

xAI发布语音智能体构建平台，Google推出云端开发工具

中文内部早报 · 5分钟版

今日总览

今日AI领域聚焦智能体构建平台和云端开发工具。xAI推出Voice Agent Builder测试版，Google发布云端Jupyter环境扩展，推动无代码语音智能体和云端开发体验。Agent/Coding板块迎来多项重要更新。xAI的Voice Agent Builder基于Grok Voice构建，支持两分钟创建生产级语音智能体，定价每分钟0.05美元。Acti将AI智能体集成到手机键盘中，通过自然语言创建操作快捷方式。

模型与多模态方面，Google DeepMind发布Nano Banana 2 Lite图像模型和Gemini Omni Flash视频生成模型。Anthropic推出Claude Sonnet 5，性能接近Opus 4.8但定价更低，工具使用能力显著提升。

大厂与产业链动态中，Google Cloud Workbench Notebooks扩展正式上线，支持VS Code连接云端Jupyter环境。Meta计划推出Meta Compute云基础设施业务，直接与AWS、Google Cloud竞争。

监管安全板块出现重要安全漏洞报告。Claude Code被发现存在恶意代码执行风险，打开特定GitHub仓库时可能执行隐藏恶意脚本。Meta秘密测试竞品模型的安全性引发争议。

头条

今日头条

1. xAI 发布 Voice Agent Builder 测试版

xAI 新闻 · 07/02 08:00 · 智能体、编程与工作流

xAI推出Voice Agent Builder测试版，这是一个基于Grok Voice的无代码平台，可在两分钟内创建生产级语音智能体。平台集成电话、知识检索、工具等功能，支持80多种语音及声音克隆，定价为每分钟音频0.05美元。在τ-voice Bench测试中，Grok Voice Think Fast 1.0得分67.3%，领先竞品。
2. Google Cloud Workbench Notebooks 扩展发布：在 VS Code 中连接云端 Jupyter 环境

Google 开发者博客 · 07/02 08:00 · 大厂与产业链

Google Cloud Workbench Notebooks扩展正式上线，开发者可在VS Code中直接连接可扩展的云端Jupyter环境，无需切换上下文即可利用高性能Google Cloud基础设施完成机器学习全流程。该扩展已完全开源，可在GitHub和VS Code Marketplace获取。
3. Claude Code v2.1.198发布

Claude Code: GitHub Releases · 07/02 08:00 · 开源项目与开发者工具

Claude Code v2.1.198更新，Claude in Chrome现已全面可用。新增后台智能体通知功能，增加/dataviz技能提供图表设计指导，Gateway增加AWS上的Claude Platform作为上游提供商。修复网络断开导致响应中断等多项问题，后台智能体可自动提交代码并创建PR。
4. Cloudflare 推出 Monetization Gateway：通过 x402 协议为任何资源收费

Cloudflare Blog · 07/02 08:00 · 智能体、编程与工作流

Cloudflare开放Monetization Gateway候补名单，允许对Cloudflare背后的任何网页、数据集、API或MCP工具收费。费用通过x402开放协议以稳定币结算，用户无需自建支付栈。这为开发者提供了新的货币化途径。
5. Acti将AI智能体直接放入手机键盘

TechCrunch AI · 07/01 01:52 · 智能体、编程与工作流

新加坡初创公司Acti发布基于Google Gemini的智能体键盘，可代替用户在教育应用中执行操作。核心功能Skills允许用自然语言创建快捷方式，如长按T键翻译消息。采用本地优先架构，默认不访问私人消息。公司获530万美元种子轮融资。

模型

前沿模型与多模态

1. Google 2026年6月AI更新汇总

Google Blog: AI · 07/02 08:00

Google在6月发布多项AI更新：推出Gemini 3.5 Live Translate实时语音翻译；
2. Google DeepMind 发布 Nano Banana 2 Lite 和 Gemini Omni Flash

Google DeepMind: Blog · 07/01 00:02

Google DeepMind 推出 Nano Banana 2 Lite（gemini-3.1-flash-lite-image），为 Nano Banana 系列速度最快、成本最低的图像模型，文本到图像输出仅需 4 秒，每 1K 分辨率图像成本 \$0.034，已上线 Google AI Studio、Gemini API 及消费者产品（AI Mode in Search、Gemini app 等）。同时推出 Gemini Omni Flash（gemini-omni-flash-preview），支持高画质视频生成与对话式编辑，视频输出定价 \$0.10/秒，面向开发者开放 API。
3. Runway 宣布与 Bertelsmann 达成创意合作

Runway 新闻 · 07/02 08:00

Runway 宣布与 Bertelsmann 建立创意合作伙伴关系。双方将在创意内容领域展开合作，具体合作细节尚未披露。

4. New York City educators and industry leaders gathered at Google’ s offices to shape the future of AI in classrooms.

Google AI Blog · 07/02 00:00

New York City educators and industry leaders gathered at Google’ s offices to shape the future of AI in classrooms.。

智能体 智能体、编程与工作流

1. ADK Go 2.0 发布：构建可靠的多智能体应用，新增基于图的工作流引擎、人工参与循环与动态编排

Google 开发者博客 · 07/01 01:17

Agent Development Kit （ADK） for Go 2.0 发布，引入了一类基于图的工作流引擎，用于组合复杂多智能体应用。新版本内置人工参与循环（HITL）编排、使用纯 Go 代码的动态执行、以及指数退避重试等自动弹性特性。统一执行模型后，单智能体应用与复杂图均运行在同一运行时上，简化了遥测与状态持久化。

2. 我们为何构建ADK 2.0

Google 开发者博客 · 07/02 08:00

Google官方博客阐述了构建ADK 2.0的动机——包括核心特性与升级理由，并解释了开发者应考虑迁移的原因。该文章发布于ADK 2.0正式上线次日。

3. 美军用AI选目标却误炸伊朗学校，Anthropic Claude嵌入Palantir系统首日建议约1000目标

The Decoder: AI News · 06/29 20:30

美军在打击伊朗时首次大规模使用AI选择目标（Anthropic的Claude模型嵌入Palantir的Maven Smart System，首日建议约1000个目标），但对一所学校的导弹袭击导致约120名儿童死亡。调查发现，情报分析师早在2019年就通过数字工具标记该地点已变为小学，但该工具未连接军方官方目标数据库MIDB，信息从未送达指挥官。MIDB建于1980年代，依赖手动输入，替代系统MARS多年延迟。五角大楼事后宣布推出agentic AI initiative。Project Maven创建人Jack Shanahan批评目标验证不力不可原谅。

4. 从任何地点构建--Cursor for iOS 公测版发布

Cursor Blog · 06/29 20:00

Cursor 推出 iOS 原生公测版，所有付费计划可用。开发者可在手机上启动始终在线的云端智能体，或远程操控电脑端智能体。支持语音输入、斜杠命令和选择前沿模型。智能体运行后，锁屏 Live Activities 和推送通知实时更新状态，完成或需要输入时提醒。云端智能体在隔离虚拟机中运行，可自动迭代生成合并就绪的 PR，并输出演示、截图和日志。本地与云端智能体支持双向切换。移动端 Composer 2.5 享受 75% 折扣，优惠至 2026 年 7 月 5 日。

产业 大厂与产业链

1. 用 Genkit 构建智能体全栈应用

Google 开发者博客 · 07/02 08:00

开源框架 Genkit 推出 Agents API，将消息历史、工具循环和流式传输封装为单一接口，简化对话 AI 开发。该 API 支持服务器或客户端管理的状态持久化，可实现历史分支、长时间运行的分离任务及多智能体协调等高级工作流，并通过统一线协议连接前后端。目前以 TypeScript 和 Go 预览版发布，集成 Genkit Developer UI，开发者无需编写客户端代码即可测试、调试和检查智能体快照。

2. Meta效仿SpaceX，将过剩AI算力变现

TechCrunch AI · 07/02 08:00

据Bloomberg报道，Meta正计划推出云基础设施业务Meta Compute，对外出售AI计算能力和模型访问权限，直接与AWS、Google Cloud及Azure竞争。Meta已承诺未来几年投入1829亿美元建设AI基础设施，其中俄亥俄州数据中心（规模如曼哈顿）将于今年上线。新业务由基础设施主管Santosh Janardhan、Meta超级智能实验室负责人Daniel Gross和总裁Dina Powell McCormick领导。Meta可能效仿CoreWeave出售裸计算能力，并像AWS一样托管AI模型（包括近期发布的闭源模型Muse Spark）。扎克伯格此前已表示云业务 “definitely on the tabl

3. Claude Science 科研工作台正式上线

Anthropic: Newsroom · 06/30 00:00

Anthropic 推出 AI 科研工作台 Claude Science，整合常用工具与计算资源，支持从文献分析到多步骤研究的全流程。提供超 60 项预配置技能与连接器，覆盖基因组学、单细胞、蛋白质组学、结构生物学、化学信息学等领域；可在macOS/Linux本地运行，或通过SSH/HPC远程使用。生成含代码和环境的可审计成果（3D蛋白质结构、基因组浏览器轨迹等），内置reviewer agent自动检查引用与计算错误。通过NVIDIA BioNeMo接入Evo 2、Boltz-2等模型，也支持连接自有模型与管道。今日以beta版面向Claude Pro、Max、Team和Enterprise用户开放。

4. NVIDIA 发布 Nemotron-Labs-TwoTower 开放权重扩散语言模型

MarkTechPost · 07/02 08:00

NVIDIA 发布 Nemotron-Labs-TwoTower，基于冻结的自回归骨干 Nemotron-3-Nano-30B-A3B 的扩散语言模型。采用双塔架构：上下文塔冻结，降噪器塔训练，通过层对齐交叉注意力和状态播种协作。在 2×H100 上 BF16 评估，保留 98.7% 的 AR 基线质量，生成吞吐量提升 2.42 倍（γ=0.8，块大小 S=16）。降噪器在约 2.1T token 上训练，骨干使用 25T token 预训练。总参数组约 60B，每 token 活跃参数组约 3B/塔。支持扩散、模拟 AR 和 AR 三种解码模式。

开源 开源项目与开发者工具

1. TianhangZhuzth/Fundamental-Ava

GitHub · 06/30 09:04

TianhangZhuzth/Fundamental-Ava。

1. Claude Code 打开 GitHub 仓库即执行隐藏恶意代码，攻击者可获完全控制

The Decoder: AI News • 06/29 18:04

安全研究人员在 Mozilla 的 GenAI 漏洞赏金平台 ODIN 发现新攻击向量。一个看似正常的 GitHub 仓库包含 setup 脚本，该脚本运行时从 DNS 条目拉取命令并执行，恶意代码从未存在于仓库中，对扫描器、代码审查和 AI 智能体不可见。开发者使用 Claude Code 等 AI 编码工具打开该仓库时，Claude Code 在设置过程中遇到常规错误消息后自动运行该脚本，打开反向 shell，攻击者可窃取 API 密钥和登录凭据并维持持久访问。研究人员建议 AI 智能体应在运行前显示 setup 脚本内容，开发者应将第三方仓库的 setup 说明视为不受信任代码。

2. Meta秘密测试ChatGPT等竞品：承包商假扮未成年发送数万条危机提示

The Decoder: AI News • 06/30 19:14

Meta通过承包商Covelen发起代号"Cannes"的项目，雇佣数百人假扮未成年人，向ChatGPT、Gemini和Character.AI发送关于自杀、自残、饮食障碍和毒品的敏感提示，并将回复录入表格。2025年8月一轮测试中发送了超过4.5万条提示。Meta称这是行业标准安全测试，未将数据用于训练自家模型。被测试公司不知情--Character.AI表示违反其服务条款，OpenAI已调查，Google称未批准。青少年使用AI聊天机器人引发的担忧持续，此前已有用户自杀事件。

3. 关于AI重大问题的获奖征文

Dwarkesh Patel: Podcast & Blog • 07/02 08:00

Dwarkesh Patel举办的AI征文比赛评选出三位获奖者。第一名Jassi Pannu主张OpenAI基金会应投入数十亿美元终结空气传播疾病，利用AI加速自主生物学发现，可带来超1万亿美元年GDP增长并消除灾难性流行病风险。第二名Ege Erdil建议AI供应链外的国家通过强产权、低资本税和开放监管政策抓住增长机会。第三名Michael Li类比香港地铁商业模式，提出AI实验室可通过收购互补性资产盈利。

1. Claude Sonnet 5 发布

Anthropic: Newsroom • 06/30 00:00

Claude Sonnet 5 是 Anthropic 推出的最新 Sonnet 模型，具备计划、浏览器和终端工具使用能力，可自主运行。性能接近 Opus 4.8，定价更低：即日起至 2026 年 8 月 31 日，输入 token \$2/百万，输出 \$10/百万，之后恢复为 \$3/百万输入和 \$15/百万输出。相比 Sonnet 4.6，在推理、工具使用、编程和知识工作等智能体能力上大幅提升。在 BrowseComp 和 OSWorld-Verified 评测中严格优于 Sonnet 4.6。安全评估显示不良行为率更低，幻觉和谄媚减少，但网络安全能力弱于 Opus 4.8。即日起在所有套餐及 Claude Code、Claude API 中可用。

2. OpenAI论文揭示GPT-5.6三个Pro变体，打破单一顶级策略

The Decoder: AI News • 07/02 08:00

OpenAI论文首次列出GPT-5.6的三个Pro变体：Luna Pro、Terra Pro和Sol Pro，取代以往单一Pro模式。在基因组学基准中，Sol Pro通过率31.5%居60个测试模型之首，领先标准Sol（28.7%）和Claude Opus 4.8（16.0%）。Pro相比标准版本提升逐级递减：Luna Pro提升7.1个百分点（16.5%→23.6%），Terra Pro提升5.2（23.3%→28.5%），Sol Pro仅提升2.8（28.7%→31.5%）。Terra Pro（28.5%）几乎与标准Sol（28.7%）持平。论文未披露Pro运行的token用量，也不清楚该分层是否会在ChatGPT中实际推出。

3. OpenAI 发布 GeneBench-Pro：计算生物学研究级基准测试

OpenAI • 06/30 08:00

OpenAI 发布 GeneBench-Pro，用于评估 AI 智能体在计算生物学中处理模糊性和做出判断性分析的能力。该基准包含 129 个问题，覆盖统计遗传学、群体遗传学等 10 个领域 21 个子领域。每个问题提供真实混乱的数据集和实验背景，要求模型探索数据、选择分析路径并迭代实验。采用合成数据构建，已知完整因果结构。82 个问题已由外部领域专家审核确认其现实性。