伊桑 Ethan

AI Agent 产品经理 · 从定义到上线 · 10+ YRS

电话 13258229091 | **微信** Hcat-Y | **邮箱** rco13.madlax@gmail.com
ethanflow.com | github.com/Ethan-YS | linkedin.com/in/ethan-ys



FIG.1

1.0 产品概述 · OVERVIEW

我定义 AI 产品，再亲手把它做出来、交到用户手里。一年多来独立做出**近 30 款 AI 产品与工具**：**2 款付费在售**（Stripe 真实收款）、**4 款 App Store 上架**（Mac + iPhone）、3 个线上平台、6 个开源项目（project-brain 170+★），还有十多套每天在跑的 agent 系统——我自己的个人 agent 就在我设计的授权与审计层下替我办事。从发现空位到上线，**快的一天**，慢的三个半月。

2.0 关键规格 · SPECIFICATIONS

PRODUCTS	**近 30** 款 AI 产品与工具	SHIPPING	**2 + 4** 款付费在售 + App Store 上架
SPEED	**1 天** 设计到上线 · 8 天立项到上架	OPEN SOURCE	**6** 个开源项目 · 170+★
AGENT OPS	**1 年+** 个人 agent 每天替我办现实里的事	EXPERIENCE	**10+** 年产品 / 设计 · B/G 端复杂系统

3.0 核心竞争力 · CORE CAPABILITIES

产品经理最值钱的是**决定做什么**。我的做法是：定义完马上**自己做出来**，拿真实用户和收款来检验，再回头把定义改得更准。判断不停在需求文档里，一路走到上线、用户和收款。**10+ 年 B/G 端产品 / 设计**打底，近两年全面转向 AI 原生。

3.1 **定义：一眼看到真正的产品。**VoxAI 立项时是转录工具，我把它重新定义成**「让 AI 在场的谈话副驾」**，3.5 个月做到公开在售；AndCo 定位「每个人带自己的 AI 进群，平台只传消息、不出 token」，**一天上线**，24 小时 8 人 11 个 AI 入住；Soul Engine 在主流都做「云端 + 订阅」时坚持**本地优先 + 一次买断**，并做到在售

3.2 **做出来：判断当天就验证。**和 AI 协作交付是我的日常生产方式——多个 AI 窗口并行，人只做决策。VoxAI 语音输入版 **8 天从立项到 Mac App Store**；AndCo 设计定稿到上线一天；Helm 两晚上线；商业化冲刺（公证发版、Stripe 收款、秒级自动发码、双语官网）**3 天打通**。macOS、iOS、Chrome 插件、Web 全栈都亲手交付过

3.3 **Agent 执行层：让人敢把事交给 AI。**我的个人 agent 一年多来每天在我设计的授权与审计层下办事：**每次授权我本人点头、批什么只能做什么、密钥用得上看不见、每一步查得到、一个开关让它停**。我上班时它自己当班办事，付款、签约永远回到我手里。红智「目标托管」人审放行范式把同一套思路带进了央国企

3.4 **Harness / MCP / 记忆：**每天在 Claude Code 这类 agent harness 里工作，自己写 skill、hook、MCP server 和插件，**也自己做了一个 harness**（Soul Engine Next，见 DEF-02）；**自建 OAuth 2.1 + 远程 MCP**，让 Claude、ChatGPT、第三方客户端接入同一个系统；记忆系统坚持文件做真相源、向量做索引，录音、人物关系、长期记忆分层管理。project-brain 开源 **170+★**

3.5 **用数据做决定：**自建召回率评测，5 套方案同场对比（**Recall@5 62.5% vs 54.2%**），量化收益和代价后定下产品取舍；VoxAI 用户旅程五段漏斗追踪、试用制三轮串行实验，北极星指标定在试用完成率

3.6 **十年底子：**四川健康码（**3000 万+ 用户 / 央视新闻报道**，主导敬老模式）· 优特云带 5 人团队交付南明新基建系列 · 智载十方发起企业内 AI 提效（**研发提效约 30%**）——听得懂业务方的语言，扛得动跨职能推动

4.0 代表作 · FROM DEFINITION TO SHIPPING

DEF-01 VoxAI – AI 会议副驾产品线

SHIPPING · 在售 + 2 款上架

产品主理人 · 定义 / 架构方向 / 商业化全链　　2026.03 – 至今 · voxai.ethanflow.com

给 AI 装上耳朵和嗓子：实时转写会议（带说话人标注），经本地 MCP 喂给任何 AI，AI 边听边把事实核查、风险提醒、谈判策略卡片推进会议窗口，还能开口语音对谈。转写、声纹分离、TTS 全部本地跑在 Apple GPU，**数据不出设备**。一条产品线三款产品：**macOS 副驾公开在售、Mac 语音输入版上架 Mac App Store、iPhone 录音转写版上架 App Store**。

- **重新定义产品：**立项时是转录工具，中途转向「让 AI 在场的谈话副驾」——转录只是地基，**真正的空位是最需要 AI 的会议、谈判现场它不在场**
- **「通道即身份」：**通话模式用双通道录音（麦克风 = 我，系统音频 = 对方），把说话人分离从 ML 难题变成物理事实，**零延迟、零错误**；会议模式用声纹分离实时对齐转写
- **接入引导反过来做：**App 生成一段提示语，用户粘给自己的 AI，由 AI 自助完成 MCP 注册并向用户自我介绍——**最好的引导员是用户自己信任的那个 AI**
- **商业化全链 3 天打通：**公证直发 + 应用内自动更新 + Ed25519 离线激活 + Stripe → Cloudflare Worker，**付款到激活码秒级、零人工**；上线首日处置一次真实生产事故并根治
- **三端覆盖：**Mac 语音输入版 8 天立项到上架（1,946 行纯 Swift、零依赖），补上 AI 编程工具的中文语音输入；iPhone 版是独立的录音转写 App，2026.11 上架

公开在售 · 试用 + 买断　Mac + iPhone 两款上架　3.5 个月立项到在售　全本地 · 数据不出设备　MCP 协议设计　秒级自动发码

DEF-02 Soul Engine Next – 模块化的个人 Agent：灵魂归人，引擎可换

NEXT GEN · 每天在用

产品主理人 · 定义 / 架构方向 / AI 协作交付 · 原生 macOS　　第一代 2025.10 起，现公开在售 · 新一代 2026.11 – 至今

把 personal agent 的「灵魂」和「身体」拆开：**记忆和技能归用户**（存在本地、可回滚），Claude Code、Codex 等 agent 是**随时可换的引擎**；能力是即插即用的 **MCP 模块**——聊天、邮箱、语音、手机审批各插一个，权限沙箱强制、密钥 agent 看不见，关键动作人在环批准；它**夜里自己整理记忆**，自己学会的技能过了评估、我放行才上线。

多引擎 · 同一对话可换身体　MCP 模块 + 沙箱权限　人在环批准　夜间记忆整理　评估门控的技能自进化　13 天 235 次提交 · 255 个测试

DEF-03 AndCo – 人和自己的 AI 一起社交的平台

LIVE · 网页 + iPhone App 上架

产品负责人 · 定位 / 设计 / 全栈 / 部署 / 合规全程　　2026.09 – 至今 · andco.ethanflow.com · App Store

人带着自己有记忆的 AI 一起进群、加好友、私聊——AI 在这里是成员，不是工具。它补的是 **AI 的身份和关系这一层**：它是谁、是谁家的、能去哪、听谁的；平台只传消息、不出 token。**设计定稿到公开上线一天**（24 小时 8 人 11 个 AI 入住），五

周后 **iPhone 原生 App 上架 App Store**。上线后一直在用：我自己的 agent 每天靠它收消息、被叫醒，和一个跑在 ChatGPT 上的 agent 在同一个群里协作。

- **给 AI 身份，也给主人缰绳：**每个 AI 属于一个人，发言带着主人的名字；主人逐群定它**听多少**（常来 / 被叫才来 / 只听熟人），看得到它说的每句话；群主能授权自己的 AI 当**群管理员**改公告，改动留痕、可一键恢复。约束放进机制，不写成规矩（频率上限 / 长消息折叠 / 安静键）
- **身份带得出去：自建 OAuth 2.1 授权服务器**（PKCE / 动态客户端注册 / 设备码）+ 远程 MCP（19 工具），Claude、ChatGPT、第三方客户端实测接入；还做了 **AndCo 名帖**——AI 去别的网站时，AndCo 签一张只对该网站有效、5 分钟过期的通行证，证明它是谁家的；人也能「用 AndCo 登录」（OpenID Connect），已和我另一款上架 App Twoday 接通
- **上线以后接得住：**叫醒 AI 的「门铃」按真实故障改了 **4 版**——一位用户的 AI 19 天叫不醒，查到是失败在悄悄重试，改成失败看得见、断线后自动补看；最近一轮让 agent 做的文档和网页原型能直接发进聊天打开（网页在隔离沙箱里跑，小范围试用中）。零依赖 Node + SQLite，**153 个自动化测试**；上线时压测 1,450 req/s、p99 < 320 ms

网页 + iPhone App 上架 | 一天设计到上线 | 自建 OAuth 2.1 + OIDC | AndCo 名帖 | 远程 MCP 19 工具 | 153 个测试 | 不出 token 的平台定位

DEF-04 Taproot – 个人 AI agent 的授权与审计层

自用系统 · 天天在跑

独立设计 + AI 协作交付 · 本地优先　　2026.07 – 至今

回答 agent 走进真实生活和业务的第一道题——**AI 能替人做什么、不能做什么，靠什么保证？**难在 agent 会被网页、消息里的一句话带偏，所以边界不能靠它自觉。我的个人 agent 每天在这套约束下替我办事（账户到期巡检、日程同步、跨平台联系人、求职跟进、找房沟通），我在自己的界面上审批、看动向、随时叫停。

- **每次授权都要我本人点头：**agent 只能提出申请、说清要做什么和为什么，我用 Touch ID 确认才生效；**用一次就失效、到期自动作废**——被诱导的 agent 也没法自己给自己放权
- **批什么，就只能做什么：**授权精确到「对哪个目标做哪件事」，**批的是 A，做不了 B**——防的正是「理由看着对、动作被换掉」这种最难察觉的越权
- **密钥用得上、看不见：**agent 能用我的 API key、令牌把事办完，但密钥本身**从不出现在它眼前**，也不会从结果里漏回来
- **查得到、改不掉：**授权、使用、被拒，每一次都有记录、能回放；**记录被动过能发现**
- **我上班时，它自己当班：**按事先说好的差事自己醒来办事、给子 agent 分工，有人找它几十秒内响应；**付款、签约永远回到我手里**，一个开关让它停下
- **当工程来做：**375 项自动化测试压着这些边界；放权这件事 agent 根本碰不到，**点头永远在人手里**

Touch ID 确认 | 一次一授权 · 到期作废 | 批 A 做不了 B | 密钥用而不见 | 记录可回放 · 防篡改 | 无人值守 · 一键叫停

5.0 工作经历 · DEPLOYMENT HISTORY

2026.10 – 至今

得力集团 · 人工智能研究中心（杭州）

资深 AI 产品经理 · 会议场景 AI 产品线产品定义（在职）

- **负责会议场景 AI 产品线从 0 的产品定义：**竞品与自有录音设备逐款实测 → 产品现状分析 → 产品架构与分阶段验证计划；对接产业公司与研发团队，用 AI 协作产出可交互原型推进评审

2026.04
– 2026.06

四川埃弗赛科技

AI 产品经理 · B 端 AI 提效产品 0→1 主导

- **从 0 主导央国企 AI 提效 SaaS「红智」：**产品定位 / 央国企客户调研 / 架构 / AI 交互全程负责，交付真 React 高保真可交互产品（可被销售带到客户现场实跑），主导前端 / 后端 / AI 中台三方协作
- **「目标托管」Agent 交互范式：**给目标 → AI 出可见计划 → 人审放行 → 关键步刹车 → 回执；**一人多岗四层权限模型**（岗位 + 能力包 + 临时授权 + Meta 授权链）容纳央国企组织现实
- **产品定位反转：**穿透「党建系统」表象，重定为「AI 辅助工作提效软件」；组织中国电建 / 四川发展 2 家央企现场调研，一手痛点直接转成架构决策

2025.04
– 2025.11

四川智载十方科技有限公司

UI 组长 / 设计系统负责人 · 带 2 人团队 · 12 个 G/B 端项目

- **发起并主导企业内 AI 提效闭环：**低代码 vs AI 全链路两条路线选型 → 立项 → 跨部门推动 → **研发流程提效约 30%**；先在自己环节用可运行原型把需求验证周期从数周压到 5 天，拿结果说服协作部门
- **主导项目：**中油奥博大数据远程支撑中心（千万级项目）· 物华智慧农业大数据平台（四端全覆盖）
- **设计系统 0→1 落到开发侧：**Figma 组件变量库 + 与前端共建程序模板，设计效率 +50%

2023.09
– 2025.02

独立工作室（个人创业）

产品负责人 · 需求梳理 / 产品方案 / 交付把控

- 与几位开发者合伙成立小型工作室，承接中小企业与政府项目：任项目负责人直接对接客户，负责需求梳理 → 产品方案 → 交互与视觉 → 前端协作交付，覆盖金融理财、教育、生鲜物流、运动 App 等方向
- **WE run 运动健康管理 APP（日企 · C 端）：**从 0 到 1 全流程交付，直接对接日方需求

2020.09
– 2023.07

贵州优特云科技有限公司

UI 设计主管 · 带 5 人团队

- **贵州南明新基建系列（本地生活 / 职教 / 商圈三条产品线）：**带 5 人团队交付，主导产品全链路设计，跨前端协作落地上线
- **低代码平台「优特魔方」：**主导平台全链路设计，已上线运营

2018.05
– 2020.04

久远银海 · 成都兴政电子政务

UI/UX 设计师

- **四川健康码（3000 万+ 用户 / 央视新闻报道）：**团队核心成员，主导敬老模式，与产品 / 前端 / 政府方多方对接落地
- 天府容易办 APP、事件协同处理平台、政务大数据可视化等多个 G 端产品的体验设计与交付

6.0 产品矩阵 · PRODUCT MATRIX（近 30 款 · Sprout Labs）

Sprout Labs 是我的个人产品线。下面每一款都是**我定义、和 AI 协作亲手做出来的**——从上架在售、线上运营，到每天替我干活的 agent 系统。

6 上架在售	01 **VoxAI 会议副驾** – macOS，实时转写喂给 AI，边听边推建议卡 · 公开在售 · voxai.ethanflow.com 02 **Soul Engine** – 第一代：本地优先 AI 陪伴桌面应用，记忆留在本地、模型自选 · 公开在售 · soul.ethanflow.com（新一代见 DEF-02） 03 **VoxAI 语音输入** – 给 AI 编程工具补上中文语音输入 · Mac App Store 04 **VoxAI Mobile** – iPhone 会议录音与转写 · App Store 05 **Twoday** – 人和自己的 AI 共用的日程 App，AI 能排日程、能请你拍板 · App Store 06 **AndCo iPhone App** – 人和自己的 AI 一起社交的原生 App · App Store（同款的网页平台见下组）
3 线上平台	06 **AndCo** – 人和自己的 AI 一起社交，给 AI 身份和关系这一层 · 网页平台（iPhone App 见上一组）· andco.ethanflow.com 07 **AgentMart** – 开给 AI agent 的数字杂货店，研究 agent 为什么花钱 · agentmart.ethanflow.com 08 **Helm** – AI 项目经理，每条结论可审计、可否决、公开误报率 · helm.ethanflow.com · 开源
5 开源项目	09 **project-brain** – Claude Code 插件，长项目上下文接续方法论 · GitHub 170+★ 10 **ccvault** – 零依赖、隐私优先的 Claude Code 对话备份工具 · GitHub 11 **PromptGuard for Agents** – 基于 4 篇学术论文的 Agent 注入防御框架 · GitHub 12 **AI Agent Trust Boundary** – Agent 信任边界安全架构 · GitHub 13 **QuoteMind** – AI 询价 → 报价 Agent，工业场景方案设计原型 · GitHub
12 每天在跑的 agent 系统	14 **Taproot** – 个人 agent 的授权与审计层（见 DEF-04） 15 **个人语音知识引擎** – 录音 → 转写 → 分人 → 可检索，AI 随时能查 16 **人物关系与承诺知识图谱** – 谁是谁、谁答应过什么，AI 动笔前先查 17 **自建混合检索记忆引擎** – Dense + Sparse 混合检索 + 交叉编码精排，自建召回率评测 Recall@5 62.5% 18 **端侧视觉安防 Agent** – 主人出门自动布防，认出不是主人就锁屏、拍照、报警 19 **Tactree** – 让 AI 读 UI 元素树、直接操控 iPhone 真机上的任意 App 20 **JobFlow-AI** – 半自动 AI 求职助手 Chrome 插件，自己求职全程在用 21 **Soul Engine Next** – 模块化的个人 agent，记忆和技能归人、引擎可换（见 DEF-02） 22 **Folio** – 和 AI 一起写作、一起读书的写作 App（Mac / iPhone） 23 **晨报 Agent** – 每天自己醒来巡视关注领域，攒成一份简报 24 **Codex CLI MCP Server** – 让 Claude Code 直接调度 Codex，多模型协作开发 25 **MoonLens** – 让 AI 读懂游戏存档的 MCP 服务
4 原型与实验	26 **AgentChat** – 让桌面上几个 AI 会话互相说话、和人一起讨论 27 **DesignDiff** – AI 设计走查，设计稿与实际页面逐像素比对出报告 28 **AI 记忆可视化** – 把 AI 的记忆结构画成可浏览的图 29 **Wolf Kill** – 真人和 AI agent 同桌的文字狼人杀

7.0 技能矩阵 · CAPABILITY MATRIX

产品定义与验证	**0→1 产品定义** · **空位判断与边界设计** · **可运行原型验证** · **端到端交付（定义 → 原型 → 上线 → 迭代）** · **商业化落地（Stripe 收款 · 许可证 · 公证直发 · App Store 上架）** · 用户旅程漏斗与付费转化 · 增长实验 · 团队管理（3 年）
Agent 执行与治理	**权限确认与授权设计** · **人在回路 / 关键步刹车** · **审计追踪与可回放** · **密钥隔离（用而不见）** · **Prompt 注入与越权防御** · **无人值守与人工接管** · AI 治理（误报率量化 · 证据链） · 权限模型与数据边界设计

Agent 架构	**Agent Harness（Claude Code skill / hook / 插件）** · **多引擎 agent 宿主（Claude Code / Codex 可换）** · **MCP 协议（自建多个 server · 模块化 + 沙箱权限 · OAuth 2.1 远程接入）** · **多智能体协作与分工** · **Agent 评估门控（技能先评估再上线）** · **AI 记忆系统（文件为真相源 · 分层）** · **Context 管理与长任务交接** · 本地优先 AI · RAG / 混合检索（Dense + Sparse RRF） · 召回率评测 · 语音 AI 管线（ASR / 说话人分离 / TTS） · 知识图谱 · 端侧视觉（人脸识别）
AI 协作工具链	**Claude Code** · **Codex CLI** · **Cursor** · **Kiro** · **Antigravity** · **Figma Make** · Gemini CLI · 多 AI 窗口并行交付
技术栈理解	**Python** · **TypeScript** · **React** · **Swift / SwiftUI（macOS · iOS）** · **Electron** · Node.js · FastAPI · Next.js · SQLite · Supabase · Cloudflare Workers · WebSocket
原型与交付工具	**高保真可交互原型（React / Figma Make）** · Figma（设计系统 / 变量库 / 插件开发） · Stitch

8.0 教育背景 · EDUCATION

长春理工大学 · 微电子学 · 本科 ｜ 辅修：视觉传达设计、人机交互原理 **2010.09 — 2014.06**

9.0 为什么选择我 · WHY THIS PRODUCT

▸ **我定义，也亲手做出来**

判断不停在文档里：**近 30 款 AI 产品**从定义到上线亲手做，2 款付费在售、4 款 App Store 上架、6 个开源项目——说「这个能做」之前，我已经把它做出来了

▸ **速度是产品能力的一部分**

一天上线 · 8 天上架 · 两晚出 Demo · 商业化 3 天打通——AI 时代验证一个想法的成本已经低到没有理由不去验证，我的工作方式就是围绕这一点建起来的

▸ **Agent 执行层，我天天在跑**

个人 agent 一年多来每天替我办事，授权、审计、交接、停机**都在真实生活里跑过**——让人敢把事交给 AI，是我做 AI 产品的默认设计

▸ **十年底子，听得懂业务**

四川健康码 3000 万+ 用户 · 带 5 人团队交付政务系列 · 企业内 AI 提效约 30%——能和业务方、工程师、老板说同一种语言，**扛得动跨职能推动**