eBook

Sécuriser l'identité pour tout protéger

Les trois principes d’une stratégie d’identité moderne pour les personnes, les machines et l’IA

okta

Quelle est la perspective de votre entreprise en ce qui concerne l'identité ?

Pour beaucoup, la première préoccupation qui vient à l'esprit est sa sécurité. Et pour cause : dans un paysage de menaces dominé par le vol d'identifiants, le phishing, le détournement de session et l'essor rapide des systèmes autonomes, l'identité est devenue la principale surface d'attaque. C'est au travers des identités que les attaquants accèdent aux systèmes sensibles, élèvent les privilèges et se déplacent latéralement dans les environnements.

Aujourd'hui, l'identité ne se réfère plus uniquement aux collaborateurs et aux clients. Elle désigne aussi les identités non humaines, les comptes de service, les workloads, les API ainsi que les agents d'IA agissant pour le compte d'utilisateurs. À mesure que les entreprises adoptent des systèmes d'IA et l'automatisation à grande échelle, le nombre d'identités qu'il est impératif de gouverner et de contrôler explose.

Pourtant, de nombreuses entreprises sont encore à la traîne. Elles restent attachées à des modèles de sécurité obsolètes, basés sur le périmètre, et comptent sur des contrôles du réseau et des terminaux incapables d'offrir une protection efficace contre les menaces centrées sur l'identité. Compte tenu du manque de visibilité sur les identités humaines, non humaines et basées sur l'IA, les équipes sécurité en sont réduites à réagir au lieu d'appliquer les politiques de manière proactive.

L'IA impose de nouveaux défis urgents en matière d'identité

Avec le déploiement d'agents d'IA autonomes et de workflows automatisés dans les entreprises, les systèmes agissent de plus en plus pour le compte des utilisateurs. Ces agents extraient des données, exécutent différentes tâches et interagissent avec de multiples applications à la vitesse des machines. Sans une couche d'identités unifiée à même d'assurer la gouvernance de ces actions, les entreprises risquent de voir apparaître une nouvelle catégorie d'identités non gérées, échappant aux contrôles de sécurité traditionnels.

Définition d'une stratégie d'identité avancée

Une stratégie d'identité moderne fait de l'identité la couche de contrôle centrale de votre écosystème technologique. Elle offre une visibilité unifiée sur les activités humaines, non humaines et basées sur l'IA, identifie les vulnérabilités avant qu'elles ne soient exploitées et permet de réagir en temps réel à l'évolution des risques.

Elle donne aussi aux entreprises la possibilité de monter en capacité en toute sécurité. Comme les agents, les services et les applications d'IA disposent de plus en plus d'autonomie, l'identité doit permettre d'implémenter un accès basé sur des politiques et le principe du moindre privilège, sans ralentir pour autant l'innovation.

Cet eBook explique pourquoi l'identité doit être la pierre angulaire de la sécurité à l'ère de l'IA, mais aussi :

- Comment les menaces liées à l'identité évoluent et se multiplient
- Pourquoi les approches traditionnelles de l'identité laissent les entreprises vulnérables
- Les trois principes définissant une stratégie d'identité moderne

La fragmentation de la pile de sécurité de l'entreprise

La dernière décennie a vu une transformation radicale de la pile technologique de l'entreprise. Les services cloud, les applications SaaS, les API et le télétravail ont changé les modes de développement et de fonctionnement des entreprises. Aujourd'hui, les agents d'IA et les systèmes automatisés accélèrent encore cette évolution. Les applications ne servent pas seulement à se connecter, elles sont capables d'agir. Les services ne se limitent plus à stocker des données, ils effectuent diverses tâches. Les systèmes d'IA extraient des informations, déclenchent des workflows et prennent des décisions impliquant de nombreux systèmes.

Dans un tel environnement, l'idée d'une unité technologique régie par un seul contrat de licence d'entreprise n'est plus réaliste. Pour rester compétitives et s'adapter rapidement, les entreprises mettent en place des écosystèmes composés de solutions de pointe. Résultat : une infrastructure puissante et flexible, mais aussi plus complexe.

Les piles technologiques modernes sont extrêmement distribuées et interconnectées. Chaque déploiement d'un nouveau service, application, API, workload ou agent d'IA introduit de nouvelles identités. Ces identités sont présentes dans les clouds, les environnements on-premise, les plateformes SaaS, les applications personnalisées et l'infrastructure. En l'absence d'un contrôle centralisé, l'identité se fragmente au sein d'un réseau complexe de systèmes et d'environnements.

Le cloisonnement des technologies entrave la visibilité

Cette fragmentation pose des risques majeurs de sécurité. Les identités humaines, les comptes de service, les identités machines et les agents d'IA résident souvent dans des systèmes distincts, caractérisés par des politiques incohérentes et une supervision insuffisante. Tous ces facteurs contribuent à une extension de la surface d'attaque et accroissent la probabilité de vol d'identifiants, d'utilisation abusive des tokens et d'élévation de privilèges qui passent souvent inaperçus.

Il est difficile pour les équipes sécurité de bénéficier d'une visibilité unifiée dans un tel environnement. Les journaux sont dispersés, les politiques incohérentes et les identités non humaines se multiplient trop rapidement pour que la gouvernance en place puisse suivre. À mesure que les systèmes d'IA gagnent en autonomie, les entreprises sont confrontées à un nouveau défi : appliquer des contrôles à la vitesse des machines.

De nombreux agents d'IA et autres services automatisés bénéficient d'identifiants persistants et d'un accès étendu à de nombreux systèmes. En l'absence d'une découverte et d'une gouvernance appropriées, ils peuvent conserver des autorisations longtemps après la fin de leur utilisation prévue. Les entreprises se retrouvent alors avec un pool grandissant d'identités à privilèges élevés, agissant dans les différents systèmes sans presque aucune supervision, ce qui élargit la surface d'attaque et aggrave l'impact potentiel d'une brèche.

Les attaquants sont bien conscients de cette transformation. L'identité est devenue le principal vecteur d'attaque, car elle est souvent le point de contrôle le moins unifié. Selon le Data Breach Investigations Report 2024 de Verizon, auquel Okta a participé, 80 % des brèches sont dues à une compromission d'identité. Et le délai moyen nécessaire pour identifier et maîtriser une brèche est toujours de l'ordre de 290 jours.

Il est temps de repenser l'identité

Toutes les entreprises sont conscientes du rôle important de l'identité dans la sécurité, mais jusqu'ici, il s'est souvent limité à l'authentification et au contrôle des accès. Rares sont celles qui accordent à l'identité un autre rôle tout aussi important, à savoir servir de couche de contrôle centrale permettant de bénéficier d'une visibilité, d'une gouvernance et d'une application de politiques à l'échelle de l'entreprise, et ce pour toutes les identités humaines et non humaines.

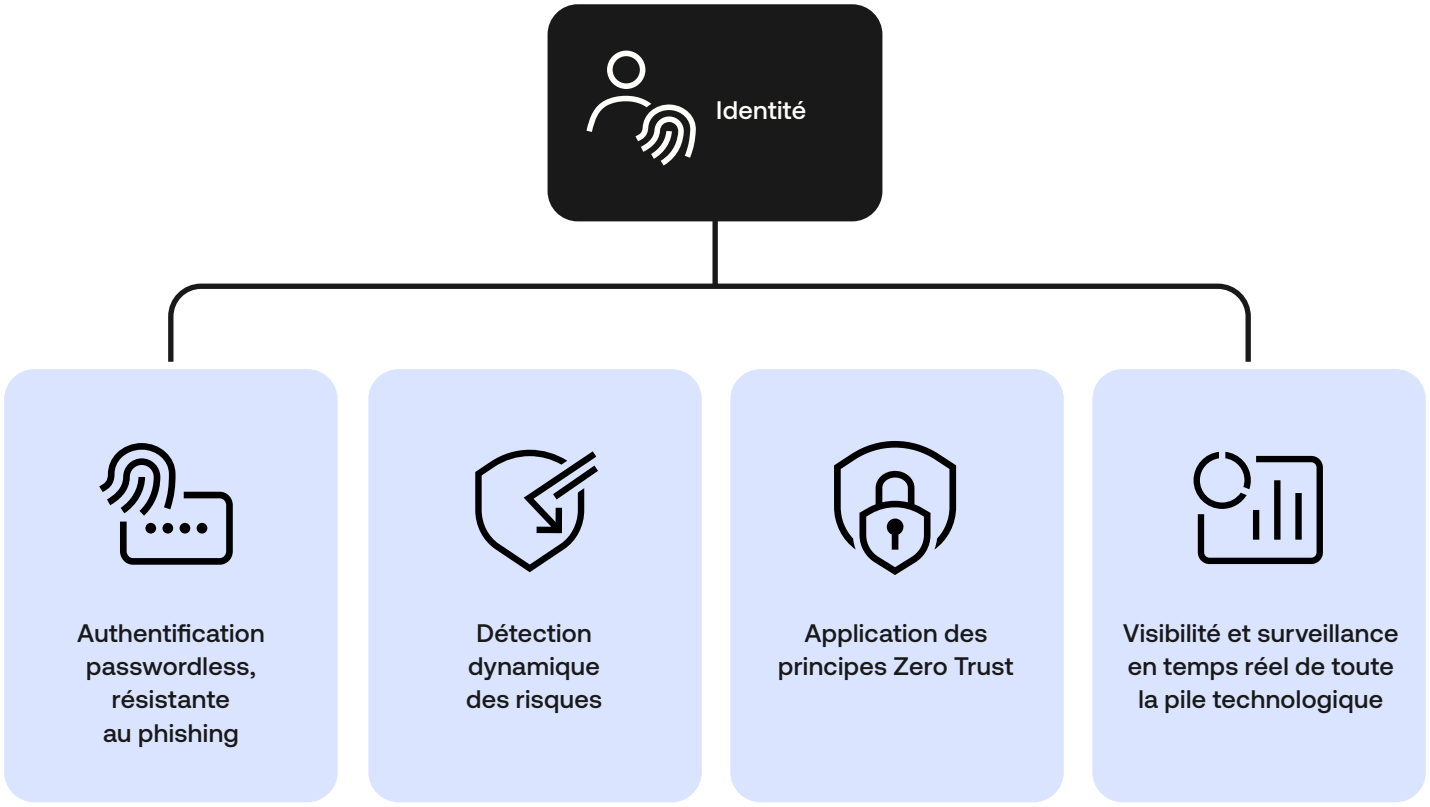
Par exemple, la plupart des entreprises comptent sur l'identité pour sécuriser l'accès via l'authentification. Or, lorsque l'identité est plus étroitement intégrée aux écosystèmes technologiques et de sécurité, elle peut faciliter l'évaluation continue des risques, l'application des politiques en temps réel et la correction automatisée, même après l'établissement d'une session. Dans les environnements où les agents d'IA et les systèmes automatisés agissent pour le compte des utilisateurs, l'identité doit vérifier non seulement qui accède à un système, mais aussi les actions autorisées par la suite.

Centralisation de l'identité dans votre écosystème de sécurité

L'on ne peut ignorer ce que les données montrent déjà : l'identité est devenue le nouvel enjeu de la cybersécurité d'entreprise. C'est au travers de celle-ci que les attaquants obtiennent un accès initial, élèvent les privilèges et se déplacent latéralement dans les environnements. C'est également ainsi que les entreprises peuvent établir la responsabilité, appliquer le principe du moindre privilège et garder le contrôle à grande échelle.

Une stratégie d'identité moderne sert de couche de connexion entre vos écosystèmes technologique et de sécurité, unifiant la visibilité, la gouvernance et l'application des politiques. Elle renforce la posture de sécurité non seulement lors de la connexion, mais aussi à chaque interaction, qu'elle soit initiée par une personne, un service ou un agent d'IA.

Pour y parvenir, les entreprises doivent disposer d'une vision plus large et stratégique de ce que l'identité représente et du rôle qu'elle peut jouer.



Les menaces à la loupe

Les acteurs malveillants misent sur l'obsolescence des approches adoptées par les entreprises en matière d'identité. Lorsque les environnements IT et de sécurité sont fragmentés, les ressources, applications et identités des différents systèmes et infrastructures sont dispersées, sans liens entre elles : cela laisse les identités humaines et non humaines vulnérables à des attaques qui ne seront probablement ni détectées, ni résolues. À l'heure où les agents d'IA et les systèmes automatisés peuvent accéder à davantage de données et effectuer plus d'actions, toute faille au niveau des contrôles d'identité a des conséquences beaucoup plus graves.

Processus manuels

Pratiques chronophages et fastidieuses en matière d'octroi des autorisations, qui exposent les décisions d'accès au risque d'erreurs humaines et de politiques incohérentes.

Visibilité lacunaire

Visibilité limitée sur la posture de sécurité en temps réel, le comportement des identités et les autorisations des utilisateurs, services, workloads et agents d'IA.

Lenteur de la réponse

Détection et correction tardives permettant aux attaquants ou aux processus automatisés malveillants d'exploiter les vulnérabilités liées à l'identité avant que les contrôles ne puissent intervenir.

Ce problème ne risque pas de disparaître de si tôt. Au contraire, il s'accentue. Les applications et services basés sur l'IA, ainsi que les identités non humaines et les agents d'IA, étendent la surface d'attaque de l'identité et accélèrent l'exécution des actions. Les attaques d'identité ne se limitent plus au vol d'identifiants. De nombreuses menaces post-authentification telles que le vol de cookies de session, la relecture de tokens et l'élévation des privilèges sont autant de nouveaux défis pour les équipes sécurité chargées de surveiller les environnements distribués.

Ajoutez à cela les risques posés par les acteurs étatiques généreusement financés, les menaces internes et les systèmes autonomes non gérés, et vous vous retrouvez face à un paysage de menaces centré sur l'identité qui évolue à la vitesse grand V.

91 %

91 % des entreprises utilisent déjà des agents d'IA, mais seulement 10 % ont une stratégie pour les gérer

(Okta)

80 %

Plus de 80 % de toutes les brèches de données sont le résultat d'attaques ciblant l'identité

(Verizon)

180 %

Les attaques liées à l'identité augmentent au rythme annuel de 180 %

(Verizon)

1,9 Mrd

1,9 milliard de cookies de session ont été volés aux collaborateurs d'entreprises Fortune 1000 en 2023

(Fortune)

okta

La sécurité passe par l'identité

Les menaces axées sur l'identité se multiplient au sein du paysage des risques. Avec l'adoption croissante des services cloud, des identités non humaines et des agents d'IA dans les entreprises, l'identité devient à la fois la première surface d'attaque et le principal point de contrôle.

L'identité n'est pas seulement une source de risques. Elle représente aussi la plus belle opportunité de reprendre le contrôle. En axant leur stratégie de sécurité sur l'identité, les entreprises peuvent passer d'une défense réactive à l'application continue de politiques, afin de vérifier les accès et les actions automatisées avant que les risques ne se transforment en répercussions bien réelles.

Grâce à une identité unifiée pour l'ensemble des utilisateurs, des services et des agents d'IA, vous disposez du socle nécessaire pour éviter les brèches et maximiser la valeur de vos investissements en sécurité et en technologies.

Les trois principes d'une stratégie d'identité moderne

Nous venons de faire le tour des enjeux liés à l'adoption d'une approche de sécurité axée sur l'identité. Penchons-nous à présent sur un aspect plus pratique, ou comment faire progresser l'identité de son stade actuel au niveau requis par un nouvel environnement intégrant l'IA.

Une plateforme d'identité cloud native moderne permet de limiter la fragmentation et de centraliser le contrôle. Elle offre une visibilité unifiée en temps réel sur l'ensemble des identités humaines et non humaines, des services et des agents d'IA, permettant ainsi aux équipes IT et sécurité d'éliminer les failles, de réduire les risques et d'accélérer la réponse.

Sa valeur repose sur trois principes fondamentaux :

Visibilité complète

Faire en sorte qu'aucune vulnérabilité, qu'elle concerne les utilisateurs, les identités non humaines ou les agents d'IA, n'échappe à la détection et soit corrigée.

Orchestration puissante

Appliquer une correction en temps réel et un contrôle des accès basé sur des politiques dans l'ensemble des systèmes, services et workflows automatisés.

Intégrations étroites et performantes

Connecter l'identité dans votre écosystème technologique et de sécurité pour bénéficier d'une gouvernance et d'une application des politiques cohérentes.

Lors de l'évaluation des solutions disponibles sur le marché, les entreprises doivent rechercher une plateforme offrant les fonctionnalités nécessaires pour respecter ces trois principes.

Principe 1

Visibilité complète

La gestion individuelle des autorisations d'accès dans les différents systèmes, services et applications mène à des failles de sécurité faciles à exploiter et à des politiques d'accès incohérentes. Avec la multiplication des identités non humaines et des agents d'IA, ces failles vont bien au-delà des comptes utilisateurs pour englober les API, les workloads et les processus automatisés.

Une plateforme moderne de gestion des identités doit centraliser et simplifier la gestion du cycle de vie des accès, tout en offrant une vue complète et en temps réel des activités liées à l'identité dans votre environnement. Elle doit offrir une visibilité unifiée sur les identités humaines, les comptes de service, les workloads et les agents d'IA afin d'aider les équipes à détecter rapidement les vulnérabilités et à appliquer les politiques de manière cohérente et à grande échelle.

Fonctionnalités principales

Gouvernance des accès et gestion du cycle de vie

Outils destinés à centraliser le provisioning et le déprovisioning dans l'ensemble des systèmes, à automatiser les processus liés aux arrivées, transferts et départs des collaborateurs et à certifier continuellement l'accès des utilisateurs et des identités non humaines.

Visibilité sur la posture et les menaces

Fonctionnalités chargées de surveiller les configurations de l'identité, de détecter les erreurs de configuration et de fournir des informations en temps réel sur les risques liés à l'identité dans l'ensemble des applications, de l'infrastructure et des systèmes pilotés par l'IA.

Contrôle des accès sensibles et à privilèges

Mesures de protection pour les identités à fort impact, y compris les comptes administrateurs, les comptes de service et les agents d'IA disposant d'autorisations élevées.

Évaluation continue des risques

Surveillance et agrégation des signaux en temps réel pour accélérer la détection et la réponse en cas d'activités suspectes, qu'elles soient le fait d'un utilisateur ou d'un système automatisé.

Checklist : votre plateforme d'identité peut-elle...

- ☐ Offrir une visibilité sur les menaces visant les utilisateurs, les identités non humaines, les agents d'IA et les comptes clients ?
- ☐ Intégrer les signaux tiers issus de votre pile technologique pour une visibilité complète et en temps réel sur les menaces ?
- ☐ Évaluer en permanence la posture d'identité par rapport aux principes Zero Trust ?
- ☐ Identifier les erreurs de configuration telles qu'une application incohérente du MFA, la prolifération des comptes ou des comptes de service avec privilèges excessifs ?
- ☐ Automatiser le provisioning et le déprovisioning en cas de changement de rôle d'un collaborateur ou lorsque les identités non humaines ne sont plus nécessaires ?
- ☐ Appliquer des contrôles d'accès granulaires pour les utilisateurs, services et agents d'IA à privilèges ?
- ☐ Découvrir les identités non humaines et surveiller leurs autorisations et leur comportement ?
- ☐ S'intégrer avec les logiciels et les annuaires RH pour bénéficier d'une gestion centralisée du cycle de vie des identités ?
- ☐ Gérer et sécuriser les identités clients à grande échelle ?

Principe 2

Orchestration puissante

Les piles de sécurité fragmentées génèrent d'énormes volumes de données sur les risques. Sans une couche de contrôle unifiée et basée sur l'identité pour analyser et exploiter ces données, les équipes doivent corréler des journaux de multiples systèmes, ce qui se traduit souvent par une intervention trop tardive. Réactive, leur posture de sécurité ne peut pas suivre le rythme des workflows automatisés, des identités non humaines et des agents d'IA qui fonctionnent, eux, à la vitesse des machines.

Une plateforme de gestion des identités moderne doit permettre aux entreprises de prévenir, de détecter et de corriger les menaces en temps réel. Au-delà de la visibilité procurée, elle doit pouvoir transformer les signaux de risque en mesures correctives automatisées pour que les comportements suspects puissent être immédiatement évalués et gérés, qu'ils soient attribuables à un utilisateur, à un compte de service ou à un agent d'IA.

Checklist : votre plateforme d'identité peut-elle...

- ☐ Simplifier la configuration des processus automatisés de correction et d'application de politiques ?
- ☐ Personnaliser les réponses en fonction des signaux de risque, des données contextuelles et de politiques dynamiques ?
- ☐ Déclencher des mesures de protection telles que l'authentification renforcée, la révocation des sessions ou la déconnexion universelle ?
- ☐ S'intégrer avec des méthodes d'authentification résistantes au phishing pour renforcer la protection en place ?
- ☐ Évaluer la posture des terminaux et les risques contextuels au cours des sessions actives ?
- ☐ Bloquer les adresses IP malveillantes ou les activités anormales en temps réel ?
- ☐ Offrir un processus sécurisé de récupération de facteurs en libre-service sans affaiblir les contrôles de sécurité ?
- ☐ Évaluer en permanence les activités liées à l'identité après l'authentification, y compris les actions automatisées et pilotées par l'IA ?

Principe 3

Intégrations étroites et performantes

La robustesse de votre écosystème technologique dépend essentiellement de la qualité des connexions entre ses composants. Sans une intégration fluide entre les applications, l'infrastructure, les outils de sécurité, les API et les systèmes d'IA, les entreprises éprouvent de grandes difficultés à appliquer des contrôles d'identité cohérents et à rentabiliser pleinement leurs investissements.

Une plateforme moderne de gestion des identités doit connecter chaque composant de l'environnement pour pouvoir mettre en place une gouvernance, une surveillance des risques et une application des politiques cohérentes. Les plateformes d'identité neutres vis-à-vis des fournisseurs permettent d'unifier les identités humaines et non humaines dans l'ensemble des solutions SaaS, de l'environnement cloud, des applications personnalisées et des systèmes pilotés par l'IA sans alourdir inutilement la charge d'intégration des équipes IT et développement.

Checklist : votre plateforme d'identité peut-elle...

- ☐ S'intégrer avec vos principales applications SaaS d'entreprise, p. ex. le CRM, l'ERP, les outils de productivité et les applications de gestion des opérations IT ?
- ☐ Étendre la protection de l'identité au-delà du provisioning et du SSO pour appliquer des contrôles avant, pendant et après l'authentification ?
- ☐ S'intégrer aux outils de sécurité de votre pile pour renforcer la détection des menaces, l'évaluation des risques et la correction automatisée ?
- ☐ Prendre en charge les API, les services et les agents d'IA à l'aide d'une gouvernance des identités et d'une application des politiques cohérentes ?
- ☐ Proposer des fonctionnalités d'automatisation no-code ou low-code pour déclencher des workflows sécurisés dans l'ensemble des systèmes ?
- ☐ Offrir l'extensibilité nécessaire pour prendre en charge de nouveaux services, applications et fonctionnalités d'IA à mesure que votre environnement évolue ?

Résultats d’une stratégie de sécurité unifiée

La sécurité unifiée, axée sur l’identité, est plus qu’un simple concept. Concrètement, elle offre des résultats mesurables qui renforcent la protection, rationalisent les opérations et permettent aux entreprises de monter en capacité en toute sécurité dans un environnement plus complexe.

Sécurité des identités et protection contre les brèches

Renforcez votre posture de sécurité en protégeant chaque identité humaine et non humaine, ce qui permet aux entreprises de détecter, de confiner et de résoudre les menaces basées sur l’identité avant qu’elles n’entraînent des brèches.

Efficacité et résilience opérationnelles

Simplifiez les opérations et réduisez la complexité en consolidant les systèmes d’identité fragmentés en une couche de contrôle unifiée qui améliore l’agilité, réduit la charge opérationnelle et raccourcit le délai de rentabilisation.

Visibilité et contrôle de l’IA

Mettez en place une gouvernance pour les agents d’IA et les systèmes automatisés en offrant une visibilité centralisée, une application cohérente des politiques et des contrôles d’accès sécurisés dans l’ensemble des workflows pilotés par l’IA.

Découvrez les principaux résultats d’une stratégie de sécurité unifiée.

okta

Vers une sécurité axée sur l'identité

Une sécurité axée sur l'identité bien implémentée prend en charge un écosystème ouvert qui permet de créer, de connecter et d'utiliser en toute simplicité et sécurité n'importe quels outils, applications ou système automatisés. Fini le cloisonnement des identités.

Fini aussi les intégrations personnalisées coûteuses et chronophages, les failles de sécurité et les déficits de visibilité dans les environnements collaborateurs, clients et machines. Dotez-vous d'une pile technologique unifiée qui repose sur l'identité et permet de bénéficier d'une gouvernance et d'une application des politiques cohérentes à chaque interaction.

Sécuriser l'identité pour tout protéger

On ne saurait trop insister sur ce point : la sécurité passe par l'identité. Pour garder une longueur d'avance sur les menaces et mettre en place une protection résiliente et durable, les responsables IT et sécurité doivent repenser la manière dont l'identité est gouvernée, contrôlée et intégrée dans leurs environnements.

Lorsque l'identité est unifiée pour l'ensemble des personnes, des identités non humaines et des systèmes automatisés, les entreprises réduisent les risques, renforcent le contrôle opérationnel et peuvent innover en toute sécurité et à grande échelle. Un socle d'identité robuste offre la protection indispensable contre des attaques de plus en plus sophistiquées, tout en apportant l'agilité requise dans les environnements distribués et basés sur l'IA d'aujourd'hui.

Pour faire progresser votre stratégie d'identité et bénéficier de recommandations ciblées d'experts Okta, consultez la page suivante ou prenez contact avec notre équipe.

À propos d'Okta
Okta, Inc. – The World's Identity Company™ – protège les identités humaines, machines et d'IA afin que chacun puisse utiliser n'importe quelle technologie en toute sécurité. Nos solutions d'identité client et collaborateur permettent aux entreprises et aux développeurs de protéger leurs agents d'IA, utilisateurs, collaborateurs et partenaires tout en renforçant la sécurité, en améliorant l'efficacité et en stimulant l'innovation. Découvrez pourquoi les plus grandes marques au monde font confiance à Okta pour l'authentification, l'autorisation et bien plus encore sur okta.com/fr.

okta

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie – France
+33 01 85 64 08 80