

Cursor被SpaceX收购，Qwen3.8开源，Anthropic生物武器过滤器失...

中文内部早报 · 5分钟版

今日总览

今日AI领域主线聚焦重大收购与模型安全问题。Cursor正式被SpaceX收购，将获得全球最大GPU集群支持。阿里通义千问发布Qwen3.8系列模型并开源。同时Anthropic披露其生物武器过滤系统近一年处于非活动状态。

Agent与Coding板块活跃，Gemini 3.7 Flash向Pro和Ultra用户开放，提升多步骤任务推理能力。小红书开源dots3-note Preview轻量模型，支持512K上下文和多模态理解。DeepSeek V4 Pro登陆硅基流动平台。

模型与多模态领域，Qwen 3.8 27B参数模型在官方基准测试中超越前代，但存在推理强度高问题。智谱发布GLM-5.3，编程能力开源第一。数学家认为LLM善于组合已知方法但缺乏创造新思路的直觉。

大厂与产业链动态中，2026年前八月开源模型生态显示中国实验室在前沿模型规模上领先。Nvidia将其对OpenAI数据中心投资从2500亿美元削减至1200亿美元。AMD与NVIDIA成为发布开源模型最多的机构。

监管安全方面，Anthropic生物武器过滤器失效期间处理了1.33亿次交互请求。多智能体系统研究显示协调式智能体群在漏洞发现方面表现优异。法院发现原告在文件中隐藏隐形AI指令试图操纵自动化审查系统。

头条

今日头条

1. Cursor正式被SpaceX收购

Cursor Blog · 08/14 20:00 · 大厂与产业链

Cursor已被SpaceX正式收购，完成自4月启动的收购流程。合并后Cursor将获得全球最大GPU集群，以构建更强且运行成本更低的模型，从而以更低价格向客户提供更强大的模型。本周三发布的Grok 4.6是双方合作成果的早期体现。

2. Qwen 3.8 27B表现出色但存在过度思考问题

Simon Willison 博客 · 08/17 08:00 · 研究、评测与方法论

阿里Qwen实验室发布Apache 2许可的27B参数视觉大模型Qwen 3.8 27B，官方基准显示其超越前代Qwen 3.6 27B及闭源Qwen 3.7-Plus。但该模型默认推理强度高导致过度思考现象。

3. Anthropic生物武器过滤器失效近一年

The Decoder · 08/16 15:20 · 前沿模型与多模态

Anthropic在安全报告中披露，其内部生物化学武器风险过滤系统近一年处于非活动状态。在此期间，约5万名外部反馈承包商运行了约1.33亿次未经滤的模型交互。

4. 顶尖数学家称LLM是强计算器但创意思维差

The Decoder · 08/16 23:31 · 智能体、编程与工作流

两位知名数学家Timothy Gowers和Peter Sarnak表示，大语言模型善于组合已知方法，但缺乏产生真正新数学思想所需的直觉能力。

5. Gemini 3.7 Flash全面上线Pro与Ultra用户

X: Gemini (@GeminiApp) · 08/15 02:06 · 智能体、编程与工作流

Gemini 3.7 Flash现已向Gemini聊天中的Pro和Ultra用户开放。该模型更新提升了多步骤任务的推理与准确性，如智能整合数十个文件和邮件为一份主文档。Gemini Spark也已运行于3.7 Flash。

模型

前沿模型与多模态

1. Anthropic 更新模型能力与产品方案

Gary Marcus: The Road to AI We Can Trust · 08/17 08:00

对 Anthropic IPO 静默期流传的 2028 年 1900 亿美元级营收预测，文章提示其多基于匿名信源和未披露算法，可帮助在追踪上市进展时区分已核实数据与传闻。

2. When 更新模型能力与产品方案

The Decoder · 08/16 19:23

据The Decoder，When 更新模型能力与产品方案。这类进展主要影响模型能力、API 选型和产品可用性。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

3. 通义千问开源 Qwen3.8 系列模型

X: 通义千问 / Qwen (@Alibaba_Qwen) · 08/14 23:02

通义千问兑现承诺，开源 Qwen3.8 系列模型。其中 Qwen3.8-27B 为原生多模态稠密模型，仅 27B 参数即全面超越 Qwen3.7-Plus，原生支持 262K 上下文，可通过 YaRN 扩展至 1M tokens，采用 Apache 2.0 许可。Max 级 Qwen3.8-2.4T-A95B 的开放权重也已同步发布。

4. World 更新模型能力与产品方案

The Decoder · 08/15 15:30

据The Decoder, World 更新模型能力与产品方案。这类进展主要影响模型能力、API 选型和产品可用性。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

智能体 智能体、编程与 workflows

1. dots3-note Preview 开源：280B 参数轻量模型，主打长程智能体与多模态推理

公众号：小红书技术（dots.llm） · 08/14 19:25

小红书技术开源 dots3-note Preview，这是 dots3 系列最轻量模型，总参数 280B、激活参数 16B，支持 512K 上下文及文本、视觉、语音多模态理解，并针对复杂推理和长程 Agent 任务优化。

2. DeepSeek V4 Pro 登陆硅基流动，1M 上下文

X：硅基流动 SiliconFlow (@SiliconFlowAI) · 08/14 12:55

DeepSeek-V4-Pro-0813 正式上线硅基流动 SiliconFlow，提供 Day-0 支持，具备 1M 上下文窗口及低/高/最大三档推理强度，更侧重编码、工具调用与智能体 workflow，仍保持 MIT 开源协议。定价为输入 \$1.32/M、输出 \$3.96/M、缓存命中 \$0.44/M。同系列 DeepSeek-V4-Flash-0731 则面向追求速度与成本效益的日常生产场景。

3. TechCrunch 更新 AI workflow 与智能体方案

TechCrunch AI · 08/14 23:43

据TechCrunch AI, TechCrunch 更新 AI workflow 与智能体方案。这类进展主要影响智能体编排、代码生成和企业 workflow 落地。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

4. Meta 更新 AI workflow 与智能体方案

TechCrunch AI · 08/14 22:00

据TechCrunch AI, Meta 更新 AI workflow 与智能体方案。这类进展主要影响智能体编排、代码生成和企业 workflow 落地。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

产业 大厂与产业链

1. 2026年夏季开源模型生态观察：中国前沿模型规模领先，AMD与NVIDIA主导发布量

Hugging Face 博客 · 08/14 08:00

2026年1至8月，Hugging Face公开模型仓库从243万增至296万，但85.6%的模型下载量不足200次，1.5%的仓库占据99.2%下载量。中国实验室月度最大开源模型参数规模在754B至2.78万亿之间，美国实验室七个月中五个月低于130B。AMD与NVIDIA各发布超200个新模型仓库，成为发布开源模型最多的机构。

2. TechCrunch 推出 AI 产业部署新进展

TechCrunch AI · 08/14 22:50

据TechCrunch AI, TechCrunch 推出 AI 产业部署新进展。这类进展主要影响云算力、硬件投入、企业采购和服务成本。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

3. Anthropic 推出 AI 产业部署新进展

TechCrunch AI · 08/16 02:58

据TechCrunch AI, Anthropic 推出 AI 产业部署新进展。这类进展主要影响云算力、硬件投入、企业采购和服务成本。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

4. OpenAI 推出 AI 产业部署新进展

The Decoder · 08/15 23:41

据The Decoder, OpenAI 推出 AI 产业部署新进展。这类进展主要影响云算力、硬件投入、企业采购和服务成本。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

监管 监管、安全与版权

1. 新兴多智能体系统的模式与问题

Hacker News · 08/16 19:17

随着AI智能体在共享代码库、市场等社会系统中承担更多任务，智能体间的真实交互将激增，其交互量可能超过人机交互。Anthropic实验显示，协调式智能体群在2700万 token运行中发现266个漏洞，远超独立并行方法的21个，但两者互补性明显。智能体虽擅长工具使用，但在长期协作与协调方面仍面临挑战。

2. TechCrunch 更新 AI 治理与安全动态

TechCrunch AI · 08/16 05:29

据TechCrunch AI, TechCrunch 更新 AI 治理与安全动态。这类进展主要影响数据、版权、安全和合规部署边界。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

3. Plaintiff 更新 AI 治理与安全动态

The Decoder · 08/15 16:00

据The Decoder, Plaintiff 更新 AI 治理与安全动态。这类进展主要影响数据、版权、安全和合规部署边界。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

研究

研究、评测与方法论

1. GLM-5.3 发布：编程能力开源第一，并涌现网络安全能力

公众号：智谱（GLM） · 08/14 13:31

智谱发布GLM-5.3，基于与GLM-5.2相同的基座，通过极致的后训练Scaling提升智能上界，编程能力较前代提升50%，在Terminal Bench 3.0等公开基准中取得开源第一，并接近Claude Fable 5。模型在白盒代码审查等安全任务中表现持平Mythos 5，在CyberGym测试中得分84.5%。模型权重将在两周后开源，即日起上线ZCode、AutoClaw等工具。

2. Optima 发布 AI 研究评测新进展

The Decoder · 08/16 13:50

据The Decoder, Optima 发布 AI 研究评测新进展。这类进展主要影响模型训练、评测方法和应用路线选择。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。

3. OpenAI 发布 AI 研究评测新进展

The Decoder · 08/16 16:12

据The Decoder, OpenAI 发布 AI 研究评测新进展。这类进展主要影响模型训练、评测方法和应用路线选择。后续需要关注官方披露的可用时间、开放范围、价格变化和第三方验证结果。