

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 Tessian Group
- Technical Account Manager



Chedy Missaoui 

chedy.missaoui@tessian.tech 

MissaouiChedy 

techdominator.com 



TESSAN GROUP
YOUR TRUST PARTNER

A close-up shot of a man with a balding head and blue eyes, wearing a dark suit, white shirt, and dark tie. He is smiling broadly, showing his teeth. The background is slightly out of focus, showing a wooden bookshelf with various books and papers.

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

Ça c'est déjà produit

- Base de Données Supprimer
- Boite mail 'nettoyer'
- Information salarial divulgué

Plan

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

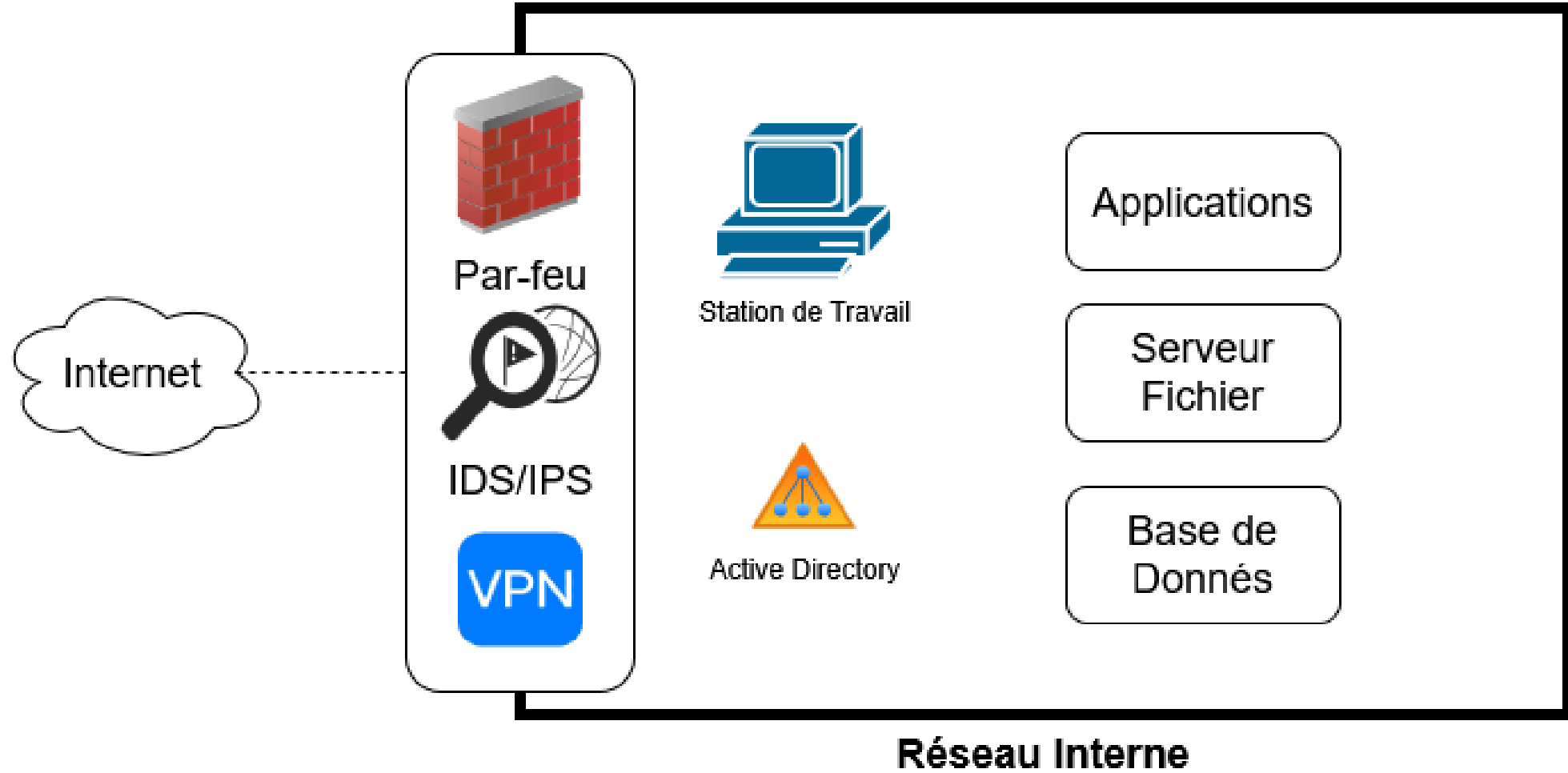
The background is a solid red color. On the left side, there are several concentric white circles of varying radii, some solid and some dashed. A single vertical white line runs down the center of the page, slightly to the left of the text.

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

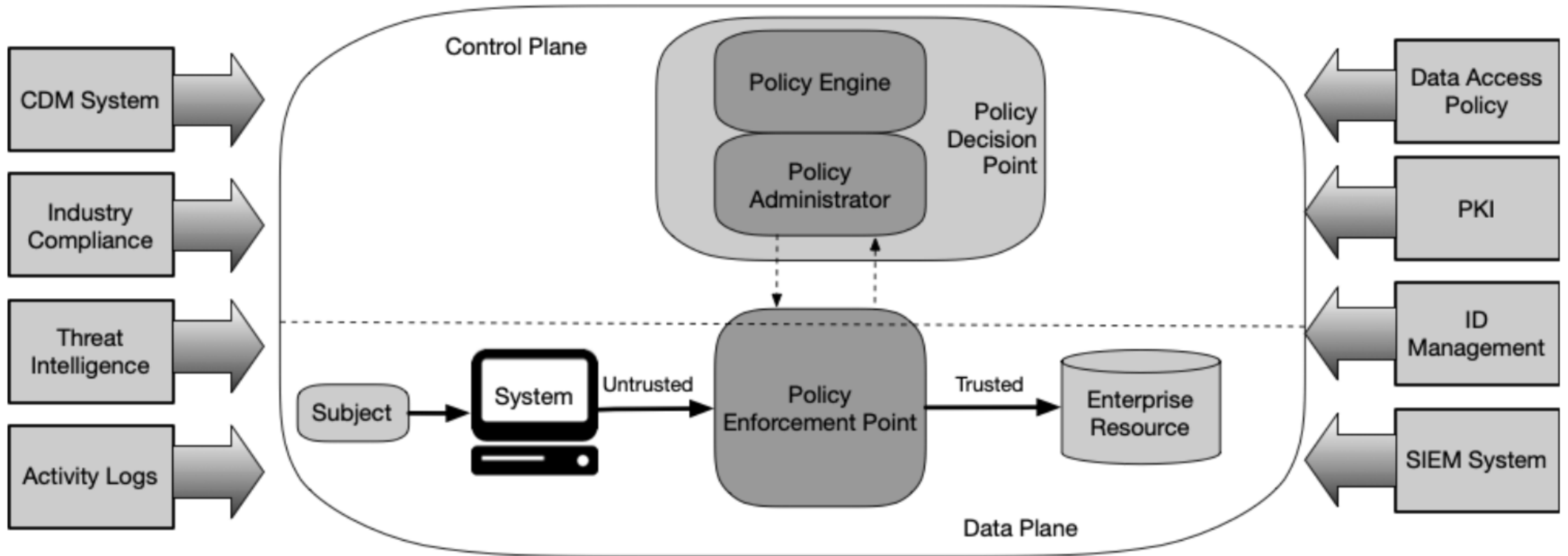


Figure 2: Core Zero Trust Logical Components

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

**Divulgarion de
Donnés**

**Responsabilités
Floues**

Abus de Privilèges

**Localisation de
Donnés**

Abus des Outils

The background is a solid red color. On the left side, there are several concentric white circles of varying radii, some solid and some dashed, creating a sense of depth and movement. The text is positioned on the right side of the image.

Aperçu Rapide de Microsoft Foundry

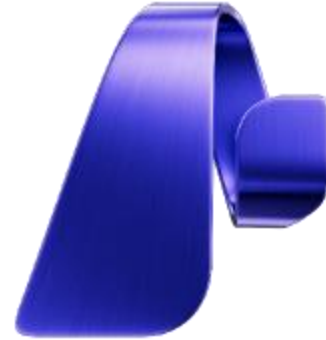
Panorama des solutions IA de Microsoft



Agent Builder
(no-code)



Copilot Studio
(low-code)



Microsoft Foundry
(pro-code)

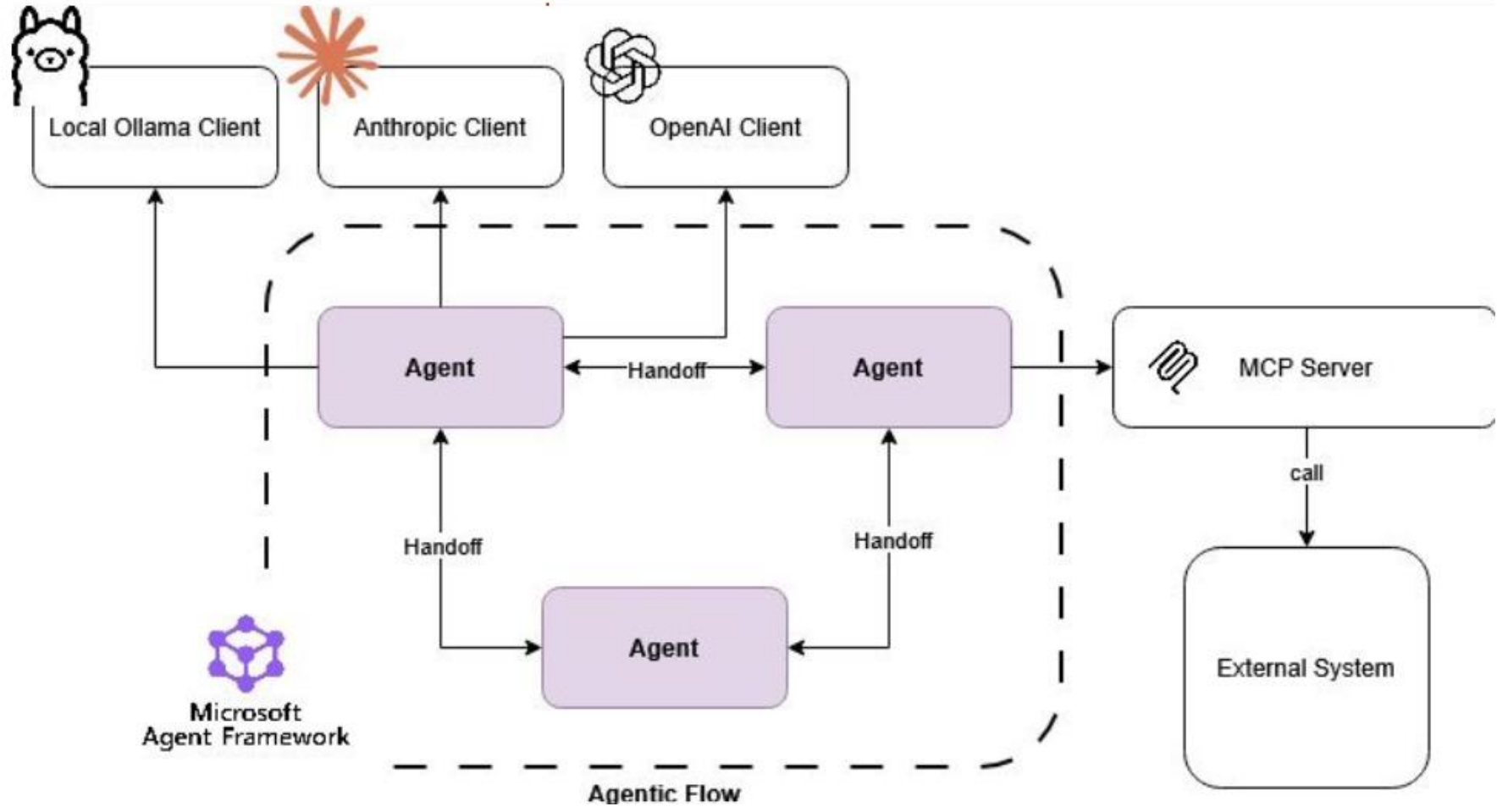


Azure ML
(pro-code
+ Machine Learning)

Microsoft Foundry

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

Microsoft Agent Framework



The background is a solid red color. On the left side, there are several concentric white circles of varying radii, some solid and some dashed. On the right side, there are several parallel white lines, some solid and some dashed, that curve towards the bottom right corner.

Identité des Agents

Identité Agent dans Entra ID

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

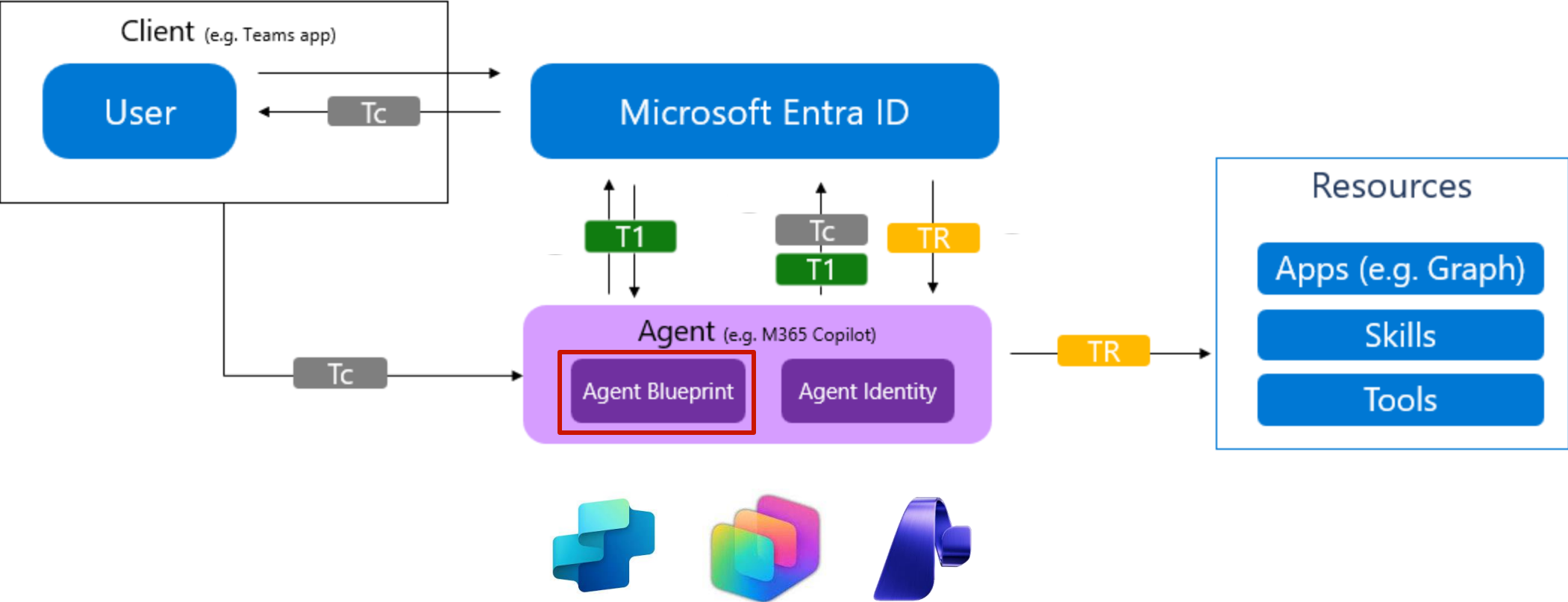
Pourquoi un Type D'identité dédié?

- 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

Agent registry

Pre-defined by Microsoft

Global

ID	AGENT NAME
	✓ Test 111
	✓ Calendaring
	✓ Document Drafting
	✗ Travel Planner
	✓ Expense Reporting

Quarantined

ID	AGENT NAME
	✗ Crypto Trading
	✗ Home Automation
	✗ Anime Downloader
	✗ Document Sniffer
	✗ Workflow Orchestration

Custom

Sales

ID	AGENT NAME	ID	AGENT NAME
	✓ Lead Scoring		✓ RFP Response
	✓ Revenue Forecasting		✓ Renewal & Upsell

Productivity

ID	AGENT NAME	ID	AGENT NAME
	✓ Email Triage		✓ Task Prioritization
	✓ Document Review		✓ Status Reporting



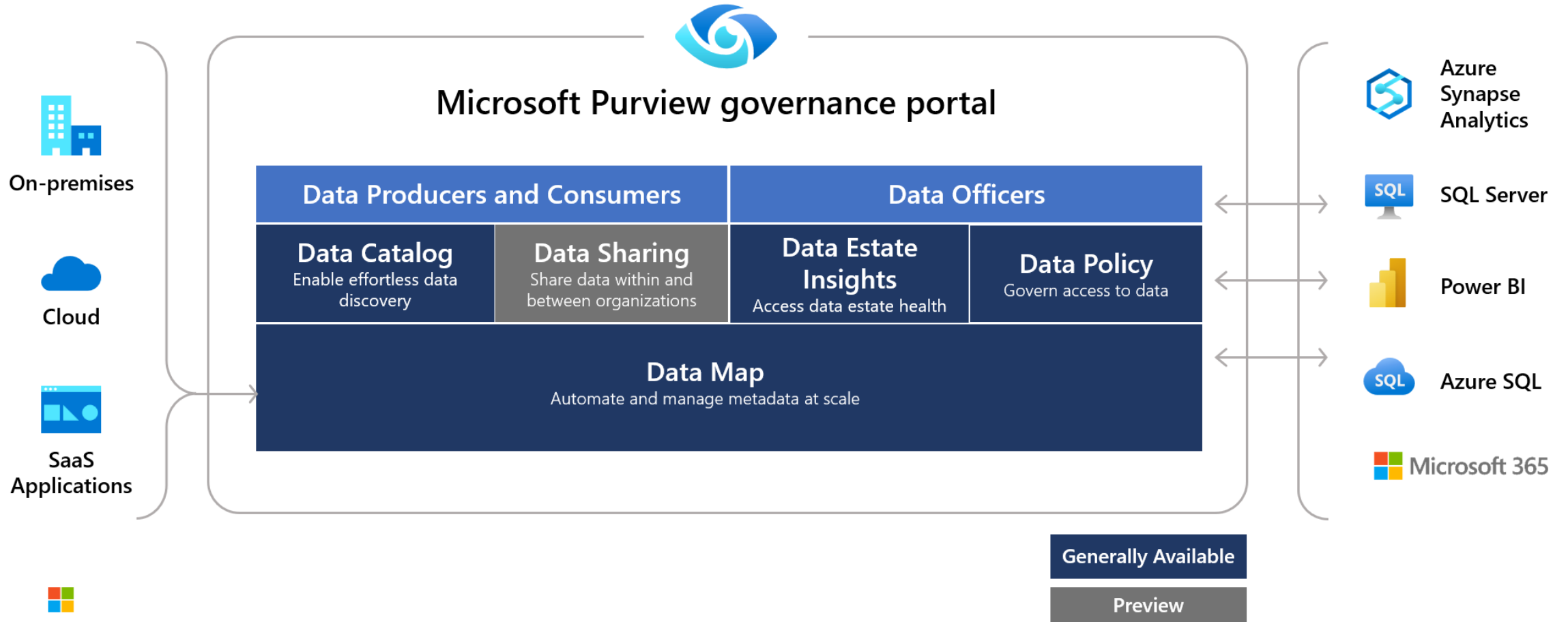
Risques liés aux Donnés



Microsoft Purview

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

Fonctionnalités de Microsoft Purview



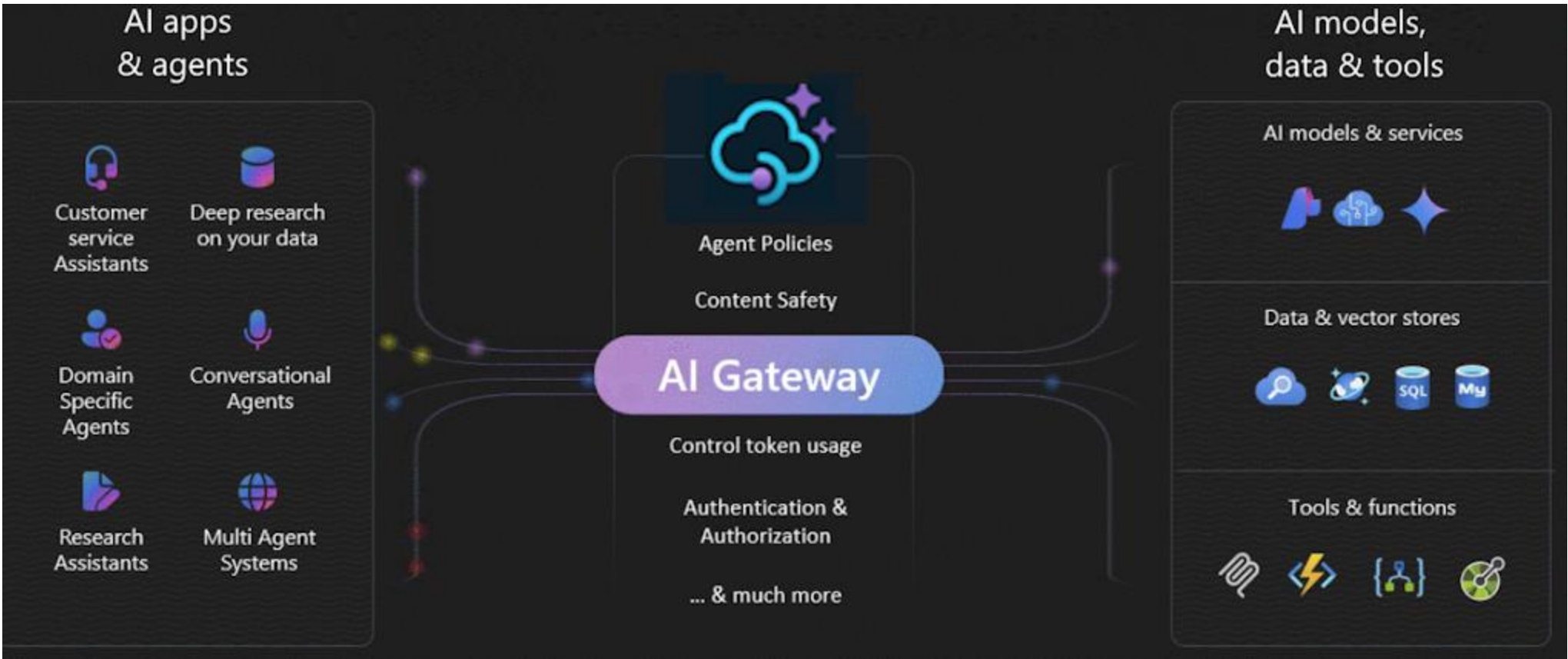
Intégrations avec Foundry

- 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 trafic Entrant et Sortant

AI Gateway



The background is a solid red color. On the left side, there are several concentric, curved white lines that sweep across the frame from the top-left towards the bottom-right. These lines vary in thickness and style, with some being solid and others dashed. The overall effect is a dynamic, modern aesthetic.

Conclusion



The background is a solid red color. On the left side, there are several concentric, semi-circular white lines that curve from the top left towards the bottom left. On the right side, there are several parallel white lines that curve from the top right towards the bottom right. The text is positioned on the right side of the slide.

**Merci !
Question?**