全球Agent日报

Global Agent Daily

期号 第004期

日期 2026-11-26 周四

时区 北京时间

资讯截止 08:07

今日核心判断

编辑观察：网站检索接口、桌面应用安装和语音转写，正在把智能体从对话接到更具体的工作入口；与此同时，微软官方披露了 Python 依赖包被未授权上传的安全事件，说明版本钉死和凭证治理已成为落地前提。选型仍须分清测试、公开预览、正式可用和地区范围。厂商给出的准确率与时延数据未经独立核验，不能写成普遍效果。国内千问Go代打电话目前主要见媒体报道，具体限制应以官方产品说明为准。

本期关注

01 Cloudflare 推出 Search for Agents，网站检索接口进入测试

02 微软公布 Agent Framework 软件包被未授权上传，仓库暂时关闭

03 Claude 可将 Artifact 安装为桌面应用，目前为测试

04 千问Go全面开放免费代打电话服务

05 Amazon Transcribe Turbo 进入公开预览，新增面向语音智能体的能力

06 DeepMind 为 Antigravity 发布质谱解析技能

01 基础设施 INFRASTRUCTURE

Cloudflare 推出 Search for Agents，网站检索接口进入测试

Cloudflare 11月25日宣布推出 Search for Agents。站点管理员可在控制台该区域 Overview 页的 Quick Actions 中打开开关，或通过 API 启用；启用后平台会自动创建 AI Search 实例、开始抓取并建立索引，并在站点域名下开放检索接口 /.well-known/search。官方会在页面中加入供智能体发现的元数据；若同时开启 Markdown for Agents，Markdown 响应也会带上同样说明。接口支持 GET 与 HTTP QUERY，返回检索到的 Markdown 内容，而不是再生成一份答案。开发者文档写明，该能力在所有套餐（含 Free）以测试（beta）提供，用量受 AI Search 定价与套餐限额约束，免费套餐每日最多抓取500页；AI Search 计费自2026年12月1日起。检索请求仍受站点的机器人管理、AI Crawl Control 和 WAF 等设置约束；官方提醒只应索引准备公开可检索的内容。厂商关于智能体发现和使用效果的说明未经独立核验。

企业意义 开通前要分清“已可启用的测试功能”和“计费已开始”；把12月1日计费、免费套餐抓取限额和公开可检索范围写入方案，不要把开关打开写成已向全部智能体稳定服务。

来源 | S1 Cloudflare Blog · 11-25 | S2 Cloudflare Changelog · 11-25 | S3 Cloudflare Docs · 无单独落款日期 | S4 Cloudflare Docs · 无单独落款日期

02 安全治理 SECURITY

微软公布 Agent Framework 软件包被未授权上传，仓库暂时关闭

微软 Agent Framework 团队11月25日发文称，因预防需要，该项目代码仓库暂时不可用，恢复时间尚未确定，并强调项目并未停更。官方说明：2026年11月17日，Python 元包 agent-framework 的 1.26.1 与 1.26.2 两个版本在未经授权的情况下被上传至 PyPI，其中包含窃取凭证的代码；这两个版本已从 PyPI 下架，技术细节见安全公告 PYSEC-2026-4388。官方称恶意代码存在于已发布的软件包中，而不在代码仓库本身；1.26.0 及更早版本、其他 Microsoft Agent Framework 的 Python 分包、.NET 包以及 Semantic Kernel 均不受影响。若已安装上述两个版本，官方要求将相关机器、容器或持续集成环境视为已受影响：轮换该环境可能触及的全部凭证，从干净镜像重建，并核查11月17日以来的云与持续集成日志；仅在原环境降级不够。若未安装，官方建议将版本固定为 agent-framework==1.26.0，并等待后续指引。事件原日期为11月17日，本期按11月25日官方说明收录。

企业意义 智能体项目要把依赖版本钉死，并检查锁文件、镜像和内部源；若环境曾安装受影响版本，应按官方步骤处理，不能只当作一次普通更新。

来源 | S5 Microsoft Agent Framework Blog · 11-25

03 开发工具 DEVELOPER TOOLS

Claude 可将 Artifact 安装为桌面应用，目前为测试

Anthropic 官方文章与发布说明日期为11月24日：“Install as app”正在 Claude for Mac 与 Windows 以测试（beta）推送，需桌面应用 0.28899.0 或更高版本，且须在线并登录后才能打开已安装应用。安装后的 Artifact 拥有独立图标和窗口，可使用 Claude 与已连接应用，并在原 Artifact 被编辑后自动更新；向 Claude 发出的请求计入所属套餐用量。权限分三档：默认仅相当于浏览器内能力；应用权限可申请通知、全局快捷键、置顶窗口等；完全访问计算机可在获准后运行程序并读写或删除文件，且不必每次再问。官方写明不会在安装前审查应用，完全访问通常仅适用于自己或组织内制作的应用，每次更新后需再次授权。该功能在各套餐推送测试：Team 默认开启但完全访问默认关闭，Enterprise 需所有者开启；已做 HIPAA 就绪配置的组织以及混合部署不可使用。帮助中心还列出：不支持 Linux、网页和移动端；由模板生成的 Docs、Slides、Sheets，以及旧版 Artifact 和 Claude Cowork 的实时 Artifact 不可安装。昨日第003期截稿前未收录，现按原日期补入48小时窗口。

企业意义 要把测试状态、管理员开关和权限分级写进试用说明；完全访问意味着可改动本地文件，不能把它写成已通过厂商审查的安全桌面分发方案。

来源 | S6 Anthropic · 11-24 | S7 Claude Help Center · 11-24 | S8 Claude Release notes · 11-24

04 中国平台动态 CHINA PLATFORM

千问Go全面开放免费代打电话服务

11月25日，经济参考网、每日经济新闻、IT之家等报道，千问Go全面开放代打电话服务，并称面向用户免费提供。报道写明：用户告知拨打对象和通话需求并授权后，千问可代为联系餐厅预订包间、向酒店询问遗失物品、联系快递员查询配送进度等，并反馈结果；同时支持定时代打电话。报道均提到：须经用户授权，通话中会主动表明AI助手身份，并设有外呼安全防护机制，对存在风险的请求进行筛查和拦截。本报已打开上述媒体报道核验，但未找到阿里或千问官方新闻稿原页，以上按媒体转引标识。报道未说明地区、号码范围、境外呼叫或企业场景限制，不能自行补写为已无限制或已对企业商用。

企业意义 可关注国内个人助手从对话走向代办电话的产品变化，但开放免费并不等于能力已稳定、可规模用于企业外呼；具体范围、次数和安全规则应以官方产品说明与账户页面为准。

来源 | S9 经济参考网 · 11-25 | S10 每日经济新闻 · 11-25 | S11 IT之家（转引） · 11-25

05 语音智能体 VOICE AGENT

Amazon Transcribe Turbo 进入公开预览，新增面向语音智能体的能力

AWS 11月25日宣布，下一代语音转写模型 Amazon Transcribe Turbo 在美国东部（俄亥俄）以公开预览提供批量与流式转写。官方称流式目前支持英语、葡萄牙语、法语、意大利语、德语和西班牙语，相对现有生产模型，英语词错误率约下降14%，其他上述语种约下降11%，格式准确率提高超过20个百分点；批量方面，英语 Turbo 已在多数 AWS 区域可用，葡萄牙语、法语、意大利语、德语、西班牙语、中文、日语、韩语和阿拉伯语进入预览，并称词错误率约低16%。官方同时介绍两项面向语音智能体的流式新能力，英语在上线时提供，其他语种计划于2026年12月底前推出：语义话轮检测根据内容和韵律判断对方是否说完，官方给出约615毫秒响应、5%打断率，并可调节；运行时语音识别提示可在每一轮前下发菜单选项、预期名称或实体类型，官方称在英语客服数据上把菜单路由准确率从87%提高到97%。上述准确率、时延和打断率为厂商测试数据，未经独立核验。两项能力官方标明不另收费；基础模型无需更改 API、代码或 SDK。地区与预览、正式可用范围以官方说明为准。

企业意义 要把“俄亥俄公开预览”“英语批量在多数区域正式可用”和“其他语种预览或后续上线”分开评估，不能把广告测试中的准确率写成已验证的普遍效果。

来源 | S12 AWS What's New · 11-25

06 科研智能体 SCIENTIFIC AGENT

DeepMind 为 Antigravity 发布质谱解析技能

Google DeepMind 11月25日发布 Mass Spec Skills for Google Antigravity，把质谱分析中的常用开源工具和公共化学数据库查询做成领域技能，由智能体按研究人员的自然语言请求调用，并整理证据供化学家复核。官方在已收录于公共谱图库的100个化合物样本上评估：在无网络、无可调用技能时，三种模型的准确识别率均低于4%；加上技能后，包括轻量模型 Gemini 3.8 Flash 在内的三种模型都在约97%的尝试中识别并核验了准确分子。该结果为官方研究口径，样本来自 MoNA 中的 Enamine REAL MS/MS 收集，且针对已有库内谱图，不是独立第三方评测，也不能外推到全部真实样品。官方同时写明：镜像分子和部分近缘异构体无法仅凭质谱区分；数据库中不存在的全新分子也不能由系统自行确认，只能提供分子式、峰归属等起点。技能现可通过 Antigravity 应用安装 Mass Spec 插件使用；企业用户可用 Google Cloud 账号登录。官方还称将向1万名科学家提供为期6个月的最高用量档免费使用，须视资格、名额和遴选情况，申请现已开放。

企业意义 这是面向科研场景的领域技能，不是通用办公智能体；引用准确率时必须保留样本范围，以及无法区分镜像分子、不能确认全新分子等限定。

来源 | S13 Google DeepMind · 11-25

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 向智能体开放网站检索或本地桌面权限前，先核对是测试还是正式可用，并把计费开始日、套餐限额和管理员开关单独写入方案，不要把“现已发布”写成已按最终规则稳定服务。

02 引入开源或第三方 Agent 框架时，应固定版本并检查锁文件、镜像和内部源；若环境变装过官方点名的受影响版本，须按说明轮换凭证并从干净镜像重建，不能只做降级。

03 个人助手代打电话仍依赖授权、身份明示和风险拦截，不能把媒体列举的生活场景写成可直接用于企业外呼的能力；语音转写的预览区域、语种范围和厂商测试数据也要分开核对。

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。