

AI 技术每日分析：多模态开源走向消费级 Agent

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 9 月 21 日

摘要

今天 AI 技术方向的新动态，集中在“多模态模型开源、消费级 Agent 规模化、企业级智能体平台和 Coding Agent 安全”四条主线上。Qwen 团队正式开源 Qwen-Image-2.1，以 7B 视觉生成参数实现文生图、图像编辑、原生 RGBA 透明图和最多 10 张参考图协同编辑，同时从 Apache 2.0 转向研究许可；Meta 个人 Agent Muse 在美国 App Store 登顶并在首周获得超过 70 万级下载，消费级 Agent 第一次出现接近 ChatGPT 早期移动端扩散速度的迹象，但围绕个人数据、邮件和金融账户连接的隐私争议同步升温；百度智能云在深圳升级“百度搭子”企业版多人协作、移动端和智能体开发平台，披露用户规模环比增长 9 倍；Air Security 公开 Plugin4Shell，指出 Claude Code、Codex、GitHub Copilot 和 Gemini CLI 等 Coding Agent 的插件更新链曾共享同类 SHA 固定绕过风险。AI 正在从“模型能力”走向更复杂的产品竞争：开放权重、终端入口、企业协作、插件生态和安全边界必须同时成立。

Contents

一、Qwen-Image-2.1 开源：7B 视觉生成模型把“生成、编辑、透 明图”合在一起	3
二、Meta Muse 登顶美国 App Store：个人 Agent 进入大众消 费市场，同时把隐私问题推到前台	4
三、百度搭子升级企业版与开发平台：通用智能体开始从个人工具 转向团队协作	4
四、Plugin4Shell 暴露 Coding Agent 供应链风险：插件生态成 为新的执行边界	5
五、Coherent 展示 3.2T 与 6.4T 光互连：AI 扩容的瓶颈开始从 GPU 转向“连接与功耗”	6
趋势观察	6
参考资料	7

一、Qwen-Image-2.1 开源：7B 视觉生成模型把“生成、编辑、透明图”合在一起

9 月 20 日，Qwen 团队正式发布 Qwen-Image-2.1 并在 Hugging Face、ModelScope 公开权重。官方模型卡显示，其视觉生成核心约 7B 参数、32 层 Single-Stream DiT，在一个模型中同时支持文生图、图像编辑、透明 RGBA 图像生成、主体提取和多参考图编辑。

与很多图像模型最值得区分的一点，是 Qwen-Image-2.1 可以一次接入最多 10 张参考图片，并支持通过圈选、涂抹或 Mask 进行局部编辑。对于电商素材、产品组合图、人物一致性和设计资产生产，这比“单次生成一张漂亮图片”更接近真实生产 workflow。项目还获得 Diffusers、ComfyUI、vLLM-Omni、SGLang 等工具的 Day-0 支持，说明开源生态成熟度正在成为模型发布的重要组成部分。

不过，新版本的许可也发生变化。Qwen-Image-2.1 使用 Qwen Research License，而此前部分 Qwen 图像模型采用 Apache 2.0。研究许可允许下载和研究使用，但商业化需要进一步确认授权。对企业开发者而言，“开放权重”不等于“可直接商用”，模型能力和许可证条款需要同时评估。

从技术趋势看，图像模型正在朝两个方向演进：一是模型本身更紧凑，降低自部署门槛；二是把生成、编辑、抠图、透明背景和多素材合成统一到一个模型中。未来视觉 AI 的竞争会越来越像设计软件，而不只是生成器。

二、Meta Muse 登顶美国 App Store：个人 Agent 进入大众消费市场，同时把隐私问题推到前台

9 月 20 日，多家媒体援引 Sensor Tower 数据称，Meta 个人 AI Agent Muse 已在美国苹果 App Store 免费榜升至第一。Muse 于 9 月 8 日上线，十天左右累计美国下载量达到 70 万级，并开始逼近 ChatGPT 当年移动端首发时期的扩散速度。

Muse 并不只是聊天机器人。它可以通过独立 Secure VM 浏览网页、处理邮件、预订服务、购物和执行长周期任务，并通过 WhatsApp、独立 App 及网页入口使用。Meta 还设计了 Sentinel 安全 Agent，对敏感外部动作进行权限判断和必要的人类确认。

真正值得关注的并不是榜单排名，而是消费级 Agent 终于进入“需要访问真实个人数据”的阶段。WIRED 9 月 20 日的体验文章重点质疑 Muse 对邮箱、金融账户和个人记忆数据的依赖，以及用户是否充分理解这些数据如何被使用。Meta 则强调其采用隔离虚拟机、权限控制和训练数据退出选项。

这会成为个人 Agent 普及的核心矛盾：Agent 越有用，就越需要邮件、日历、支付、联系人和浏览器权限；权限越多，安全与隐私风险也越大。未来个人 Agent 的竞争很可能不是“谁回答得更好”，而是谁能用更少数据完成更多任务，并提供更透明的授权与撤销机制。

三、百度搭子升级企业版与开发平台：通用智能体开始从个人工具转向团队协作

9 月 20 日，百度智能云在深圳举行超级智能体大会。百度搭子升级企业版多人协作能力，并发布企业版移动端和智能体开发平台，同时启动生态共创计划。

百度披露，百度搭子用户规模环比增长 9 倍，交付物需求环比增长 4.3 倍，专家套件使用量环比增长 7.3 倍。上述指标属于企业自披露，但能够反映一个明确变化：用户开始把智能体用于“完成交付物”，而不是只做搜索和问答。

企业版升级的重点是多人协作和跨端同步。百度还推出硬件标准化 API，使智能体能力、记忆和用户状态可以在不同终端之间同步，目前已接入部分家庭硬件和具身智能设备。这条路线意味着智能体平台正在从“一个网页应用”扩展成企业协作与终端连接层。

对企业市场而言，真正的竞争会落到权限、团队知识、任务状态、移动端、硬件接口和开发平台上。谁能让智能体进入组织流程、形成可复用的角色和工作模板，谁才有机会成为企业 AI 工作台。

四、Plugin4Shell 暴露 Coding Agent 供应链风险：插件生态成为新的执行边界

9 月 20 日，安全研究机构 Air Security 公开漏洞细节后，多个安全媒体继续跟进 Plugin4Shell。问题涉及 Claude Code、OpenAI Codex、GitHub Copilot 和 Google Gemini CLI 等 Coding Agent 的插件更新机制：攻击者如果控制插件仓库，可以利用 Git 引用与 SHA 固定验证之间的缺口，让 Agent 执行与用户预期不同的代码。

Anthropic 和 OpenAI 已经修复相关问题；公开报道显示，GitHub Copilot 和 Gemini CLI 在披露时的处理状态并不一致，部分产品需要升级、迁移或采取额外防护措施。厂商状态仍应以各自最新安全公告为准。

这类漏洞和普通 IDE 插件风险不同。Coding Agent 通常拥有项目文件、Shell、Git、云凭据甚至部署工具权限，插件一旦进入执行链，影响范围可能远超过代码编辑器本身。Agent 生态越开放，供应链验证就越重要。

未来企业 Coding Agent 的最低安全要求应逐渐包括：插件来源签名、实际 Commit 校验、最小权限运行、Sandbox 隔离、外部命令审计和自动更新回滚。Agent 市场正在经历与浏览器扩展、开源包管理类似的安全成熟过程，只是权限更高、自动执行能力更强。

五、Coherent 展示 3.2T 与 6.4T 光互连：AI 扩容的瓶颈开始从 GPU 转向“连接与功耗”

9 月 20 日，Coherent 公布其在 ECOC 2026 展示的新一代 AI 数据中心光通信技术，包括 3.2T 可插拔收发器、6.4T Near-Packaged Optics 光引擎，以及面向 CPO、NPO 和芯片间连接的 PhotonLink 平台。

AI 基础设施的关注点过去主要集中在 GPU 数量，但训练和推理集群扩大之后，节点之间的数据移动、电力和散热开始成为更重要的瓶颈。Coherent 强调，下一代 AI 网络不仅需要更高带宽，还要同时解决功耗、封装密度和热管理。

这说明 AI 基础设施正在进一步专业化。GPU、交换芯片、光模块、硅光、光纤和热管理之间的协同，决定一个大型 AI 集群最终能否稳定扩展。未来“推理成本”不仅取决于模型和 GPU，也取决于网络和数据移动效率。

趋势观察

今天的 AI 技术主线不是某一个模型刷新榜单，而是完整技术栈在快速成形：Qwen-Image-2.1 代表多模态开源模型继续轻量化和统一化；Muse 代表消费级 Agent 进入真实账户和个人数据；百度搭子把智能体推进团队协作和多终端；Plugin4Shell 提醒开发者插件供应链已成为新的攻击面；Coherent 则说明 AI 规模化正在把创新压力传导到光互连和基础设施。AI 正在从“模型时代”进入“系统时代”。

参考资料

- Qwen / Hugging Face | Qwen-Image-2.1 模型卡 | 2026-09-20 | 核验 7B 视觉生成参数、RGBA、多参考图和统一生成编辑。<https://huggingface.co/Qwen/Qwen-Image-2.1>
- Qwen / GitHub | Qwen-Image-2.1 | 2026-09-20 | 核验 Day-0 Diffusers、ComfyUI、vLLM-Omni 和 SGLang 支持。<https://github.com/QwenLM/Qwen-Image-2.1>
- Qwen | Qwen Research License Agreement | 2026-09-20 | 核验许可证变化。<https://huggingface.co/Qwen/Qwen-Image-2.1/blob/main/LICENSE>
- Meta | Introducing Muse | 2026-09-08 | 核验 Secure VM、Sentinel 和个人 Agent 产品机制。<https://about.fb.com/news/2026/09/introducing-muse-personal-ai-agent/>
- WIRED | Meta's Muse Is Better at Surveilling Than Helping Me | 2026-09-20 | 补充个人数据与隐私争议。<https://www.wired.com/story/metase-muse-is-better-at-surveilling-than-helping-me>
- 百度智能云大会相关报道 | 百度搭子用户规模与企业版升级 | 2026-09-20 | 核验多人协作、移动端和开发平台。<https://www.guandian.cn/article/20260920/604506.html>
- 新浪财经 / 时代周报 | 百度搭子用户规模环比增长 9 倍 | 2026-09-20 | 交叉核验企业披露数据和硬件 API 生态。<https://finance.sina.com.cn/roll/2026-09-20/doc-inisnnkt1438202.shtml>
- Beckmann / Air Security 资料汇总 | Plugin4Shell | 2026-09-20 | 核验 Coding Agent 插件供应链风险。<https://beckmann.ai/en/security/2026-09/plugin4shell-ai-coding-agents>

- BleepingComputer | Codex sandbox escape 相关报道 | 2026-09-20 | 背景资料,观察 Coding Agent 执行边界风险。<https://www.bleepingcomputer.com/news/security/researchers-escape-openai-codex-sandbox-to-run-commands-on-host/>
- Coherent | AI Infrastructure at ECOC 2026 | 2026-09-20 | 核验 3.2T、6.4T NPO 与 AI 光互连方案。<https://www.globenewswire.com/news-release/2026/09/20/3365104/11543/en/coherent-showcases-optical-innovations-to-scale-ai-infrastructure-at-ecoc-2026.html>

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>