

FOR YOU / 今日重点 · 主编导读

Agent 走进业务，权限与成本走到台前

微软把内部 Agent 当作需要持续治理的参与者；Modal 实测 Vera CPU 的沙箱并发；亚马逊参与新的核能开发项目。今天看 AI 从“能做什么”走向“如何可靠运行”。

权限可控、运行可测、资源可交付，才是从演示走向业务的下一步。

企业 Agent 需要持续授权

微软把治理重心放到执行前的权限与风险判断。

[Microsoft：治理企业内部 Agent](#)

CPU 等待，也会消耗 GPU 预算

Modal 的 Vera 测试把焦点放到多任务争用与沙箱吞吐。

[Modal：Vera CPU 沙箱并发测试](#)

融资开始押注团队协作

Town 的1.08亿美元B轮，关注助手之间如何交接工作。

[Town：1.08亿美元B轮融资公告](#)

01 / AI公司

2026-10-19 · 新消息

微软谈内部 Agent 治理：权限不能一授了之

微软在10月19日文章中指出，内部 Agent 也可能权限过大，必须持续检查其行为并调整行动权限。公司将7月已公布的 Project Perception 安全架构延伸到内部 Agent 治理，强调身份、数据、网络与运行时共同控制。

对采购和部署团队，关键是能否在一次高风险操作发生前拦截、留痕和收回权限，而不只是监测模型输出。这是微软对治理架构的说明，不能等同于新产品正式上市或已经验证所有 Agent 安全。

[Microsoft：治理企业内部 Agent](#)

2026-10-19 · 新消息

Copilot 模型策略 API 正式可用，模型治理可接入自动化

GitHub 正式开放 Copilot 模型策略 API，企业可读取和更新企业、组织、企业团队及企业应用层级的模型访问设置。同日另有一批 Copilot 模型退出服务，管理员需同步核对替代模型与内部允许清单。

价值在于把模型准入接进现有配置与审计流程，减少逐个界面维护。接口管理的是可用模型策略，不能替代代码审查、数据分级或工具执行权限；迁移也应按实际模型名核对。

[GitHub：Copilot 模型策略 API 正式可用](#)

[GitHub：10月19日模型停用清单](#)

02 / 热点 AI 产品追踪

产品	版本 / 日期	变化与来源
Claude Code	v2.1.304 2026-10-20 本期更新 · stable	稳定版：新增人工决定工具授权、只读检查 Managed Agents 安全配置。 10/19 UTC 发布，北京时间10/20。 Claude Code v2.1.304 发布记录
Qwen Code	v0.25.3 2026-10-19 本期更新 · stable	稳定版：测试失败视图支持校验与回退；快照子 Agent 不能改文件或运行命令。 Qwen Code v0.25.3 发布记录
GitHub Copilot	Model policy API (GA) 2026-10-19 本期更新 · stable	正式可用：四层级模型策略读写接口，管理模型准入，不是工具执行授权。 GitHub: Copilot 模型策略 API 正式可用
DeepSeek V4.1 Flash	1017 2026-10-17 近期版本 · stable	10/17 已核实版本基线：1017 更新及 Search/Fetch；不重复计入今日新闻。 DeepSeek 官方更新日志

03 / AI芯片

2026-10-19 · 新消息

Modal 实测 Vera CPU：沙箱并发比单任务速度更值得看

Modal 收到首台 Vera CPU 服务器后，以50组 Terminal-Bench 标准解与验证器构造 CPU 测试，去掉网络调用并预热容器。公司报告并发吞吐量约翻倍，但空闲机器上的单任务延迟并非全面领先。

Agent 沙箱和强化学习环境会争用 CPU；CPU 等待还可能拖慢 GPU 训练。这里更有用的指标是拥挤时的吞吐与尾部延迟。结果来自 Modal 自测；其现有 x86 基础设施迁向 Arm 仍需改造，文章没有宣布全量上线。

[Modal: Vera CPU 沙箱并发测试](#)

10/15 UTC 首发 · 七日观察

Meta/AMD 训练论文：换硬件也要改模型和软件

Meta 与 AMD 作者的论文以推荐模型训练为例，说明如何围绕 MI350X 的内存与计算特点调整模型、内核和软件。相对直接移植的基线，端到端训练吞吐最高达到其1.5倍；贡献已进入 PyTorch、Triton 与 ROCm 生态。

这项观察适合评估替代加速器的团队：采购差价之外，还要计算移植、调优和功耗。1.5倍不是“比 NVIDIA 快1.5倍”，也不能推广到所有大模型；论文属于参与企业自报的生产实践。

[arXiv: Meta/AMD 论文原始提交记录](#)

[Meta/AMD: 推荐模型训练协同设计论文](#)

04 / 具身智能

10/13 UTC 首发 · 七日观察

RoboSimStudio：让机器人仿真的物理参数可检查、可修改

RoboSimStudio 基于 Newton 构建交互式工具，把接触模型、求解器和物理参数显式交给人和编程 Agent 调整。论文讨论视觉与力反馈校准；项目演示从机器人任务视频建立仿真，再把改进后的策略放回真实机器人。

价值在于缩短“仿真看起来对、真机却失败”的排查过程。它连接了数字 Agent 与实体机器人训练，仍是研究工具和特定任务实验；尚不能据此宣称工厂交付能力或通用自主操作已经成熟。

[arXiv: RoboSimStudio 论文](#)

[RoboSimStudio: 机器人任务仿真演示](#)

05 / 基础设施

10/19 发布指南 · 日期粒度

Gemini MCP Apps 开发指南：交互界面之外，还要两层鉴权

Google Cloud 发布 MCP Apps 实施指南：工具可在 Gemini Enterprise 内提供交互界面，后端部署在私有 Cloud Run。指南明确区分调用服务的 IAM 身份和最终用户的 OAuth 身份；仅允许服务访问，并不代表用户权限已验证。

用户在组件内调整内容，可减少重复的模型往返；部署团队则要核对两层授权、最小权限和工具启用。这里报道的是新指南及架构细节，没有把文章日期视作整个 MCP Apps 标准或产品的首次正式发布。

[Google Cloud: Gemini MCP Apps 开发指南](#)

2026-10-19 · 新消息

亚马逊参与960 MW核能项目：开发资金先于供电交付

X-energy 与 AEP 签署联合开发协议，拟在印第安纳州原 Breed 煤电站附近评估12台 Xe-100 小型模块化反应堆，总目标960 MW。亚马逊将按开发里程碑提供资金；公告强调的是可行性工作，而非电站已开工或已经供电。

对数据中心，能源保障越来越早进入项目开发，但签约容量不能直接算作可用算力。后续仍需观察工程可行性、许可、投资决策和建设进度，且960 MW是发电目标，不是数据中心IT负载。

[X-energy: 印第安纳核能项目开发协议](#)

06 / 监管政策

10/19 公开 · 原令7/24签署

DHS 公开7月 DeepSeek 限制令，采购审查延伸至第三方实现

10月19日进入公开查阅的 DHS 通知附上7月24日签署的限制令，针对联邦文职机构采购和信息系统，范围包含 DeepSeek、关联实体及使用其实现开发的第三方产品与服务。正式公报排期为10月20日。

本期的新事实是公开披露，不能写成10月19日才签发或从今天重新起算整改期。供应商需要核对模型依赖与具体适用范围；该文件并不是面向所有美国个人或私营企业的普遍使用禁令。

[DHS: DeepSeek 限制令公开通知及签署附件](#)

07 / 商业动态

2026-10-19 · 新消息

Town 宣布1.08亿美元B轮，瞄准跨人的 Agent 协作

Town 宣布1.08亿美元B轮融资，由 Forerunner Ventures 与 Menlo Ventures 共同领投，公司估值10亿美元。其 Townie 助手连接邮件、文档和日历，并让不同成员的助手在获准范围内交换信息、交接任务。

资金押注的是团队之间等待信息和确认的成本，而不只是单人生成效率。融资额与估值来自公司公告；共享权限、持续使用和真实协作效果仍需客户验证，不能用融资成功替代产品成效。

[Town: 1.08亿美元B轮融资公告](#)

10/19 合作公告 · 日期粒度

Cognizant 扩大 Gemini 交付团队，规模不等于已实现收入

Cognizant 与 Google Cloud 宣布扩大合作，成立 Gemini Frontier Capability Group，配置超过18,000名专门人员。公司称超过55,000名员工完成 Build with Gemini 工作坊，初期聚焦旧系统现代化、开发体验、业务流程和网络防御。

这说明企业 AI 采用仍依赖架构、集成与行业交付。18,000人是资源配置，55,000人是培训完成口径，都不是新增招聘、项目数量或已确认收入；后续应看客户上线与可衡量的运营结果。

[Cognizant 与 Google Cloud 扩大合作](#)

08 / AI股市

美股存储走强，A股内部仍分化

最近完整收盘中，西部数据上涨6.09%、Sandisk上涨5.53%、美光上涨2.97%；A股长鑫科技下跌7.77%，佰维存储上涨2.94%。韩股海力士、三星分别上涨0.39%和1.16%，同属存储链条也不代表同步表现。

观察清单不是行业指数。美、A、韩股为10/19收盘，港股因休市为10/16；各市场不同步、保留原币种。腾讯涨跌幅未核实留空；不据此推断新闻驱动原因。数据为 Stock Analysis 带归属的有限摘录。

存储与内存

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
美光 / MU	US / USD	904.90	+2.97%	2026-10-19 Stock Analysis · MU
Sandisk / SNDK	US / USD	1,371.12	+5.53%	2026-10-19 Stock Analysis · SNDK
SK海力士 / 000660	KR / KRW	1,277,000	+0.39%	2026-10-19 Stock Analysis · 000660
三星电子 / 005930	KR / KRW	218,000	+1.16%	2026-10-19 Stock Analysis · 005930
长鑫科技 / 688825	CN / CNY	41.52	-7.77%	2026-10-19 Stock Analysis · 688825

存储设备及配套

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
西部数据 / WDC	US / USD	352.21	+6.09%	2026-10-19 Stock Analysis · WDC
希捷 / STX	US / USD	660.81	+3.41%	2026-10-19 Stock Analysis · STX
澜起科技 / 688008	CN / CNY	165.25	-2.33%	2026-10-19 Stock Analysis · 688008
兆易创新 / 603986	CN / CNY	282.44	+0.21%	2026-10-19 Stock Analysis · 603986
江波龙 / 301308	CN / CNY	242.80	+0.48%	2026-10-19 Stock Analysis · 301308
佰维存储 / 688525	CN / CNY	157.98	+2.94%	2026-10-19 Stock Analysis · 688525

算力芯片与制造

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
博通 / AVGO	US / USD	334.59	+1.78%	2026-10-19 Stock Analysis · AVGO
台积电ADR / TSM	US / USD	420.22	+1.84%	2026-10-19 Stock Analysis · TSM
NVIDIA / NVDA	US / USD	217.09	+1.38%	2026-10-19 Stock Analysis · NVDA
AMD / AMD	US / USD	538.05	+1.76%	2026-10-19 Stock Analysis · AMD
Intel / INTC	US / USD	92.03	+2.43%	2026-10-19 Stock Analysis · INTC
寒武纪 / 688256	CN / CNY	928.51	+1.48%	2026-10-19 Stock Analysis · 688256
海光信息 / 688041	CN / CNY	191.50	-0.54%	2026-10-19 Stock Analysis · 688041
中芯国际 / 00981	HK / HKD	52.40	+0.48%	2026-10-16 Stock Analysis · 00981

互联与供电散热

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
Arista / ANET	US / USD	182.95	+3.37%	2026-10-19 Stock Analysis · ANET
Vertiv / VRT	US / USD	206.08	-0.16%	2026-10-19 Stock Analysis · VRT

平台与应用

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
微软 / MSFT	US / USD	533.52	+0.84%	2026-10-19 Stock Analysis · MSFT
Alphabet / GOOGL	US / USD	344.18	+1.05%	2026-10-19 Stock Analysis · GOOGL
Meta / META	US / USD	705.44	-0.55%	2026-10-19 Stock Analysis · META
亚马逊 / AMZN	US / USD	262.45	+4.98%	2026-10-19 Stock Analysis · AMZN
科大讯飞 / 002230	CN / CNY	36.12	+0.33%	2026-10-19 Stock Analysis · 002230
百度 / 09888	HK / HKD	79.45	+1.40%	2026-10-16 Stock Analysis · 09888
阿里巴巴 / 09988	HK / HKD	108.80	+2.26%	2026-10-16 Stock Analysis · 09988
腾讯 / 00700	HK / HKD	417.80	—	2026-10-16 Stock Analysis · 00700
商汤 / 00020	HK / HKD	1.16	+1.32%	2026-10-16 Stock Analysis · 00020

接下来值得验证：企业能否在 Agent 执行前及时收回权限，CPU 并发收益能否转化为真实任务成本下降，以及能源开发协议何时跨过建设与投运门槛。