AI 技术每日分析

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 4 月 16 日

摘要

全球人工智能领域的核心焦点从单纯的模型参数竞赛，急剧转向了由顶尖大模型（尤其是 Anthropic 的 Mythos）引发的安全风暴、政策博弈与商业重构。美国财政部及美联储的紧急介入，标志着超级 AI 模型的网络安全威胁已上升至国家金融安全级别；同时，Anthropic 与 OpenAI 在" 极端 AI 责任法案" 上的公开对立，彻底揭开了头部 AI 企业在监管路线上的战略分歧。在商业与资本市场，CoreWeave 因与 Anthropic 的算力合作实现股价暴涨，凸显了新兴 AI 云服务商的崛起；而传统企业软件（SaaS）巨头如 Workday 的核心高管流失，则进一步验证了 AI 工具对传统工作流软件的底层冲击。此外，医疗健康领域的跨界融合以及资本市场对头部 AI 企业估值的重新审视，共同构成了今日的产业全貌。

Contents

1 网络安全与金融监管风暴：国家级预警与紧急磋商

Anthropic 旗下最新旗舰模型 Mythos 自发布以来，因其在网络攻防领域展现出的超预期能力，迅速引发了美国金融监管层的高度警觉。这一事件标志着超级 AI 模型的安全威胁已从技术圈的学术讨论，正式上升至

国家金融安全的核心议程。

1.1 财政部寻求底层访问权限

Bloomberg Law 于 4 月 15 日率先披露，美国财政部正在与 Anthropic 进行非公开磋商，要求获得 Mythos 模型的底层技术访问权限，以评估其对金融基础设施（包括银行核心系统、支付网络及证券交易平台）可能构成的网络安全风险。BetaNews 的跟进报道进一步证实，财政部的关切并非空穴来风——内部安全评估显示，Mythos 在模拟测试中成功识别并利用了多个此前未知的金融系统漏洞。

1.2 华尔街闭门紧急磋商

事态的严重性促使美国最高层级的金融决策者迅速行动。财政部长 Scott Bessent 与美联储主席 Jerome Powell 于 4 月 15 日联合召集了华尔街主要银行的 CEO 进行闭门紧急磋商。会议的核心议题包括：评估 AI 驱动的网络攻击对系统性金融风险的潜在放大效应、讨论是否需要建立针对超级 AI 模型的金融安全专项审查机制，以及协调公私部门在 AI 网络安全防御上的资源投入。

1.3 AI 安全研究所发布最佳实践指南

与政府层面的紧急应对同步，美国 AI 安全研究所（AISI）于同日发布了一份面向 AI 开发者和部署者的《AI 模型网络安全最佳实践指南》。该指南首次明确提出，对于具备高级代码生成和网络交互能力的大模型，开发者有义务在发布前进行独立的第三方”红队”网络安全压力测试，并向相关监管机构报告测试结果。

2 政策分歧公开化：AI 巨头的监管路线之争

在安全风暴持续发酵的背景下，AI 行业内部在监管路线上的深层分歧也被彻底公开化。WIRED 于 4 月 15 日发表的深度调查报道，揭

示了 Anthropic 与 OpenAI 在美国国会正在审议的”极端 AI 责任法案”（Extreme AI Liability Act）上截然对立的立场。

2.1 Anthropic 的坚决反对

Anthropic 公开表示反对该法案的核心条款，认为其对 AI 开发者施加的无限连带责任将严重阻碍创新，并可能导致美国在全球 AI 竞赛中落后。Anthropic 的游说团队向国会议员提交了详细的反对意见书，主张应以行业自律和现有法律框架为基础，而非创设全新的、可能过于严苛的监管体系。

2.2 OpenAI 的战略性支持

与之形成鲜明对比的是，OpenAI 对该法案表达了有条件的支持。分析人士指出，OpenAI 的立场可能包含深层的战略考量——作为目前估值最高、资源最雄厚的 AI 企业，严格的监管门槛实际上会大幅提高后来者的进入壁垒，从而巩固其市场领导地位。WIRED 的报道将这一策略定性为潜在的”监管捕获”（Regulatory Capture）行为。

2.3 行业生态的连锁反应

这一公开分歧的影响远超两家公司本身。它迫使整个 AI 生态系统的参与者——从中小型初创企业到云服务提供商，再到下游应用开发者——必须在两条截然不同的监管路线之间做出选择和押注，深刻影响着未来数年的行业格局。

3 算力基础设施格局裂变：新兴云服务商的狂飙

在资本市场层面，算力基础设施领域正在经历一场剧烈的格局裂变。新兴 AI 云服务商 CoreWeave 成为本周最耀眼的明星。

3.1 股价暴涨的背后

CoreWeave 股价在 4 月 15 日单日暴涨 12%，过去五个交易日累计涨幅高达 40%。这一惊人表现的直接催化剂是其与 Anthropic 签署的一份大规模、长期算力供应合作协议。根据协议，CoreWeave 将为 Anthropic 提供专用的 GPU 集群，以支撑其下一代模型的训练和大规模推理部署。

3.2 打破三大公有云垄断

CoreWeave 的崛起具有深远的产业意义。长期以来，全球 AI 算力市场被 AWS、Azure 和 Google Cloud 三大公有云巨头所垄断。CoreWeave 通过专注于 AI/ML 工作负载的 GPU 即服务（GPU-as-a-Service）模式，以更灵活的定价、更低的延迟和更高的 GPU 利用率，成功切入了这一市场。与 Anthropic 的合作不仅验证了其商业模式的可行性，更向市场发出了一个明确信号：头部 AI 实验室正在积极寻求算力供应的多元化，以降低对单一云服务商的依赖。

3.3 资本市场的重新定价

华尔街分析师纷纷上调 CoreWeave 的目标价，认为其正在从一家”小众 GPU 租赁商”蜕变为 AI 基础设施领域的关键玩家。这一趋势也带动了 Lambda Labs、Crusoe Energy 等同类 AI 算力初创企业的估值水涨船高。

4 企业级软件（SaaS）的生存危机与人才”虹吸”效应

AI 浪潮对传统企业软件行业的冲击正在从产品层面蔓延至人才层面。4 月 15 日，企业级人力资源与财务管理软件巨头 Workday 确认，其前首席技术官（CTO）已正式加入 Anthropic，担任高级副总裁，负责企业级 AI 产品战略。

4.1 核心高管的”用脚投票”

这一人事变动在 SaaS 行业引发了强烈震动。Workday 的前 CTO 是该公司技术架构的核心缔造者之一，其离职加入一家 AI 原生公司，被业界解读为传统 SaaS 高管层对自身行业前景的一次”用脚投票”。这并非孤例——过去六个月内，Salesforce、ServiceNow、SAP 等多家 SaaS 巨头均有 C 级或 VP 级高管流向 AI 初创企业。

4.2 AI Agent 对传统工作流的替代威胁

人才流失的深层原因在于，AI Agent（智能体）正在从根本上威胁传统 SaaS 的商业模式。以 Workday 为例，其核心价值在于提供标准化的人力资源管理和财务规划工作流。然而，随着大模型驱动的 AI Agent 日益成熟，企业用户开始意识到，许多此前需要通过复杂 SaaS 界面手动完成的任务（如费用报销审批、员工入职流程、财务报表生成），完全可以由 AI Agent 自动化执行，且成本更低、效率更高。

4.3 SaaS 行业的转型压力

面对这一生存性威胁，传统 SaaS 企业正被迫加速自身的 AI 转型。但讽刺的是，它们最需要的 AI 人才，恰恰正在被 Anthropic、OpenAI 等 AI 原生公司以更高的薪酬、更前沿的技术挑战和更大的股权激励所”虹吸”。

5 跨界布局与市场估值重估

AI 产业的影响力正在加速向传统行业渗透，同时资本市场也在对头部 AI 企业的估值进行冷静的重新审视。

5.1 医疗健康领域的跨界融合

全球制药巨头诺华（Novartis）的 CEO Vas Narasimhan 于 4 月 15 日正式加入 Anthropic 董事会。这一任命意义重大——Narasimhan 是全

球 Top 10 制药企业中首位加入 AI 公司董事会的现任 CEO。此举被解读为 Anthropic 在医疗健康 AI 领域的重大战略布局信号，预示着大模型在药物研发、临床试验设计和精准医疗等领域的应用将进入加速期。

5.2 OpenAI 估值遭投资者质疑

与 Anthropic 的积极扩张形成对比的是，OpenAI 的部分早期投资者开始公开质疑其 8520 亿美元估值的合理性。The Economic Times 报道，多位投资者在近期的闭门会议上表达了对 OpenAI 营收增速放缓、利润率持续为负以及日益激烈的市场竞争的担忧。有分析师指出，如果 OpenAI 无法在 2026 年下半年实现显著的盈利改善，其 IPO 定价可能面临大幅下调的风险。

5.3 DeepSeek 的常规运维

值得一提的是，中国 AI 企业 DeepSeek 近期的动态相对平静，主要集中在处理常规的服务异常和系统维护工作。这与此前其因模型性能突破而引发的全球关注形成了鲜明对比，也反映出 AI 行业的竞争节奏——技术突破往往是脉冲式的，而日常运维和商业化落地才是持续的挑战。

6 参考文献

1. Bloomberg Law (2026-04-15), Treasury Seeks Under-the-Hood Access to Anthropic's Mythos AI Model.
2. BetaNews (2026-04-15), Anthropic Mythos Raises Cybersecurity Alarms Across Financial Sector.
3. The Economic Times (2026-04-15), Treasury Secretary Bessent, Fed Chair Powell Hold Emergency Meeting with Wall Street CEOs on AI Cyber Risks.
4. WIRED (2026-04-15), Anthropic and OpenAI Split on Extreme AI Li-

ability Act, Exposing Industry Fault Lines.

5. PYMNTS (2026-04-15), CoreWeave Stock Surges 12% on Anthropic Compute Deal, Up 40% in Five Days.
6. The Information (2026-04-15), CoreWeave's Anthropic Partnership Signals Shift Away from Big Three Cloud Monopoly.
7. Business Insider (2026-04-15), Workday's Former CTO Joins Anthropic as AI Talent War Intensifies.
8. Reuters (2026-04-15), Novartis CEO Vas Narasimhan Joins Anthropic Board in Historic Pharma-AI Crossover.
9. The Economic Times (2026-04-15), OpenAI Investors Question $852 Billion Valuation Amid Revenue Growth Concerns.
10. AISI (2026-04-15), Cybersecurity Best Practices for Advanced AI Model Developers and Deployers.

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