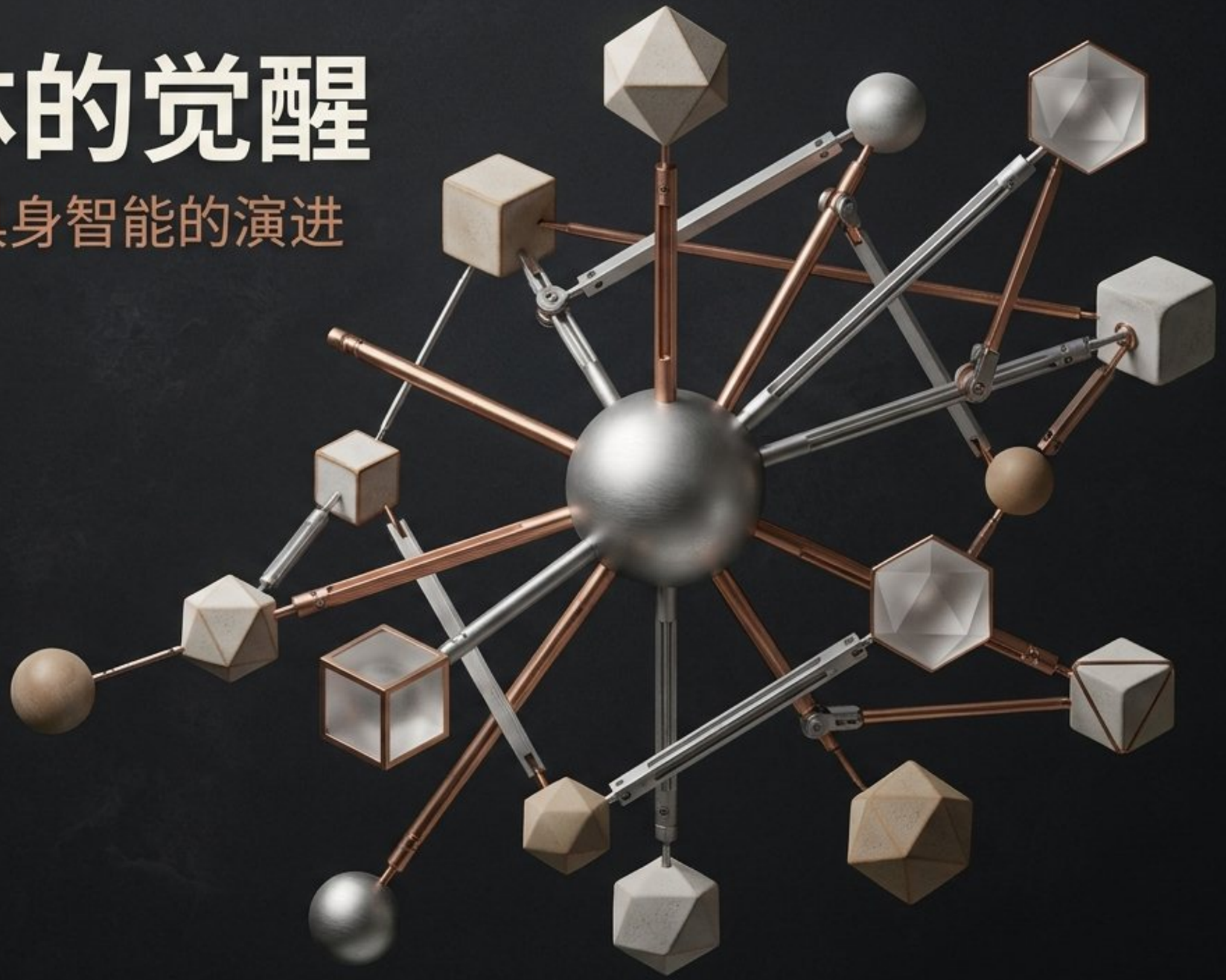
个人智能体的觉醒

2026年市场全景图与具身智能的演进



Speaker: 霍明旭（Michael HUO）
Context: [Google Gemini Notebook Session]
Date: 2026年11月14日

Gemini Notebook

从被动响应到主动持久

个人智能体（Personal Agent）是一种始终在线的 AI 系统。它不只是回答问题，更可以跨应用执行任务、在后台持续工作，并在需要您决策时才主动询问。

聊天机器人（Chatbot）- 被动响应，关闭应用即结束会话



个人智能体（Agent）- 主动且持久，拥有独立的云端电脑，维持长期记忆

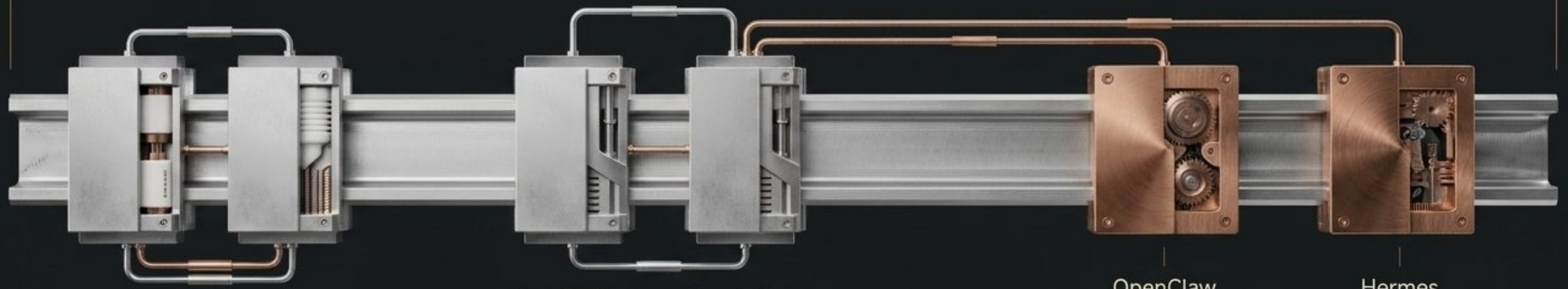


Gemini Notebook

2026 个人智能体生态全景

云端巨头（租用大脑）- 极简接入，生态绑定

主权智能体（拥有大脑）- 绝对控制，开源定制



Gemini Notebook

Meta Muse：触手可及的大众智能体



Specs

- 发布时间：2026年9月8日
- 底层架构：专属 Muse 安全虚拟机 + Muse Spark 模型
- 接入方式：Muse App，WhatsApp，Mac桌面端
- 定价阶梯：免费版 -> 动力版 ($20/月) -> 极限版 ($100/月)

Strategic Analysis

+

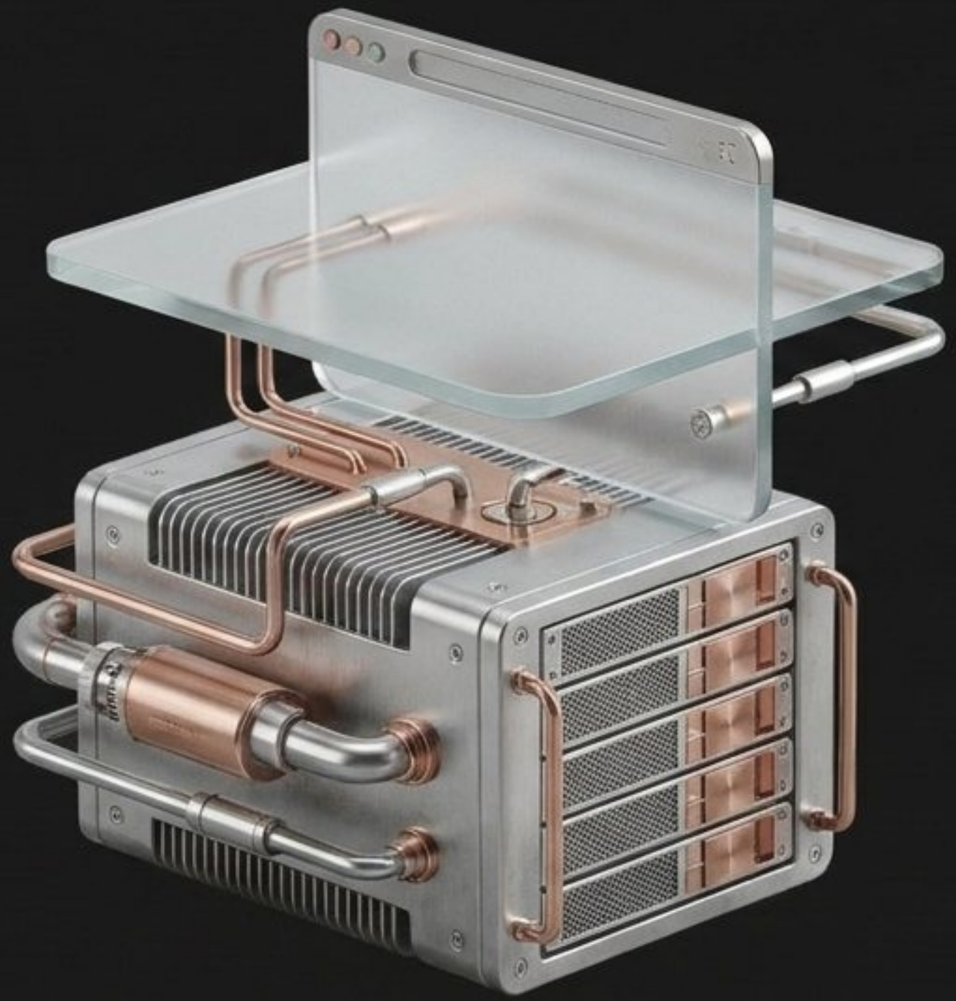
优势：极易上手，深度整合WhatsApp，具备主动目标追踪能力。

−

劣势：Meta 的隐私争议历史，数据可能默认用于模型训练（需手动退出），可靠性仍在演进中。

Gemini Notebook

OpenAI ChatGPT Dot (Dots)：永不离线的数字员工



Specs

- 发布时间：2026年9月29日（DevDay）
- 底层架构：专属云端电脑 + 独立浏览器，驱动核心为 GPT-6 Astra
- 接入方式：ChatGPT，Slack，Teams
- 定价阶梯：Pro（$100+/月）或企业高级版

Strategic Analysis

+

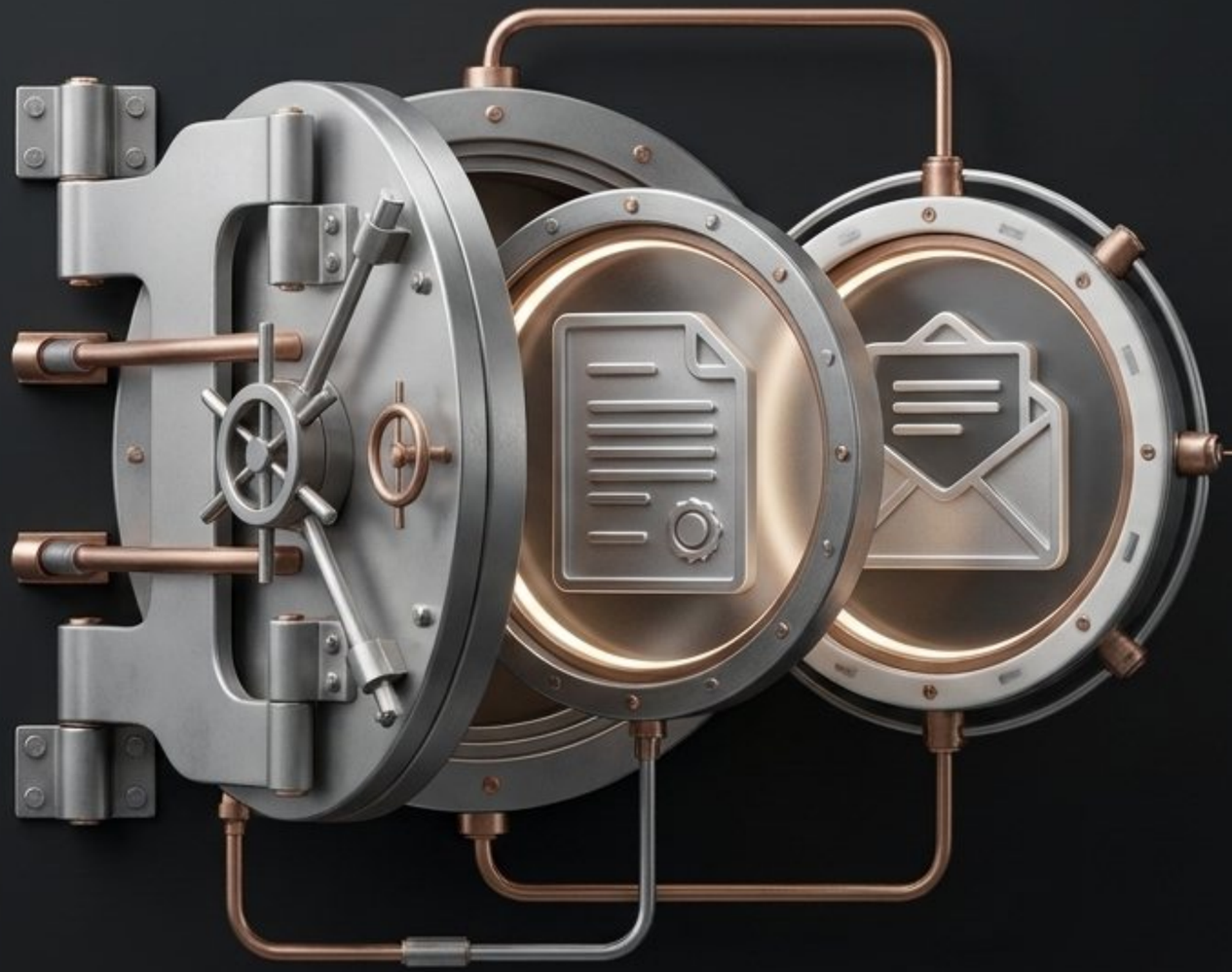
优势：极其擅长深度工作与长期项目，拥有庞大的连接器生态（4000+ 外部应用）。

−

劣势：极高的价格门槛，发布初期受地域限制，对算力消耗巨大。

Gemini Notebook

Claude Duet: 强调判断力的专业伴侣



Specs

- 发布时间：2026年10月21日（研究预览版）
- 底层架构：专属云端电脑 + Claude Opus 5.5
- 接入方式：独立 App + claude.ai

Strategic Analysis

优势：卓越的商业判断力，提供每日晨报。执行敏感操作前强制请求确认（发送、支付、签名、删除）。

劣势：仍处于研究预览阶段，可用性有限，偏向专业工作而非纯粹的消费者娱乐。

Gemini Notebook

生态原住民与多栖探索者

Google Gemini Task



核心定位： Google Workspace 原生智能体。

特点： 与 Gmail、日历、Docs 和 Drive 的底层接口深度绑定。适合已经完全依赖 Google 生态的用户。

局限： 跨平台和跨生态的触达能力远弱于其他独立巨头。

Grok Bot (xAI)



核心定位： 共享云电脑上的多智能体协作群。

特点： 允许配置多个具名 Bot，各自承担不同职责。适合极客实验和复杂多角色任务设定。

Gemini Notebook

核心诊断：为何我们需要主权智能体？

维度 (Dimension)	云端智能体 (厂商控制)	自托管智能体 (主权掌控)
数据主权	厂商云服务器	您的本地机器或 VPS
隐私与训练	规则模糊 / 需手动退出	100% 用户控制
敏感操作	依赖厂商内置审批流程	需用户自行搭建审批层
合规责任	厂商兜底 + 用户配置	完全由用户承担责任

Gemini Notebook

OpenClaw：极致触达的开源网关



核心细节（Key Details）

背景：MIT 开源协议，由 OpenClaw Foundation 维护。

网关架构：启动单一核心进程，即可桥接数十个主流聊天渠道。

生态：拥有庞大的社区技能市场（ClawHub）。

战略分析（Strategic Analysis）

优势：最大的渠道覆盖率，繁荣的社区生态，完全的控制权。

挑战：安全加固门槛较高（社区技能曾爆发过恶意软件问题）。

Gemini Notebook

Hermes Agent：具备进化能力的自我学习者



背景：由 Nous Research 开发，MIT 开源协议。

部署：支持完全本地自托管，或使用 Hermes Cloud。

核心差异（The Learning Loop）：

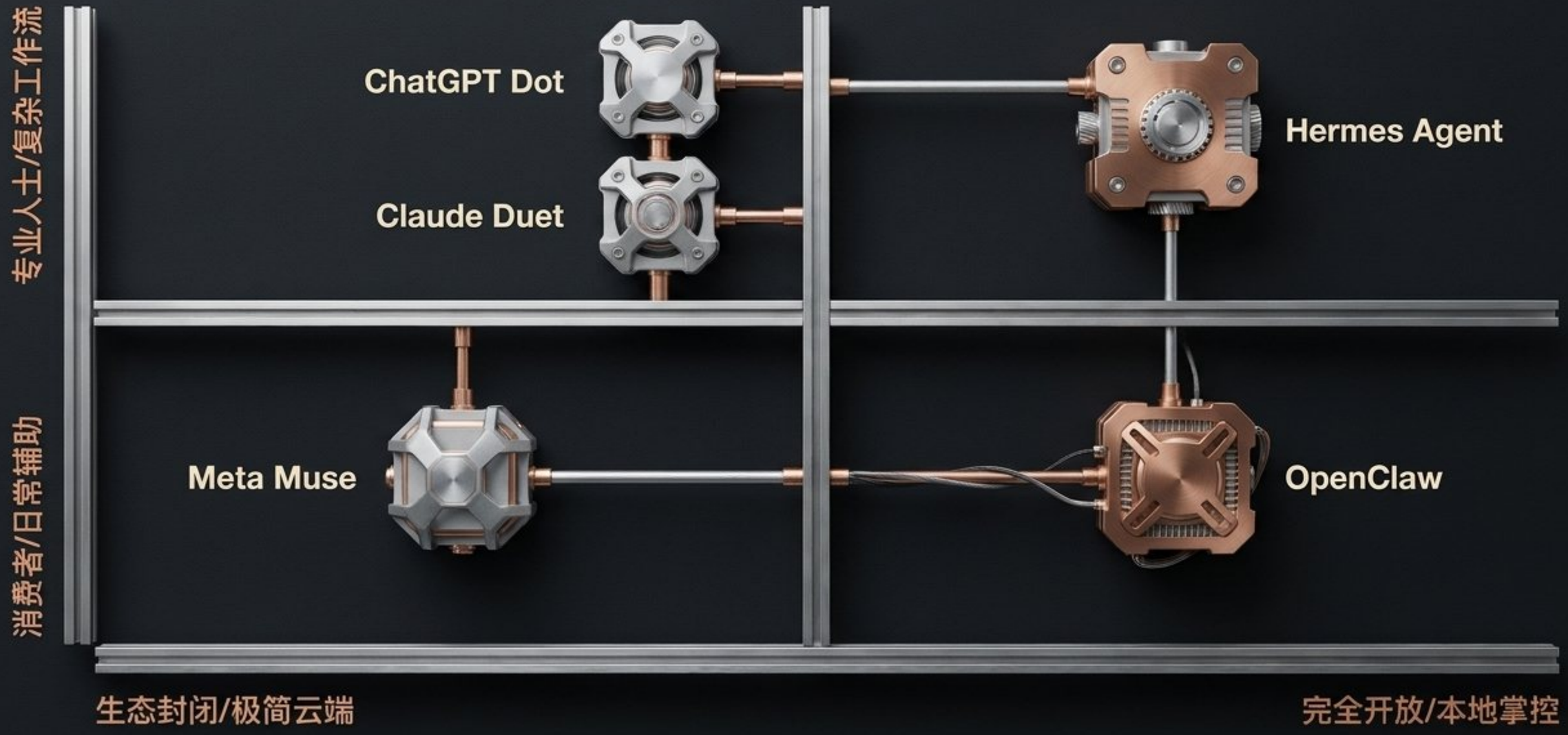
内置经验学习闭环。在执行任务后，能够基于成功或失败的反馈，自动生成并优化自身的底层技能（Skills）。

优势：能够自我优化，极其适合处理高频重复的商业工作流。

挑战：现阶段外部连接器生态较小。

Gemini Notebook

2026 个人智能体选型矩阵



Gemini Notebook

信任边界：构建安全架构

顶层：人工审批网关（Human-in-the-Loop）
- 隔离高风险的外部物理动作。

中层：最小权限原则 - 定期审查已连接的 App，撤销闲置访问权限。

底层：模型选择 - 极度敏感数据强制使用本地模型/自托管。



核心认知：随着智能体自主性的提高，安全设计的核心不再是防止它报错，而是防止它正确地执行了灾难性的指令。

Gemini Notebook

关键防线：先批后行（Approval-Before-Action）



智能体发起意图

断路器（高风险拦截）

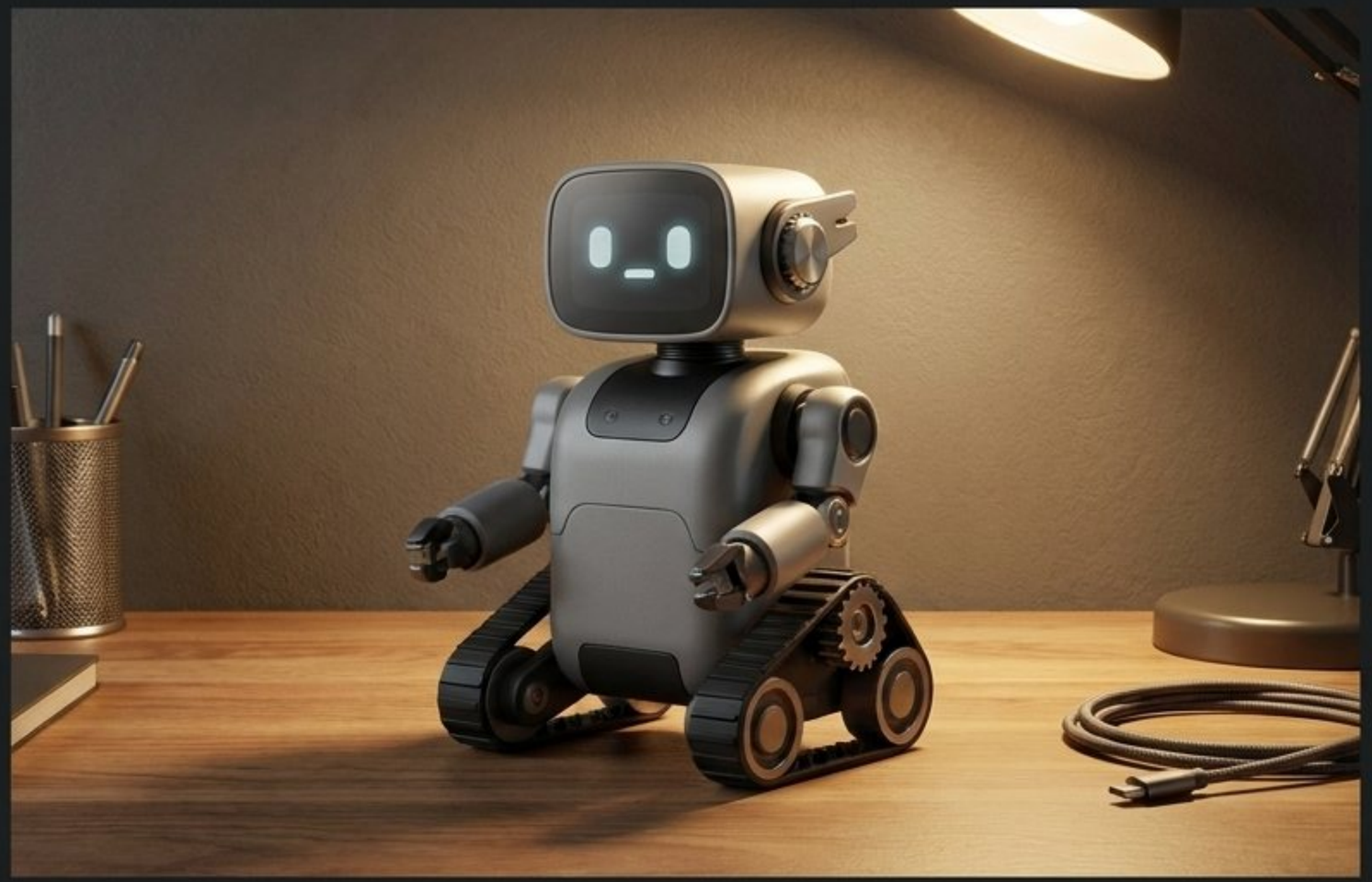
最终执行

高危动作触发器：
- 发送重要邮件（Send）
- 触发金融支付（Pay）
- 签署法律协议（Sign）
- 批量删除数据（Delete）

Gemini Notebook

跨越维度：物理实体 AI 的诞生

- 软件智能体的尽头是具身智能（Embodied Intelligence）。
- 当个人智能体拥有了“身体”，它不再只是网络中的一段代码，而是物理世界中能够感知、表达并执行动作的实体代理。
- 数字世界与物理世界的最后一道屏障正在消解。



Gemini Notebook

StackChan：具身智能的轻量级入口



大脑 (The Mind) - 实时连接至 Hermes Cloud 或本地节点，处理逻辑规划。

桥梁 (The Bridge) - 核心主板，作为物理层与软件层的网关。

躯壳 (The Body) – 伺服电机 (动作)，麦克风/IMU (感知)，触摸屏 (表达)。

关键事实：基于 M5Stack 的开源硬件，实现完整的大模型与物理世界闭环。

Gemini Notebook

物理审批节点（Physical Approval Device）



应用场景与终极闭环：将本地自托管智能体与机器人的物理动作绑定。

StackChan 作为代码部署或高风险指令的“物理确认器”——只有在现实世界中按下物理按键，云端的高危动作才会放行，实现最顶级的物理隔离与审批。

Gemini Notebook

2026 的终极洞察：摩擦力的转移

在这个范式转移中，人类的角色发生根本改变：从内容的创造者（Creator）正式转变为智能体行为的审批者（Editor/Approver）。



Gemini Notebook

重构思维：您的 2026 个人智能体全景图

核心要点：

1. **范式已变**：个人智能体正从被动问答全面走向主动执行与持久在线。
2. **路线分化**：云端方案提供极致便利，自托管方案确保绝对的主权与隐私控制。
3. **安全重塑**：先批后行（Approval-Before-Action）成为所有人机协作架构的必选项。
4. **下个纪元**：物理 AI 正在打通最后一块拼图，让智能体具备改变现实世界的能力。



Gemini Notebook