

Kore.ai 推出 Autoloop, 企业 Agent 进入持续纠错阶段

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 10 日

摘要

10 月 9 日的几条更新，落点都在具体任务怎么做、做完怎么检查。Kore.ai 宣布 Autoloop 正式可用，用状态轨迹和可执行工作流持续评测、优化企业 Agent；Qwen 公开 Qwen-Image-2.1-Turbo 模型卡，7B 图像模型推荐 8 步采样；Conway Research 发布面向工具调用的 Underdog-Saluki-27B 低比特模型，尝试降低本地运行的显存需求；OpenAI 将用于分类、选择和评分的 Decisions API 推向公开测试。安全方面，据路透社报道，ARTEX 网络安全 Agent 的开发者在韩国银行攻击争议后停止开源代码。这些进展提醒我们，评价 AI 系统不能只看通用聊天榜单，还要看它在特定任务中的表现、运行过程能否追踪，以及权限和成本是否可控。

Contents

一、Kore.ai 推出 Autoloop：企业 Agent 开始把“持续纠错”做成产品功能	2
二、Qwen-Image-2.1-Turbo 开放模型卡：图像生成优化进入“八步采样”阶段	2
三、Conway Research 推出 Underdog-Saluki-27B：量化模型开始针对工具调用单独优化	3
四、OpenAI 推出 Decisions API 公开测试：让小型判断任务退出长文本生成流程	4
五、ARTEX 转向闭源：网络安全 Agent 的双重用途边界受到审视	4

趋势观察	5
参考资料	5

一、Kore.ai 推出 Autoloop：企业 Agent 开始把“持续纠错”做成产品功能

10 月 9 日，企业智能体平台厂商 Kore.ai 宣布 Autoloop 正式可用。它面向 Artemis 平台的 Agent，提供构建、测试、诊断和持续优化功能。评估不只看回答是否流畅，还覆盖任务完成、事实准确性、业务规则、安全、行为一致性、用户体验和成本七个维度。[1]

产品中有两个值得看具体怎么用的组件：StateTrace 记录任务移交、状态变化、工具调用与上下文，供团队定位失败环节；Agent Blueprint Language (ABL) 把路由、委派、工具使用、业务规则和安全护栏写成可执行状态机，让修改能对应到流程节点。企业 Agent 的麻烦往往在这里：偶发错误难复现，修好一个环节又可能影响其他步骤。

Kore.ai 还援引自身调查称，较高比例的企业遇到过 Agent 动作无法撤销或错误无法追溯的问题。调查结果和产品效果都是厂商口径，不能据此推断它在不同行业都同样可靠。企业更该用自己的任务反复测试：成功率有多高，回滚错误要付出多少成本，日志是否完整，修订后有没有引入新缺陷。底座模型之外，Agent 运维也需要单独做工程验收。

二、Qwen-Image-2.1-Turbo 开放模型卡：图像生成优化进入“八步采样”阶段

Qwen 团队发布了 Qwen-Image-2.1-Turbo 模型资源。公开模型卡写明：模型规模 7B，推荐 8 步采样，支持图像生成、编辑、文字排版和多参考图组合，并提供横版 16:9、竖版 9:16 等分辨率设置。[2]

图像生成的成本不只取决于参数量。每张图要跑多少步、占用多少显存、输出什么分辨率，也会影响实际体验。推荐采样压到 8 步，便于创作者多试几次，再根据结果修改；设计工作台也更容易把生成、检查和修改

接成一套交互流程。但步数少不代表各种硬件上的延迟都会同比下降，细节保真、文字准确率和多图一致性仍要分别测。

许可也要看清楚。模型卡标注的是 **Qwen Research License**；能访问权重，不等于拿到了 Apache 2.0 式的无限制商业使用许可。若用于企业宣传、版权素材或客户设计交付，需先核对许可条款和第三方素材权利。这次更新值得关注的，是高分辨率视觉生成的反复试做成本能否降低，而不只是模型变得更大。

三、Conway Research 推出 Underdog-Saluki-27B：量化模型开始针对工具调用单独优化

10 月 9 日，小型研究团队 Conway Research 公开了 Underdog-Saluki-27B 模型及技术说明。它以 Qwen 系列 27B 模型为基础，着力在极低比特表示下保留结构化工具调用、JSON 输出和多步任务能力，而非只提高通用写作分数。公开资料称，2-bit GGUF 版本约 7.89GB，可供研究低成本本地 Agent 运行。[3][4]

过去评测量化模型，常看常识、数学和语言基准；Agent 落到业务里，还得准确填写函数参数、工具名和字段，并按顺序调用。答案写得顺，一旦工具参数总是填错，自动化任务也跑不起来。因此，工具调用正确率开始成为模型压缩时需要单独考量的指标。

团队公布的对照成绩来自自建任务和特定测试配置，不能理解成“2-bit 模型所有能力都超过原模型”。企业若要放进私有化工作台，最好固定 MCP 工具、权限和业务数据，重复测调用成功率、非法动作次数、推理延迟以及 CPU/GPU 实际占用。

四、OpenAI 推出 Decisions API 公开测试：让小型判断任务退出长文本生成流程

OpenAI 开发者文档显示，Decisions API 已进入公开测试，使用独立端点 ‘POST /v1/decisions’。开发者提交文本或图像和要回答的问题，接口可返回条件概率、固定选项选择，或按等级量化的评分；目前仅支持 ‘gpt-6-luna’ 模型。[5]

内容分流、风险评级、工单优先级和场景路由，很多时候只需要结构明确、能直接交给软件处理的判断，不需要一段长篇解释。这是它与传统对话 API 的区别。官方称，这类任务的响应速度可达常规 Responses API 的约十倍；这一数字来自指定任务和配置，接入实际业务时仍需复测。[6]

接口能给出判断，不代表审批可以省去。输出概率也不能直接当作校准过的真实风险。尤其涉及人事、金融、医疗或其他高风险业务，阈值要依据历史数据、误报漏报代价和人工复核机制来设定。生成式模型处理表达和复杂推理，专用决策接口处理高频、可量化的判断；两者各有适用范围。

五、ARTEX 转向闭源：网络安全 Agent 的双重用途边界受到审视

据路透社 10 月 9 日报道，ARTEX 网络安全 Agent 的开发者在工具被卷入韩国银行网络攻击的相关调查和舆论后，停止公开源代码。报道涉及安全研究机构、调查机关和开发者等不同来源；工具可能被利用，不等于开发者实施了攻击，责任仍需依法调查认定。[7]

自动扫描、漏洞分析和权限测试能帮防守方尽快找到隐患，缺少用户身份核验、目标授权和行为范围限制时，同一套自动化流程也可能遭到滥用。关闭源代码并不能独自消除风险：模型能力、工具链和替代项目依然

可能存在。

安全团队需要留下授权证明和任务日志，对危险操作做隔离，并设置网络访问控制和异常中止机制。开源社区则仍要权衡怎样既方便审计，又降低滥用风险。对 Agent 安全的检查，也不能只停在恶意提示词上，还要覆盖执行链上的权限与责任。

趋势观察

这五条动态分别涉及企业 Agent、视觉生成、模型压缩、专用判断接口和网络安全。放在一起看，技术选型正变得更具体：复杂生成、高频判断、流程状态和操作权限，不必都压在同一个通用模型上。企业做验收时，除了比较模型能力，还应逐项核对重复任务成功率、推理成本、许可条款和行为日志；能否稳定运行，最终要在自己的业务流程里测出来。

参考资料

1. **Express Computer / Kore.ai** | 《Kore.ai launches Autoloop to continuously optimise enterprise AI agents》 | 2026-10-09 | 用途：核验 GA 发布、StateTrace、ABL 与七维评估。
<https://www.expresscomputer.in/news/kore-ai-autoloop-enterprise-ai-agents/139737/>
2. **Qwen / Hugging Face 官方模型卡** | 《Qwen-Image-2.1-Turbo》 | 2026-10-09 访问 | 用途：核验 7B、8 步推荐采样、输出规格和研究许可。
<https://huggingface.co/Qwen/Qwen-Image-2.1-Turbo>
3. **Conway Research / Hugging Face** | 《Underdog-Saluki-27B-1.0》 | 2026-10-09 访问 | 用途：核验模型权重、低比特发布与使用方法。

<https://huggingface.co/ConwayResearch/Underdog-Saluki-27B-1.0>

4. **MarkTechPost** | 《Meet the Underdog Saluki 27B: A 2-Bit Qwen...》
| 2026-10-09 | 用途：交叉了解量化与工具调用评测，相关成绩视为厂商自报。

<https://www.marktechpost.com/2026/10/09/meet-the-underdog-saluki-27b-a-2-bit-qwen3-8-27b-that-beats-the-original-at-tool-calling/>

5. **OpenAI 开发者文档** | 《Decisions》 | 2026-10-09 访问 | 用途：核验公开测试、接口、返回类型和支持模型。

<https://developers.openai.com/api/docs/guides/decisions>

6. **MarkTechPost** | 《OpenAI Decisions API Hits Public Beta with 10x Faster Typed Answers》 | 2026-10-09 | 用途：对照新品发布与厂商速度说明。

<https://www.marktechpost.com/2026/10/09/openai-decisions-api-hits-public-beta-with-10x-faster-typed-answers/>

7. **Reuters** | 《Chinese developer makes ARTEX AI agent closed source after Korean bank hack》 | 2026-10-09 | 用途：核验停止开源及争议的调查边界。

<https://www.reuters.com/world/china/chinese-developer-makes-artex-ai-agent-closed-source-after-korean-bank-hack-2026-10-09/>

8. **MarkTechPost** | 《Alibaba Qwen Releases Qwen-Image-2.1-Turbo》

| 2026-10-09 | 用途：补充端侧和采样效率行业分析，优先以模型卡为准。

<https://www.marktechpost.com/2026/10/09/alibaba-qwen-releases-qwen-image-2-1-turbo-an-8-step-7b-image-model/>

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>