

AI 技术每日分析：Google 为 Anthropic 搭建近 2000 亿美元算力融资机器

中国高技术产业发展促进会新质生产力工作委员会

博雅云创 & 中科创新驱动

2026 年 8 月 5 日星期三

摘要

最新技术和产业信息显示，企业级 AI 竞争正在从“部署更多智能体”转向“管住智能体、筹到算力、建立治理能力”。AI 安全公司 Obsidian Security 完成 8500 万美元 D 轮融资，估值达到 11 亿美元，企业客户中允许智能体接触业务数据的比例快速上升；Google 为 Anthropic 设计的算力融资结构规模接近 2000 亿美元，把芯片采购、数据中心、电力和私募信贷连接成长期基础设施安排；Anthropic 任命首位全球事务负责人，强化政府关系和国际政策协调；美国白宫则与 Meta、Anthropic、Google 和 OpenAI 举行会议，推动前沿模型自愿网络安全测试进入执行阶段。AI 产业的关键门槛正在由模型能力扩大到身份权限、算力融资、政策协调和发布前验证。

目录

一、Obsidian Security 融资 8500 万美元，智能体权限治理成为独立赛道	3
二、Google 为 Anthropic 搭建近 2000 亿美元算力融资机器	3
三、Anthropic 设置首位全球事务负责人，治理能力进入组织架构	4

四、白宫与四家模型企业会谈，发布前安全测试进入执行讨论	5
趋势观察	5
参考资料	6

一、Obsidian Security 融资 8500 万美元，智能体权限治理成为独立赛道

路透社 8 月 4 日报道，Obsidian Security 完成 8500 万美元 D 轮融资，估值达到 11 亿美元。本轮由 Crescent Cove Advisors 领投，Greylock Partners 和 Menlo Ventures 等原有投资者参与。公司计划利用资金扩展面向企业 AI 智能体的监控和治理平台，并推动业务达到正向现金流。

Obsidian 披露，接近 70% 的客户已经允许 AI 智能体访问或处理企业业务数据，涉及客户记录、源代码、办公协作和第三方 SaaS 系统。智能体与传统员工账号的差别在于，它可以连续调用多个应用、跨系统传递数据，并在较短时间内完成大量操作。一旦权限配置过宽，单次提示注入、凭证泄漏或第三方应用失陷，都可能形成更大的数据暴露范围。

这类风险推动安全产品从“保护模型输入输出”转向“治理非人身份”。企业需要识别每个智能体使用的账号、令牌和应用连接，持续判断其实际权限是否超过业务需要，并在高风险操作发生前实施阻断。Obsidian 把 Microsoft Copilot Studio、Salesforce Agentforce 和 Claude 等平台纳入统一监控，反映出智能体安全正在形成类似身份治理和 SaaS 安全的独立产品层。

对企业采购者而言，智能体上线前应建立应用白名单、最小权限、敏感数据分级和行为审计；上线后则需要持续检查权限漂移、异常调用和跨应用数据流。模型能力越强，运行时治理的重要性越高。

二、Google 为 Anthropic 搭建近 2000 亿美元算力融资机器

《金融时报》8 月 4 日报道，Google 围绕 Anthropic 的 TPU 基础设施建立了一套总规模接近 2000 亿美元的融资安排。相关结构覆盖芯片采购、

数据中心建设、电力供应和私募信贷，其中 Anthropic 计划采购约 1500 亿美元计算设备，Google 与 Broadcom 之间的 TPU 硬件订单规模约 1280 亿美元，并通过特殊目的载体和长期合同分散资金与资产风险。

这一模式说明，前沿模型竞争已经超出传统云服务采购。模型公司需要锁定多年芯片供应和电力容量，云平台则希望把客户需求转化为稳定的基础设施合同，但又不愿把全部建设成本一次性压在自身资产负债表上。私募信贷、设备融资和数据中心租赁因此成为 AI 产业链的重要组成部分。

对 Anthropic 而言，长期算力安排有利于稳定训练和推理资源，但也意味着更高的固定成本和更强的平台绑定。对 Google 而言，TPU 订单能够扩大自研芯片生态，并通过云服务、设备和金融结构形成更深的客户关系。

这类交易将影响模型价格和市场格局。未来模型公司的竞争力不只取决于算法团队，还取决于能否获得低成本资本、长期电力、可靠芯片和高利用率。算力如果不能转化为足够的 API、企业服务和用户收入，融资结构也会放大经营压力。

三、Anthropic 设置首位全球事务负责人，治理能力进入组织架构

路透社 8 月 4 日报道，Anthropic 任命 Mariano-Florentino Cuéllar 为首位首席全球事务官，负责公共政策、政府关系和国际事务。Cuéllar 曾担任加州最高法院法官，并在斯坦福大学、卡内基国际和平基金会及 Anthropic 长期利益信托中承担治理职务。

这一任命发生在 AI 企业与各国政府关系日益复杂的背景下。前沿模型涉及出口管制、网络安全、版权、公共部门采购、国家安全和数据跨境，政策团队已经不再只是应对监管，而是直接影响模型何时发布、在哪些市场提供、可以服务哪些客户。

Anthropic 近年来强调安全和公共利益定位，同时也在扩大企业和政府业务。设立全球事务负责人，有助于把政策判断前移到产品、市场和基础设施决策中，减少技术团队与外部规则之间的信息差。

对于 AI 创业公司，这一变化具有示范意义。随着模型进入金融、医疗、教育和政府场景，合规与公共事务不能在产品完成后补做。企业需要在设计阶段明确数据来源、能力边界、风险分级和地区差异，治理能力正在成为产品工程的一部分。

四、白宫与四家模型企业会谈，发布前安全测试进入执行讨论

路透社 8 月 4 日报道，Meta、Anthropic、Google 和 OpenAI 代表与美国白宫顾问举行会议，讨论前沿模型自愿网络安全测试框架。该框架延续 6 月行政命令的思路，鼓励开发者在模型公开或商业发布前，为政府和可信合作方提供有限时间的评测访问。

与传统基准测试相比，网络安全评测需要检查模型在真实工具、代码环境和外部资源中的行为。重点不仅包括模型是否能发现漏洞，还包括它是否绕过沙箱、扩大权限、持续攻击或访问测试范围之外的系统。

自愿框架的价值在于降低强制许可对创新速度的影响，同时为政府和企业建立协作渠道。但其可信度取决于测试范围是否透明、第三方是否真正独立、重大事件是否披露，以及企业能否证明已实施有效缓解措施。

近期智能体越界事件已经表明，前沿能力测试不能只查看最终答案。模型轨迹、工具调用、网络连接和异常停止过程都应纳入审计。未来“可发布”可能不再只是一个模型分数，而是一套系统级证据。

趋势观察

当天四条动态分别对应企业 AI 的四个基础能力：Obsidian 解决智能体权限和行为治理，Google 与 Anthropic 解决长期算力融资，Anthropic 补

齐全球政策组织，白宫推动发布前安全验证。模型能力仍在快速提升，但决定产品能否进入大规模生产环境的，越来越是运行时控制、资本结构、政策协调和第三方验证。

参考资料

1. Reuters: 《Obsidian Security raises funding at \$1.1 billion valuation on AI security demand》, 2026-08-04。用途：核验 8500 万美元 D 轮融资、11 亿美元估值、客户智能体使用情况及资金用途。<https://www.reuters.com/technology/obsidian-security-raises-funding-11-billion-valuation-ai-security-demand-2026-08-04/>
2. Obsidian Security: 《Security built for how enterprises actually operate》, 持续更新。用途：补充 AI 智能体权限、SaaS 连接和非人身份治理的产品定位。<https://www.obsidiansecurity.com/company>
3. Obsidian Security: 《End-to-End SaaS Supply Chain Protection as Agentic AI Adoption Accelerates》, 2026-01-22。用途：补充智能体连接多个 SaaS 应用后形成的供应链风险。<https://www.obsidiansecurity.com/news/obsidian-security-announces-end-to-end-saas-supply-chain-security>
4. Financial Times: 《Google builds \$200bn financing machine for Anthropic AI infrastructure》, 2026-08-04。用途：核验 Google、Anthropic、Broadcom 及私募信贷构成的算力融资结构。<https://www.ft.com/content/549f2e23-5aa2-49c7-9ea6-a9784ab7087c>
5. Google Cloud: 《AI infrastructure at Next '26》, 2026 年。用途：补充 Google TPU、AI Hypercomputer、网络和存储基础设施能力。<https://cloud.google.com/ai/infrastructure-at-next-26>

[//cloud.google.com/blog/products/compute/ai-infrastructure-at-next26](https://cloud.google.com/blog/products/compute/ai-infrastructure-at-next26)

6. Reuters: 《Anthropic names global affairs chief to tackle AI policy》, 2026-08-04。用途: 核验 Cuéllar 任命及其职责范围。<https://www.reuters.com/world/anthropic-names-global-affairs-chief-tackle-ai-policy-trump-tensions-persist-2026-08-04/>
7. Anthropic: 《Mariano-Florentino Cuéllar appointed to Anthropic's Long-Term Benefit Trust》, 2026-01-21。用途: 补充其法律、治理和国际事务背景。<https://www.anthropic.com/news/mariano-florentino-long-term-benefit-trust>
8. Reuters: 《Meta, Anthropic, Google, OpenAI meet with White House amid rogue AI agent concerns》, 2026-08-04。用途: 核验白宫会议、参与企业和自愿测试讨论。<https://www.reuters.com/legal/litigation/meta-anthropic-google-openai-meet-with-trump-white-house-amid-rogue-ai-agent-2026-08-04/>
9. The White House: 《Promoting Advanced Artificial Intelligence Innovation and Security》, 2026-06-02。用途: 补充发布前自愿评测框架的政策依据。<https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>
10. arXiv: 《Securing the AI Agent: A Unified Framework for Multi-Layer Agent Red Teaming》, 2026-06-30。用途: 补充基础设施、协议工具、智能体行为和模型四层安全评测框架。<https://arxiv.org/abs/2606.31227>

联系我们，请扫描二维码



新质生产力工作委员会
官方公众号



工业智能算网
gyznsw.cn

新质生产力工作委员会：

中国高技术产业发展促进会新质生产力工作委员会，专注于推动工业人工智能、智能制造、数字化转型等前沿技术发展，为企业提供政策解读、技术咨询和产业对接服务。

工业智能算网：

专注于工业人工智能、新质生产力、工业软件 CAE、智能制造等前沿技术。提供每日动态分析、技术趋势解读、解决方案分享，推动工业智能化转型。

网站地址：<https://gyznsw.cn>