



La minute de l'expert

Amine MIRHOM, Cloud Solution Architect

Sur le terrain, la question n'est plus si nos clients vont déployer des agents IA, mais comment ils vont les garder sous contrôle. C'est tout l'enjeu **d'Agent 365**, annoncé à Ignite 2025 : le control plane qui permet de gérer et sécuriser l'ensemble de sa flotte d'agents — Microsoft (Copilot Studio) comme tiers ou open source.

Ce qu'il faut retenir côté sécurité :

 **Une identité par agent** — chaque agent reçoit un *Agent ID* dans Microsoft Entra : responsable désigné, cycle de vie maîtrisé, accès au juste besoin.

 **Fin des angles morts** — télémétrie, tableaux de bord et alertes pour savoir en temps réel quel agent tourne, qui l'a créé et ce qu'il fait.

 **La sécurité que vous connaissez déjà** — Entra pour l'identité, Purview pour la conformité et l'audit, Defender pour la détection. Pas de pile parallèle à réinventer.

Le conseil : ne pas attendre le déploiement massif pour poser la gouvernance. Le *shadow AI* se construit vite. Cartographier les agents existants et désigner un responsable pour chacun — Agent 365 fournira le socle pour industrialiser.