Comment la prolifération des identités masque les menaces (et comment y remédier)

Avec une stratégie de sécurité moderne, axée sur l'identité

Votre entreprise grandit et évolue. Votre profil de risque aussi.

Pour améliorer l'agilité et la collaboration à distance, les entreprises concurrentielles comme la vôtre dépendent désormais d'un écosystème de solutions de pointe. Ces piles technologiques soigneusement constituées profitent à l'entreprise elle-même, mais aussi à ses clients et partenaires. Par contre, elles vous exposent également à certains risques.

L'essor des agents d'IA et des systèmes agentiques ne fait qu'aggraver le problème. Si ces agents offrent de nouvelles opportunités d'améliorer l'efficacité et la prestation de services, ils étendent également la surface d'attaque et entraînent de nouveaux risques qui exigent d'autres approches en matière de sécurité.

En raison de la fragmentation des environnements IT, les identités humaines et non humaines sont dispersées dans une multitude de systèmes et infrastructures.

La visibilité de la posture de sécurité de votre entreprise en pâtit et le risque d'être victime de brèches coûteuses augmente. Pour protéger les informations sensibles de votre entreprise et lui permettre d'embrasser pleinement l'ère de l'IA, il vous faut avant tout bénéficier d'une visibilité de bout en bout et en temps réel sur toutes les menaces d'identité et renforcer votre capacité à y remédier en temps réel.

Les agents d'IA n'ont pas eu à passer des entretiens d'embauche et pourtant, ils font partie de vos effectifs

Pour de nombreuses entreprises, l'adoption des agents d'IA manque cruellement de rigueur. Ces agents sont créés et déployés à un rythme que les équipes IT et sécurité n'arrivent pas à suivre. Elles n'ont parfois aucun moyen d'identifier les agents actifs, les ressources auxquelles ils peuvent accéder, ou encore leur comportement. Du point de vue de la sécurité, l'avènement des agents d'IA a entraîné l'apparition d'un nombre croissant de zones d'ombre, et donc de failles de sécurité, dans l'environnement d'entreprise.

L'adoption de l'IA dépasse souvent le dispositif de sécurité et de gouvernance en place

91 % des entreprises utilisent déjà des agents d'IA*

Par contraste, seuls **44 %** de ces entreprises ont mis en place une stratégie de gouvernance**

*Okta, AI at Work 2025 : sécurisation des agents d'IA

**The Times, 2025

Une sécurité des identités unifiée pour une meilleure visibilité sur les identités humaines et non humaines

Les piles technologiques et de sécurité fragmentées génèrent un volume considérable de données sur les risques et les menaces potentielles. Vos équipes se retrouvent contraintes de passer en revue les logs et d'identifier elles-mêmes les risques à traiter en priorité, ce qui rend la remédiation en temps réel quasi impossible.

En d'autres termes, la fragmentation des identités empêche d'identifier les vulnérabilités majeures de votre entreprise. Elle ralentit la détection et la réponse aux menaces, donnant aux acteurs malveillants tout loisir d'infliger des dommages importants à l'aide d'identifiants volés. Pire encore, si ces agents d'IA sont insuffisamment sécurisés, ils peuvent exposer ou partager par inadvertance des informations sensibles. Sans une visibilité complète sur les ressources auxquelles les agents peuvent accéder et la configuration de leurs privilèges d'accès, les entreprises s'exposent à des risques incontrôlables dans un paysage de menaces toujours plus sophistiqué.

Pour mieux gérer ces risques, les processus et systèmes d'identité doivent être unifiés au sein d'une seule plateforme adaptée à l'IA pour renforcer l'efficacité et le contrôle. Cette approche unifiée en matière d'identités peut être mise en œuvre grâce aux plateformes de gestion des identités avancées. En étendant cette approche unifiée aux clients et aux partenaires commerciaux, et plus seulement au personnel, les entreprises peuvent éliminer le cloisonnement des données des collaborateurs et des clients afin de garantir une expérience de connexion fluide et sécurisée qui renforce la confiance dans la marque.

Des résultats concrets avec Okta

Okta Platform permet d'adopter une approche robuste et extrêmement simplifiée de la sécurité axée sur l'identité. Grâce à un large éventail de produits et fonctionnalités, Okta offre une protection en temps réel de bout en bout contre les menaces sophistiquées, sans alourdir vos workflows ou nuire à l'expérience utilisateur.

Comment bénéficier d'une visibilité complète sur toutes les menaces d'identité

(et favoriser la remédiation en temps réel)

Une remédiation des risques efficace commence par une vue centralisée de votre profil de risque qui synthétise les signaux de sécurité en informations exploitables en temps réel.

Du point de vue de la gestion des identités clients, vous protégez ainsi les données sensibles en accélérant la détection et la réponse aux menaces telles que l'usurpation de compte, la fraude et la compromission des identifiants.

De plus, la remédiation ne peut pas se reposer sur des actions manuelles et lentes. Votre solution d'identité doit associer des informations en temps réel à des workflows de remédiation automatisés qui peuvent être adaptés aux besoins spécifiques de votre entreprise.

Tout cela est possible grâce à une identité unifiée. En intégrant des mécanismes résistants au phishing avec un moteur d'analyse des risques axé sur l'identité, vous bénéficiez d'une visibilité en temps réel sur les menaces émergentes. Qu'il s'agisse de protéger vos collaborateurs ou vos clients, un tel niveau de protection est indispensable dans le paysage des menaces actuel — et seule une approche unifiée de l'identité peut y parvenir.

Bénéficiez d'une visibilité totale sur les principaux cas d'usage :

- Onboarding sécurisé des collaborateurs
- Protection continue pour tous les groupes d'utilisateurs
- Sécurisation des environnements hybrides et on-premise
- Déconnexion des utilisateurs compromis

Onboarding sécurisé des collaborateurs

Les approches classiques en matière d'identité imposent souvent aux équipes IT d'utiliser des processus manuels d'onboarding/offboarding, à la fois chronophages et sujets à erreur.

Les plateformes d'identité unifiées modernes permettent aux nouveaux utilisateurs (collaborateurs, prestataires, partenaires ou autres identités externes) d'accéder facilement et en toute sécurité aux outils dont ils ont besoin, sans délai ni faille de sécurité.

Automatisation du provisioning/ déprovisioning sécurisé pour faire gagner du temps aux équipes IT

Déploiement du MFA pour vérifier les identités des collaborateurs en toute sécurité lors de l'onboarding

Gestion des accès à l'ensemble des applications et systèmes pour chaque collaborateur, via un tableau de bord centralisé

Simplifiez l'onboarding sans sacrifier la sécurité :

SANTÉ : provisioning rapide du personnel infirmier itinérant et d'autres collaborateurs externes, sans risque d'octroyer des privilèges excessifs

COMMERCE DE DÉTAIL : onboarding simplifié des saisonniers et d'autres postes à rotation importante pour le renfort rapide et sécurisé de votre personnel

ENSEIGNEMENT : octroi d'un accès sécurisé et basé sur les rôles aux nouveaux étudiants, enseignants et personnels administratifs dès le premier jour

Déploiement d'une protection continue pour tous les groupes d'utilisateurs

Lorsque l'identité est fragmentée au sein de l'entreprise, le manque de visibilité centralisée complique considérablement la détection et la réponse aux menaces en temps réel.

Avec Okta, les entreprises peuvent détecter, répondre et neutraliser les menaces d'identité dans l'ensemble des groupes d'utilisateurs gérés (dont les collaborateurs, les clients et les partenaires commerciaux, pour les identités humaines et non humaines) grâce à des politiques d'authentification forte, basées sur les risques, et à des outils intelligents de réponse aux menaces.

Unification des systèmes d'identité, tout en séparant les utilisateurs en groupes distincts pour des raisons de sécurité

Isolement et remédiation des comptes ou terminaux compromis en temps réel

Gestion sécurisée des agents d'IA et révocation de leur accès en temps réel en cas de comportement à risque

Adoptez une stratégie cohérente pour la protection des identités humaines et non humaines :

SANTÉ : attribuez et appliquez facilement des contrôles d'accès basés sur les groupes d'utilisateurs et résolvez les brèches potentielles en temps réel.

COMMERCE DE DÉTAIL : déployez en toute sécurité des assistants d'achat pilotés par l'IA sans risquer de mettre en péril la confidentialité des clients (ou des informations commerciales sensibles).

Sécurisation des environnements hybrides et on-premise

Les environnements hybrides complexes exigent une approche IAM qui simplifie la gestion distribuée des identités et des politiques de sécurité, tout en étendant les mesures de sécurité avancées aux identités et ressources on-premise.

Politiques d'authentification basées sur les risques étendues aux applications et à l'infrastructure on-premise, pour une sécurité adaptative déployée dans tout l'environnement

Contrôle des accès unifié et élimination des privilèges permanents dans les environnements distribués

Détection, réponse et neutralisation des menaces d'identité pour l'ensemble des terminaux gérés

Simplifiez et renforcez la sécurité des identités :

SANTÉ : protégez les données des patients, tout en mettant les informations et les ressources critiques à la disposition des professionnels de la santé, où qu'ils se trouvent, grâce à une solution IAM cloud.

COMMERCE DE DÉTAIL : étendez les principes de sécurité cloud des identités aux systèmes spécialisés on-premise afin de renforcer la sécurité sur site.

Avec Okta

Grâce à une approche moderne et unifiée en matière de sécurité des identités, une entreprise peut respecter ses obligations de conformité tout en bénéficiant d'une posture de sécurité renforcée, d'effectifs plus productifs, d'une clientèle fidèle, d'une efficacité opérationnelle améliorée et d'une croissance continue de ses activités.

L'écosystème de sécurité des identités d'Okta fournit un framework unifié pour la gestion et la sécurisation de toutes les identités, humaines et non humaines, dans divers environnements : une condition essentielle pour bénéficier d'une visibilité et d'un contrôle complets. En gérant la gouvernance des identités avec Okta, les entreprises peuvent démontrer de façon proactive leur conformité aux exigences réglementaires et parvenir à une posture de sécurité robuste et auditable qui satisfait à la fois les auditeurs internes et les organismes de réglementation externes.

Identity Security Posture Management

Découvrez et corrigez en permanence les risques liés à l'identité et les erreurs de configuration.

Découvrir Identity Security Posture Management

Identity Governance

Appliquez le principe du moindre privilège en automatisant l'évaluation des accès des utilisateurs et leur provisioning.

Découvrir Identity Governance

Okta Privileged Access

Unifiez la gouvernance et le contrôle des accès pour l'ensemble de votre infrastructure critique.

Découvrir Okta Privileged Access

Device Access

Étendez l'authentification passwordless hautement sécurisée d'Okta aux ordinateurs de bureau et aux terminaux, dès la première connexion.

Découvrir Device Access

Identity Threat Protection

Utilisez Okta AI pour détecter et neutraliser automatiquement les menaces d'identité en temps réel.

Découvrir Identity Threat Protection

Une visibilité optimale pour une sécurité efficace

Dans un paysage des risques défini par des menaces toujours plus sophistiquées, l'approche la plus efficace pour un avenir sûr et résilient consiste à adopter une sécurité axée sur l'identité.

Toutefois, pour tenir cette promesse d'une protection renforcée, il vous faut éliminer la fragmentation des identités qui met en péril votre écosystème de sécurité et permet aux menaces de passer entre les mailles du filet.

La plateforme en action :

Regarder la démo

Consulter le site web