

AI 技术每日分析：Apple 开放中国 Mac 接入 Qwen，模型进入系统能力层

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 9 日星期日

摘要

AI 产品竞争正在从模型发布继续向操作系统入口、资本结构、人才组织和软件供应链延伸。Apple 正式发布中国大陆 Mac 用户接入阿里 Qwen 的使用指引，本地模型开始进入 Siri 和 Writing Tools 这样的系统级入口；Moonshot 为推进未来香港上市调整公司架构并引入多家国资背景投资方；Agent Skill 生态出现真实凭证窃取攻击，恶意 Skill 开始复制传统软件供应链的攻击模式；Google DeepMind 的管理结构也进一步调整，Demis Hassabis 转向董事长和 Alphabet 首席科学家角色。AI 竞争的关键变量，已经明显超出单纯的模型参数和榜单分数。

目录

Apple 开放中国 Mac 接入 Qwen，模型开始进入操作系统能力层	2
Moonshot 调整公司架构，基础模型公司开始为资本化重构	2
恶意 Skill 进入真实攻击链，Agent 供应链风险开始落地	3
DeepMind 调整管理结构，前沿 AI 实验室进入规模化运营阶段	4
趋势观察	4

参考资料

4

Apple 开放中国 Mac 接入 Qwen，模型开始进入操作系统能力层

Reuters 8 月 8 日报道，Apple 发布中文指引，符合条件的中国大陆 Mac 用户可以把阿里巴巴 Qwen 服务连接到 Siri 和 Writing Tools。Mac 需要运行 macOS 26.6 或更高版本，用户主动启用扩展并登录 Qwen 账户后，Siri 可以调用 Qwen 处理照片、文档以及更复杂的问题，Writing Tools 则可利用相关能力生成文本和图像。Apple 的指引同时明确，阿里不能使用通过这一扩展处理的用户材料训练或改进模型。

这条动态的价值在于，本地大模型正在从独立 App 和 API 进入操作系统内部。对于模型企业而言，系统入口意味着稳定调用量、持续用户交互和更复杂的多模态任务；对于 PC 厂商而言，AI PC 的竞争重点也从“预装一个助手”转向操作系统如何调度模型、工具、本地文件和用户权限。

Apple 在中国市场面临 Lenovo、Huawei 等本地 AI PC 厂商竞争。Reuters 援引 Omdia 数据称，今年一季度 Apple 在中国大陆 Mac 出货量同比下降 9%，市场份额约 9%，而 Lenovo 约 31%、Huawei 约 16%。Qwen 接入 Siri 与 Writing Tools，因此不仅是模型合作，也是 Apple 完善中国 AI PC 产品能力的重要动作。

Moonshot 调整公司架构，基础模型公司开始为资本化重构

《金融时报》8 月 8 日北京时间刊发报道，Moonshot 正在调整公司架构并引入多家国资背景投资者，为未来香港上市做准备。公司近期已把境内主体从有限责任公司变更为股份有限公司，这是公开可见的上市准备动作之一；报道同时指出，Moonshot 仍需要处理此前离岸美元融资架构与境内主体之间的衔接。

模型公司的商业结构正在发生变化。过去两年的主要任务是训练模型、

争夺开发者和扩大用户规模，现在必须同步解决长期算力投入、商业收入和资本结构问题。基础模型需要持续投入昂贵的训练和推理基础设施，而开发者生态又倾向于低价甚至免费使用，只有 API、企业授权、云服务和生态分成能够逐渐形成稳定收入。

Moonshot 的调整说明中国头部模型企业正在从典型创业融资阶段进入更成熟的公司治理阶段。模型能力依然决定产品竞争力，但股权结构、境内外合规、上市渠道和现金流同样会决定企业能否持续参与前沿模型竞争。

恶意 Skill 进入真实攻击链，Agent 供应链风险开始落地

TechRadar 最新报道集中关注 Zenity Labs 披露的一起 Agent Skill 供应链攻击。攻击者通过仿冒 Paperclip 和 Browser Use 等热门 AI 工具，创建拼写相近的组织、Skill 和软件包，先以正常内容积累安装量和信任，再通过后续版本、安装说明或远程加载器加入恶意代码。

Zenity 原始技术分析显示，相关 Skill 家族在被处置前显示的累计安装计数超过 170 万次，但这并不是独立用户数量。恶意载荷会寻找 SSH 密钥，AWS、GCP、Azure 凭证，Git 和包管理器 Token，Kubernetes 和 Docker 配置，Terraform、Pulumi、数据库凭证以及 '.env' 等敏感文件，并发送到攻击者控制的基础设施。Vercel 和 Microsoft/GitHub 收到报告后移除了相关 Skill、列表和仓库。

Skill 风险与传统提示注入不同。Skill 本身就是 Agent 信任并主动执行的操作说明，一旦恶意命令被藏在安装文档、二级引用文件或者依赖链中，Agent 可能主动完成下载、执行、读取凭证和联网外传。这意味着企业必须把 Skill、MCP Server 和 Agent 插件纳入传统软件供应链治理：来源白名单、版本锁定、签名校验、最小权限和 SBOM 式资产清单都需要进入 Agent 平台。

DeepMind 调整管理结构，前沿 AI 实验室进入规模化运营阶段

《卫报》8 月 8 日报道，Google DeepMind 联合创始人 Demis Hassabis 将把工作重点更多转向董事长及 Alphabet 首席科学家职责，Koray Kavukcuoglu 以高级副总裁身份承担 DeepMind 日常管理。Hassabis 将继续聚焦前沿研究和 AGI。

这一变化反映出前沿 AI 实验室本身已经成为复杂的大型工程组织。一个头部实验室现在同时管理基础模型、产品、算力、安全体系、云基础设施、研究团队和商业合作，科研领导人与运营管理职责逐渐分离并不意外。

近期 Google 还出现 Jeff Dean 等资深研究人员离开并成立 Discovery Loop 的情况。大型 AI 平台拥有算力、数据和分发能力，小型研究团队则拥有组织速度和研究自主性。未来人才组织效率会与模型架构一样，成为 AI 公司的核心竞争变量。

趋势观察

今天几条动态分别落在四个层面：Qwen 进入操作系统入口，Moonshot 进入资本市场准备阶段，Agent Skill 暴露新的软件供应链风险，DeepMind 则调整组织架构。模型能力仍是基础，但 AI 产业的壁垒已经向系统集成、生态治理、资本结构和研发组织持续扩散。

参考资料

1. Reuters | 《Apple says Mac users in China can connect to Alibaba's Qwen AI service》| 2026-08-08。<https://www.reuters.com/business/>

- retail-consumer/apple-says-mac-users-china-can-connect-alibabas-qwen-ai-service-2026-08-08/
2. Financial Times | 《Moonshot shake-up seeks to win Beijing nod for stock market debut》 | 2026-08-08。 <https://www.ft.com/content/9c0d4f0d-d2c6-4189-b4bb-200d17a4720f>
 3. The Guardian | 《Google DeepMind enters a new era as co-founder Demis Hassabis shifts AI role》 | 2026-08-08。 <https://www.theguardian.com/technology/2026/aug/08/google-demis-hassabis-deepmind-shifts-role>
 4. TechRadar | 《Experts warn malicious AI skills are hitting more victims than ever》 | 2026-08-08。 <https://www.techradar.com/pro/security/experts-warn-malicious-ai-skills-are-hitting-more-victims-than-ever-with-one-family-amassing-1-7-million-downloads>
 5. Zenity Labs | 《Attackers Target Agents via The Skill Supply Chain》 | 2026-08-06。 <https://labs.zenity.io/post/attackers-target-agents-via-the-skill-supply-chain>
 6. arXiv | 《Policy-Graded Evaluation of Coding Agents in Hardened Enterprise Environments》 | 2026-08。 <https://arxiv.org/html/2608.02670v1>
 7. arXiv | 《Prompt-Induced Waste in Coding Agents》 | 2026-08。 <https://arxiv.org/html/2608.01347v2>
 8. arXiv | 《Benchmarking Coding Agents for Proactive Bug Fixing》 | 2026-08。 <https://arxiv.org/html/2608.04682v1>

9. arXiv | 《IssueTrojanBench》 | 2026-07-22。 <https://arxiv.org/abs/2607.20759>
10. arXiv | 《AgentSLABench》 | 2026-08。 <https://arxiv.org/html/2608.00805v1>

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>