

Workday lance Agent Passport pour sécuriser et gouverner les agents IA à grande échelle

*Agent Passport évalue chaque agent au regard de référentiels reconnus du secteur, notamment l'OWASP LLM Top 10, le NIST AI RMF et MITRE ATLAS*

*Cisco rejoint l'initiative en tant que partenaire de lancement afin de tester de manière indépendante les agents IA de Workday grâce à Cisco AI Defense*

**PARIS, 18 juin 2026 - Workday DevCon - [Workday, Inc.](https://www.workday.com)** (NASDAQ : WDAY), la plateforme IA d'entreprise pour les ressources humaines, la finance et les systèmes d'information, annonce Agent Passport, une solution qui teste et vérifie chaque agent d'IA, qu'il ait été développé par Workday ou par un tiers, avant sa mise en production, puis en assure une surveillance continue. Chaque attestation est associée à un référentiel public reconnu du secteur, tel que l'OWASP LLM Top 10, le NIST AI RMF ou MITRE ATLAS. Les équipes de sécurité disposent ainsi d'une preuve signée et vérifiable des contrôles réalisés sur chaque agent ainsi que de l'organisme ayant effectué ces évaluations.

Agent Passport fournit aux entreprises une preuve vérifiée attestant que chaque agent a été évalué face aux risques les plus critiques avant sa mise en production, notamment les injections d'instructions, les contournements de garde-fous et détournements d'objectifs, l'extraction des consignes système, les fuites de données collaborateurs et la génération de contenus dangereux. Chaque résultat est associé à un référentiel public reconnu et signé par le partenaire ayant réalisé les tests, garantissant ainsi un niveau d'indépendance, d'auditabilité et de comparabilité entre les agents issus de fournisseurs différents.

Lorsqu'un agent tente d'exécuter une tâche, Agent Passport en supervise le comportement en temps réel et autorise, bloque ou redirige l'action selon les règles définies par l'entreprise. Si un problème est détecté, une simple révocation permet d'interrompre, de limiter ou de restreindre automatiquement l'activité des agents concernés conformément aux politiques de sécurité en vigueur.

*« Les agents d'IA prennent désormais en charge les activités les plus sensibles de l'entreprise, qu'il s'agisse de l'intégration des collaborateurs ou du traitement des paiements. Un seul agent insuffisamment sécurisé peut provoquer des fuites de données, compromettre la conformité et exposer l'entreprise à une crise de réputation », déclare **Dean Arnold, Vice President, AI Platform, Workday.** « Agent Passport permet aux entreprises d'avoir l'assurance que chaque agent a été testé et vérifié de manière indépendante, tout en leur donnant la capacité d'en interrompre immédiatement l'activité à l'échelle de l'organisation dès qu'un risque est identifié. »*

#### **Une norme commune, élaborée avec les leaders de l'industrie**

La plupart des plateformes proposant des tests de sécurité des agents réalisent elles-mêmes ces évaluations, ce qui signifie que les clients reçoivent une validation de sécurité délivrée par le même fournisseur que celui ayant développé l'agent. Workday a su instaurer une relation de confiance solide avec ses clients grâce à son large portefeuille de solutions d'IA pour les ressources humaines et la finance. L'entreprise renforce cette confiance en s'appuyant sur des standards ouverts et sur des partenariats avec des acteurs de référence de la sécurité agentique et de la conformité réglementaire. Les évaluations sont ainsi réalisées de manière indépendante et transparente, et les résultats peuvent être comparés entre des agents issus de fournisseurs différents.

Le rapport associé à chaque agent repose sur trois niveaux. Le premier couvre les grands piliers de confiance définis et maintenus à jour par Workday, notamment la protection contre les attaques, le comportement sécurisé en phase d'exécution et la supervision humaine. Le deuxième correspond à un ensemble de critères précis et vérifiables associés à des référentiels publics, tels que la résistance à des techniques d'attaque connues. Le troisième rassemble les résultats signés par le partenaire ayant réalisé les tests, délivrés par des tiers de confiance reconnus, à commencer par Cisco.

Chaque contrôle étant associé à un référentiel public, les équipes de sécurité peuvent, pour la première fois, comparer des agents issus de fournisseurs différents sur des bases communes. Si deux agents obtiennent la même validation délivrée par des partenaires distincts, les entreprises ont l'assurance qu'ils ont été évalués selon les mêmes exigences.

#### **Des attestations indépendantes délivrées par les spécialistes de la sécurité agentique**

[Cisco](https://www.cisco.com) est le partenaire de lancement d'Agent Passport. Grâce à Cisco AI Defense, l'entreprise évalue de manière indépendante les agents d'IA exécutés dans Workday au regard des principaux référentiels de sécurité avant leur déploiement, puis assure leur protection continue en phase d'exécution contre les injections d'instructions, les fuites de données, les contournements de garde-fous et les actions à risque.

Cisco AI Defense vérifie notamment que l'agent résiste aux tentatives de modification de ses consignes, empêche la divulgation

de ses instructions internes, protège les informations sensibles des collaborateurs contre toute fuite et bloque les réponses dangereuses ou non conformes aux politiques de l'entreprise avant qu'elles ne parviennent à un utilisateur. Ces validations sont essentielles pour tous les agents, mais elles sont incontournables pour ceux qui traitent des données de paie, d'avantages sociaux ou de gestion financière.

« Les agents seront bientôt omniprésents dans les entreprises et cette généralisation ne pourra se faire que si les équipes de sécurité disposent d'une preuve claire, signée et vérifiable des contrôles réalisés sur chacun d'eux », explique **DJ Sampath, Senior Vice President et General Manager, AI Software & Platform, Cisco**. « Cisco AI Defense a précisément été conçu pour répondre à ce besoin de validation et nous sommes ravis de collaborer avec Workday afin de sécuriser cette nouvelle main-d'œuvre agentique. »

#### Disponibilité

Agent Passport sera proposé aux premiers clients dans le cadre d'un programme d'accès anticipé au second semestre 2026. Une disponibilité générale est prévue avant la fin de l'année 2026.

Le partenariat entre Workday et Cisco est déjà opérationnel. Les fonctionnalités communes seront progressivement déployées au cours des prochains trimestres.

#### Pour en savoir plus

- Découvrez comment [Workday et Cisco](#) collaborent pour définir les standards de la sécurité agentique en entreprise.
- Découvrez comment [Workday Build](#) est désormais prêt pour les agents et permet aux développeurs de concevoir, connecter et vérifier des agents d'IA pour les ressources humaines, la finance et l'informatique.
- Découvrez comment les dernières évolutions de [Workday Data Cloud](#) permettent d'intégrer de manière sécurisée des données RH et financières en temps réel dans des environnements d'IA, d'analyse et des applications existantes, sans reconstruire les chaînes de données.
- Découvrez [les trois approches proposées par Workday](#) pour développer des applications et des agents d'IA tout en conservant la maîtrise et la sécurité des environnements.

#### À propos de Workday

Workday agit au cœur des fonctions les plus critiques de l'entreprise : les ressources humaines, la finance et les systèmes d'information, où le droit à l'erreur est très limité. En associant étroitement l'intelligence artificielle au contexte, à un cadre sécurisé et à des processus de confiance qui font fonctionner les entreprises, Workday va au-delà d'une IA qui assiste les utilisateurs, en déployant des agents capables d'agir et de produire des résultats concrets. Plus de 11 500 entreprises dans le monde, dont plus de 65 % des entreprises du Fortune 500, font confiance à Workday. Pour en savoir plus, rendez-vous sur [le site de Workday](#).

#### Méthodologie

L'étude a été réalisée en ligne en mars et avril 2026 par **Hanover Research**, pour le compte de la **Workday Foundation**. Les répondants ont été recrutés via un panel. L'analyse repose sur un échantillon final de **2 150 répondants**, après nettoyage des données et contrôle qualité. Les personnes interrogées sont des salariés à temps plein travaillant dans des organisations de plus de **3 500 collaborateurs**. Elles utilisent activement l'intelligence artificielle **au moins une fois par semaine** dans le cadre de leurs fonctions ou encadrent directement des collaborateurs qui utilisent l'IA. **Échantillons** : résultats issus du **Human Connection Workplace Index** de Workday. Échantillon France : **n = 200**. Échantillon EMEA (Royaume-Uni, France et Allemagne) : **n = 600**. Échantillon mondial : **n = 2 150 salariés à temps plein**, répartis dans **sept pays**, travaillant au sein d'organisations de plus de **3 500 collaborateurs** et utilisant activement l'intelligence artificielle.

© 2026 Workday, Inc. Tous droits réservés. Workday et le logo Workday sont des marques déposées de Workday, Inc. Toutes les autres marques et noms de produits sont des marques commerciales ou déposées de leurs détenteurs respectifs.

#### Contact presse

[Workday@rumeurpublique.fr](mailto:Workday@rumeurpublique.fr)

---

<https://fr-fr.newsroom.workday.com/2026-06-18-Workday-lance-Agent-Passport-pour-securiser-et-gouverner-les-agentes-IA-a-grande-echelle>