全球Agent日报

Global Agent Daily

期号	日期	时区	资讯截止
第003期	2026-11-25 周三	北京时间	08:03

今日核心判断

编辑观察：个人智能体出现英国地区上线和国内邀请制公测；企业侧则把重点放在受治理的 MCP 接入、过程确认和伙伴平台，而不是只增加演示功能。选型应分清正式可用、公开测试、即将推出和地区限制。厂商披露的用户规模与效率数据未经独立核验，不能写成普遍效果。

本期关注

01 Anthropic 让 MCP 服务器可下发技能，任务与确认已正式可用

02 谷歌 Workspace 智能体接入通道正式可用，部分规则将分步生效

03 豆包“小豆”开启邀请制公测

04 华为云发布智能体伙伴开放计划

05 Meta 个人智能体 Muse 在英国上线

06 西门子 Eigen 工程智能体扩展至流程工业

01 开发协议

DEVELOPER PROTOCOL

Anthropic 让 MCP 服务器可下发技能，任务与确认已正式可用

Anthropic 11月24日宣布，Skills over MCP 在 Claude 与 Claude Code 进入公开测试：MCP 服务器可随工具一并下发技能，供 Claude 在需要时加载，处理更长的多步骤工作。该能力对 Pro、Max、Ultra 默认开启，Team 需管理员启用，Enterprise 即将推出。同日，Tasks（后台执行耗时操作）和 Elicitation（中途以表单或链接征求确认，例如付费或删除前）对上述个人套餐正式可用，并正在向 Team 和 Enterprise 组织推送。File Uploads 可将 PDF、表格和图片交给服务器且不经过上下文窗口，官方标明即将推出。文中 Shopify、HubSpot、Atlassian 为例举，Carta 相关能力尚未上线；上述均为厂商说明，未经本报独立核验。

企业意义 要把公开测试、正式可用、即将推出、套餐和管理员开关分开评估；过程确认和后台任务改变的是协作方式，不代表可取消人工复核。

来源 | S1 Anthropic · 11-24

02 企业协作

ENTERPRISE COLLABORATION

谷歌 Workspace 智能体接入通道正式可用，部分规则将分步生效

Google Workspace 博客11月24日宣布，Workspace MCP 服务器与 CLI 正式可用，作为谷歌管理的智能体接入入口。MCP 服务器面向云端和网页智能体，可在安全边界内调用 Gmail、Drive、Docs、Sheets、Slides、Calendar、Chat 和 Tasks（Keep 即将加入）；CLI 面向本地和桌面智能体，提供范围登录与 IT 防护。官方同时说明：Workspace AI Tools Addendum 要求经 MCP 或 CLI 而非传统 REST API 接入，技术强制自2027年2月1日起实施；外部智能体须使用专用 OAuth 客户端和最小权限，用量配额将于2027年4月1日起计费；高影响操作需按 IT 策略取得用户确认。限时审批、用户侧查看与撤销，以及阻止外部智能体访问特定邮件和文件，官方标明即将推出。实施细节以官方文档和客户协议为准。

企业意义 接入通道“现已正式可用”并不等于全部防护已经生效；报价和方案需单独核对强制执行日期、计费开始时间，以及地区和套餐适用范围。

来源 | S2 Google Workspace Blog · 11-24

03 中国平台动态

CHINA PLATFORM

豆包“小豆”开启邀请制公测

11月24日，豆包旗下个人AI助理“小豆”开启邀请制公测。官方产品页称，其可结合记忆与已连接应用主动提醒、跟进任务，授权后可使用抖音、飞书、日历、健康和地理位置等信息。新华财经、首都之窗转引北京日报报道称，这是探索性产品，相关能力将逐步放开并在豆包主端提供；官方演示包括确认后补货下单、按节点发送资料、代打电话询问餐位，以及把长期目标拆成每日提醒。报道写明：代打电话目前仅覆盖餐厅、酒店、门店等生活服务，不支持境外和私人电话；初期须凭邀请码体验，新用户有一定免费额度。演示情景不能等同已对全部用户开放的稳定能力。

企业意义 可关注个人智能体从问答转向持续跟进的产品形态，但公测范围、邀请门槛、电话场景限制和免费额度都需以产品页与账户说明为准，不宜写成已全面商用。

来源 | S3 豆包产品页 · 无落款日期 | S4 新华财经 · 11-24 | S5 首都之窗（转引北京日报） · 11-24

04 中国平台生态

CHINA ECOSYSTEM

华为云发布智能体伙伴开放计划

据科技日报、IT之家11月24日报道，华为云当天在杭州举行智能体伙伴开放计划发布会暨智果生态大会，联合中软国际、软通动力、德勤等首批30多家伙伴，开放智果 AgentArts 平台，以及集办 OfficeAce、码道 CodeArts 等产品与开发工具。报道转述，AgentArts 开放开发、运行与治理能力，包括长程任务、独立安全沙箱、全链路可观测和权限管控；合作模式分为在线配置快速集成，以及面向有研发能力伙伴的深度定制，并称可向特定伙伴和客户开放源代码。文中企业与开发者规模、智能体资产数量及集办、码道注册用户数均为转述的厂商主张，未经独立核验。本报未找到华为云新闻稿原页，以上按媒体转引标识。

企业意义 生态开放计划不等于即可交付的行业方案；评估时应核对开放模块、商业分工、源代码开放条件和账号所属区域，不把发布会规模数据直接写入对客材料。

来源 | S6 科技日报 · 11-24 | S7 IT之家（转引） · 11-24

05 个人智能体

PERSONAL AGENT

Meta 个人智能体 Muse 在英国上线

Meta 于11月23日宣布（新闻稿页面同时标注11月24日），个人智能体 Muse 向英国18岁及以上用户开放，可在 iOS、Android、muse.ai 和 WhatsApp 使用，官方称未来数月将登陆 Meta AI 眼镜；基础使用免费，另有可选订阅。发送邮件或购物等重要操作前需用户批准，购物须每次确认；无法查看用户密码和支付方式，登录凭据存放在安全凭据库。每个 Muse 拥有独立的云端虚拟电脑，对话及其中数据不进入 Meta 广告系统；用于改进模型的选项默认开启，可在设置中关闭，官方称不会用私人邮件或 Instagram 私信做训练。支付可走 Stripe 的 Onelink 或部分商店的 Shop Pay。此次是英国地区上线，不是全球或中国可用；PayPal 等连接器官方标明即将推出。昨日第002期截稿前未收录，现按原日期补入48小时窗口。

企业意义 境外个人智能体的地区、年龄、授权和支付安排不能直接套用到国内项目；若做对标，应单独评估数据出境、应用授权和人工确认机制。

来源 | S8 Meta Newsroom · 11-23 | S9 Meta Newsroom · 11-23

06 工业智能体

INDUSTRIAL AGENT

西门子 Eigen 工程智能体扩展至流程工业

西门子11月24日发布新闻稿，宣布 Eigen Engineering Agent 扩展到化工、制药、水处理和能源等流程工业，可在 SIMATIC PCS 7 中规划、执行并校验工程任务。官方强调该智能体仅用于工程配置，不介入运行中的生产装置。新闻稿称，2026年7月至10月付费许可数量增长超过两倍，已在30多个国家使用，并已于7月在中国、本月在印度推出；对选定工程任务给出最高约60%的节省潜力，实际效果取决于项目复杂度、范围、既有经验和标准化程度。代码校验在介绍期内免费，数月后计划转为付费；安全工程相关能力仍由工程师负责。文中 ANDRITZ Metals 称部分任务速度提升一倍，属于客户转述，并非普遍基准。

企业意义 工业场景首先要分清“工程设计辅助”与“生产运行控制”；厂商许可增长和效率数字需在具体系统和项目中复核，不能写成已验证的普遍收益。

来源 | S10 Siemens · 11-24

落地观察

以下为编辑观察，与新闻事实分开，不构成收益或合规保证。

01 接入协议正在成为企业落地的前门：先核对哪些能力已正式可用，哪些仍是公开测试或即将推出，并把2027年强制执行和计费日期单独列入方案风险，不要把“现已发布”写成“已按最终规则上线”。

02 个人智能体仍高度依赖地区、邀请码和人工确认。对英国 Muse 与国内“小豆”应分别看待可用范围，不把演示中的下单、代打电话或跨应用办理写成可规模交付的能力。

03 面对伙伴开放和工业扩展，宜先问清开放模块、工程与运行边界以及数据驻留，再评估是否适合本地试点；发布会中的用户量和效率数据应作为厂商主张保留，不写入对客承诺。

可信中创（北京）数字科技有限公司整理。本报依据公开资料简要改写，不构成产品推荐、投资建议或法律意见，不表示本机构与所引主体存在合作。