AI 每日简报 Daily Brief

覆盖窗口（Asia/Shanghai）：11-18 20:33 — 11-20 08:33 | 最近 36 小时 | 已排除往期重复 9 条

15	33	4	11
入选条目	清洗后候选	聚合站来源	源站直达补充

今日综述 / TODAY'S BRIEF

今日最突出的信号是 AI agent 正从对话界面走向可执行操作的入口：Google 为 macOS 版 Gemini 上线 computer use，可在本地文件、桌面应用与网页间完成多步骤任务；Apple 招聘工程师自研可跨应用操作的 agentic 助手；Meta 则据报将以 300 美元的 Muse Charm 把对话 agent 做成独立硬件。与此同时，平台竞争转向存量用户与开发者效率，Gemini 推出跨助手聊天记录迁移，并在 API 中以 Tool Retrieval 按需加载工具以降低 token 与延迟。企业侧，OpenAI 用 Codex 构建 Performance Factory，三个多月完成逾 1700 次性能回退调查，并把 Codex 延伸至安全审查场景，显示 agent 工作流正被用于自身工程维护。治理层面，英国议会委员会建议立法将恶意滥用 AI 入刑并设立可叫停服务的监管机构，美国政府则在讨论要求企业披露使用中国 AI 模型的情况，监管关注点从模型能力转向部署责任与供应链依赖。英伟达 CEO 黄仁勋因丑闻辞职、股价较 10 月高点下跌近 40%，尽管季度营收翻倍，构成当日最大的公司层面冲击。

The dominant signal today is that AI agents are moving from conversational interfaces to actionable entry points: Google launched computer use for Gemini on macOS, enabling multi-step tasks across local files, desktop apps and the web; Apple is hiring engineers to build an agentic assistant that operates across apps; and Meta is reportedly pricing its Muse Charm screen device with a conversational agent at $300. Platform competition is also shifting toward retaining existing users and developer efficiency, with Gemini adding chat-history migration from other assistants and previewing Tool Retrieval in its API to load tool schemas on demand and cut input tokens and latency. On the enterprise side, OpenAI built its Performance Factory on Codex, completing over 1,700 regression investigations in just over three months, and extended Codex into security review, showing agent workflows being applied to its own engineering upkeep. On governance, a UK parliamentary committee recommended criminalizing malicious AI misuse and creating a regulator empowered to halt services, while the US government is discussing disclosure requirements for companies using Chinese AI models, shifting regulatory focus from model capability toward deployment accountability and supply-chain dependence. The resignation of Nvidia CEO Jensen Huang amid scandal, with shares down nearly 40% from their October peak despite doubled quarterly revenue, was the day's biggest company-level shock.

本期数据 · AT A GLANCE

来源：The Verge 7 | OpenAI 3 | Gemini 2 | Hotminute 1 | Google 1 | LinkedIn 1

分类：产品与应用 11 | 政策与监管 2 | 行业观察 1 | 硬件与算力 1

今日要闻 · TOP STORIES

15 条 · 双语

01 行业观察

英伟达CEO黄仁勋因丑闻辞职，股价大跌

A brief history of Nvidia's recent stock fluctuations

The Verge · 11-20 05:59 · 源站直达

英伟达前CEO黄仁勋因婚外情及涉嫌间谍丑闻辞职，董事会称不会让其复职并已启动继任者搜寻。尽管第三季度营收同比翻倍至1158亿美元、Vera Rubin平台出货近200亿美元，公司股价仍较10月6日高点下跌近40%。

> Nvidia former CEO Jensen Huang resigned amid an extramarital affair and an alleged espionage scandal; the board said it will not reinstate him and has begun an executive search. Despite Q3 revenue more than doubling year over year to $115.8 billion and nearly $20 billion from the Vera Rubin platform, the stock is down nearly 40 percent from its October 6 peak.

- 黄仁勋辞职，董事会称不复职并寻继任者
- Q3营收1158亿美元，同比翻倍超预期
- 股价较10月6日高点跌近40%

原文：https://www.theverge.com/ai-artificial-intelligence/1038063/nvidia-stock-market-price-earnings

02 政策与监管

英国议员建议立法将 AI 滥用入刑

UK MPs want to criminalise the misuse of AI

Hotminute · 11-19 21:35 · 聚合

英国商业、创新、科学与贸易委员会发布报告，建议在下一届议会会期推出《AI 安全与安保法案》，将恶意滥用 AI 入刑，并建立责任制度、对 AI 运营方设定义务。报告警告，当前存在风险阈值缺失、无法定模型访问权、前沿 AI 训练与测试管控不足等安全缺口，并建议设立独立于 AI Security Institute 的新监管机构，有权叫停 AI 服务、强制企业暂停高风险训练。

> A report by the UK Business, Innovation, Science and Trade Committee recommends a new AI Safety and Security Bill in the next parliamentary session to criminalise the misuse of AI for harm, establish a liability regime and impose duties on AI operators. It warns of critical safety gaps, including no defined risk thresholds, no statutory access to models and insufficient controls on frontier AI training and testing, and proposes a new regulator separate from the AI Security Institute with powers to halt AI services and compel companies to pause high-risk training.

- 委员会建议新立法将恶意滥用 AI 入刑
- 拟设独立监管机构，可叫停 AI 服务
- 当前缺风险阈值与模型法定访问权

原文：https://hotminute.co.uk/2026/11/19/uk-mps-want-to-criminalise-the-misuse-of-ai/

03 产品与应用

Apple 招聘工程师自研 AI agent

Apple is hiring engineers to build its own AI agent

The Verge · 11-20 06:31 · 源站直达

据 Bloomberg 发现的招聘信息，Apple 正招募工程师主导开发一款 agentic AI 助手，可浏览网页、跨应用操作、编写代码并调用服务。该岗位将与 Siri、UI Frameworks 和 Apple Foundation Models 团队紧密协作，显示 Apple 计划为 Siri 增加更多 agent 能力，以追赶 Meta、OpenAI、Anthropic 和 Google 的同类产品。

> According to a job listing spotted by Bloomberg, Apple is hiring an engineer to lead the creation of an agentic AI assistant that can browse the web, work across apps, write code, and call services. The role will work closely with Apple's Siri, UI Frameworks, and Apple Foundation Models teams, signaling plans to give Siri more agentic capabilities as Apple moves to compete with similar offerings from Meta, OpenAI, Anthropic, and Google.

- 招聘信息显示 Apple 招募工程师主导 agentic AI 助手开发
- 该 agent 可浏览网页、跨应用操作、写代码、调用服务
- 岗位需与 Siri、UI Frameworks、Foundation Models 团队协作

原文：https://www.theverge.com/tech/1038227/apple-ai-agent-engineer-job-listing

04 硬件与算力

Meta Muse Charm 传定价 300 美元

Meta's Muse Charm might cost $300

The Verge · 11-20 04:22 · 源站直达

据 The Information 报道，Meta 计划将可对话 Muse AI agent 的带屏小设备 Muse Charm 定价为 300 美元，并预计在 12 月假日季前出货。该设备由 CEO Mark Zuckerberg 今年早些时候发布，内置实时语音与 avatar 技术，并配备指纹传感器，还附带 Verizon 提供的 12 个月免费 5G 数据套餐。这一定价显示 Meta 正把 AI agent 从手机应用延伸到独立硬件入口。

> According to The Information, Meta plans to price the Muse Charm, a small screen-equipped gadget for chatting with its Muse AI agent, at $300, with shipping expected in time for the December holidays. CEO Mark Zuckerberg unveiled the device earlier this year, saying it packs the full Muse experience including real-time voice and avatar technology, a fingerprint sensor, and a free 12-month Verizon 5G data plan. The pricing signals Meta's push to extend its AI agent beyond phone apps into a standalone hardware entry point.

- The Information：Muse Charm 定价 300 美元
- 预计 12 月假日季前出货
- 附赠 Verizon 12 个月免费 5G 套餐

原文：https://www.theverge.com/tech/1038087/meta-muse-charm-ai-price

05 产品与应用

Gemini 支持从其他 AI 应用迁移历史记录

ICYMI: Transfer your history from other AI apps into Gemini

Gemini · 11-20 04:30 · 聚合

Gemini 推出迁移功能，用户可将其他 AI 助手的偏好、上下文与聊天记录导入 Gemini。迁移分两步：先复制 Gemini 提供的提示词到旧工具生成摘要并回填，再从旧服务商导出聊天记录 ZIP 上传。此举降低了用户切换助手的迁移成本，是 Gemini 争夺存量用户的产品动作。

> Gemini launched a migration feature that lets users import preferences, context and chat history from other AI assistants. The process has two steps: copy a prompt from Gemini's import settings into the previous AI tool to generate a summary and paste the response back, then export a ZIP of chat history from the old provider and upload it in Gemini's settings. The move lowers switching costs and is a product play by Gemini to capture existing users from rival assistants.

- 偏好与上下文通过提示词摘要方式迁移
- 聊天记录以 ZIP 导出后上传至 Gemini
- 降低用户从其他 AI 助手切换的成本

原文：https://blog.google/innovation-and-ai/products/gemini-app/switch-ai-assistants-transfer-history/

06 产品与应用

Gemini API 推出 Tool Retrieval 预览

Introducing Tool Retrieval in the Gemini API

Google · 11-20 02:00 · 源站直达 · 另见 Google DeepMind、Gemini

Google 在 Gemini API 的 Interactions API 中以预览形式推出 Tool Retrieval，开发者可通过添加 tool_search 工具并设置 defer_loading: true，让模型按需加载工具参数 schema，而非在每次请求中发送完整工具库。该功能旨在降低输入 token 与延迟，并在工具库规模扩大时保持工具选择准确率，支持 Gemini 3.6 及之后模型（含全部 Gemini 4 模型）。

> Google launched Tool Retrieval in preview in the Gemini API's Interactions API. By adding a tool_search tool and setting defer_loading: true, developers let models load tool parameter schemas on demand instead of sending the full tool library with every request. The feature aims to cut input tokens and latency while keeping tool selection accurate as tool libraries scale, and works with Gemini 3.6 and later models, including all Gemini 4 models.

- 按需加载工具 schema，减少输入 token 与延迟
- 无需自建索引，服务端完成搜索
- 兼容 prefix caching 与远程 MCP 服务器

原文：https://blog.google/innovation-and-ai/technology/developers-tools/gemini-api-tool-retrieval/

07 产品与应用

Gemini 在 Mac 上线 computer use 功能

Let Gemini tackle repetitive chores on your Mac

Gemini · 11-20 01:00 · 聚合

Google 为 Mac 版 Gemini 应用推出 computer use 功能，可在隔离的后台窗口中自动完成跨本地文件、桌面应用和网页的多步骤任务，用户需逐项批准操作并自行选择可访问的应用。该功能以英文在美国首发，需 Apple Silicon 芯片与 macOS Sequoia 15.0+，面向 Google AI Plus、Pro、Ultra 个人账户用户。这标志着 Gemini 从对话助手向可执行桌面操作的任务代理延伸。

> Google launched computer use in the Gemini app for Mac, letting it automate multi-step tasks across local files, desktop apps and the web inside an isolated background window, with users approving each action and choosing which apps it can access. The feature rolls out first in English in the U.S., requires an Apple Silicon Mac running macOS Sequoia 15.0+ and is available to Google AI Plus, Pro and Ultra personal accounts. It marks Gemini's expansion from a chat assistant into an agent that can operate a desktop.

- 后台隔离窗口执行，主屏幕与光标不受影响
- 用户逐项批准操作，可随时暂停并限定应用权限
- 英文美国首发，需 Apple Silicon 与 macOS 15.0+

原文：https://blog.google/innovation-and-ai/products/gemini-app/computer-use-mac/

08 产品与应用

OpenAI 用 Codex 打造性能工厂保障 ChatGPT 速度

How OpenAI's Performance Factory keeps ChatGPT fast

OpenAI · 11-19 16:00 · 源站直达

OpenAI 介绍其基于 Codex 构建的 Performance Factory 系统，可在云端自动调查并修复性能回退问题。其中 Regression Workflow 在三个多月内完成逾 1700 次调查，定位 600 多起根因，日均自动调查 17 次。该系统将性能工程从人工排查推进到端到端 agent 工作流，为大规模 agentic 开发下的性能维护提供了可复用范式。

> OpenAI detailed the Performance Factory, a Codex-powered cloud system that autonomously investigates and fixes performance regressions. Its first Regression Workflow tracked more than 1,700 investigations and root-caused over 600 cases in just over three months, averaging 17 automated investigations per day. The system moves performance engineering from manual debugging to end-to-end agent workflows, offering a reusable model for maintaining performance amid rapid agentic development.

- Regression Workflow 三个多月完成 1700 多次调查
- 自动定位 600 多起性能回退根因，日均 17 次
- 系统由任务服务、调度循环、云端执行与订阅四部分组成

原文：https://openai.com/index/how-openai-performance-factory-keeps-chatgpt-fast

09 产品与应用

OpenAI 发布 Daybreak Red 监督式安全调查参考架构

Deploying Daybreak Red

OpenAI · 11-19 08:00 · 源站直达

OpenAI 发布 Daybreak Red 的参考架构，用于在隔离环境中开展受监督的安全调查。指南涵盖架构设计、安全控制、环境配置以及调查的运行与监控。这为企业在受控条件下使用 AI 进行安全调查提供了可复用的部署范式。

> OpenAI published a reference architecture for running supervised security investigations with Daybreak Red in an isolated environment. The guide covers architecture, safety controls, environment configuration, and how to run and monitor an investigation, offering enterprises a reusable deployment pattern for AI-assisted security work under controlled conditions.

- 面向受监督安全调查的参考架构
- 涵盖安全控制与环境配置
- 说明调查的运行与监控方式

原文：https://openai.com/business/learn/deploying-daybreak-red

10 产品与应用

OpenAI 发布 Codex 安全插件演示

Explore the Codex Security Plugin

OpenAI · 11-19 08:00 · 源站直达

OpenAI 发布 Codex Security Plugin 的演示视频，展示从入门到查看结果记录的完整工作流。该插件面向企业安全场景，体现 OpenAI 将 Codex 能力延伸至安全审查环节的产品方向。

> OpenAI released a demo of the Codex Security Plugin, walking through the workflow from getting started to reviewing the results shown in the recording. The plugin targets enterprise security use cases, signaling OpenAI's push to extend Codex into security review workflows.

- 演示覆盖从入门到结果查看的完整流程
- 面向企业安全场景的 Codex 插件
- 以录屏形式展示实际工作流

原文：https://openai.com/business/learn/codex-security-plugin-demo

11 政策与监管

美政府拟要求企业披露使用中国AI模型情况

EXCLUSIVE: Trump administration weighs forcing US firms to disclose Chinese AI use

LinkedIn · 11-19 09:05 · 聚合

据三名知情人士透露，特朗普政府正考虑要求美国企业公开披露其使用中国AI模型的情况，该计划由财政部与白宫科技政策办公室讨论推进。方案拟适用于Airbnb等使用阿里巴巴Qwen模型的企业，要求其在网站上公示相关信息，目的是在不施加新限制的前提下抑制对中国技术的依赖。此举反映美国政府内部对强大中国开源权重模型扩散的担忧正在上升。

> The Trump administration is considering requiring US companies to publicly disclose their use of Chinese AI models, according to three people familiar with the matter. The plan, discussed by the Treasury Department and the White House Office of Science and Technology Policy, would apply to firms such as Airbnb, which uses Alibaba's Qwen model, and require them to post that information on their websites. It reflects a growing push within the government to counter the spread of powerful Chinese open-weight AI models without imposing new restrictions.

- 财政部与白宫科技政策办公室参与讨论该计划
- 拟要求企业在网站公示所用中国模型信息
- Airbnb因客服使用阿里Qwen模型被举例

原文：https://www.linkedin.com/posts/alexandraalper_exclusive-trump-administration-weighs-forcing-activity-7528854177955905537-Zkx_

12 产品与应用

Google 首页新增 AI 对话侧边栏

Google is putting AI chats right on the homepage

The Verge · 11-20 04:05 · 源站直达

Google 更新搜索首页，新增可折叠侧边栏，用于查看并继续 AI Mode 对话。该功能已在桌面端全球上线，反映用户搜索行为从一次性查询转向多轮追问。这是 Google 首页长期以来的又一次重大改版。

> Google is updating its homepage with a collapsible sidebar that lets users view and continue their AI Mode chats. The feature is rolling out globally on desktop, reflecting a shift from one-off queries toward multi-turn follow-up questions, and marks another major change to Google's long-static homepage.

- 首页左侧灰色条可展开 AI 对话侧边栏
- 支持查看历史、新建对话、搜索对话及连接 Gemini Notebook
- 桌面端全球上线，官方称测试中显著提升持续探索体验

原文：https://www.theverge.com/tech/1038059/google-search-homepage-ai-chats

13 产品与应用

Gemini macOS 版上线 computer use 功能

Gemini on Mac can now use your computer

The Verge · 11-20 02:21 · 源站直达

Google 为 macOS 版 Gemini 应用加入 computer use 能力，可跨本地文件、桌面应用和网页完成多步骤任务，如填表、做演示、发布商品。用户可自行选择 Gemini 能访问哪些应用，并通过聊天窗口中的实时预览查看其操作过程。该功能目前仅面向美国用户以英文推出，时点早于 Apple 对 Mac「完全磁盘访问」权限施加新限制。

> Google has added computer use to its Gemini app for macOS, letting it complete multi-step tasks across local files, desktop apps, and the web, such as filling in forms, making presentations, and listing items for sale. Users can choose which apps Gemini may access and follow along via a live preview in the chat window. The feature is rolling out in English for US users, ahead of Apple's new restrictions on Mac apps requesting full disk access.

- 可跨本地文件、桌面应用与网页执行多步骤任务
- 用户可限定可访问应用，并实时预览操作过程
- 目前仅美国英文用户可用，早于 Apple 新权限限制

原文：https://www.theverge.com/tech/1037902/google-gemini-macos-ai-computer-use

14 产品与应用

实测 Apple Watch 的 Siri Recap 常驻监听摘要功能

I let Apple's always-listening AI summarize my life for two weeks

The Verge · 11-19 21:00 · 源站直达

The Verge 记者在 Apple Watch Ultra 4 上测试 Siri Recap 两周，该功能可常驻监听对话并由 AI 生成摘要。Apple 以本地处理、Secure Enclave、Private Cloud Compute 和不保存原始音频等方式强化隐私，但代价是 Siri 难以分辨对话场景、摘要缺乏归因，实用性受限。

> The Verge tested Siri Recap on the Apple Watch Ultra 4 for two weeks; the feature ambiently listens to conversations and uses AI to generate summaries. Apple emphasizes privacy through on-device processing, a secure enclave, Private Cloud Compute, and no saved raw audio, but the trade-off is that Siri struggles to distinguish real conversations and produces summaries lacking attribution, limiting usefulness.

- 功能需手动开启，摘要可设 1/3/7 天自动删除
- 音频在 S11 芯片安全隔区处理后即删，多数处理在本地
- 无录音提示，且 Siri 难辨对话，摘要常出错

原文：https://www.theverge.com/tech/1037100/apple-siri-recap-audio-intelligence-hands-on

15 产品与应用

ChatGPT 上线实时听写，边说话边转写

ChatGPT can transcribe as you speak now with Live Dictation

The Verge · 11-19 23:16 · 源站直达

OpenAI 为 ChatGPT 推出 Live Dictation 功能，可在用户说话时实时转写音频提示，无需等录音结束，并取消了语音听写的 10 分钟时长限制。该功能已在网页版、桌面端及 iOS、Android 应用上面向所有套餐全球推送，用户可点击音频波形查看实时转写文本并在提示框中编辑。这提升了语音输入的效率与可用性，也延续了 OpenAI 今年对语音交互能力的持续改造。

> OpenAI launched Live Dictation in ChatGPT, which transcribes audio prompts as you speak instead of waiting for the recording to finish, and it removed the 10-minute limit on voice dictation. The feature is rolling out globally to all ChatGPT plans on the web, desktop app, and iOS and Android apps, and users can tap the audio waveform to view the live transcript and edit it in the prompt box. The update speeds up voice input and extends OpenAI's broader rework of ChatGPT's voice capabilities this year.

- 说话即转写，无需等录音结束
- 取消语音听写 10 分钟时长限制
- 全套餐全球推送，覆盖网页与移动端

原文：https://www.theverge.com/ai-artificial-intelligence/1037634/openai-chatgpt-live-dictation

生成信息：2026-11-20 08:33（Asia/Shanghai），耗时 204.9 秒。
本简报由程序自动生成，双语内容由模型翻译与归纳，请以原文链接为准。