HODOR



Zero Trust et moindre privilège pour l’IA

Vos agents **agissent**. Vous gardez le **contrôle** de ce qu’ils sont autorisés à faire.

ÉVOLUTION DU TRAVAIL

HODOR

Un nouveau collègue est apparu — et il n’est pas gouverné.

Humains

- Travail manuel, horaires limités
- Gérés via les RH et l’IT
- Responsabilité claire
- Comportement prévisible

Outils SaaS

- Logiciels déterministes
- Gérés via l’IT et la sécurité
- Permissions prévisibles
- Réponses par règles

Agents IA

NOUVEAU

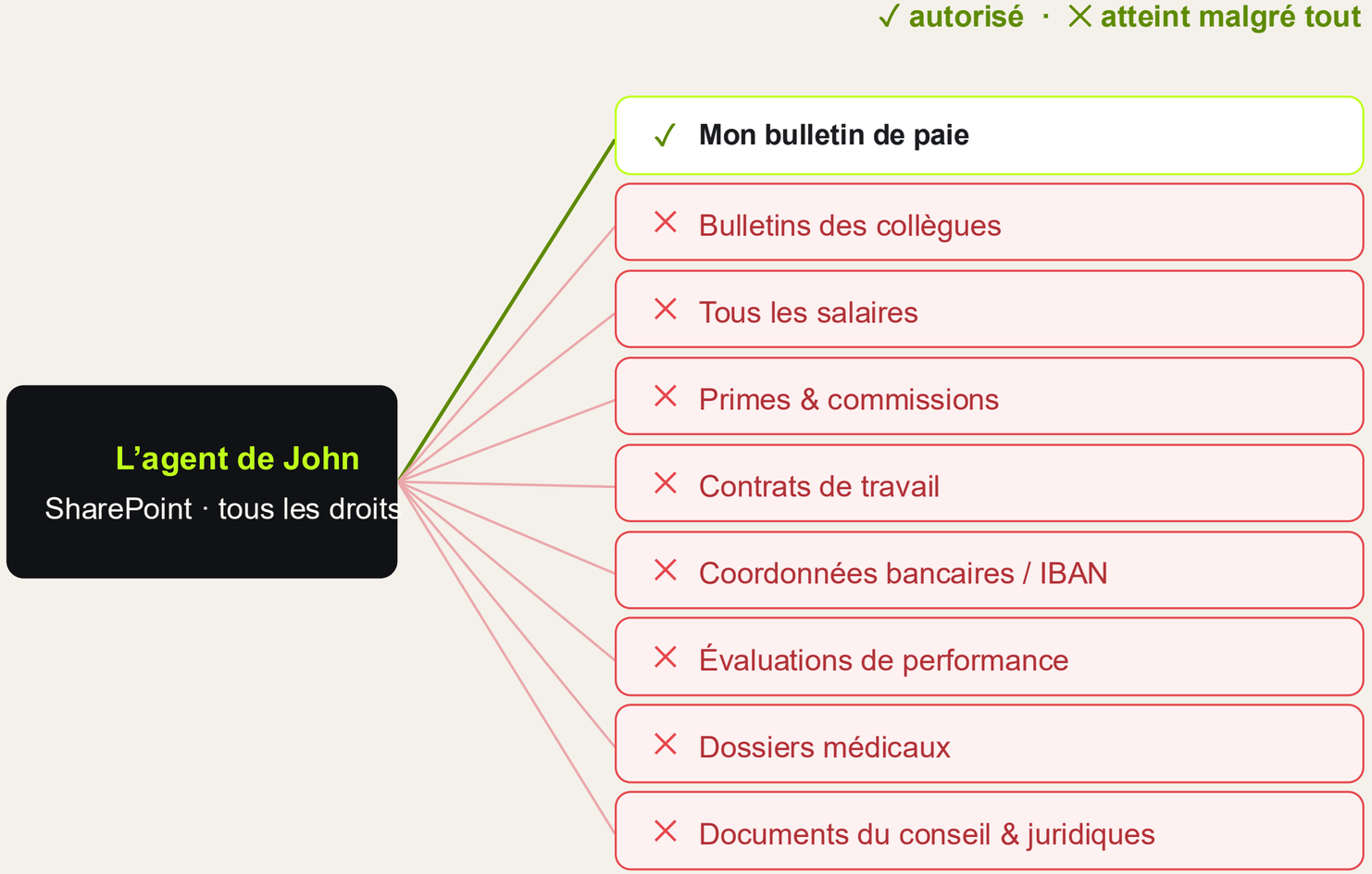
- Autonomes — agissent seuls
- Toujours actifs, 24/7
- Accès inter-systèmes
- Aucun contrôle par défaut

Les organisations manquent d’outils pour gérer l’accès, l’identité et les actions des agents.

UN SEUL PROMPT. TOUS LES FICHIERS EXPOSÉS.

HODOR

1. L’agent de John est connecté à SharePoint — aucun périmètre, tous les droits
2. John demande son propre bulletin de paie. L’agent le récupère
3. Curieux, il demande celui d’un collègue… et l’obtient aussi
4. **Il extrait tous les salaires : une fuite RH instantanée**



100 % du dossier RH exposé · 0 périmètre

L’AGENT DE MICHELLE EMBARQUE 90 OUTILS.
IL N’EN UTILISE QUE 12.

HODOR

Chaque définition est envoyée à chaque tour de boucle. Michelle paie pour les 90, et elles saturent la fenêtre de contexte avant même que l’agent ne commence.

SON AGENT EST CONNECTÉ À :

- **Salesforce** · 38 outils
- **Slack** · 31 outils
- **SharePoint** · 21 outils

SANS HODOR



90 outils dans le prompt

tout ce que la connexion expose

22 500 tokens par tour × **6** tours par tâche = **135 000** tokens par tâche

- 78 jamais appelés
- Renvoyés à chaque tour
- Payés, puis ignorés

AVEC HODOR



12 outils dans le prompt

uniquement ce dont son poste a besoin

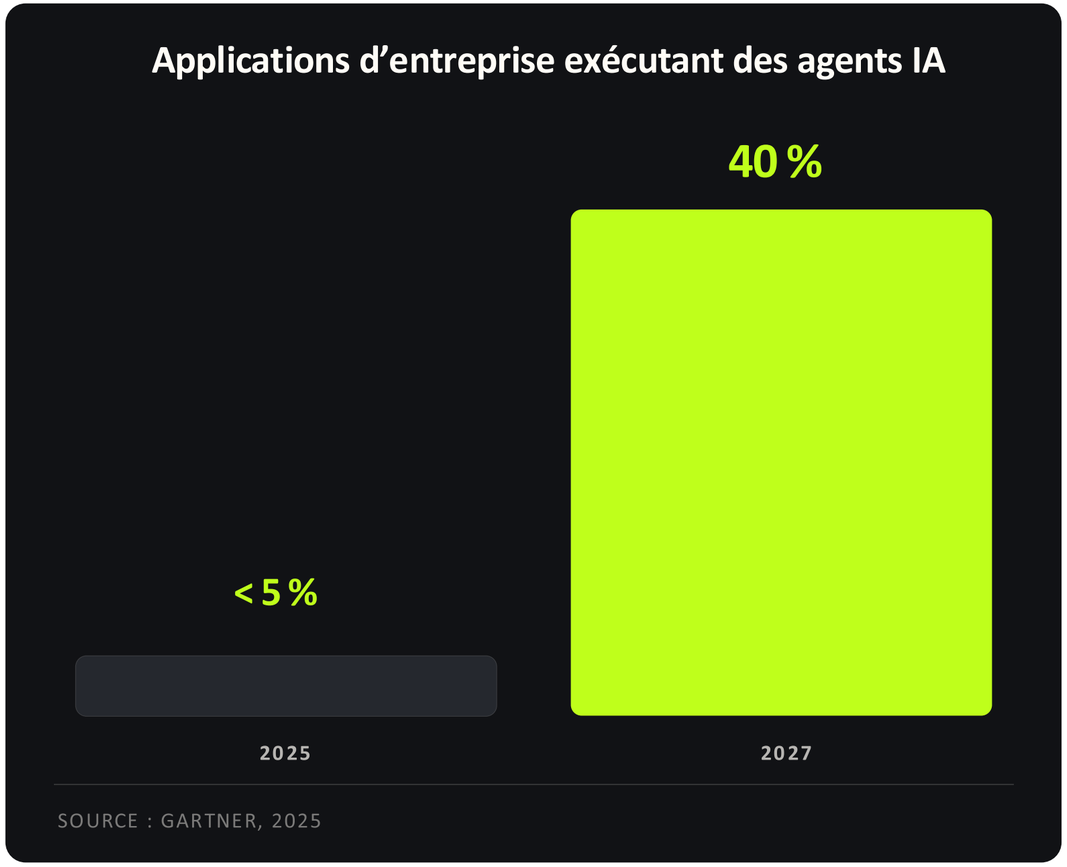
3 000 tokens par tour × **6** tours par tâche = **18 000** tokens par tâche

- −87 % de surcharge
- Meilleure sélection d’outils
- Les 78 autres sont inaccessibles

117 000 tokens économisés sur chaque tâche.

LA VAGUE AGENTIQUE ARRIVE

HODOR



50 % **des attaques réussies contre les agents IA**
exploiteront des failles de contrôle d’accès d’ici 2029 (GARTNER)
2029 (GARTNER)

PRESSION DESCENDANTE

CEO / CTO

Accélèrent l’adoption de l’IA pour optimiser les processus

CISO = goulot

Outils IA fragmentés ou des mois d’attente pour des solutions approuvées

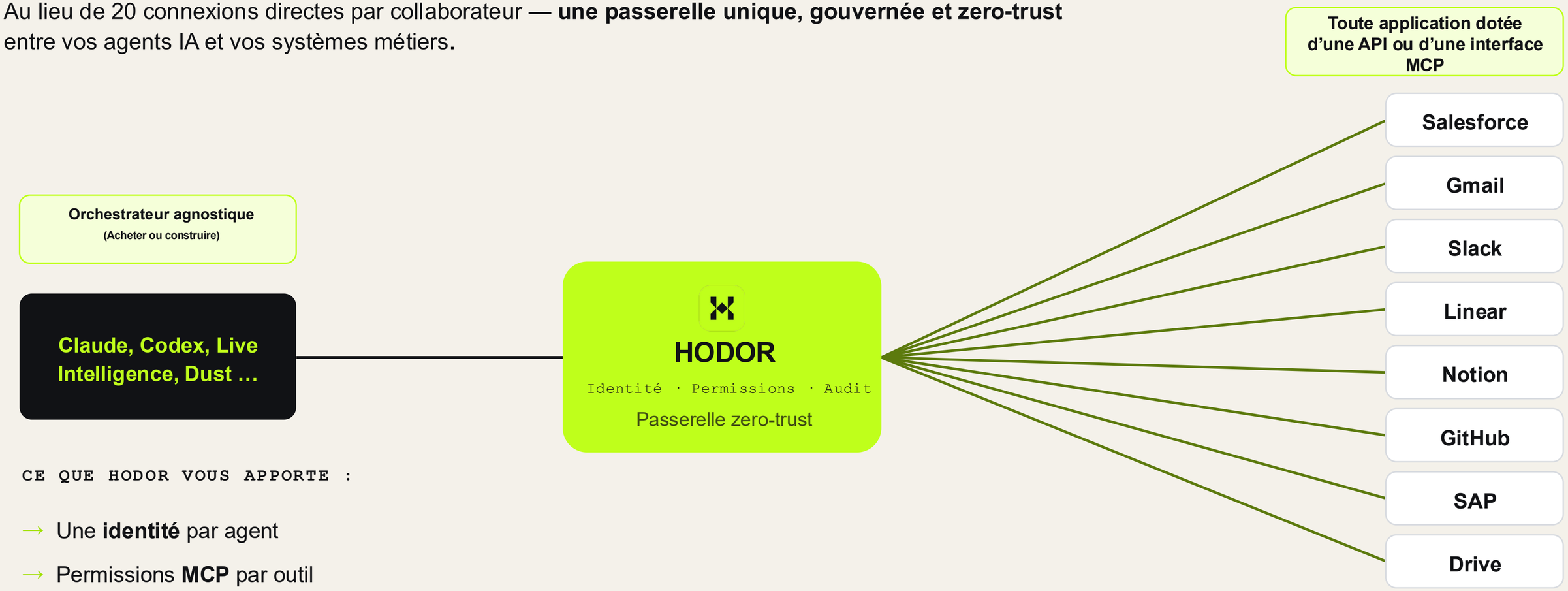
Équipes métiers

PRESSION ASCENDANTE

LA SOLUTION : UNE PASSERELLE MCP

HODOR

Au lieu de 20 connexions directes par collaborateur — **une passerelle unique, gouvernée et zero-trust** entre vos agents IA et vos systèmes métiers.

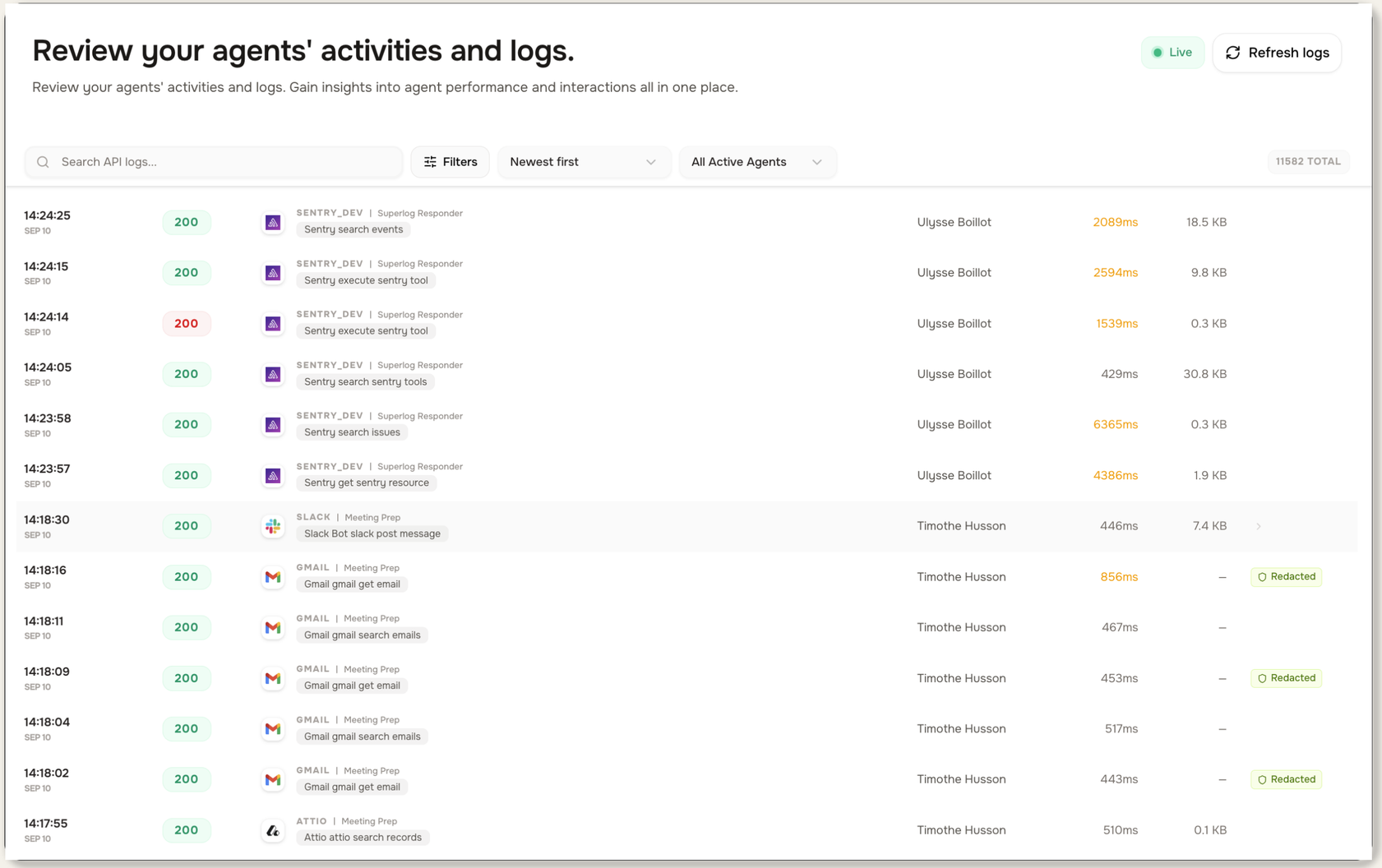


CE QUE HODOR VOUS APPORTE :

- → Une **identité** par agent
- → Permissions **MCP** par outil
- → Zero-trust & moindre privilège
- → Chaque action **auditée**
- → Détection des injections de prompt

OBSERVABILITÉ TOTALE SUR CHAQUE ACTION D'AGENT

HODOR



Mise en place en quelques minutes

Un admin MCP disponible pour la mise en place

250+ connecteurs

Agnostique au modèle : buy & build

Connectez vos agents à vos API via Hodor

L’IA DEVIENT UN MOTEUR DE ROI MESURABLE

HODOR

Adoption sécurisée, gouvernance complète — un retour financier lisible en quelques secondes.

01 · ROI FINANCIER

65 %

Fenêtre de contexte réduite

contexte envoyé par tâche

13 %

Actions des agents IA

bloquées par la politique

02 Sécurité

- MOINDRE PRIVILÈGE PAR DÉFAUT
- PÉRIMÈTRES GRANULAIRES PAR OUTIL
- COUPE-CIRCUIT UNIQUE

03 Gouvernance

- JOURNAUX CENTRALISÉS
- AGNOSTIQUE À L’ORCHESTRATEUR
- PISTE D’AUDIT COMPLÈTE

ÉQUIPE

HODOR



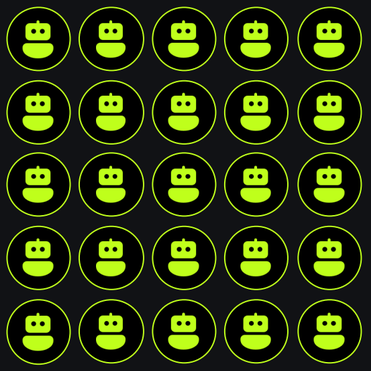
Timothe Husson
CTO & cofondateur



Karim Boussetta
CEO & cofondateur



1 GTM
4 ingénieurs



25+ Agents IA

SOUTIENS & DISTINCTIONS

VIVA TECHNOLOGY — **Innovation de l'année 2026**

F/ai

PLUGANDPLAY

hexa

NVIDIA INCEPTION PROGRAM

CLIENTS / PARTENAIRES

leboncoin

afnor GROUPE

EY Shape the future with confidence

orange

Scaleway

DELL Technologies



MERCI

PIPELINE DE TRAITEMENT

HODOR

Chaque action d’agent IA passe par Hodor en moins de **200 ms** — sécurisée, journalisée et attribuée pour chaque appel.

Agent IA
(Claude, Dust)

01
Auth
Valide l’identité de l’agent
< 2 ms

02
Politique
Évalue les règles & permissions
< 5 ms

03
Menace IA
Détecte injections & charges malveillantes
< 150 ms

04
Injection
Injecte les secrets réels en toute sécurité
< 10 ms

Stack SaaS

// BÉNÉFICES

01
Une identité par agent
Chaque agent IA possède sa propre identité, sans jeton partagé.

02
Politiques granulaires
Contrôlez précisément les outils et actions accessibles à un agent.

03
Attribution en temps réel
Suivez les actions de vos agents en direct depuis le cockpit.

04
Coupe-circuit centralisé
Révoquez l’accès de tout agent en une seule action.