Comment contrôler les agents d'IA et les autres identités non humaines

Grâce à une stratégie de sécurité moderne, axée sur l'identité

Les identités non humaines peuvent améliorer les performances de l'entreprise, mais au prix d'un niveau de risque plus élevé.

L'utilisation d'identités non humaines pour les communications entre machines, services et agents d'IA s'est rapidement généralisée dans un certain nombre de secteurs, et pour cause : elles dopent les capacités de base des entreprises en matière de collaboration, d'innovation et de productivité.

Cependant, si les identités non humaines préparent les entreprises à un avenir optimisé par l'IA, elles constituent également un nouveau vecteur d'attaque. Les agents d'IA, en particulier, engendrent des vulnérabilités uniques car ils se comportent différemment des utilisateurs humains et des logiciels traditionnels, et nécessitent souvent un accès à des données ultrasensibles. Ces caractéristiques en font des cibles de choix pour les acteurs malveillants, mais compliquent leur sécurisation pour les entreprises.

En l'absence d'une approche de sécurité unifiée, axée sur l'identité, les entreprises qui utilisent les identités non humaines augmentent considérablement leurs risques en négligeant souvent de sécuriser une surface d'attaque qui ne cesse de s'étendre.

Dans certaines entreprises :

Les identités non humaines sont désormais **50 fois plus nombreuses que les identités humaines.**

Forbes

46 % des entreprises ont subi une compromission d'identifiants ou de comptes d'identités non humaines au cours de l'année écoulée (et **26%** le soupçonnent).

TechTarget ESG

Une nouvelle génération de risques

L'utilisation des identités non humaines a augmenté parallèlement à l'utilisation croissante des services et des plateformes cloud telles qu'AWS de manière à étendre leur utilisation aux outils d'IA générative, à l'IA, à l'automatisation et aux workflows numériques. Les systèmes d'entreprise doivent pouvoir interagir de manière sécurisée et efficace sans nécessiter une surveillance humaine constante. Les identités non humaines, notamment les comptes de service utilisés par les agents d'IA, rendent ces interactions possibles en permettant aux applications et aux services de s'authentifier entre eux, ce qui facilite l'automatisation des tâches, l'échange de données et les processus opérationnels complexes qui seraient sans cela impossibles à gérer par le personnel, ou du moins extrêmement chronophages.

Compte tenu de la grande vulnérabilité des identités non humaines, les entreprises doivent envisager des stratégies capables d'atténuer ce nouveau risque. Si les secrets, clés et/ou tokens utilisés par ces identités pour s'authentifier tombent entre de mauvaises mains, des adversaires pourraient obtenir un accès quasi illimité aux applications et données sensibles.

En particulier lorsque des identités non humaines sont utilisées avec des outils d'IA générative, tels que les chatbots et les assistants numériques, l'entreprise peut être exposée à une multitude de nouvelles menaces en raison de l'incapacité de ces outils à fournir un contexte utilisateur :

Injection d'invites et empoisonnement des données

Les cybercriminels peuvent manipuler les invites ou injecter du contenu malveillant, ce qui peut amener les outils d'IA générative à générer des informations inappropriées ou inexactes à partir de leurs sources de données.

Accès « fantôme » et déplacement latéral

Les acteurs malveillants peuvent exploiter les outils d'IA générative pour accéder à des contenus sensibles à partir de systèmes connectés (par exemple, Salesforce, Jira, wikis internes) interrogés par ces outils.

Exposition excessive des données

Les outils d'IA générative ont souvent accès à d'importants volumes de données sensibles. Si le contexte utilisateur n'est pas correctement transmis aux sources de données sous-jacentes, les utilisateurs pourraient accéder à des informations que leur rôle ne leur donne pas le droit de consulter.

51 % des entreprises ont déployé des agents d'IA.

PagerDuty

Seuls **15 %** des équipes sécurité s'estiment capables de prévenir les brèches liées aux identités non humaines.

Cloud Security Alliance

Le risque particulier posé par les agents d'IA

Les risques et avantages potentiels des identités non humaines sont particulièrement évidents dans le cas des agents d'IA. En raison de leur capacité à agir en toute autonomie pour le compte de personnes et d'entreprises, les agents d'IA permettent d'atteindre des niveaux d'efficacité opérationnelle et de personnalisation du service client inimaginables jusqu'il y a peu.

Il s'agit malheureusement d'une arme à double tranchant. Les agents d'IA dépendent des données, des ressources et des retours pour s'améliorer continuellement, ce qui nécessite un accès autorisé et authentifié. Cet accès étendu fait identités non humaines une cible particulièrement prisée par les acteurs malveillants.

Dans de nombreuses entreprises, les identités non humaines et machines sont peu, voire pas du tout surveillées. Trop souvent, ces identités possèdent des autorisations excessives, ne sont jamais renouvelées ou restent actives une fois leur finalité atteinte, les rendant vulnérables à une exploitation malveillante. Dans les environnements IT et de sécurité où les fonctions d'identité sont dispersées dans différents systèmes et applications, ces vulnérabilités ont tendance à passer inaperçues jusqu'à ce qu'il soit trop tard.

L'identité représente une vulnérabilité, la sécurité de l'identité est la solution.

En conclusion :

La meilleure défense contre les vulnérabilités liées aux identités non humaines commence par éliminer les systèmes d'identité fragmentés qui nuisent à la visibilité et créent des failles en termes d'authentification. En unifiant les systèmes d'identité au sein d'une plateforme unique, les entreprises peuvent mieux contrôler leurs identités non humaines tout en optimisant l'administration. Les plateformes de gestion des identités modernes vous permettent de mettre en œuvre cette approche unifiée de la sécurité.

C'est particulièrement important lors du développement de solutions d'IA générative sur Amazon Bedrock, où un déploiement rapide doit s'accompagner d'un contrôle d'accès sécurisé. Okta représente le point de contrôle des identités pour votre environnement Bedrock en veillant à ce que seuls les utilisateurs et les agents d'IA autorisés puissent accéder aux modèles et services sensibles.

Avec Okta

Okta Platform offre une approche robuste et simplifiée de la gestion des identités non humaines et machines. En unifiant la gestion des identités de votre entreprise au sein d'un écosystème de sécurité des identités, Okta vous aide à éliminer les angles morts et vous offre une visibilité complète sur l'emplacement de vos identités non humaines et sur les ressources auxquelles elles peuvent accéder.

Identity Security Posture Management

- Assure une surveillance et une analyse continues des risques liés aux identités non humaines.
- Détecte automatiquement les comptes de service locaux non fédérés et signale les identités non humaines à risque.
- Détecte les failles MFA et l'utilisation abusive d'identifiants pour les identités machines.
- Vérifie la conformité grâce à une mise en correspondance avec les frameworks et propose des workflows de remédiation guidés pour les problèmes de sécurité liés aux identités non humaines.

Okta Privileged Access

- Gère de manière sécurisée les mots de passe des comptes de service et applique des politiques définissant les identités autorisées à accéder aux ressources, ainsi que la durée de cet accès.
- Renouvelle automatiquement les secrets pour prévenir l'exposition des identifiants à validité prolongée.
- Audite et surveille les identités (humaines ou non) ayant déconnecté le compte.

Intégrations de sécurité des identités

Il s'agit d'intégrations de sécurité avancées avec les applications SaaS qui permettent d'éviter tout accès prolongé des identités non humaines et protègent celles-ci dans l'ensemble de votre écosystème.

- **Gestion du cycle de vie et des droits :** automatisez le provisioning et le déprovisioning des identités non humaines, et assurez ainsi un accès en flux tendu (JIT).
- **Application unifiée du SSO et des politiques :** étendez le SSO et les politiques de sécurité aux comptes de service et aux identités machines.
- **Automatisation des workflows et clôture de session :** permet d'éviter les identités non humaines orphelines en automatisant l'offboarding et la clôture de session.

Okta + Amazon : la solution pour sécuriser l'IA générative

En fournissant une assistance pilotée par l'IA générative aux développeurs utilisant AWS, Amazon Q transforme la manière dont les développeurs, les analystes en veille économique, les agents des centres de contact et d'autres équipes clés accomplissent leur travail.

Désormais, en combinant l'efficacité, la productivité et la qualité de l'expérience client d'Amazon Q et la suite d'outils de sécurité adaptés à l'IA d'Okta, les entreprises peuvent intégrer l'IA générative à leurs opérations de base en limitant leur exposition aux nouvelles sources de risques.

Implémentation sécurisée de l'IA générative

Protégez les données stockées dans Amazon Q contre tout accès non autorisé grâce à la sécurité des identités conçue pour les entreprises d'Okta, tout en rationalisant la gestion des identités à l'aide des outils de gestion du cycle de vie automatisés d'Okta.

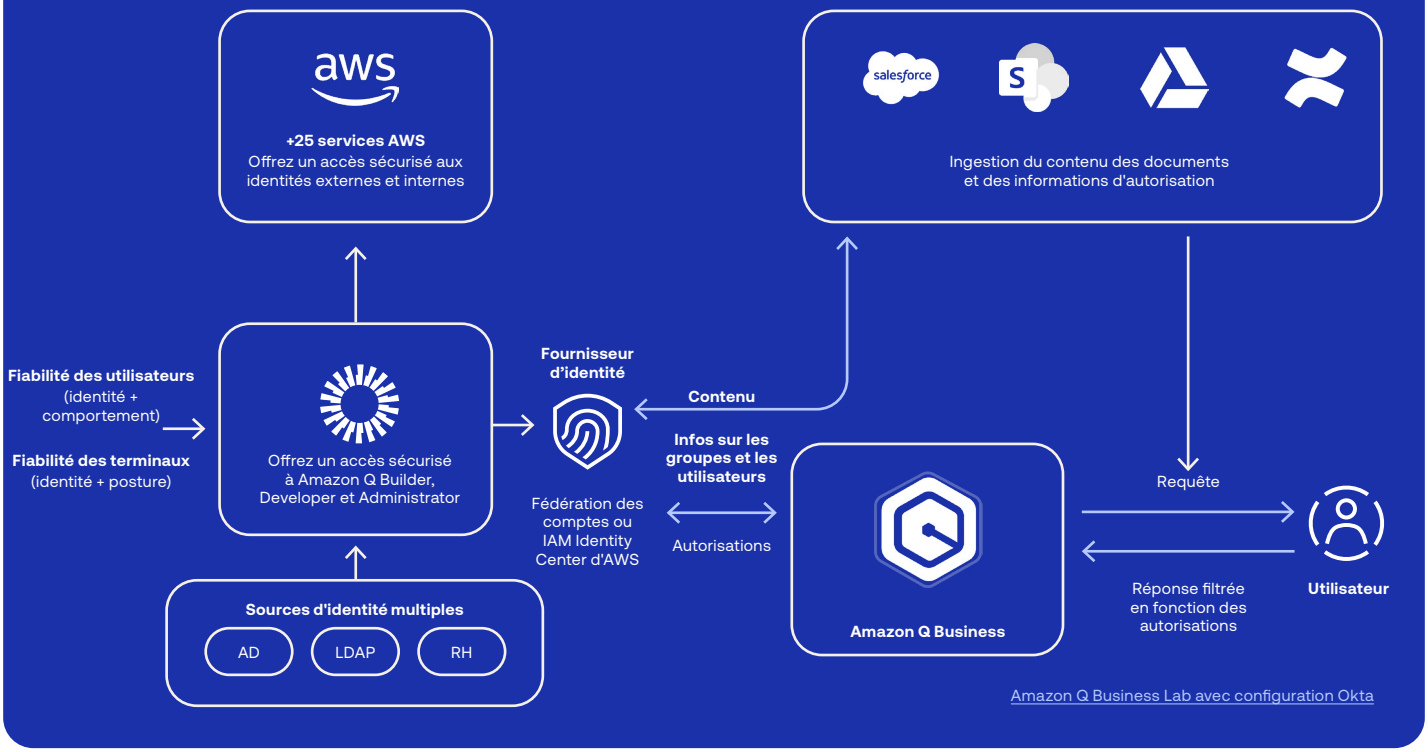
Optimisation de la productivité

Donnez à vos équipes les moyens d'être plus créatives et productives grâce à l'assistance d'Amazon Q. Générez des résumés de réunion, créez du contenu et exécutez des tâches sans exposer vos données à de nouveaux risques.

Accès transparent

Offrez un accès simplifié et sécurisé grâce à des autorisations basées sur les rôles pour accéder à des ensembles de données spécifiques. Maîtrisez mieux vos coûts en octroyant des abonnements sur demande ou selon des critères automatisés.

Profitez de toutes les opportunités offertes par Amazon Q Business avec Okta



Mettez à profit vos identités non humaines, en toute sécurité

En très peu de temps, l'IA est passée d'un éventuel atout pour l'avenir à une nécessité immédiate. La capacité à tirer pleinement parti des outils modernes tels que les agents d'IA est un enjeu crucial pour les entreprises qui souhaitent rester concurrentielles. Toutefois, l'utilisation efficace des identités non humaines dépend aussi de la capacité de votre entreprise à les sécuriser.

Avec Okta, les workflows optimisés par l'IA s'exécutent sur une plateforme d'identité unifiée qui élimine la fragmentation et les risques qu'elle comporte, et renforce les bases de votre environnement de sécurité, tout cela grâce à l'écosystème de sécurité des identités d'Okta.

C'est pourquoi AWS et Okta collaborent afin de fournir des bases sûres pour la prochaine génération d'automatisation intelligente. Que vous déployiez des agents d'IA dans AWS ou que vous tiriez parti d'Amazon Q au sein de vos équipes, la plateforme d'identité d'Okta vous aide à garantir la sécurité, la gouvernance et l'auditabilité de ces identités.

Vous souhaitez en savoir plus sur l'unification de votre stratégie de sécurité grâce à l'écosystème de sécurité des identités d'Okta ? Prenez contact avec notre équipe et découvrez Okta Platform en action.