖系统层到应用层

Browser Use

多模态模型驱动网页自动化

数据处理与自动化操作平台
电商、生活服务、
招聘、内容平台等
数据爬取、巡检
自动化操作

Computer Use

Linux和Windows应用感知和控制

自有软件的自动化操作
跨软件操作
RPA–>APA

Mobile Use

应用大规模智能运行

数据处理与自动化操作平台
电商、生活服务、
招聘、内容平台等
数据爬取、巡检
自动化操作

Code Space

高效安全的隔离代码运行

实时工具自建的基石
数据分析
代码自动化测试
AI编码代理

全球化部署

基于阿里云基础设施、分布式全局部署、
低延迟高稳定性、一致的服务体验

安全隔离

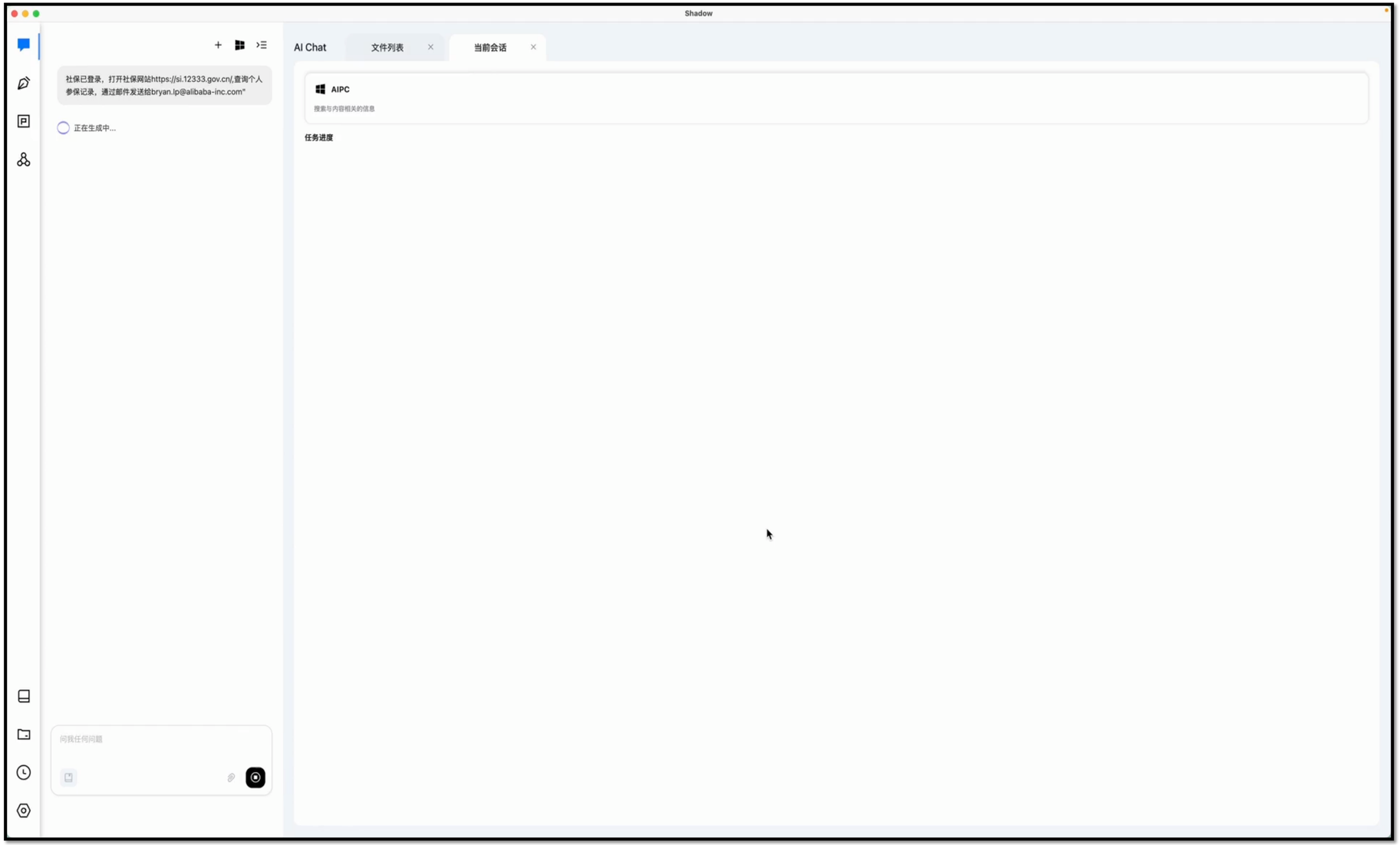
多层安全防护、权限严格隔离、
数据加密传输、企业级安全保障

弹性高并发

支持弹性伸缩、动态资源调配、
大规模并发、高峰流量应对

Browser Use Demo

当Agent的任务完全在浏览器中完成，且不涉及本地系统或移动端 App 时，应选择 Browser Use。适用场景：网页自动化操作、Web 应用自动化测试等。



自动化完成业务流程

智能体与阿里云AgentBay配合，通过以下步骤填写表单、发送邮件:

1、智能体直接发起任务

2、唤起阿里云AgentBay

3、创建BrowserUse沙箱环境

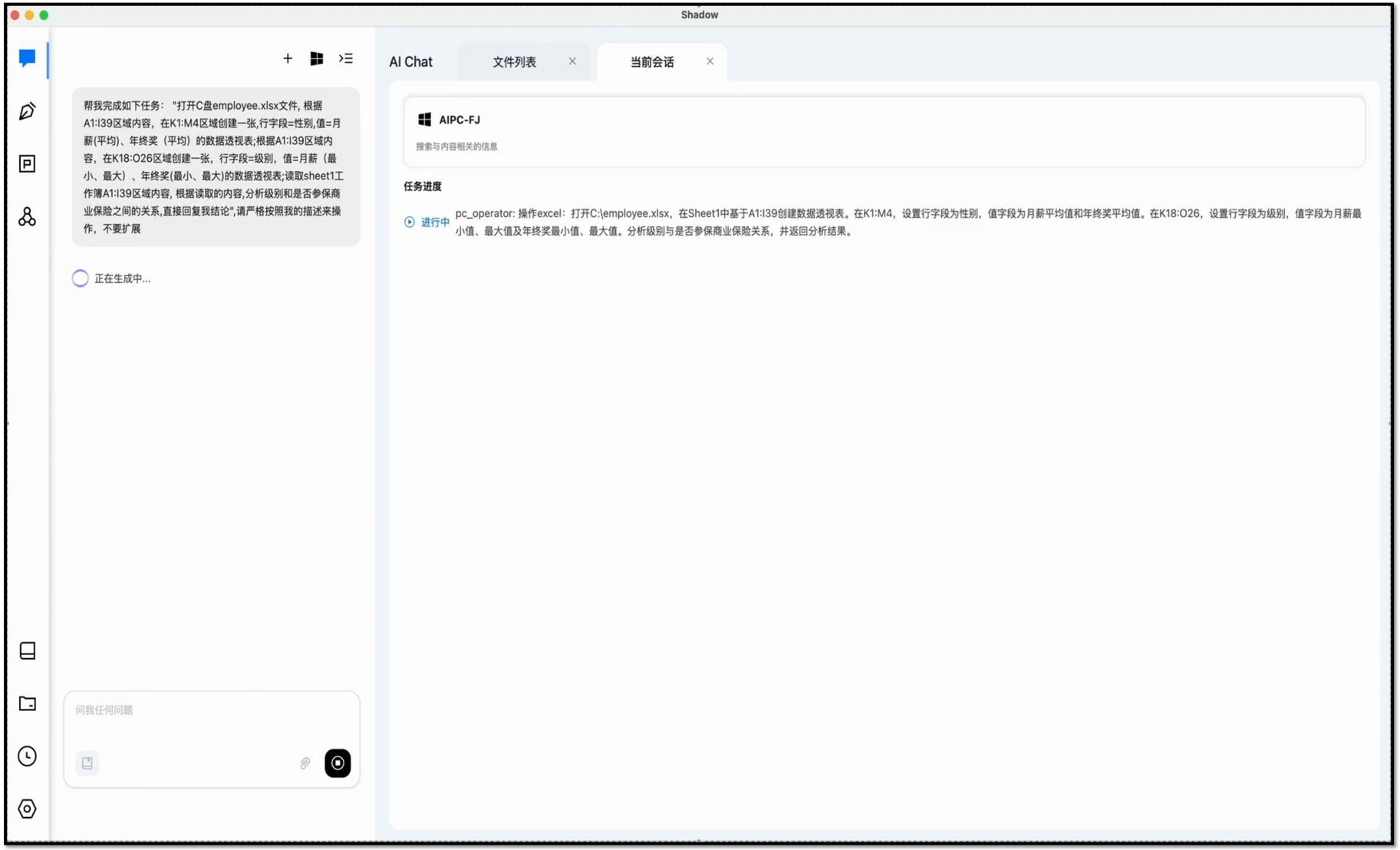
4、填写表单

5、发送邮件

6、完成业务指定流程

Computer Use Demo

当Agent的任务依赖完整操作系统、需要在Windows/Linux系统安装自定义的软件应用时，应选择 Computer Use。适用场景：专用系统操作自动化、跨应用数据流转等。



操作办公软件完成数据统计

智能体与阿里云AgentBay配合，通过以下步骤完成用户下发的任务：

1、用户通过自然语言输入任务

2、智能体拆解任务

3、唤起阿里云AgentBay

4、创建ComputerUse沙箱环境

5、调用ComputerUse内的工具

6、操作办公软件并进行数据统计

Mobile Use Demo

当Agent的任务必须在 Android 手机环境或原生 App 中执行，尤其是涉及社媒运营或移动测试时，应选择 Mobile Use。适用场景：Android App 自动化测试、社交媒体矩阵运营、移动端行为模拟等。

智能体与阿里云AgentBay配合，通过以下步骤进行应用批量测试任务：

1、智能体直接发起批量测试任务

2、唤起阿里云AgentBay

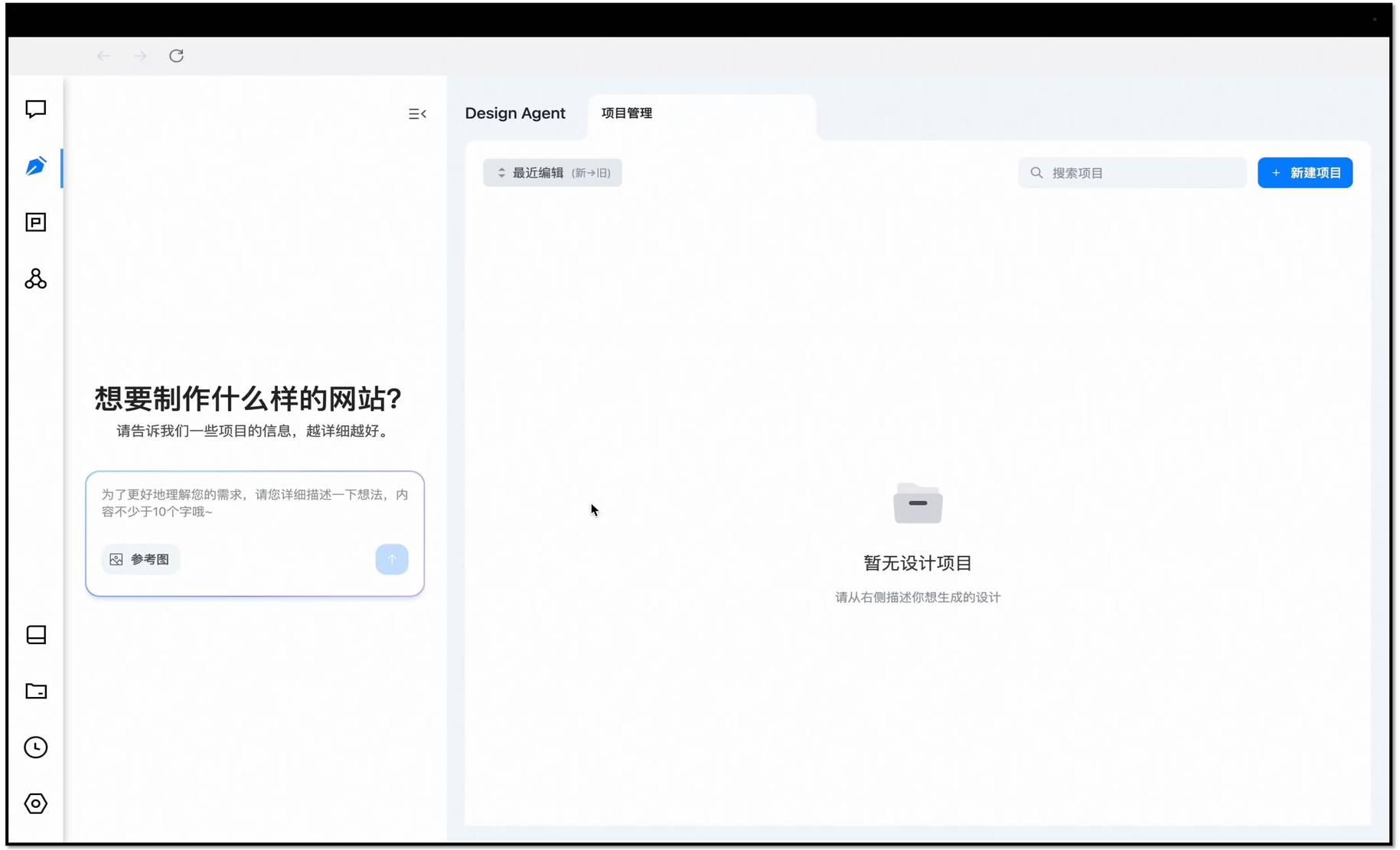
3、创建多个不同配置的MobileUse环境

4、批量完成应用自动化测试

5、返回执行结果给智能体，并形成测试报告

CodeSpace Demo

当Agent的任务以代码执行为中心、无需图形界面、强调可扩展性与隔离性时，应选择 CodeSpace。适用场景：大规模执行AI生成的代码、代码质量检测等。



智能体与阿里云AgentBay配合，通过以下步骤进行网站搭建:

1、用户输入网站构建提示词

2、唤起阿里云AgentBay CodeSpace

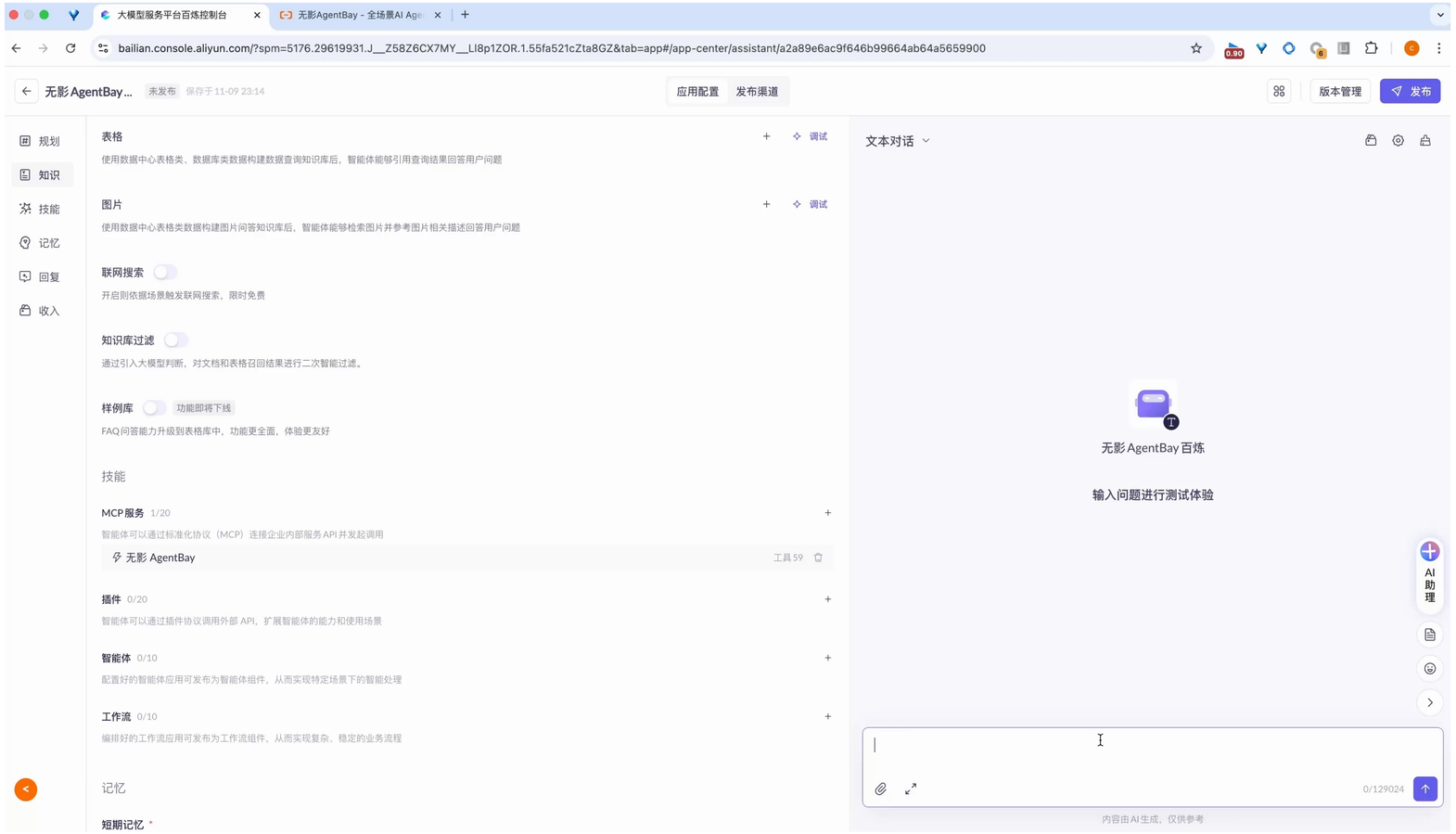
3、大模型生成前端页面代码并在Code space完成网页部署

4、通过AgentBay提供的文件监听能力，对网页指定元素实时编辑

5、通过浏览器访问最终网站生成效果

MCP Server Demo

AgentBay的MCP调用可以在阿里云百炼进行体验。



案例特点：

易接入：通过MCP接入，客户的主Agent可以用自然语言表达任务和需求；

可视化调试：通常情况下隐藏在背后的沙箱，被简单的调用出来，非常方便开发者调试自己的Agent；

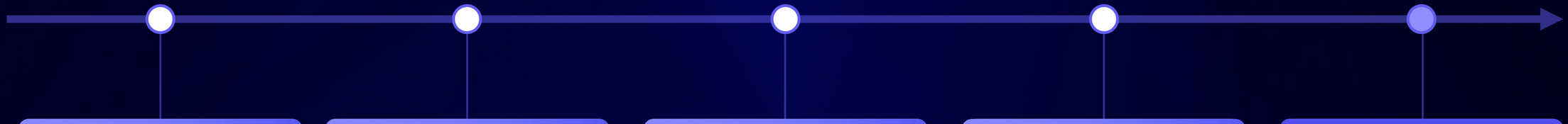
强大的界面解析能力：环境能够理解页面元素，把关键信息准确返回。

总结：

这种“无需关注沙箱复杂运维，无需理解复杂工具设计，脱离沉重编程任务，完全贴近智能体”的开发习惯，正是新时代开发Agent应用的全新范式。

阿里云

全流程自由定制：满足个性化工具链与环境需求



云环境镜像
自由定制

- Windows镜像自定义
- Linux环境集成
- Android系统定制
- Fingerprint按需定制

MCP Server
自由定制与托管

- 定制MCP工具链
- 功能灵活扩展
- SSE实时事件驱动通信
- 生态即插即用

网络配置
自由定制

- 流量路由灵活
- 端口映射自定义
- VPC安全隔离
- 多样代理支持

实例生命
周期管理

- 镜像与资源定制
- 启动顺序可控
- 性能监控自定义
- 优雅关闭、保存、回收
- 自定义销毁策略

更多...
自由定制

- 任务结果按需归档知识库
- 模型与工具灵活组合
- 日志采集方式自选
- 备份策略灵活配置

...

焕新功能：AgentBay端到端体验升级

更智能	更易用	更流畅
无影自研 GUI 引擎驱动环境	标准工具箱集成与 MCP 适配	无影自研 ASP 远程串流协议赋能

>99.9%	>10w	<500ms
会话创建成功率	单地域实时并发数	会话创建时长

终端用户体验

端侧交互	端云输入法	多端 Native SDK	画面自适应

云环境易用性	状态持久化	多地域部署
	IP池	指纹模式

开发集成

SDK	端口重定向	Context管理	文件监听	多语言
	内网通信	Extension	Cookbook	

管控运维	Image Builder	CLI Client	动态会话策略	画面策略
	MCP迭代	高级网络	网络重定向	

焕新功能： AgentBay企业级安全管理套件

端

提示注入攻击检测

识别并阻止用户输入中的恶意指令，防止AI被诱导执行危险操作

敏感指令过滤

拦截包含系统命令、文件删除等敏感指令的输入，确保AI不执行危险操作

输出过滤

审查AI输出内容，过滤敏感信息、恶意代码，确保输出安全合规

云

流量审计

记录和分析AI访问互联网的流量数据，提供网络使用情况的审计追踪

网络行为管理

控制AI的网络访问权限，限制外部连接，防止数据泄露和恶意通信

进程管控

管理云环境中可运行的软件进程，确保只有授权的程序能够执行

阿里云

无影AgentBay的典型应用场景

通用 Agent

典型场景：通用AI Agent产品任务形式较多，需要云端执行环境，如网页浏览、代码执行、文件操作、系统控制等多样化任务。

典型需求：标准化的云端沙箱环境，支持多种编程语言和工具链，实时交互和状态管理，环境隔离和数据安全，API接口便于集成。

APA
（Agent Process Automation）

典型场景：从传统基于规则的RPA升级到AI驱动的智能自动化，需要处理非结构化数据和复杂决策场景。

典型需求：长期运行的自动化环境，支持视觉识别和自然语言处理要与现有企业系统集成，要求流程监控和异常处理，支持人机协作和人工干预。

Agent开发平台

典型场景：为开发者提供Agent开发、测试、部署的一站式平台，需要为用户提供临时沙箱环境执行任务。

典型需求：需要多环境沙箱支持，要求快速环境创建和销毁，需要用户权限管理和资源隔离，要求任务监控和日志记录，需要开发者工具和SDK支持。

AI 设计 Agent

典型场景：UI/UX设计、原型制作、设计代码生成的AI设计助手，需要前端托管和发布环境。

典型需求：前端代码运行和预览环境持设计工具和原型制作，代码生成和优化，设计资源管理和版本控制，多平台发布和部署。

Coding Agent

典型场景：代码生成、编译、调试、测试，需要安全的代码执行环境和开发工具链。

典型需求：多语言编程环境，代码安全隔离执行，集成开发工具和调试器，支持版本控制和项目管理，代码质量分析和安全扫描。

智能终端

典型场景：智能眼镜、AR/VR设备、等端侧算力不足的智能终端，需要云端环境执行复杂AI任务。

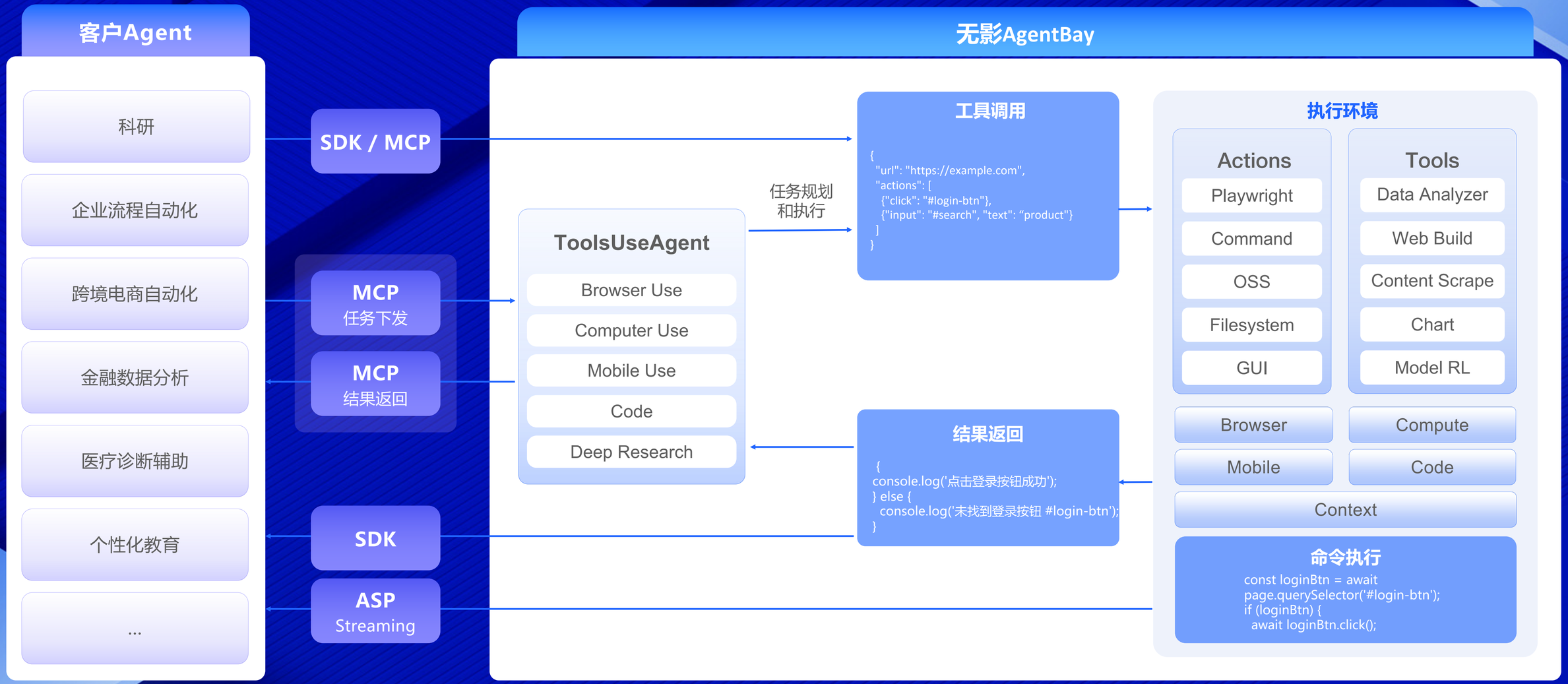
典型需求：低延迟的云端计算环境，支持多模态输入输出，实时数据同步和状态管理。

流程智能化改造的大企业

典型场景：企业将传统人工业务流程改造为AI驱动的智能化流程，涉及数据采集、处理、分析和决策的自动化。包括但不限于企业内部客服、金融合规检查、制造业质量控制、电商客服自动化、医疗诊断辅助、政府政务流程、能源监控运维等。

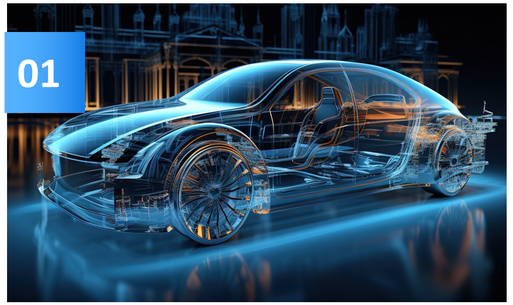
典型需求：需要云端算力执行复杂AI任务，要求安全隔离的企业级环境，需要快速集成现有业务系统，内网接入，要求数据合规和审计追踪，跨平台数据流转和状态持久化。

基于 AgentBay 的 Agent 简化工作流程



AgentBay 助力千行百业 Agent 构建

01



汽车制造

- 智能生产线监控与预测性维护
- 供应链数据实时采集与分析
- 质量检测自动化与缺陷识别
- 生产计划智能优化调度
- 设备故障预警与远程诊断

02

电商零售

- 多平台商品信息自动获取
- 价格监控与竞品分析
- 库存管理智能预警
- 客户服务自动化响应
- 营销活动效果实时追踪

03

金融科技

- 多源数据采集与风险识别
- 合规监控与异常交易检测
- 客户画像智能分析
- 交易系统自动化测试
- 金融报告自动生成

04

企业 SaaS 服务

- 跨平台数据同步与整合
- 业务流程自动化执行
- 客户行为分析与预测
- 客户成功运营
- 多租户数据隔离处理

多平台数据获取 | UI 自动化任务执行 | 代码与数据智能处理 | 持久化状态管理 | 企业级安全保障

AgentBay 能力基座

AgentBay助力深度调研 Agent秒开过万实例

智能数据处理

执行数据清洗、去重、结构化处理

知识沉淀

将调研结果转化为结构化知识库

实时监控

ASP协议支持人工实时查看和干预调研过程

安全隔离

每个调研任务在独立环境中执行，数据零留存

AgentBay为软件开发Agent提供安全高效代码运行环境

多语言开发支持

预置Python、Node.js、Java、Go、C++等主流开发环境

依赖管理自动化

自动处理包依赖、版本冲突、环境变量配置，支持Docker、npm、pip等包管理器

版本控制增强

支持Git工作流，自动生成提交信息、变更日志、发布说明

安全代码执行

代码在沙箱中安全执行，防止恶意代码影响本地环境

基于 AgentBay快速构建企业流程自动化Agent

跨系统集成

Browser Agent操作Web系统，PC Agent操作桌面应用

异常处理

预置支持流程中断、重试、人工干预等异常处理机制

状态持久化

Memory Agent保存流程状态，支持断点续传

RPA增强

结合AI能力，支持非结构化数据处理和决策

相关材料

SDK地址（包括cookbook、集成指南、代码实例）：https://github.com/aliyun/wuying-agentbay-sdk

产详页：https://www.aliyun.com/product/agentbay

产品文档：https://help.aliyun.com/zh/agentbay/product-overview/

控制台：https://agentbay.console.aliyun.com/

阿里云 | 计算，为了无法计算的价值