精选快讯　软件快讯　2026年11月17日 20:00

IndyKite推出基于意图的访问控制，限制AI智能体仅执行指定任务

要点

- IndyKite宣布在AgentControl产品中推出基于意图的访问控制（IBAC），该功能现已可用。
- 在技术实现上，IBAC利用IndyKite的知识图谱，基于实体间的关系和信任度决定每一步可触及的数据范围。
- IBAC基于OAuth2、OpenID AuthZEN、A2A和MCP标准构建，可作为代理或边车部署在现有智能体和MCP服务器之前，无需重构现有架构。

IndyKite宣布在AgentControl产品中推出基于意图的访问控制（IBAC），该功能现已可用。IBAC旨在解决多智能体工作流中的权限管理问题，通过将主体请求转化为结构化意图，并在每个执行步骤中强制执行最小权限原则，确保智能体仅获得完成当前任务所需的最低访问权限。

在技术实现上，IBAC利用IndyKite的知识图谱，基于实体间的关系和信任度决定每一步可触及的数据范围。系统使用OpenID AuthZEN语义将请求翻译为结构化意图，后续决策由规则引擎而非模型判断做出，以提高确定性和安全性。意图被封装在签名的IndyKite令牌中，附加在委托链的每个参与者上并在智能体间传递。为防止权限升级，下游智能体的意图只能匹配或缩小原始意图，不能扩大权限范围。

IBAC基于OAuth2、OpenID AuthZEN、A2A和MCP标准构建，可作为代理或边车部署在现有智能体和MCP服务器之前，无需重构现有架构。IndyKite Intent Agent捕获层以开源形式在GitHub提供。此外，IndyKite正将该模型扩展至智能体本身，使智能体声明的目的成为其不可逾越的边界，进一步限制AI智能体仅执行指定任务。

报道来源：natlawreview、desmoinesregister、einnews、einpresswire

来源网站：https://www.inews.today/