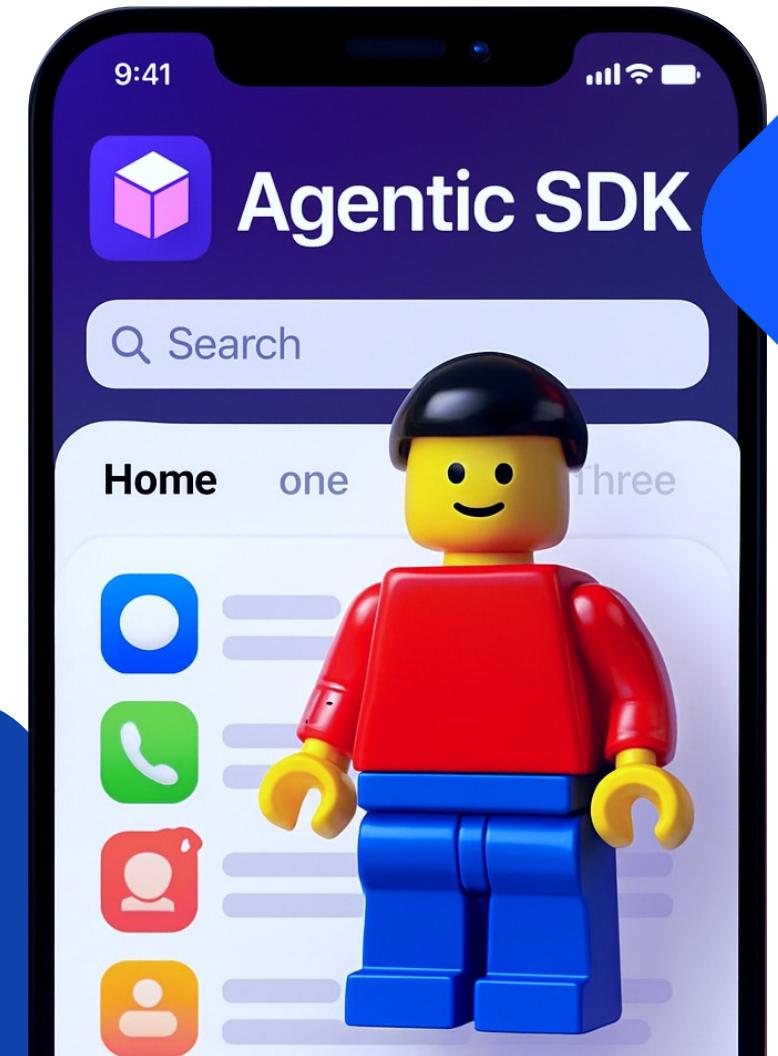
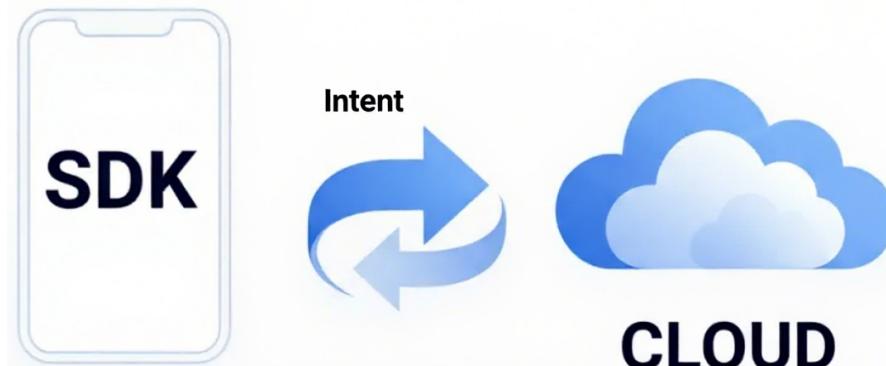


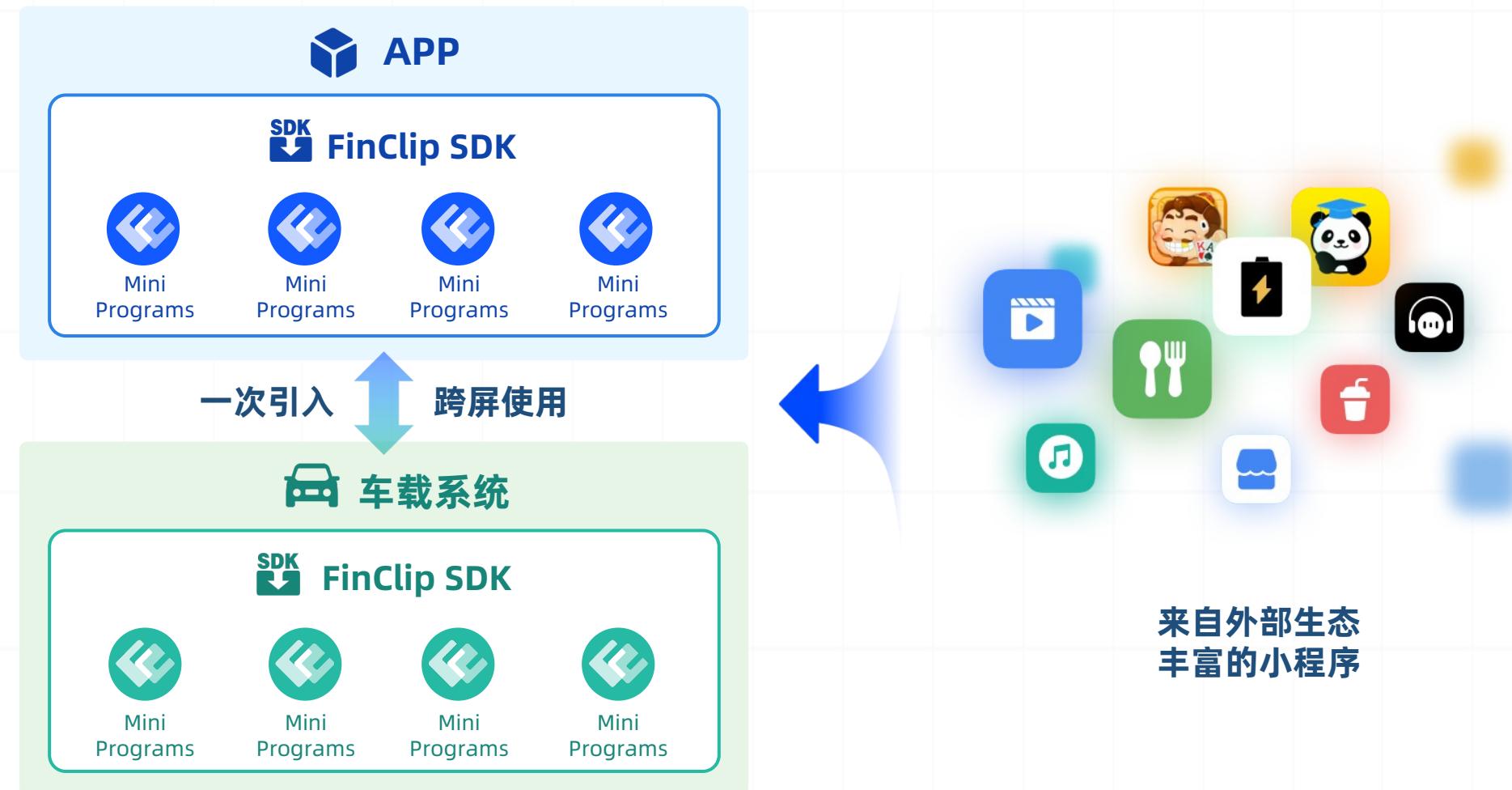
FinClip :

从小程序容器到 Agentic 容器

让每个 APP 在可信沙箱中调度 MiniApp 与 Agent



FinClip：兼容 微信 & W3C Mini-App 等规范或推荐标准的小程序容器







小程序运行时 = 订制WebView + 小程序容器 + 安全沙箱



浏览器 = 内核 + 沙箱

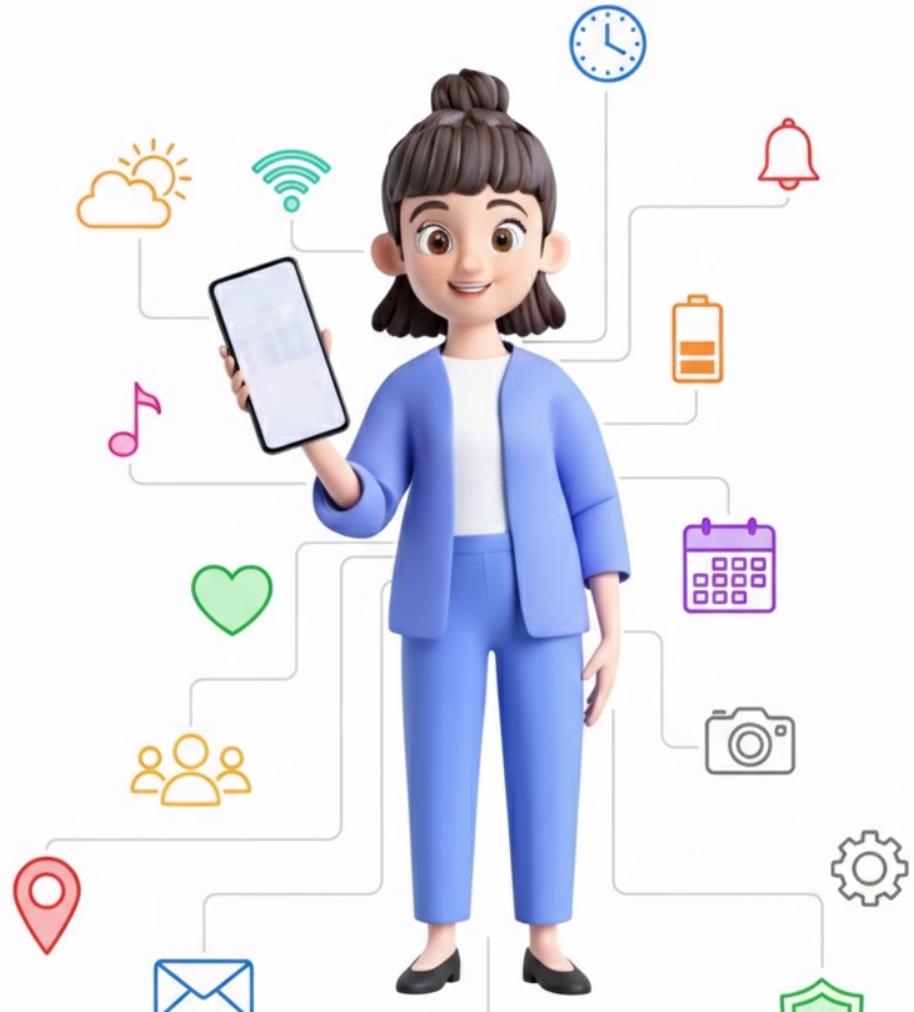
- 随身设备**

谁能不带手机出门?
→ 而 PC 浏览器只在桌面场景里
- 更丰富的上下文**

它知道你的时空、应用数据、联系人、日历 ...
→ PC 浏览器几乎一无所知
- 更自然、轻量的入口**

每天第一眼看的不是电脑，而是手机
→ 移动端才是服务的第一入口
- 更强大的能力触点**

支付、相机、定位都在它手里
→ 这些是 PC 无法直接提供的原生能力

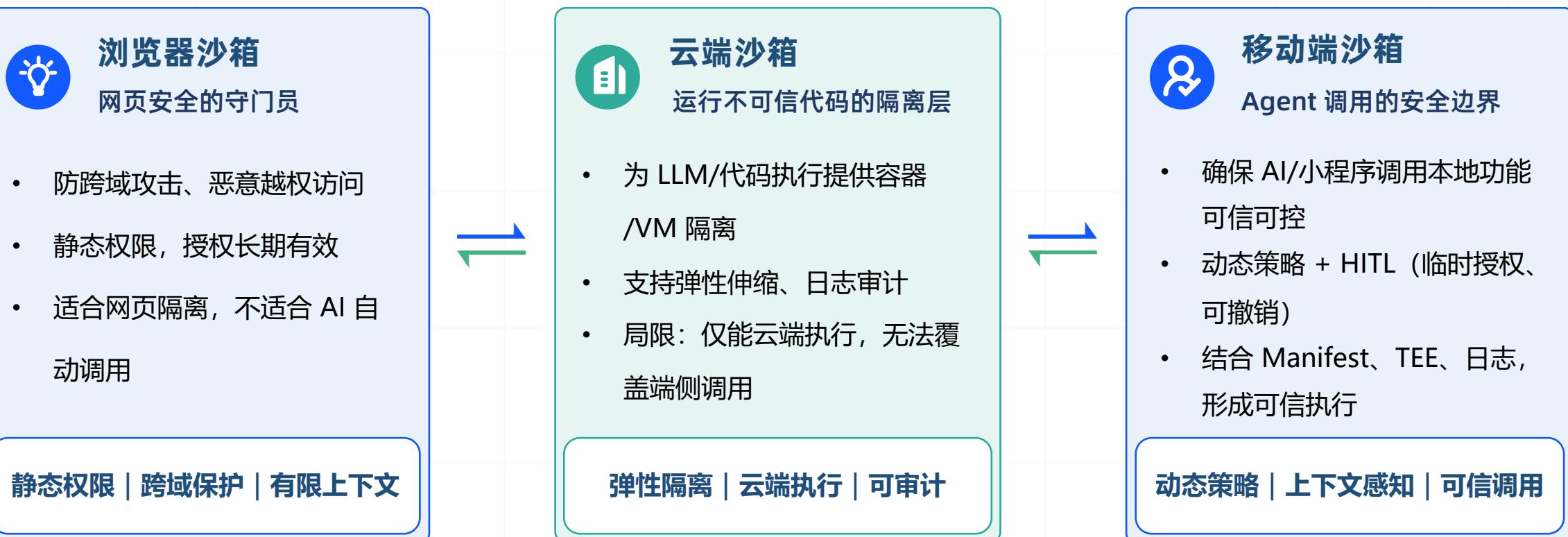


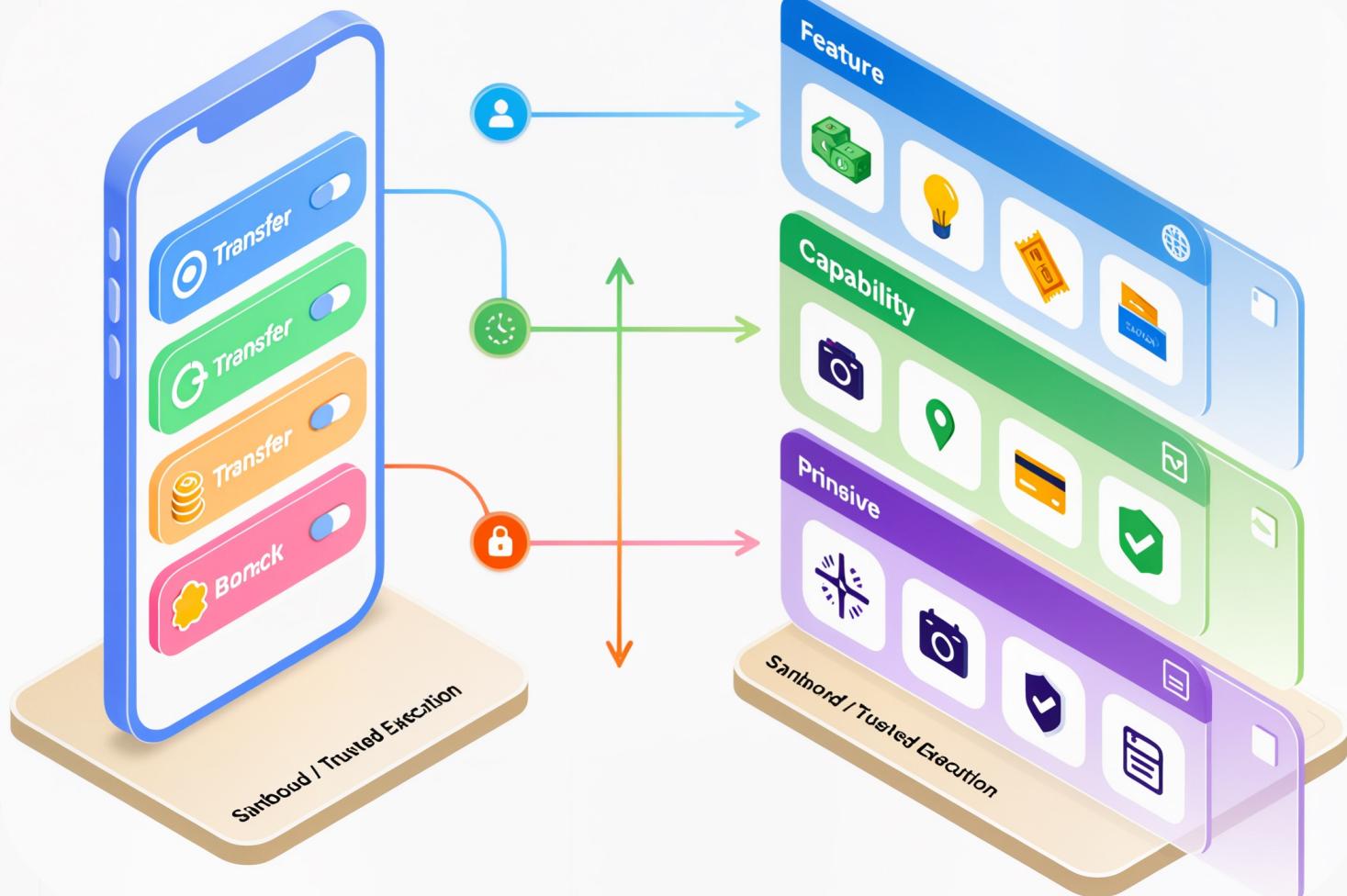
私人化个性化场景上下文 + 用户意图 → 智能体提供高质量服务的关键

如何无缝、安全连接 Agents？



- Agent 在云端使用工具执行任务，需在安全隔离的沙箱环境进行 - Agent专用的云上沙箱技术正在涌现
- Agent 在云端决策，浏览器充当PEP（Policy Enforcement Point），在本地沙箱化使用工具执行任务 – AI浏览器技术的出现
- Agent 在云端决策，APP 充当PEP，调用本地原生能力或者 WebView/小程序 页面工具 – FinClip SDK



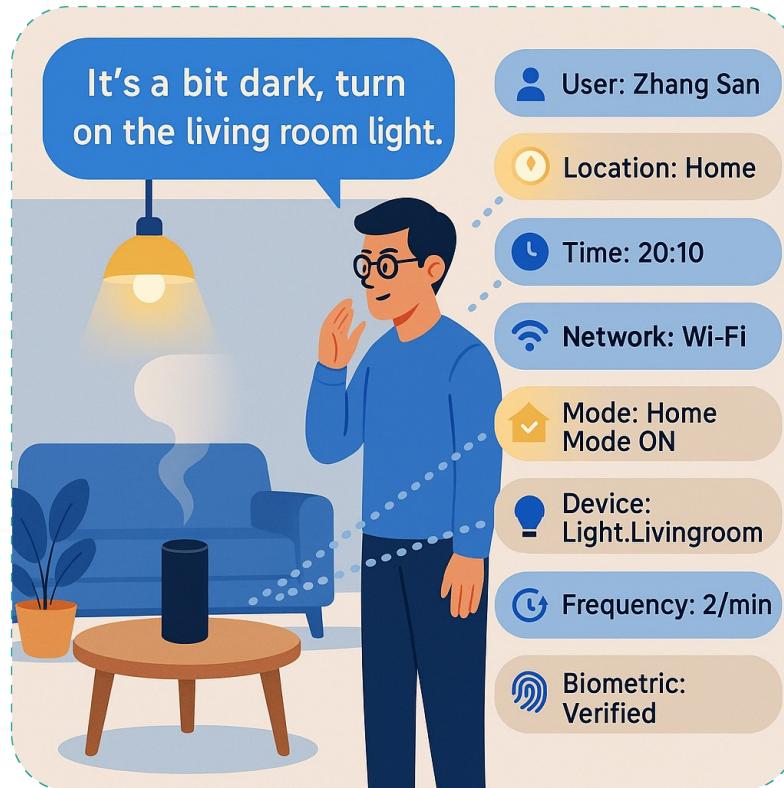


三层映射：功能 → 能力 → 原语

- Feature (功能) : 用户操作
(转账、订票、开灯)
- Capability (能力) : 系统接口
(Camera、Location、Payment)
- Primitive (原语) : 最小执行单元
(get_gps_location、capture_photo)

沙箱管控

- 高层控 Feature，中层控 Capability，
底层控 Primitive
- 让 Agent 调用安全、高效，符合最小权限原则



👉 电子围栏 · Capability 动态配置

基于用户身份、位置、时间、网络等上下文，动态启用或禁用特定 Capability (如灯光控制、传感器读取)

👉 HITL 授权 · 策略约束 · 可审计回溯

调用前需人工确认，作用范围受限，操作全程可追溯



👉 上下文识别 · Feature 拆解

“我要定投” → 拆解为风险评估、产品选择、支付等子任务



👉 云端编排 · 路由调度 · ConvoUI 呈现

云端聚合子任务，用户端通过 ConvoUI 浮层确认，最终交付完整 Feature



动态策略与 HITL：临时 · 有边界 · 可追溯



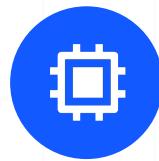
业务策略

- 将安全与合规规则沉淀为组织级策略
- 支撑精细化治理与差异化运营，延展到行业/生态



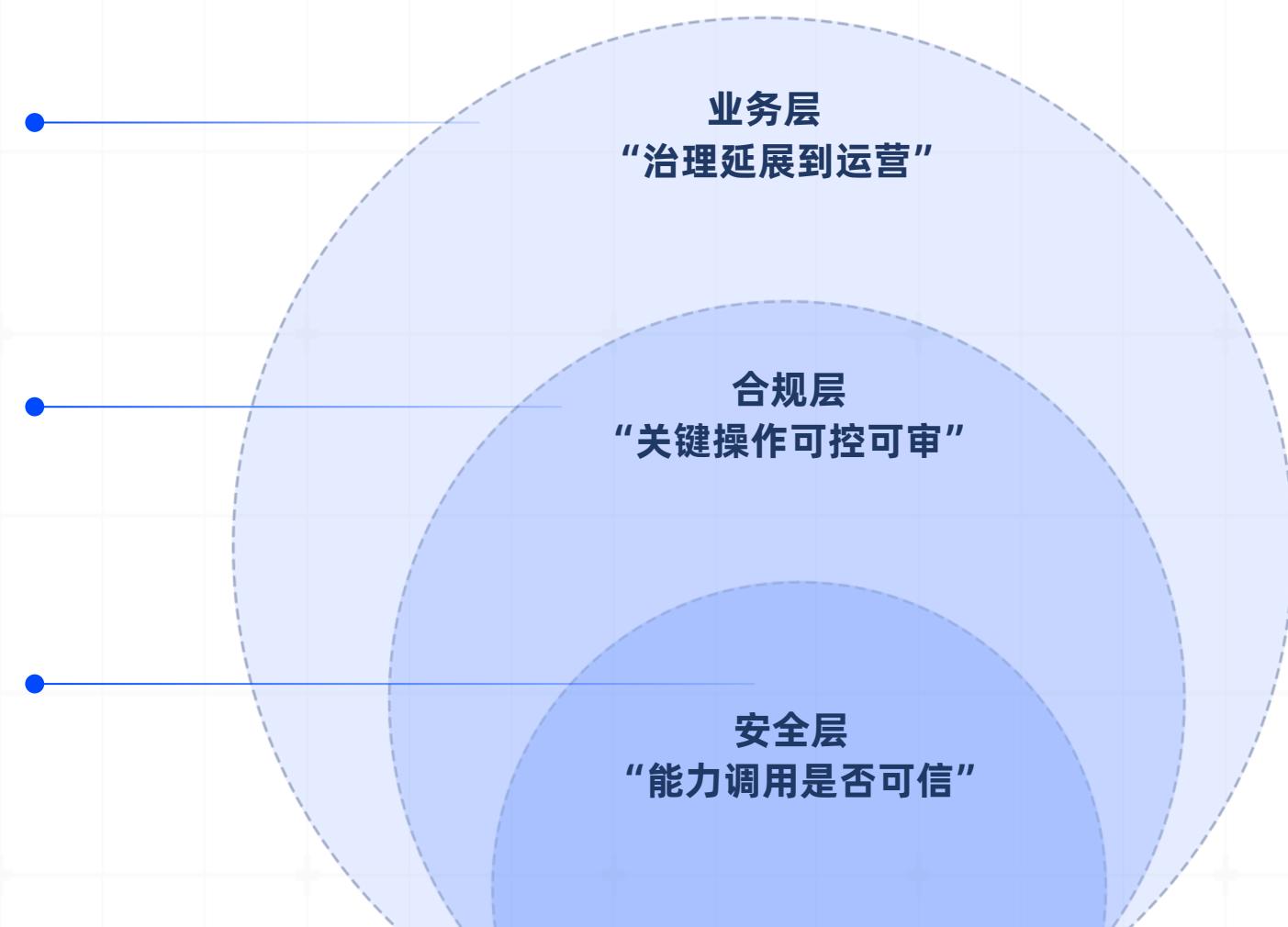
合规策略

- 在关键 Feature 调用中引入风控、审批与用户确认
- 全程记录 Capability 调用轨迹，支持审计与追溯



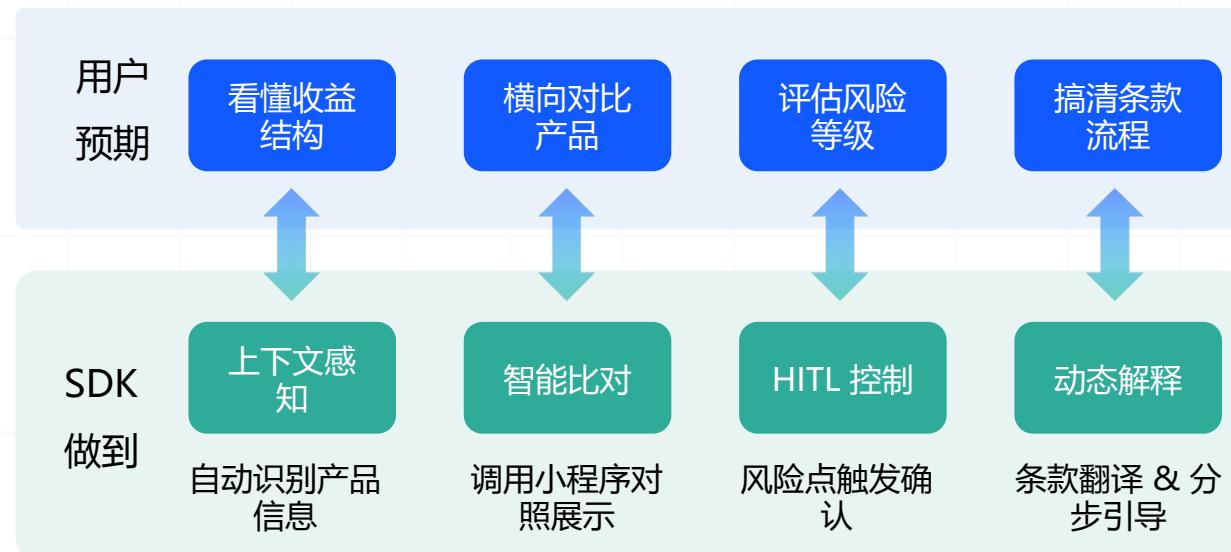
安全策略

- 判断系统能力调用是否可信，最小化权限暴露（如支付、定位）
- 通过 Primitive 控制限流、脱敏与调用频率



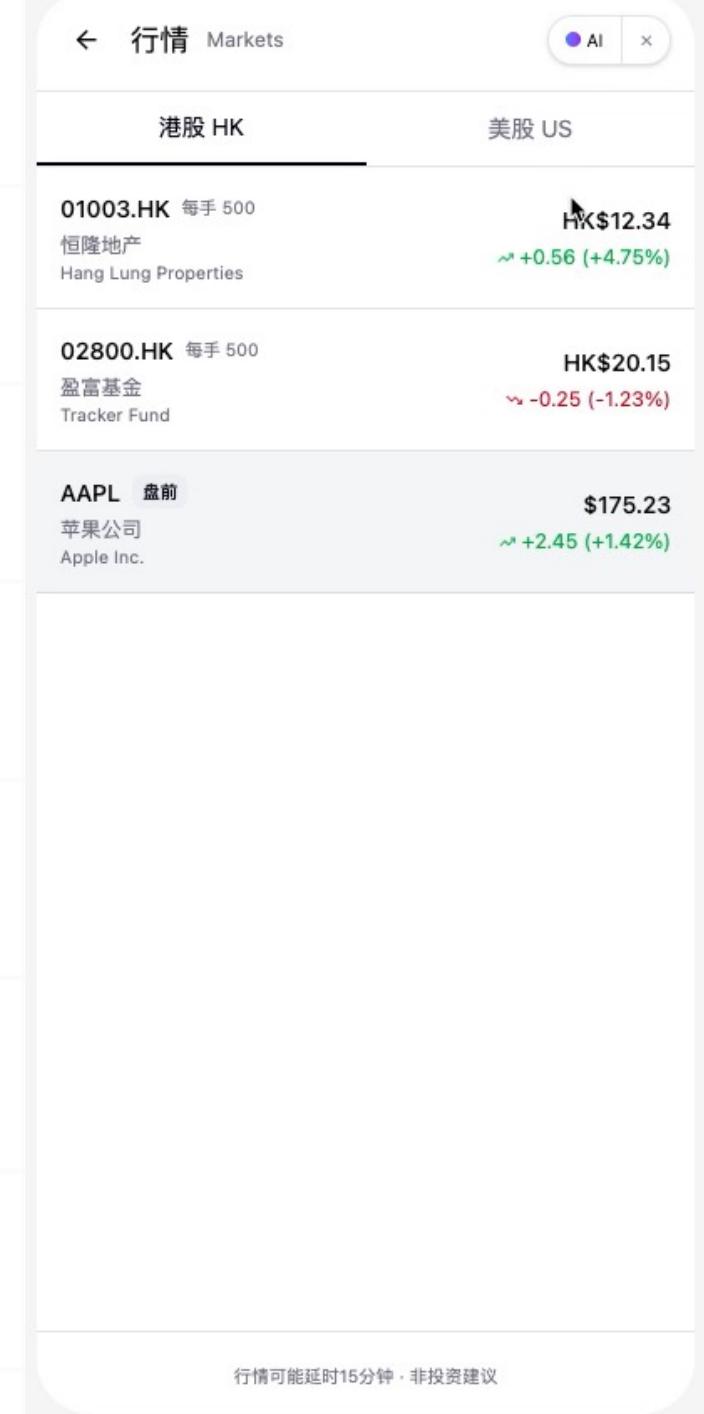
内容脱敏

真实场景：用户理财



核心能力：

- 上下文管理：感知用户意图、状态、环境
- 功能调度：在 App 内安全调用原生 / 小程序 / H5 功能



AI 原生化

- 给任何 APP 一个低门槛入口，让它自然过渡到 AI 时代



安全可信

- 所有云端调用都在沙箱内运行，合规、安全、可控



用户掌控

- 通过 Human in the Loop，每一步人机协同都由用户确认



上下文驱动

- 端侧实时数据组织与脱敏，让 AI 拥有准确、省成本的上下文



对话交互

- 帮 APP 升级为 ConvoUI，自然语言就是新入口

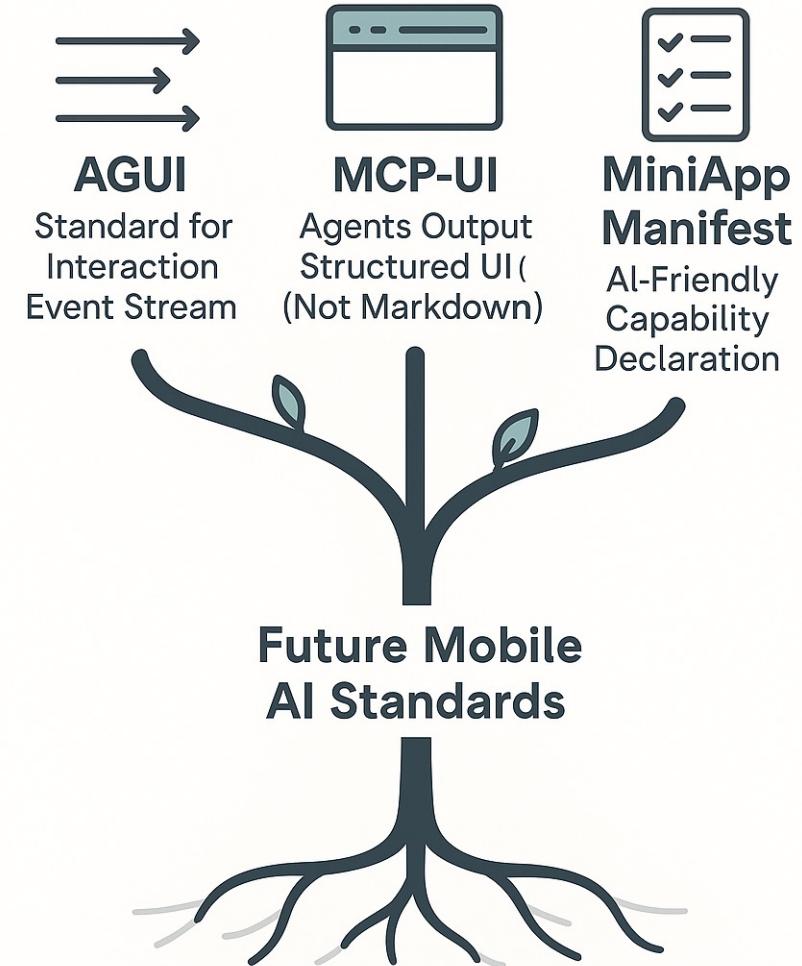


商业模式

- 生态模式 (类 Vercel AI SDK) : 开放 SDK, 联动云厂商和 Agent 开发者, 带来更多增值方案
- 企业部署 (私有化 / 混合云) : 满足金融、政企对安全合规的要求, 支持本地与云端的一体化调度

标准化路线讨论

- 推动 AGUI、MCP-UI、MiniApp Manifest 等标准化
 - AGUI: 统一交互事件流, 打通智能体与应用
 - MCP-UI: 用结构化 UI 替代 Markdown, 结果更可执行
 - MiniApp Manifest: AI 友好扩展, 让功能声明清晰、可控
- 让移动端 AI 的交互与能力更可复用、更可落地



800+ 家
服务客户企业

40+ 项
发放软著专利

7+ 年
小程序领域经验

90+ 人
研发设计与支持人员

- 作为云原生开发模式在中国的最早践行者之一，凡泰极客以“自主创新、中立可靠、灵活开放”为设计理念，致力于为不同体量的企业数字化转型的提供整体解决方案，也是目前唯一的非垄断小程序数字生态服务商。
- FinClip 小程序数字管理平台是国内首个企业级小程序生态产品，已经在银行、证券、政企、电商、航空、园区、零售、教育等多个行业落地，为数百家企业用户提供先进的小程序全流程生态方案。
- 公司总部位于深圳，并在全国多个省市布局研发支持机构，办公室分布于北京、上海、广州、成都。

凡泰极客在深
圳正式成立

基金行业突破
年度合同收入近千万

年度合同收入突破两千万
转化不同业态落地方案

低功耗响应方案上线
开发鸿蒙版技术支持方案

2017

2018

2019

2020

2021

2022

2023

2024

券商、银行客户突
破完成 A 轮融资

FinClip 小程序平台上线
大型股份制银行签约合同

央国企销售网络落地
国有六大银行新突破

FinClip Cloud 重构版
正式上线



感谢聆听

从试用到交流，从想法到合作

FinClip × Agentic SDK 期待与你携手

