

Google 发布 Gemini 4 Argon, 整合复杂任务与跨应用执行

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 10 月 14 日

摘要

10 月 13 日, 国际 AI 技术领域有四项值得关注的进展。Google 推出 Gemini 4 Argon, 进一步整合复杂任务推理、编程和跨应用执行; 安全初创公司 Pluto Security 结束隐身阶段, 披露累计融资 4200 万美元, 着手监测员工自建的 AI 应用、技能及 MCP 连接器; Workday 与 Anthropic 达成新合作, 让 Claude 和 Sana 智能体共享任务上下文, 并沿用人力资源、财务系统已有的权限规则; 美国运通发布 Intent Intelligence 技术方案, 用用户签署的购买意图、金额上限、时效和支付凭据范围约束智能体交易。模型能独立完成的工作越多, 任务状态、权限、资金和审计记录就越需要有可验证的约束。

Contents

一、Google 发布 Gemini 4 Argon: 复杂任务入口进一步合并	2
二、Pluto Security 披露累计 4200 万美元融资: 影子 AI 与员工自建工具成为新安全对象	2
三、Workday 与 Anthropic 新签合同: 企业 Agent 推理层服从业务规则层	3
四、美国运通提出 Intent Intelligence: 让智能体付款有明确授权边界	4
趋势观察	4
参考资料	5

一、Google 发布 Gemini 4 Argon：复杂任务入口进一步合并

10 月 13 日，Google 正式推出 Gemini 4 Argon。据 Google 公告，付费 Google AI Pro 和 Ultra 用户可在 Gemini 应用中使用新模型。macOS 版 Gemini 进一步接入 Antigravity 编码界面，用户可从聊天转向代码任务；主对话窗口也新增任务入口，可调用超过 40 种应用连接。路透社报道，新模型还通过 API 提供给开发者和企业，最初每百万输入 Token 收费 2 美元、每百万输出 Token 收费 10 美元。这是阶段性介绍价格，不能当作长期成本承诺。[Google 公告](<https://blog.google/innovation-and-ai/products/gemini-app/gemini-4-argon-availability/>)；[Reuters 报道](<https://www.reuters.com/business/google-launches-flagship-ai-model-gemini-4-argon-developers-businesses-2026-10-13/>)。

这次更新更值得看的是使用路径：用户从提出问题，到交给模型执行，再到进入开发工具，步骤被接在同一个入口里。但企业任务能否顺利跑完，还要看第三方连接器、身份授权、异常恢复和成本上限。Google 公布的性能与生产率改善，仍属于厂商或试点口径，有待独立评测和企业实际流程复测。新模型也并未向所有免费用户全面开放，使用前须核对地区、订阅级别和接口权限。

二、Pluto Security 披露累计 4200 万美元融资：影子 AI 与员工自建工具成为新安全对象

10 月 13 日，安全初创公司 Pluto Security 结束隐身阶段，披露累计获得约 4200 万美元融资，包括 850 万美元种子轮和约 3400 万美元后续融资。据 TechCrunch 报道，其产品追踪企业内部使用的 AI 工具、Agent、技能、浏览器扩展和 MCP 服务器，并尝试在 Agent 越权操作

时实时干预。公司负责人称，企业客户已超过 30 家，年化经常性收入超过 200 万美元；这些经营数据目前仍是企业自述。[TechCrunch 报道](<https://techcrunch.com/2026/10/13/pluto-security-raises-42m-as-ai-gives-enterprise-security-teams-a-new-headache/>)。

安全团队过去盘点的主要是终端、服务器和 SaaS 账号，如今还得看员工自己搭建了什么。一张用生成式工具做的表单、一个 MCP 插件或数据分析 Agent，都可能读取客户信息、运行命令，或把内容发往外部地址。一味阻断又容易妨碍创新，因此这类产品尝试同时做好组件发现、权限识别、动作记录和危险调用拦截。其效果要看误报率、覆盖率、业务延迟和审计记录能否复现，融资额本身说明不了技术水平。

三、Workday 与 Anthropic 新签合同：企业 Agent 推理层服从业务规则层

10 月 13 日，Workday 与 Anthropic 在 Workday Rising 大会期间宣布新合作。双方计划通过模型上下文协议(MCP)连接 Claude 和 Workday 的 Sana 智能体：员工可在 Claude 中查询获授权的人事、财务信息，完成获准的操作；Sana 也可在复杂流程中调用 Claude 处理特定推理任务。Workday 强调，操作仍须遵守原有角色权限、业务规则和审计要求。Sana-in-Claude 插件目前只对早期客户开放，预计 2026 年早些时候全面上市；Agent-Ready Tools 已通过 Workday Extend AI 向客户提供。[Workday 官方公告](<https://newsroom.workday.com/2026-10-13-Workday-and-Anthropic-Announce-New-Partnership-to-Connect-Reasoning-to-the-Rules-That-Run-the-Business,-Wherever-People-Choose-to-Work>)。

此前 IT 服务商与模型公司的合作多着眼于系统集成，这次还涉及一个更具体的问题：外部模型能做哪些判断，权威业务系统又必须保留哪些决定权。比如薪酬调整、招聘编制或发票例外审批，模型可以解释情况、

提出匹配建议、处理材料；实际执行仍应由原系统核验权限，并留下审批记录。宣布合作不等于所有客户都已上线。企业后续评估 Agent 平台，可重点核查系统记录是否仍是唯一权威来源、审批能否撤销，以及跨平台调用是否传输了超出需要的敏感数据。

四、美国运通提出 Intent Intelligence：让智能体付款有明确授权边界

10 月 13 日，美国运通技术团队发表《Intent Intelligence: Building Trust in Agentic Commerce》，提出用 Create Intent API 记录用户确认的购买意图，包括最大金额、指定商户、到期时间、交易次数和商品条件。用户完成适当的身份验证及签署后，系统生成 Intent ID 和 Proof of Intent Token，并可据此提供受约束的支付凭据。[American Express 技术原文](<https://americanexpress.io/intent-intelligence-building-trust-in-agentic-commerce/>)。

智能体自动购物时，“用户说过可以买”和“用户批准了这笔交易”并不相同。换了商品、价格变了、合单购买，或同一指令被重复执行，都可能引发纠纷。美国运通的方案试图把自然语言意图转成可核查的交易条件，让发卡机构在授权和处理争议时有一致的证据可用。目前公开的是技术架构和服务构想，并非全球所有商户已接入，也不意味着智能体能跳过付款确认。开发者还需考虑交易幂等、令牌过期、撤销及异常退款。

趋势观察

模型正从理解文本走向执行任务。安全公司盯住运行时动作，业务软件要求遵守原系统规则，支付机构则希望用户授权留有证据。评估这类系统，不能只看任务完成率，还要看调用来源、权限越界率、单位任务成本、审批记录是否完整，以及出错后能否恢复。缺了这些控制，持续交给智能

体处理业务就很难让人放心。

参考资料

1. **Google 官方博客** | 《Gemini 4 Argon comes to the Gemini app》 | 2026-10-13 | 用途：确认新模型、付费用户开放范围、Antigravity 与跨应用任务入口。
<https://blog.google/innovation-and-ai/products/gemini-app/gemini-4-argon-availability/>
2. **Reuters** | 《Google launches flagship AI model Gemini 4 Argon for developers, businesses》 | 2026-10-13 | 用途：交叉核验 API 发布、阶段性价格和商业竞争背景。
<https://www.reuters.com/business/google-launches-flagship-ai-model-gemini-4-argon-developers-businesses-2026-10-13/>
3. **The Verge** | 《Google releases Gemini 4 Argon》 | 2026-10-13 | 用途：核对产品入口和发布时点。
<https://www.theverge.com/ai-artificial-intelligence/1009862/google-releases-gemini-4-argon>
4. **TechCrunch** | 《Pluto Security raises \$42M as AI gives enterprise security teams a new headache》 | 2026-10-13 | 用途：核验融资构成、运行时控制及公司自报客户数据。
<https://techcrunch.com/2026/10/13/pluto-security-raises-42m-as-ai-gives-enterprise-security-teams-a-new-headache/>
5. **TokenPost** | 《Pluto Security Raises \$42 Million for Enterprise AI

Workspace Security》 | 2026-10-13 | 用途：交叉核验累计融资和 AI 组件监测定位。

<https://www.tokenpost.com/news/business/31386>

6. **Workday 官方新闻室** | 《Workday and Anthropic Announce New Partnership to Connect Reasoning to the Rules That Run the Business》 | 2026-10-13 | 用途：核验 Sana、Claude、MCP、权限审计与早期开放安排。

<https://newsroom.workday.com/2026-10-13-Workday-and-Anthropic-Announce-New-Partnership-to-Connect-Reasoning-to-the-Rules-That-Run-the-Business,-Wherever-People-Choose-to-Work>

7. **American Express Technology** | 《Intent Intelligence: Building Trust in Agentic Commerce》 | 2026-10-13 | 用途：核验意图确认、支付限额、令牌和身份验证设计。

<https://americanexpress.io/intent-intelligence-building-trust-in-agentic-commerce/>

8. **VentureBeat** | 《OpenAI' s AI agent platform is used by twice as many companies as Anthropic' s, new VentureBeat survey finds》 | 2026-10-13 | 用途：背景观察 Agent 框架更换和工具链成本，不用样本调查替代总体统计。

<https://venturebeat.com/orchestration/openais-ai-agent-platform-is-used-by-twice-as-many-companies-as-anthropics-new-venturebeat-survey-finds>

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>