全球Agent日报

Global Agent Daily

期号	日期	时区	资讯截止
第001期	2026-11-23 周一	北京时间	09:29

今日核心判断

过去72小时，全球Agent竞争的重心正从“能不能把任务做完”，转向“能不能在规则里行动、留下记录，并在不该看的数据前停下来”。电脑操控和常驻式智能体继续进入更多产品，治理与隐私防护也同步加码。以上为编辑观点，不是对市场结果的预测。

本期关注

01 谷歌上线执行前语义治理策略（预览）
02 腾讯 WorkBuddy 电脑操控进入公测
03 AWS Quick 更新流程与多智能体协同
04 Signal 限制系统级智能体读取屏幕
05 Amazon Connect Resolutions 正式商用
06 ChatGPT 商务标准版开始推送 Dots

01 安全治理

SAFETY & GOVERNANCE

谷歌为智能体增加执行前语义治理策略

11月20日，Google Developers Blog 发文称，Gemini 平台预览上线 Semantic governance policies（语义治理策略）。智能体提出工具调用后、实际执行前，由独立策略执行点（目前为 Agent Gateway）检查企业用自然语言写的规则，以及该调用是否偏离用户原意（意图检查默认开启）。两项都通过才执行，否则拦截并写入 Cloud Logging。官方说明，判定由大模型评审作出，结果可能不稳定，建议先用演练模式再强制拦截；流式响应暂不评估；该能力不能替代法务和合规审查。同日介绍的 Agent Anomaly Detection 仍为私有预览，日志送入其项目后可监测 Google Cloud 以外的智能体；文中案例为官方测试示例。

> **企业意义** 仅有权限还不够，还要检查“这一次调用是否合规、是否被带偏”，并留下记录。评估时应分清预览与正式可用，先核对其误拦和漏拦。

来源 | S1 Google Developers Blog · 11-20 | S2 Google Developers Blog · 11-20

02 平台产品

PLATFORM & PRODUCT

腾讯 WorkBuddy 电脑操控进入公测

11月20日，腾讯 WorkBuddy 官方账号宣布上线电脑操控（Computer Use）能力。据每日经济新闻、IT之家报道，该能力可识别当前界面并执行点击、输入、滚动等操作，不必等待目标软件开放接口。目前为公测，支持 macOS 与 Windows，需更新至 5.11.0 及以上，并开启功能、完成授权；识别效果会因软件而异。报道转述官方建议：涉及登录、授权、支付、提交、删除等敏感操作时，应保持在场监控。腾讯云官方文档写明，企业版可由管理员配置策略，默认对所有成员关闭。

> **企业意义** 对要在现有桌面软件里跑流程、又缺少接口的团队，可小范围试点。公测不等于生产就绪，支付和删除等动作应默认人工确认。

来源 | S3 每日经济新闻 · 11-20 | S4 IT之家 · 11-20 | S5 腾讯云文档 · 11-10

03 工具生态

TOOLS & ECOSYSTEM

AWS Quick 更新流程编排与多智能体协同

11月20日，AWS 官方博客宣布 AWS Quick 更新。用户可在对话中描述业务流程，由 Quick 生成 flow，把智能体、技能、工具和数据编排在一起，并加入确定性步骤。一次请求也可并行调用多个专职智能体，再合并为一条回复。网页端可展示待办与每日简报，并在关闭浏览器后继续运行任务。管理员侧新增提示词护栏（预览）和按组分配权限，并支持简体、繁体中文等语种。官方称写操作会先征求许可，功能在已开通区域内可用。文中示例为说明性例子，所引客户成效为厂商转述，本文未作独立验证。

> **企业意义** 适合关注“把个人经验变成团队可重复流程”的企业。评估时应核对所在区域、护栏仍为预览，以及写操作是否由本组织配置。

来源 | S6 AWS Machine Learning Blog · 11-20

04 安全治理

SAFETY & GOVERNANCE

Signal 限制系统级智能体读取聊天屏幕

11月20日，Signal 总裁 Meredith Whittaker 在官方博客写道，将限制操作系统内置的 AI 智能体捕获和存储 Signal 数据：在 iOS 27 上阻止应用内截屏；在可检测到 AI 助手试图读取屏幕的 Android 版本上自动开启“屏幕安全”。用户可关闭该保护，但官方称关闭后可能使对话暴露，并使其隐私保证失效。官方承认方案并不完整，例如无法覆盖经文件系统等途径的访问，且目前无法在 macOS 上可靠拦截截屏，因而呼吁苹果、谷歌和微软提供明确的退出接口。支持文档载明：Android 需 8.35.1 或更高，iPhone 需 8.37 且为 iOS 27 或更高；iPhone 默认开启 Block Siri AI。

> **企业意义** 系统级助手进入日常应用后，应用层隐私边界会被重新定义。做智能体方案时，不能把读取屏幕或调用辅助功能当成默认权限。

来源 | S7 Signal Blog · 11-20 | S8 Signal Support · 查阅 2026-11-23

05 企业应用

ENTERPRISE ADOPTION

Amazon Connect Resolutions 正式商用

11月19日（略超出72小时窗口，作为必要背景保留原日期），AWS 宣布 Amazon Connect Resolutions 正式可用。该方案面向退款、交易争议、欺诈调查、保险理赔等高并发运营工作，把智能体推理与确定性工作流结合起来。管理者可用自然语言或标准作业程序生成 Work plan，并补齐例外、规则和审批阈值；每份请求打开 Case，由预制、配置或自有智能体收集信息并跨应用执行，人工处理审批和例外。官方称结果会核验并记录全部动作。缩短处理时间、降低服务成本等表述属厂商主张，本文未引用经独立核验的量化结果。

> **企业意义** 可观察“自然语言生成作业计划 + 人工审批 + 全程留痕”是否更接近可审计的生产流程。落地仍须按本企业政策单独评估。

来源 | S9 AWS What's New · 11-19

06 平台产品

PLATFORM & PRODUCT

ChatGPT Business Standard 开始推送 Dots

OpenAI 于11月19日在 ChatGPT Business 更新说明中写道，正向美国符合条件的 Business Standard 成员推送 dots；获得权限后，可在工作区创建一个个人 dot，用于持续推进项目（如准备周报），并适用星期限制。另据帮助中心，dots 也在向部分 Plus 用户逐步开放，但欧洲经济区、英国和瑞士当前不在其列；企业版工作区在11月18日后默认开放，除非管理员退出。文档提示，客服无法为单个账户开通，套餐与数据驻地等会影响资格。Dots 最初于2026年9月29日发布，本期只记录范围扩大，不把它写成新品首发。

> **企业意义** 常驻式个人智能体正在进入更常见的商务套餐，但范围和用量都有边界。试点前应核对本地区和套餐是否已开通，并设置审批与停用策略。

来源 | S10 OpenAI Help Center · 11-19 | S11 OpenAI Help Center · 查阅 2026-11-23

落地观察

以下为观察，与上文事实分开，不构成收益承诺、合规保证或法律意见。

01 预览、公测和正式可用不是同一阶段。演示或试点前，先核对开通范围、管理员开关和默认关闭策略。

02 把“能调用工具”和“这一次调用该不该发生”分开设计：敏感动作默认人工确认，并保留可审计记录。

03 系统级或桌面级操控可能与应用隐私设置冲突。权限申请应最小必要，并允许被拒绝后改为只读方案。

本报依据公开资料整理，不构成产品推荐、投资建议或法律意见，也不表示本机构与所引主体存在合作。