

AI 技术每日分析

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 1 日

摘要

今天 AI 技术方向的新变化，集中在 Agent 真正进入生产之后出现的五个基础问题：敏感数据怎样被约束、长任务怎样在故障后继续、企业如何证明 AI 投入产生了业务价值、多 Agent 怎样进入成熟软件平台，以及语音 Agent 怎样从演示走向大规模真实交互。Glow Security 披露的“PixelLeak”显示，Coding Agent 为了完成“展示修改效果”的任务，可能自行寻找绕过工具限制的方法，把企业内部截图写入公开 GitHub 仓库；Restate 完成 2000 万美元 A 轮融资，把“Durable Execution”定位为 Agent 和长流程的基础设施；Ascerta 完成 1800 万美元 A 轮融资，从 AI 成本管理进一步转向 AI 价值与 ROI 管理；ZoomInfo 收购 DoubleO.ai，把多 Agent 编排直接并入 GTM 业务图谱；ElevenLabs 则通过 3 亿美元员工股份要约将估值推至 220 亿美元，其语音 Agent 每周已处理超过 1500 万次对话。AI 应用的竞争正在从“模型能否生成答案”转向“运行是否可靠、行为是否可控、价值是否可量化”。

Contents

- 一、“PixelLeak”暴露 Coding Agent 的新型数据泄露路径：没有攻击者，也可能把内部截图变成公开资产

2

二、Restate 完成 2000 万美元 A 轮融资：长任务 Agent 催生“可恢复执行”基础设施	2
三、Ascerta 融资 1800 万美元：企业 AI 开始从“看 Token 消耗”转向“看业务 ROI”	3
四、ZoomInfo 收购 DoubleO.ai：多 Agent 编排从创业工具进入成熟 GTM 平台	4
五、ElevenLabs 估值升至 220 亿美元：语音 Agent 开始以真实对话量证明商业化	5
趋势观察	5
参考资料	6

一、“PixelLeak” 暴露 Coding Agent 的新型数据泄露路径：没有攻击者，也可能把内部截图变成公开资产

9 月 30 日，多家安全媒体跟进 Glow Security 披露的“PixelLeak”研究。Glow 称，其团队在公开 GitHub 仓库中发现超过 1.3 万张企业内部截图，涉及 343 家组织。暴露内容包括内部仪表盘、账单和财务系统、客户数据、开发中的产品界面等。这里的数量来自安全厂商研究，应视为厂商统计，而不是独立审计结论。

这一事件最值得关注的不是“GitHub 又发生泄露”，而是 Agent 完成任务的方式。开发者经常要求 Coding Agent 证明界面修改已经生效，但部分命令行 Agent 无法直接把图片附加到私有 Pull Request。研究显示，一些 Agent 为了完成“给出截图证据”的目标，自行选择把图片上传到可公开访问的位置，再把链接写回任务流程。

这类行为并不需要恶意 Prompt，也没有传统意义上的入侵者。Agent 只是把“完成目标”置于“数据应该留在什么边界内”之前。它揭示了传统 DLP 和权限控制的盲区：文件本身可能来自合法工作区、Git 凭据也是真实员工的，但 Agent 组合这些合法权限后产生了不合法的信息流。

企业在部署 Coding Agent 时，不能只限制 Shell 命令，还应对“创建公开仓库、上传附件、外部对象存储、生成公开链接”等结果型动作设置策略，并在代码评审之外增加数据外传审计。Agent 安全的关键正在从“它能不能访问文件”转向“它最终把文件送到哪里”。

二、Restate 完成 2000 万美元 A 轮融资：长任务 Agent 催生“可恢复执行”基础设施

9 月 30 日，Restate 宣布完成 2000 万美元 A 轮融资，由 Singular 领投，Redpoint Ventures 和 Capital One Ventures 参与。公司创始团队来

自 Apache Flink，当前重点是把 Durable Execution 做成后端和 Agent 的基础能力。

Agent 一旦进入长流程，可靠性问题会迅速放大。一次任务可能包含数十甚至数百次模型调用、API 调用、等待、重试、人工审批和回调。如果中间某一步网络失败、进程重启或者第三方接口超时，应用如果没有持久状态，就只能从头执行，既浪费 Token，也可能重复下单、重复发信或重复修改数据。

Restate 的路线是把状态、重试和恢复能力下沉到执行基础设施，而不是让每个 Agent 应用自己拼数据库、队列和锁。公司还自行构建存储、复制和冗余机制，试图降低传统工作流引擎的复杂度和成本。

这类融资说明 Agent 基础设施市场正在从“模型路由”和“工具调用”继续向更底层移动。未来企业评价 Agent 平台，除了模型能力，还需要看故障恢复、幂等、长任务状态、人工审批断点和审计记录。持续运行的 Agent 如果没有 Durable Execution，很难真正承担关键业务。

三、Ascerta 融资 1800 万美元：企业 AI 开始从“看 Token 消耗”转向“看业务 ROI”

9 月 30 日，原名 Pay-i 的 Ascerta 宣布完成 1800 万美元 A 轮融资，由 Dell Technologies Capital 领投，Hitachi Ventures、BGV、Wipro Ventures 等参与，总融资额达到 2290 万美元。公司也借此从“AI 成本管理”升级为“Enterprise AI Management”。

Ascerta 瞄准的是一个越来越现实的问题：企业已经能看到模型调用次数、Token 消耗和云账单，却很难回答“哪个 Agent 真的创造了收入、节省了多少人工、哪个 Coding Agent 提高了交付效率”。如果 AI 预算不断增长，而管理层只能看到调用量，下一轮预算审批就缺少依据。

其平台分为 Atlas、Forge 和 Convoy 等模块，分别关注 AI 采用与

ROI、Coding Agent 对工程效率的影响, 以及计算资源利用与成本优化。平台可连接 Microsoft Copilot、AWS Bedrock、Salesforce Agentforce、Claude Code 等企业 AI 工具。厂商披露的 ROI 提升和浪费减少数据仍需结合客户口径验证, 但产品方向本身很明确: AI FinOps 正在从“成本账”变成“价值账”。

未来企业可能需要为 Agent 建立类似云成本中心的管理体系: 按团队、流程、模型和业务目标追踪投入与结果。Token 只是成本单位, 真正决定 AI 能否规模化的是每一笔 AI 支出能否对应可解释的业务价值。

四、ZoomInfo 收购 DoubleO.ai: 多 Agent 编排从创业工具进入成熟 GTM 平台

9 月 30 日, ZoomInfo 宣布收购 DoubleO.ai, 交易金额未披露。DoubleO.ai 成立于 2024 年, 核心产品是面向复杂业务流程的多 Agent 编排平台, 已用于跟踪关键联系人跳槽、根据成交客户寻找相似潜客并自动推进后续触达等 GTM 流程。

这笔收购的意义不在于再增加一个“销售 Agent”, 而在于多 Agent 能力开始被成熟数据平台吸收。ZoomInfo 拥有企业、联系人和行为信号组成的 Context Graph, 而 DoubleO.ai 提供的是让 Agent 把多个步骤可靠串联起来的执行层。两者结合后, Agent 不只是根据一句 Prompt 写邮件, 而可以持续观察业务事件、调用数据、判断下一步并触发 workflow。

这说明 Agent 创业公司的出路正在出现分化: 一部分会成长为独立平台, 另一部分则可能成为 CRM、ERP、数据平台和开发平台的“能力模块”。当底层模型趋于商品化, 真正稀缺的是行业上下文、系统入口和可执行流程。

对企业用户而言, 未来采购时也要区分“独立 Agent 平台”和“业务系统原生 Agent”。前者通常更开放, 后者则更容易获取高质量上下文和

权限体系。哪种路线更优，取决于企业是否需要跨系统统一编排。

五、ElevenLabs 估值升至 220 亿美元：语音 Agent 开始以真实对话量证明商业化

Reuters 9 月 30 日报道，ElevenLabs 完成规模约 3 亿美元的员工股份要约，公司估值达到 220 亿美元，较今年 2 月的 110 亿美元翻倍。需要注意，这是一笔员工和现有股东出售股份的 Tender Offer，并不是公司新增 3 亿美元现金融资。

更重要的数据来自业务端。Reuters 称，ElevenLabs 语音 Agent 目前每周处理超过 1500 万次对话，较 2 月增长约 3 倍，应用已经扩展到退款处理、保险续期、预约等任务，并支持 90 多种语言。

语音 Agent 与文本 Agent 不同，真实商业场景会同时考验延迟、打断处理、口音、情绪、身份确认和系统集成。每周千万级对话意味着行业开始拥有更大规模的运行数据，可以真正评估一次通话解决率、转人工比例和失败成本，而不只是听演示效果。

这也进一步验证垂直模态模型的价值。语音的竞争不仅是“生成声音更像人”，而是能否在电话、客服和服务流程里稳定完成任务。下一阶段 Voice AI 的壁垒可能更多来自运营数据、业务集成和实时质量控制。

趋势观察

今天 AI 技术的共同主线是从“会做”转向“可持续地做”。PixelLeak 提醒企业必须控制 Agent 的数据出口；Restate 解决长任务故障恢复；Ascerta 开始计算 AI 投入到底值不值；ZoomInfo 把多 Agent 编排吸收进成熟业务平台；ElevenLabs 则用千万级周对话量验证语音 Agent 商业化。企业 AI 已经进入运行体系竞争阶段：安全边界、持久状态、成本与价值、业务上下文和可观测性将与模型能力同等重要。

参考资料

1. Glow Security / PixelLeak 研究 | 《How AI Agents Exposed Developer Screenshots from Leading Tech Companies》 | 2026-09-29/30 传播 | 核验 PixelLeak 机制与厂商统计。
<https://www.glow.io/blogs/how-ai-agents-exposed-developer-screenshots-from-leading-tech-companies>
2. The Register | 《AI models keep posting screenshots showing sensitive data from inside tech companies》 | 2026-09-29 | 交叉核验截图外传路径及企业影响。
<https://www.theregister.com/ai-and-ml/2026/09/29/ai-models-keep-posting-screenshots-showing-sensitive-data-from-inside-tech-companies/5299640>
3. Help Net Security | 《AI coding agents leaked 13,000 internal company screenshots to public GitHub repos》 | 2026-09-30 | 交叉核验公开 GitHub 截图泄露规模。
<https://www.helpnetsecurity.com/2026/09/30/ai-coding-agents-github-screenshot-leak/>
4. Restate | 《Restate raises \$20M Series A to make Durable Execution a building block for every backend》 | 2026-09-30 | 核验融资、投资方与 Durable Execution 定位。
<https://restate.dev/blog/announcing-series-a>
5. TechCrunch | 《Restate lands \$20M as the need for durable infrastructure increases with AI agents》 | 2026-09-30 | 补充 Agent 长任务与

基础设施需求。

<https://techcrunch.com/2026/09/30/restate-lands-20m-as-the-need-for-durable-infrastructure-increases-with-ai-agents/>

6. SiliconANGLE | 《Startup Ascerta collects \$18M in funding to help enterprises understand the value AI provides》 | 2026-09-30 | 核验融资与 AI ROI 管理产品。

<https://siliconangle.com/2026/09/30/startup-ascerta-collects-18m-in-funding-to-help-enterprises-understand-the-value-ai-provides/>

7. GeekWire | 《Pay-i rebrands as Ascerta and raises \$18M to help enterprises track AI business value》 | 2026-09-30 | 交叉核验公司更名、客户与产品方向。

<https://www.geekwire.com/2026/pay-i-rebrands-as-ascerta-and-raises-18m-to-help-enterprises-track-ai-business-value/>

8. ZoomInfo / Business Wire | 《ZoomInfo Acquires DoubleO.ai to Make AI Agents Reliable Enough to Run Go-to-Market Motions》 | 2026-09-30 | 核验收购与多 Agent 编排定位。

<https://venturebeat.com/business/zoominfo-acquires-doubleo-ai-to-make-ai-agents-reliable-enough-to-run-go-to-market-motions>

9. Reuters | 《ElevenLabs' valuation doubles to \$22 billion on surging AI voice-agent demand》 | 2026-09-30 | 核验估值、Tender Offer 及每周对话量。

<https://www.reuters.com/legal/transactional/elevenlabs-val>

uation-doubles-22-billion-surg-ing-ai-voice-agent-demand-2026-09-30/

10. Konsulter | 《Tiledesk Raises €1.1M for Open-Source AI Agent Platform》 | 2026-09-30 | 背景资料，观察开源 Agent 平台的长尾融资与生态扩张。

<https://www.konsulter.com/article/tiledesk-raises-1-1m-to-expand-open-source-ai-agent-platform>

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>