AI Agent (Autonomní agent)

AI Agent je systém založený na umělé inteligenci (obvykle velkém jazykovém modelu – LLM), který není omezen pouze na pasivní odpovídání, ale dokáže aktivně využívat nástroje, plánovat postupy a samostatně rozhodovat o dalších krocích k vyřešení zadaného úkolu.

Klíčové komponenty agenta

Aby se z „modelu“ stal „agent“, potřebuje čtyři základní pilíře:

- **Mozek (LLM):** Slouží jako centrální řídicí jednotka pro uvažování a rozhodování.
- **Plánování (Planning):** Agent dokáže rozložit složitý úkol na menší, zvládnutelné podúkoly (např. pomocí techniky Chain-of-Thought).
- **Paměť (Memory):**
  - *Krátkodobá:* Kontext aktuální konverzace.
  - *Dlouhodobá:* Schopnost ukládat a vyhledávat informace v externích databázích (Vektory/RAG).
- **Nástroje (Tools/Action):** Schopnost volat externí API, prohlížet internet, spouštět kód nebo ovládat software.

Rozdíl: Chatbot vs. AI Agent

Vlastnost	Klasický Chatbot	AI Agent
Interakce	Reaktivní (odpoví na dotaz)	Proaktivní (navrhuje a koná)
Cíl	Vygenerovat text	Dosáhnout výsledku (např. rezervace letenky)
Nezávislost	Čeká na každý další prompt	Pracuje v cyklech, dokud není hotovo
Nástroje	Obvykle omezené	Široká škála (Python, prohlížeč, API)

Typické pracovní cykly (Agentic Workflow)

Agenti často pracují v uzavřených smyčkách:

```
1. **Percepce:** Analýza zadání uživatele.
2. **Plánování:** "Co musím udělat jako první?"
3. **Akce:** Vyhledání informace nebo spuštění kódu.
4. **Reflexe:** "Dosáhl jsem výsledku? Pokud ne, co musím změnit?"
```

Příklady využití v praxi

- **Kódování:** Agent (např. Devin nebo GitHub Copilot Workspace) dokáže najít chybu v kódu, navrhnout opravu, otestovat ji a nasadit.
- **Průzkum trhu:** Agent dokáže projít 20 webových stránek konkurence, vytáhnout ceny do tabulky a poslat shrnutí e-mailem.

- **Osobní asistent:** Naplánování celé dovolené včetně rezervací, hlídání rozpočtu a synchronizace s kalendářem.

—

Populární frameworky pro agenty

- **LangChain:** Nejrozšířenější knihovna pro propojování LLM s nástroji.
- **AutoGPT / BabyAGI:** První experimenty s plně autonomními agenty.
- **CrewAI / Microsoft AutoGen:** Systémy pro spolupráci více agentů najednou (Multi-agent systems).

> **Bezpečnostní varování:** Jelikož agenti mohou samostatně spouštět kód a přistupovat k internetu, je kritické definovat jim mantinely (tzv. „Guardrails“), aby nedošlo k nechtěným akcím nebo smazání dat.

Související: LLM, RAG, Python