

Sådan hænger Microsofts agent-styring sammen

Identitet, ejerskab, adgang og opdagelse. De fire lag der skal ligge, før dine AI-agenter må røre noget der betyder noget.

- **Styringen skal ligge først. Så må agenterne handle.**

PROBLEMET

Hos mange enterprise-kunder kører AI-butikken for fuld skrue, og infrastrukturen til agenterne bliver lagt, mens der bliver kørt på den. Uden identitet, en navngiven ejer og klare adgangsbetingelser er der ingen der kan se, styre eller stå på mål for de agenter, der allerede er i drift.

DEN RIGTIGE RÆKKEFØLGE

- 1 Identitet.** Hver agent får sin egen identitet i Entra Agent ID.
- 2 Navngiven ejer.** Et menneske står bag hver agent. Forlader personen virksomheden, flytter ejerskabet automatisk til lederen.
- 3 Adgang og data.** Purview sorterer, hvilke data agenten må bruge, og på hvilke betingelser.
- 4 Register og opdagelse.** Agent 365 samler registret og finder også de agenter, ingen vidste var der.

Det føles bagvendt at bygge styringen samtidig med driften. Men det er den rigtige rækkefølge: de tre første lag skal ligge, før en agent må lave noget, der betyder noget.

START HER

Det praktiske sted at begynde er Copilot. I har den allerede, IT har godkendt den, og de agenter, jeres kolleger bygger i Copilot Studio, er dem I kan se og styre allerede i dag.

BYGGEKLODSENE

Entra Agent ID

Giver hver agent en identitet og en navngiven ejer, med automatisk overdragelse til lederen.

Agent 365

Register, adgangsstyring og opdagelse. Finder også lokale agenter gennem Defender og Intune. Alment tilgængelig 1. maj 2026.

Purview

Styrer hvilke data agenterne må bruge.

Copilot Studio

Der hvor kollegerne bygger agenter, I kan se og styre i dag.

GODT AT VIDE

Det er ikke et fravalg af Claude eller andre specialiserede agenter. Microsoft-plattformen lover at holde styr på lidt af hvert.

TRE SPØRGSMÅL AT STILLE INTERNT

- 1** Ved I, hvor mange agenter der allerede kører hos jer, og hvem der ejer dem?
- 2** Har hver agent en navngiven ejer, og hvad sker der, når personen stopper?
- 3** Hvilke data må jeres agenter bruge, og hvem har besluttet det?