Orchestrer la Confiance

Gouverner et sécuriser les Agents IA Microsoft Foundry

ZTDAYS TUNIS 2026

Zero Trust Days – Tunis – Avril 2026

Chedy Missaoui

- Microsoft MVP
- Architecte DevOps & Cloud a Tessan Group
- Technical Account Manager

Microsoft® Most Valuable Professional

Chedy Missaoui

chedy.missaoui@tessan.tech

MissaouiChedy

techdominator.com

TESSAN GROUP

YOUR TRUST PARTNER


Que peut-il mal se passer
avec les agents IA ?

Ça c’est déjà produit

- Base de Donnés Supprimer
- Boite mail ‘nettoyer’
- Information salarial divulgé

Plan

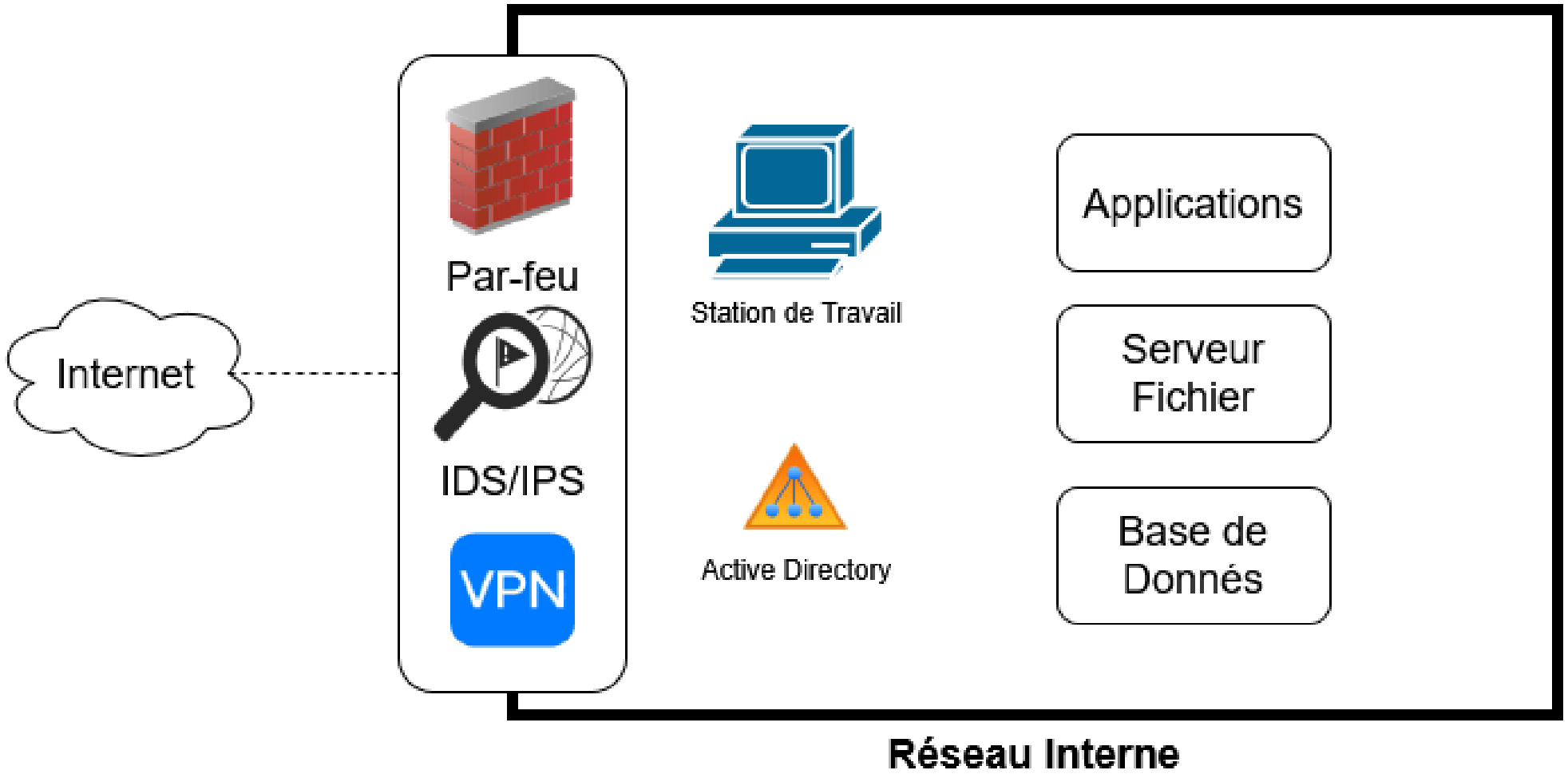
- Agents IA, Zero Trust et Enjeux de Sécurité
- Aperçu Rapide de Microsoft Foundry
- Identité des Agents
- Risques liés aux Donnés
- Risques du traffic Entrant et Sortant

Agents IA, Zero Trust et Enjeux de Sécurité

Architecture Zero Trust

- «Ne Jamais faire confiance, toujours vérifié »
- Une rupture avec la sécurité périmétrique, avec 0 confiance implicite
- Formalisé par ‘NIST Special Publication 800-207’

Avant le Zero Trust



Pourquoi la sécurité périmétrique ne suffit-elle plus?

- Cloud SaaS
- Télétravail
- Ordinateurs et Téléphones Portables
- Acteur Malveillant Interne

Principes du Zero Trust

- Vérifier Explicitement (Identité, permissions…)
- Moindre Privilèges
- Supposer la Compromission (Surveillance, Défense en Profondeur)

Avec Zero Trust

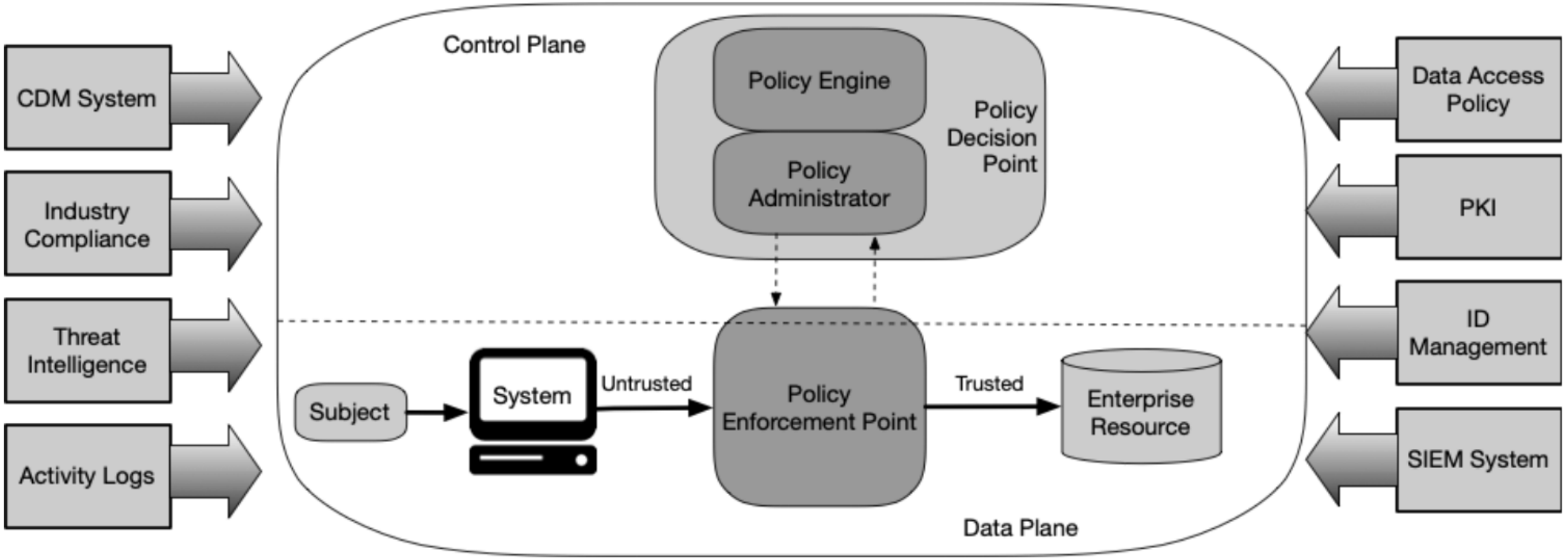


Figure 2: Core Zero Trust Logical Components

Challenges Sécurité des Agent IA

- Non-Determinisme
- Identité Mal-Définie
- Vulnérabilités LLM
- Audit Multi-Agents
- Injection de Prompt
- SKILLS Malveillant
- Shadow AI
- Divulgation de Donnés
- Responsabilités Floues
- Abus de Privilèges
- Localisation de Donnés
- Abus des Outils

Challenges Sécurité des Agent IA

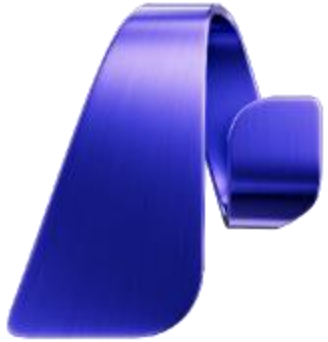
Non-Determinisme	**Identité Mal-Définie**	Vulnérabilités LLM
Audit Multi-Agents	Injection de Prompt	SKILLS Malveillant
Shadow AI	**Divulgation de Donnés**	**Responsabilités Floues**
Abus de Privilèges	**Localisation de Donnés**	**Abus des Outils**

Aperçu Rapide de Microsoft Foundry

Panorama des solutions IA de Microsoft

Agent Builder
(no-code)

Copilot Studio
(low-code)



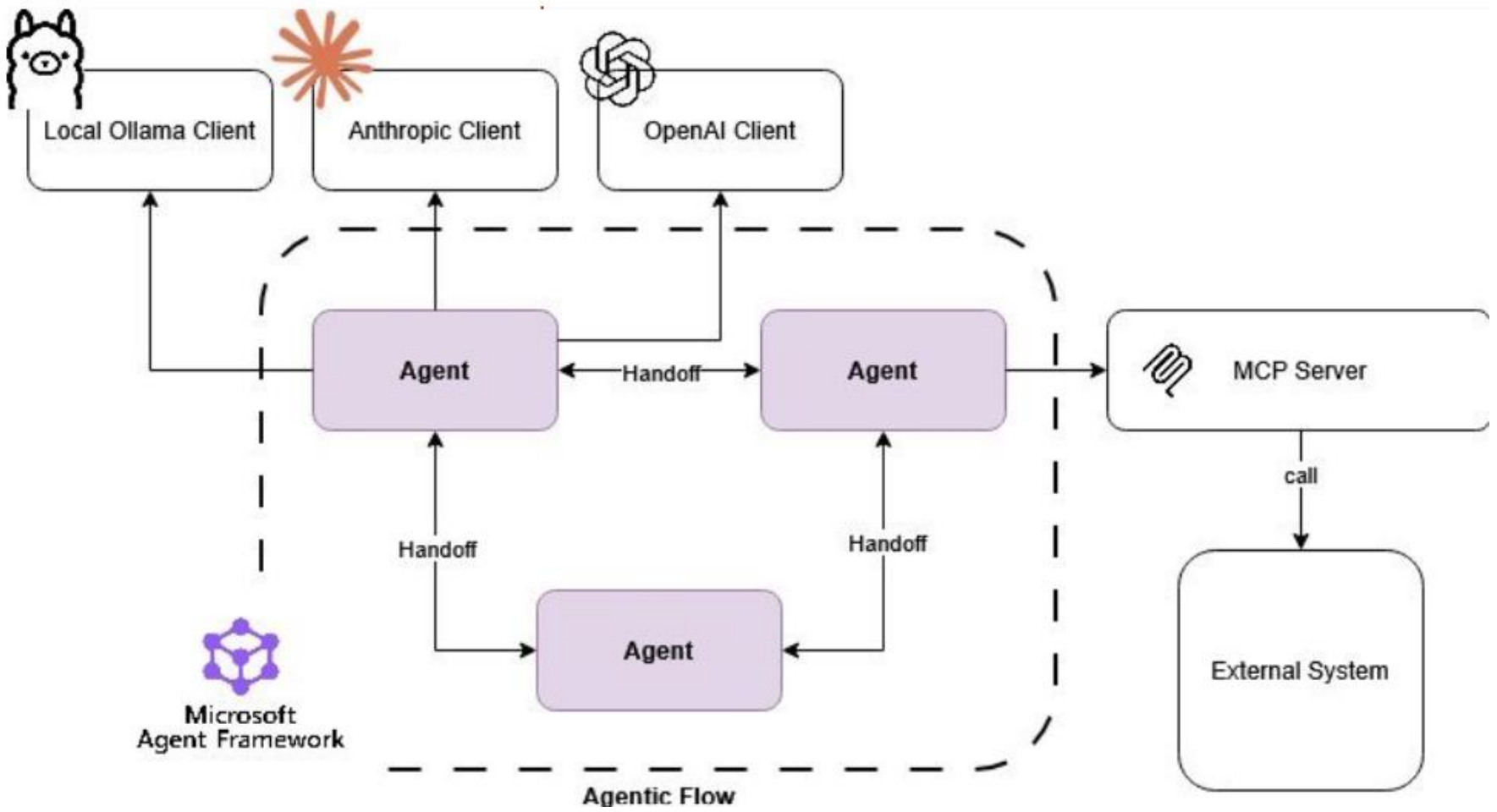
Microsoft Foundry
(pro-code)

Azure ML
(pro-code
+ Machine Learning)

Microsoft Foundry

- Catalogue de Model Riche
- Agent Service
- Accès API au modèle déployer
- RAG, MCP, Mémoire

Microsoft Agent Framework



Identité des Agents

Identité Agent dans Entra ID

- Type spécifique d’identité pour les agents
- Résout la problématique d’ambiguïté

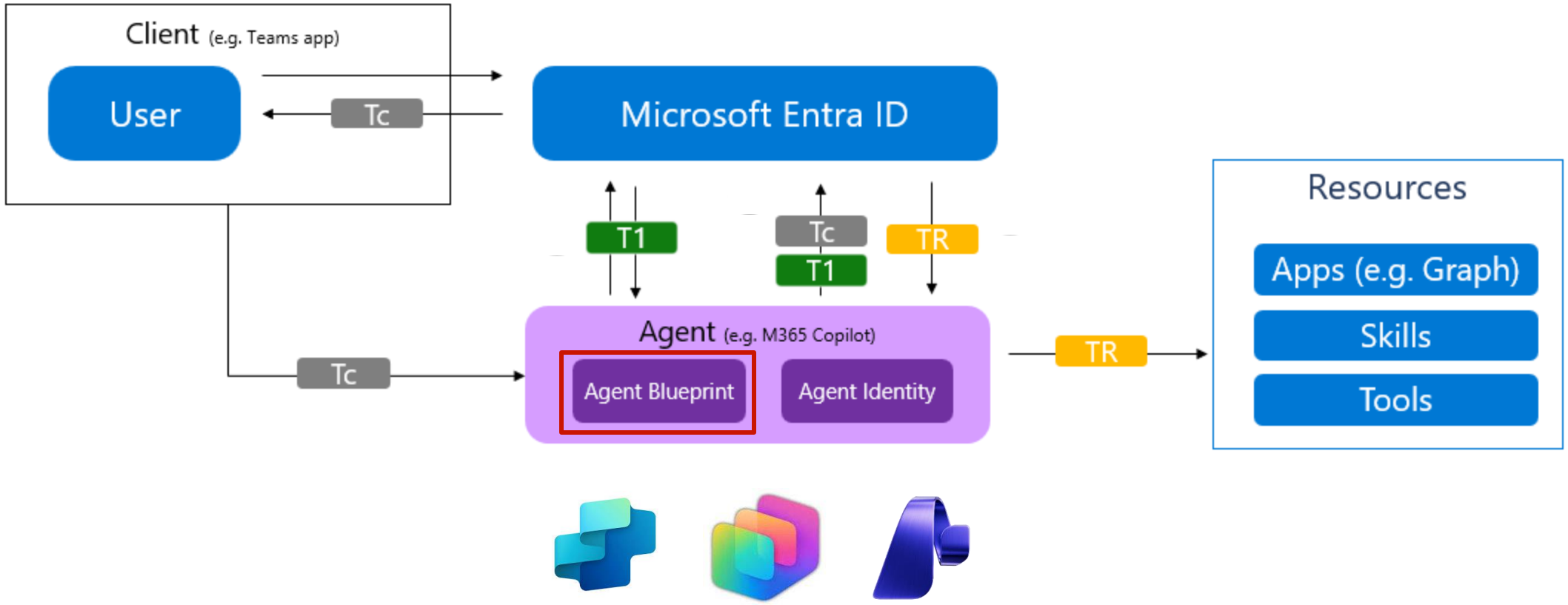
Pourquoi un Type D’identité dédié?

- Comportements normaux pour des agents mais pas pour des applications classiques
- Les Agents sont Non Déterministes
- Facilité d’audit

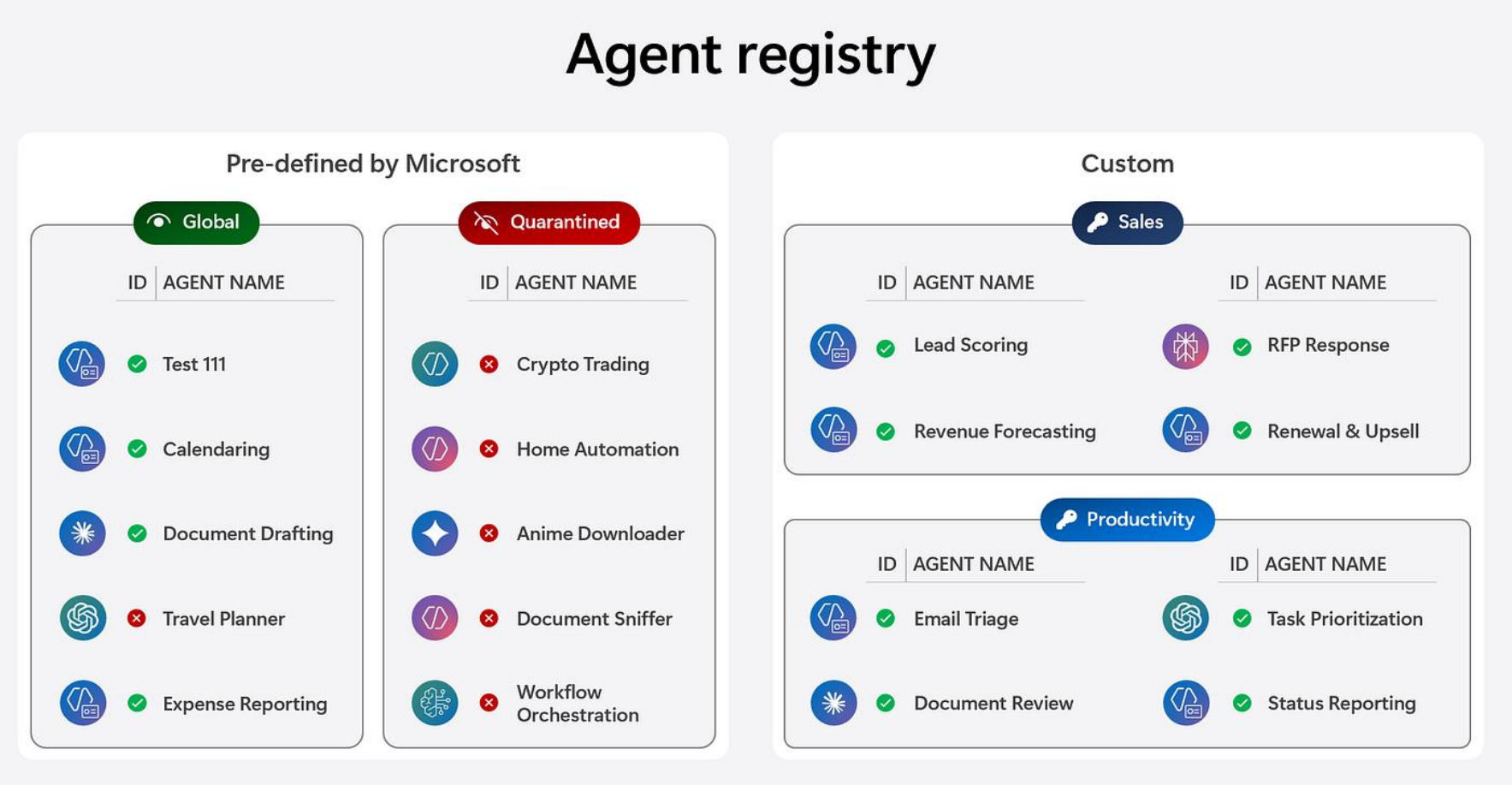
Caractéristiques des identités agents

- Propriétaire
- Sponsor
- Impossible d’assigner des privilèges élevés

Blueprint d’identité



Registre D’Agent

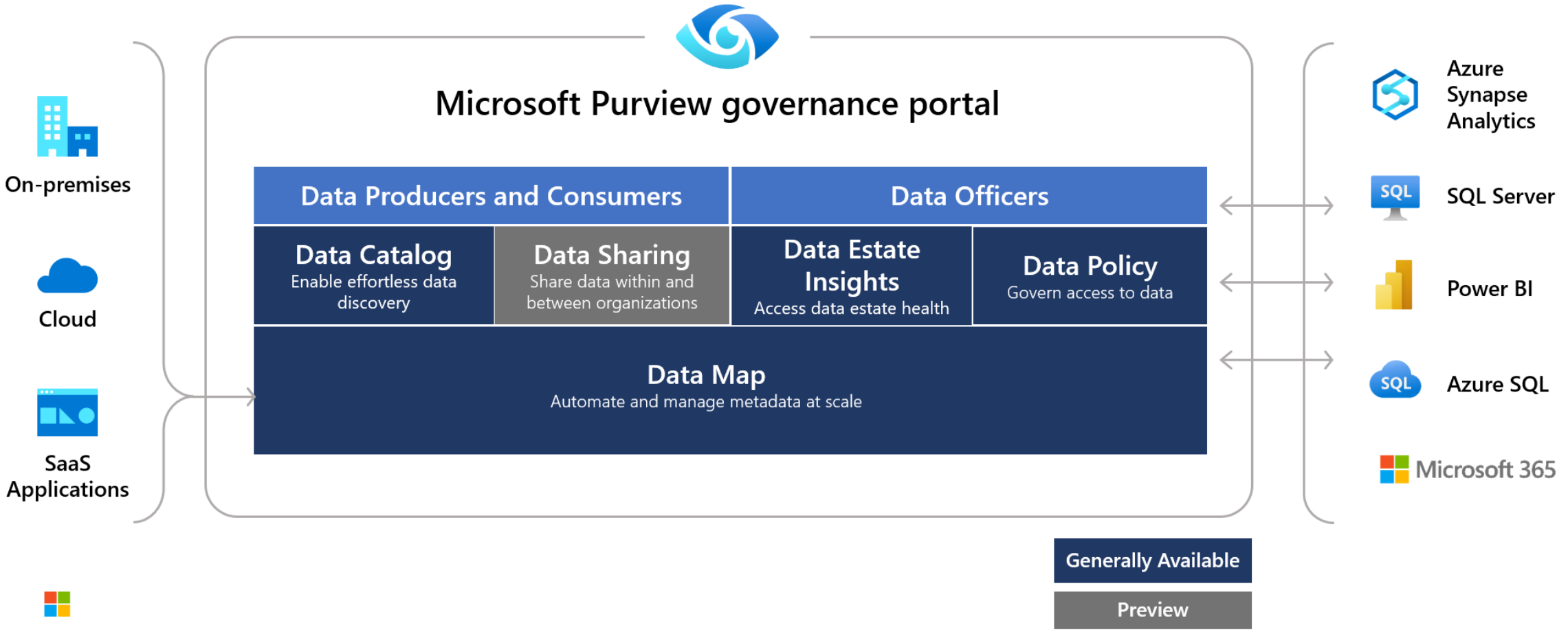


Risques liés aux Donnés

Microsoft Purview

- Platform unifié de gouvernance de donnés
- Bien Intégré dans l'écosystéme Microsoft et au-delà
- Essentielle pour la découverte et la traçabilité des donnés

Fonctionnalités de Microsoft Purview



Intégrations avec Foundry

- Intégration configurable depuis Foundry
- Les Données manipuler par les agents sont sujet à audit
- Les politiques de protection de donnés définie sont appliqué sur les agents

Risques du traffic Entrant et Sortant

AI Gateway


AI apps
& agents
Customer service Assistants
Deep research on your data
Domain Specific Agents
Conversational Agents
Research Assistants
Multi Agent Systems
Agent Policies
Content Safety
AI Gateway
Control token usage
Authentication & Authorization
... & much more
AI models, data & tools
AI models & services
Data & vector stores
SQL
My
Tools & functions

Conclusion


AI AGENTS
SECURITY PROBLEMS?
MORE MONEY
FOR MY BUSINESS
imgflip.com

Merci !
Question?