eBook

Sécuriser l'identité pour tout protéger

Les trois principes d’une stratégie d’identité moderne

okta

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

Il est probable qu'elle pense d'abord à la sécurité, et pour cause. Dans un paysage des menaces dominé par le vol d'identifiants et les attaques de phishing, il est clair que l'identité joue un rôle crucial dans les stratégies élaborées par les acteurs malveillants pour infiltrer les réseaux critiques et accéder aux informations sensibles. C'est pourquoi l'identité doit se trouver au centre de l'approche de sécurité moderne, de bout en bout, de n'importe quelle entreprise tournée vers l'avenir.

Et pourtant, trop d'entreprises s'efforcent encore de combler leur retard. Elles restent bloquées sur le paradigme désormais dépassé du périmètre sécurisé. Même si elles sont de plus en plus conscientes que les outils de sécurité conventionnels axés sur le réseau et le terminal offrent peu de protection contre les attaques sophistiquées basées sur l'identité, elles peinent à disposer de la visibilité nécessaire pour appréhender correctement les risques et les corriger efficacement.

Définition d'une stratégie d'identité avancée

Une stratégie de l'identité avancée doit permettre de gagner en visibilité dans tout l'environnement de l'identité, d'identifier les vulnérabilités pour renforcer la posture de sécurité et de répondre de façon rapide et efficace aux attaques potentielles. Il est tout aussi crucial que cette stratégie puisse offrir cette protection renforcée tout en autorisant une connectivité et une expérience fluides, essentielles au succès des entreprises aujourd'hui.

Cet eBook explique pourquoi l'identité doit être la pierre angulaire de la sécurité et des technologies des entreprises, mais aussi :

- Pourquoi les menaces liées à l'identité se sont multipliées
- Pourquoi les approches traditionnelles de l'identité laissent les entreprises vulnérables
- Trois principes guidant l'adoption de l'identité moderne

La fragmentation de la pile de sécurité de l'entreprise

La pile technologique des entreprises a considérablement changé au cours des dix dernières années. L'adoption rapide des services cloud, des applications SaaS et du télétravail a profondément transformé la façon dont nous collaborons et communiquons. Dans un environnement professionnel où les technologies constituent un aspect clé de la différenciation, le maintien de l'unité technologique sous un seul accord de licence est devenu une notion obsolète. Aujourd'hui, les entreprises savent qu'il leur faut intégrer l'agilité et la performance à leurs produits et aux technologies destinées aux collaborateurs et clients à l'aide d'une panoplie de solutions de pointe.

Les piles technologiques modernes sont extrêmement sophistiquées — et tout aussi complexes. Des réseaux de solutions isolées en constante expansion se traduisent par des environnements IT fragmentés et caractérisés par la dispersion des ressources métier (et des identités associées) dans un ensemble de systèmes, d'applications et d'infrastructures à la fois enchevêtré et déconnecté.

Le cloisonnement des technologies entrave la visibilité

Cette fragmentation est à l'origine de facteurs de risque majeurs. Elle accroît la surface d'attaque accessible aux acteurs malveillants en cloisonnant les identités dans différents emplacements et rend d'autant plus probables le vol et l'exploitation d'identifiants. À cela s'ajoute la quasi-impossibilité pour les équipes sécurité de bénéficier de la visibilité totale indispensable pour accéder aux composants nécessaires afin de corriger les vulnérabilités et de neutraliser les risques posés à l'identité.

Les acteurs malveillants sont parfaitement conscients que l'identité représente un angle mort toujours plus important dans les grandes entreprises, ce qui en fait aujourd'hui le principal vecteur d'attaque. D'après l'édition 2024 du *Verizon Data Breach Investigations Report*, auquel Okta a participé, 80 % des brèches impliquent une forme ou l'autre de compromission des identités. Un autre chiffre encore plus préoccupant est le nombre d'entreprises qui ne sont toujours pas préparées à cette nouvelle réalité : en 2024, il fallait 290 jours en moyenne pour identifier et maîtriser une brèche de données.

Il est temps de repenser l'identité

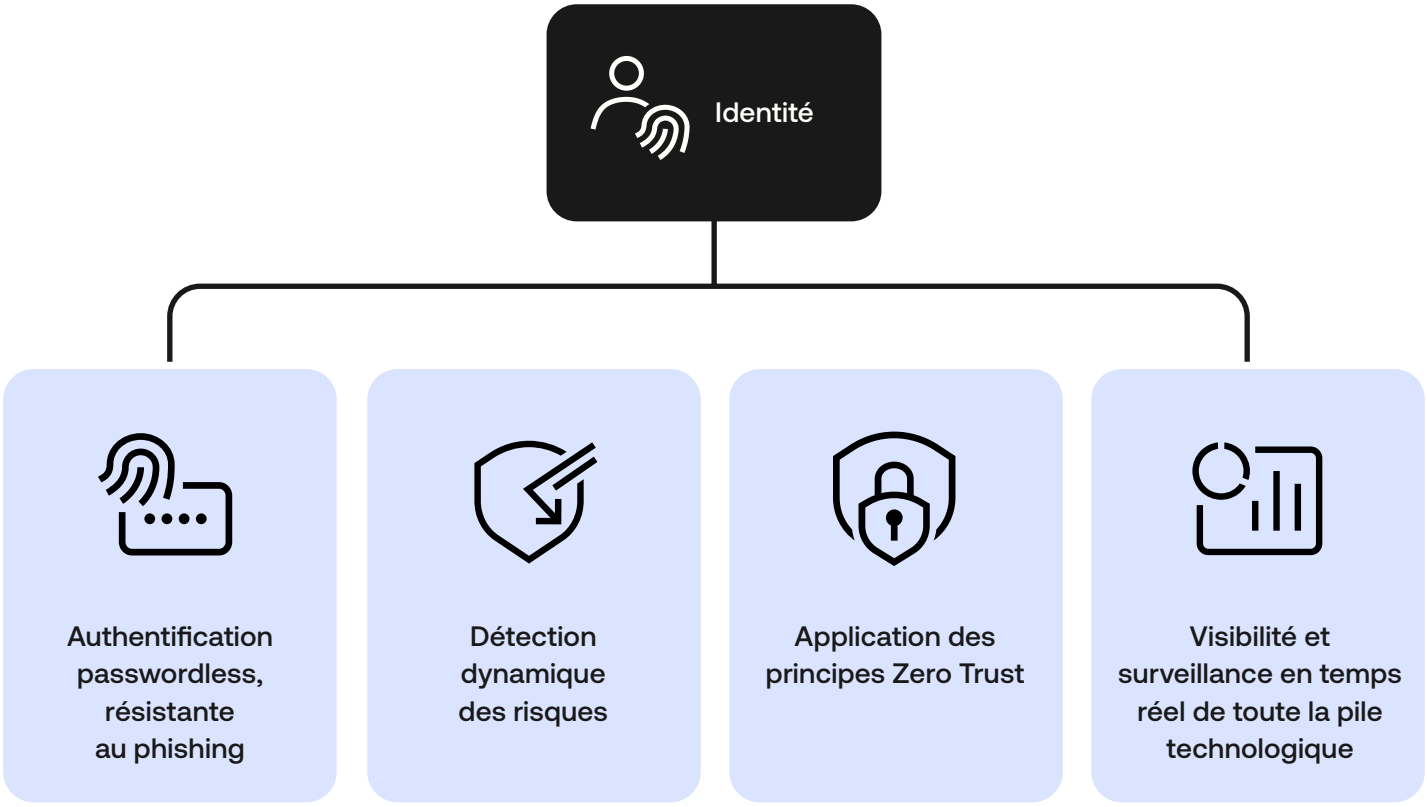
Si toutes les entreprises sont conscientes du rôle important de l'identité dans la sécurité, la plupart d'entre elles limitent ce rôle au contrôle des accès. Rares sont celles qui voient dans l'identité un écosystème essentiel pour bénéficier d'une visibilité et d'informations sur la sécurité de l'entreprise.

Ainsi, la vaste majorité des entreprises comptent sur l'identité pour offrir un accès fluide allié à une authentification sécurisée. Mais en intégrant plus étroitement ces fonctionnalités d'identité à leurs écosystèmes technologiques et de sécurité, les entreprises peuvent bénéficier d'une détection dynamique des risques en temps réel ou prendre en charge des stratégies de remédiation automatique après qu'un acteur malveillant s'est authentifié à l'aide d'identifiants volés. Ce ne sont là que quelques exemples illustrant comment l'identité peut permettre aux équipes sécurité d'adopter une approche proactive plus fiable pour renforcer leur niveau de protection.

Centralisation de l'identité dans votre écosystème de sécurité

Négliger ce potentiel revient à ignorer ce que nous savons déjà, à savoir que l'identité est devenue le champ de bataille de la cybersécurité d'une entreprise. C'est le moyen utilisé par les acteurs malveillants pour s'insinuer dans un environnement, mais aussi celui dont se servent les équipes sécurité les plus efficaces pour bloquer les accès indésirables. Une stratégie d'identité avancée peut servir de fil rouge pour optimiser chaque composante de votre environnement de sécurité, afin de le doter d'un dispositif plus robuste et unifié face à des menaces toujours plus sophistiquées.

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. Si les environnements IT et de sécurité sont fragmentés, les ressources, applications et identités des différents systèmes et infrastructures sont dispersées et donc vulnérables à des attaques qui ne seront probablement ni détectées, ni résolues. Leurs conséquences peuvent aller du simple désagrément à la catastrophe.

Processus manuels

Pratiques chronophages et fastidieuses en matière d'octroi des autorisations, qui exposent les contrôles d'accès au risque d'erreurs humaines

Visibilité lacunaire

Manque de visibilité sur la posture de sécurité en temps réel et les autorisations individuelles dans l'ensemble des systèmes et applications de l'entreprise

Lenteur de la réponse

Réponses tardives qui permettent aux acteurs malveillants d'exploiter les vulnérabilités liées à l'identité, avec à la clé des brèches coûteuses et préjudiciables

Loin de se résoudre, le problème s'aggrave. Les utilisateurs, de même que les applications et services assistés par l'intelligence artificielle rendent les risques posés à l'identité encore plus difficiles à détecter et à neutraliser. Pour ne rien arranger, les attaques ciblant l'identité ne se contentent plus de voler des identifiants. Les menaces post-authentification, notamment le piratage des cookies de session, ne font que compliquer la surveillance déjà difficile des informations des logs pour détecter les activités suspectes. Si vous ajoutez à cela le risque omniprésent des attaques commanditées par les États et les menaces internes difficiles à détecter, vous vous retrouvez dans une situation extrêmement délicate, où les risques ne feront qu'empirer.

80 %

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

(Verizon)

180 %

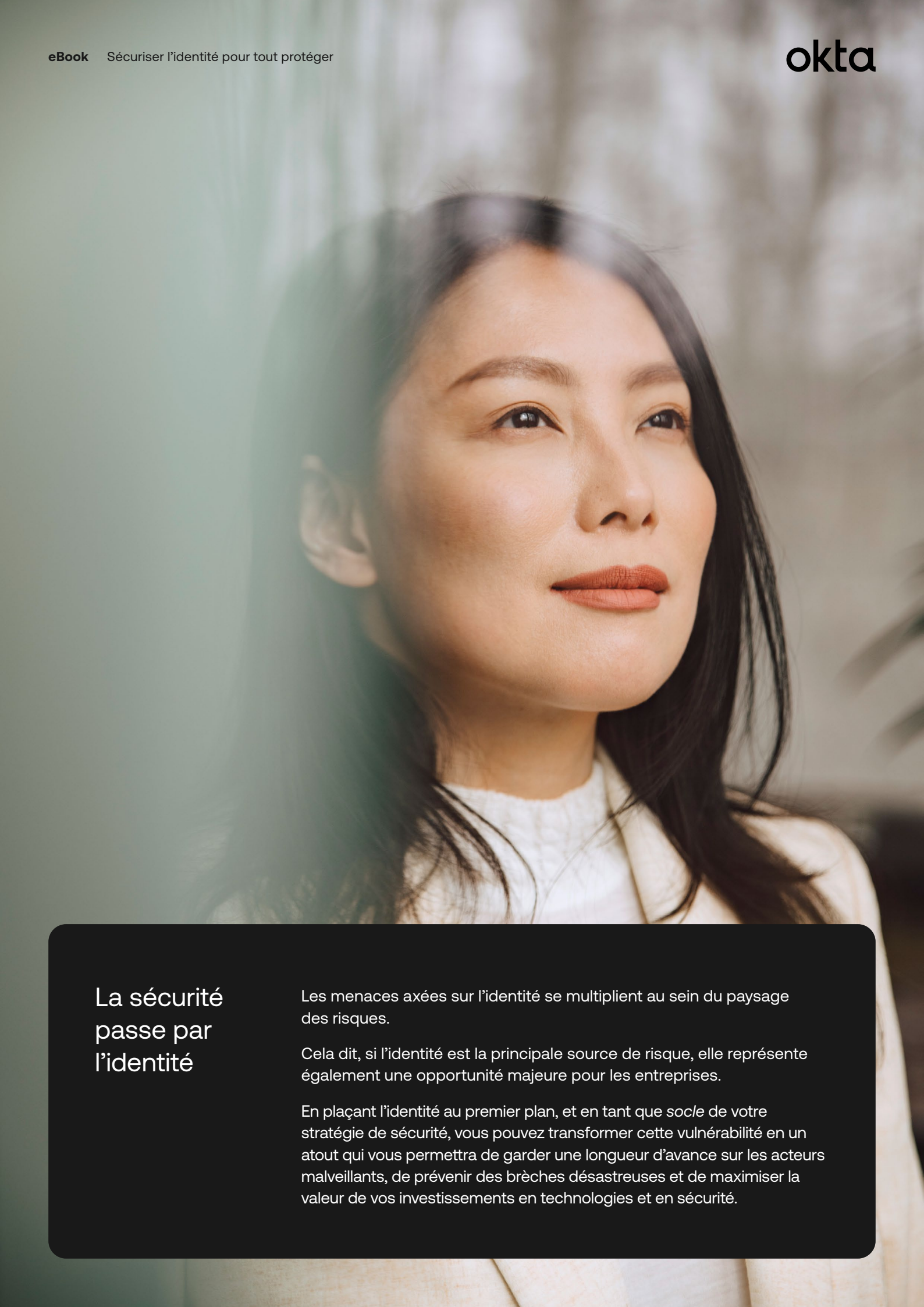
Les attaques liées à l'identité augmentent au rythme annuel de 180 %

(Verizon)

1,9 Mrd

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

(Fortune)



La sécurité passe par l'identité

Les menaces axées sur l'identité se multiplient au sein du paysage des risques.

Cela dit, si l'identité est la principale source de risque, elle représente également une opportunité majeure pour les entreprises.

En plaçant l'identité au premier plan, et en tant que *socle* de votre stratégie de sécurité, vous pouvez transformer cette vulnérabilité en un atout qui vous permettra de garder une longueur d'avance sur les acteurs malveillants, de prévenir des brèches désastreuses et de maximiser la valeur de vos investissements en technologies et en sécurité.

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.

Une solution d'identité cloud native moderne permet d'accélérer la résolution des problèmes de fragmentation. Elle offre des contrôles centralisés ainsi qu'une visibilité unifiée en temps réel sur l'ensemble des systèmes et des applications, permettant ainsi aux équipes IT et sécurité d'éliminer les angles morts, de réduire les risques et d'accélérer la réponse.

Ses atouts sont de trois ordres :

Visibilité complète
pour veiller à ce que chaque vulnérabilité soit identifiée et résolue

Orchestration puissante
pour appliquer des mesures correctives en temps réel en cas de brèche potentielle

Intégrations étroites et performantes
pour exploiter pleinement la connectivité dans les piles technologiques et sécurité de l'entreprise

Lorsqu'elles veulent se doter d'une solution d'identité moderne, les entreprises doivent rechercher une plateforme capable de répondre à ces attentes sur les trois fronts.

Principe 1

Visibilité complète

La gestion individuelle des autorisations d'accès dans les différents systèmes et applications mène à des failles de sécurité faciles à exploiter et à des politiques d'accès constamment affaiblies par l'erreur humaine.

Une solution d'identité moderne doit offrir à vos équipes des outils capables de centraliser et de simplifier le provisioning et déprovisioning des accès. Elle doit également fournir une vue complète en temps réel de toutes les menaces ciblant l'identité dans votre entreprise, que ce soit au niveau de l'administration ou lors de l'exécution, et offrir ainsi des expériences fluides et sûres à l'ensemble de vos collaborateurs, partenaires et clients.

Administration

- Outils de gouvernance qui offrent une vue complète des accès pour l'ensemble des systèmes et applications, avec des fonctionnalités complètes de provisioning et déprovisioning automatisés et granulaires
- Outils de gestion de la posture de sécurité qui simplifient l'analyse et la surveillance des vulnérabilités et des identités clients dans toute l'entreprise

Exécution

- Outils de gestion des accès à privilèges offrant des mécanismes de protection spécifiques pour les informations protégées, sans créer de friction excessive pour les équipes IT et les utilisateurs finaux
- Fonctionnalités de réponse aux menaces en temps réel qui s'appuient sur l'automatisation et la surveillance des risques de l'entreprise pour neutraliser de façon rapide et efficace les menaces potentielles

Checklist : votre solution d'identité peut-elle…

- ☐ Offrir la visibilité nécessaire sur tout l'environnement : systèmes, terminaux, ressources et comptes clients ?
- ☐ Intégrer les signaux tiers issus de votre pile technologique (en plus des signaux propriétaires de votre fournisseur d'identité) pour offrir une visibilité complète et en temps réel sur les menaces ?
- ☐ Exécuter des analyses automatisées de tous vos outils et évaluer votre environnement en fonction d'un ensemble agrégé de frameworks Zero Trust ?
- ☐ Identifier de façon proactive les vulnérabilités et les failles de sécurité avant qu'elles soient exploitées ?
- ☐ Continuellement mettre au jour les failles et erreurs de configuration critiques, notamment une application incohérente du MFA, la multiplication des comptes et les politiques d'authentification client faibles ?
- ☐ Automatiser le provisioning et le déprovisioning en cas de départ ou réaffectation d'un collaborateur dans l'entreprise ou de modification du profil de risque d'un client ?
- ☐ Offrir un accès sécurisé aux informations hautement protégées et le personnaliser en fonction de l'utilisateur et du cas d'usage ?
- ☐ Découvrir les identités non humaines et définir des autorisations granulaires pour celles-ci afin de réduire la surface d'attaque de votre entreprise ?
- ☐ S'intégrer avec les logiciels et les annuaires RH pour bénéficier d'une gestion consolidée des informations et autorisations des collaborateurs ?
- ☐ Se connecter aux systèmes de gestion des identités clients pour gérer et sécuriser les comptes clients à grande échelle ?

Principe 2

Orchestration puissante

Les piles de sécurité fragmentées génèrent un volume considérable de données sur les risques et menaces potentielles. Cependant, sans un outil unifié et optimisé par l'identité pour analyser et exploiter concrètement ces données, vos équipes se retrouvent contraintes d'examiner les journaux et de tenter de dresser un tableau — souvent tardif — des risques exigeant une attention immédiate. Résultat : une solution de sécurité trop lente qui empêche toute remédiation en temps réel.

Une solution d'identité moderne doit offrir à vos équipes des outils capables de prévenir, détecter et neutraliser rapidement les menaces en temps réel. Outre la visibilité complète décrite précédemment, les entreprises ont besoin de fonctionnalités optimisées par l'identité pour simplifier *l'interprétation et la prise de décisions* basées sur cette visibilité globale afin de contrer les acteurs malveillants avant qu'ils ne puissent causer de réels dommages.

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

- ☐ Simplifier la configuration des mesures de remédiation automatisées ?
- ☐ Offrir une personnalisation granulaire des mesures de remédiation basées sur les facteurs de risque, les politiques et autres informations contextuelles ?
- ☐ Déclencher des réponses efficaces telles que la déconnexion universelle pour se protéger contre des brèches potentielles ?
- ☐ Communiquer constamment avec vos outils d'authentification résistante au phishing pour améliorer continuellement la stratégie de remédiation ?
- ☐ Procéder à des contrôles de sécurité sur les terminaux au cours d'une session active ?
- ☐ Bloquer de façon proactive les adresses IP malveillantes ?
- ☐ Permettre aux collaborateurs et clients de configurer la récupération en libre-service de facteurs résistants au phishing pour simplifier et sécuriser l'utilisation ?
- ☐ Détecter continuellement les menaces après l'authentification utilisateur ?

Principe 3

Intégrations étroites et performantes

La puissance de votre pile technologique dépend de ses connexions internes. Sans une intégration harmonieuse des composants de votre pile technologique, il est impossible d'exploiter pleinement la valeur de vos investissements en technologies et sécurité et de réaliser un ROI complet.

Une solution d'identité moderne doit connecter tous les composants pour optimiser la gestion des risques et l'efficience. Les plateformes d'identité indépendantes offrent ce niveau d'intégration sans trop solliciter les équipes IT et développement pour l'écriture d'un code personnalisé.

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

- ☐ S'intégrer harmonieusement 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 ?
- ☐ Fournir des fonctionnalités de sécurité des identités riches qui vont au-delà du simple provisioning et du SSO, pour offrir une protection pour ces applications avant, pendant et après la connexion ?
- ☐ S'intégrer avec les composants essentiels de votre pile de sécurité pour améliorer la surveillance des risques, la détection des menaces et leur remédiation ?
- ☐ Offrir aux équipes IT et de développement des options no-code pour créer facilement des flux d'automatisation qui déclenchent certaines fonctions dans l'ensemble des applications ?
- ☐ Tirer parti des fonctionnalités d'extensibilité qui assurent une connectivité continue avec des applications et systèmes que l'entreprise pourrait ajouter par la suite ?

Résultats d'une stratégie de sécurité unifiée

La sécurité unifiée et axée sur l'identité est plus qu'un concept. Dans la pratique, elle englobe une série de résultats concrets qui, ensemble, possèdent une incidence mesurable sur la façon dont votre entreprise protège les ressources critiques, simplifie les workflows quotidiens et améliore les performances de toutes les opérations métier.

- Visibilité sur toutes les menaces visant l'identité et remédiation en temps réel
- Élimination totale des privilèges permanents et application systématique du principe du moindre privilège
- Mise en œuvre éprouvée des principes Zero Trust
- Contrôle renforcé des identités non humaines et machines
- Rentabilisation des investissements en technologies et sécurité

Découvrez les cinq principaux résultats d'une stratégie de sécurité unifiée.

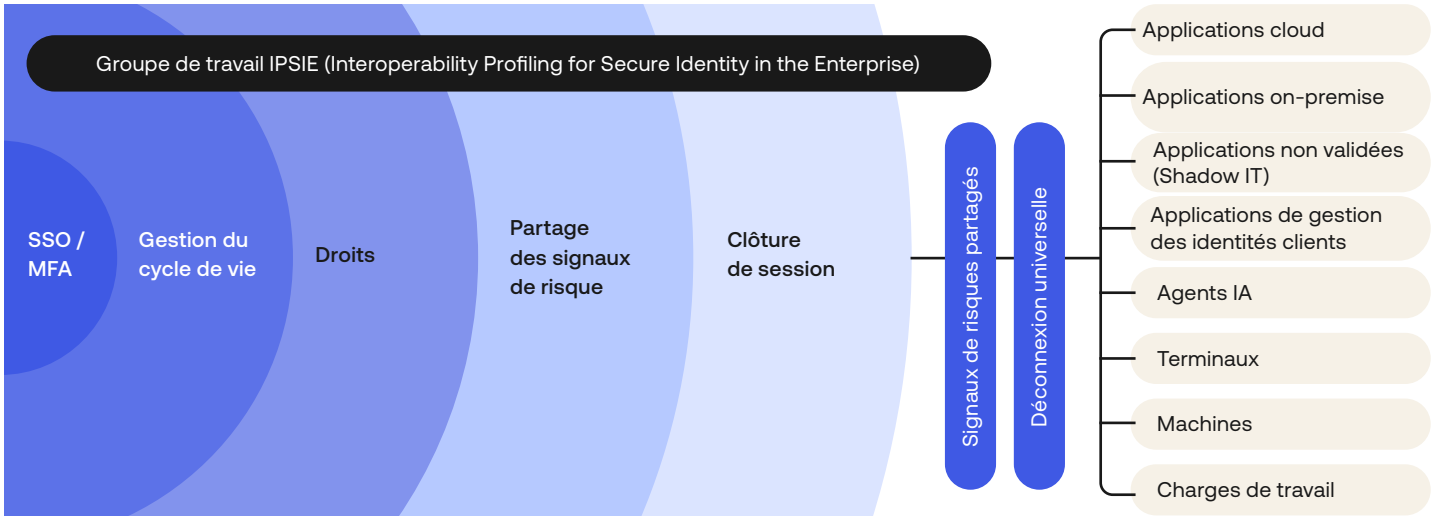
Vers une sécurité axée sur l'identité

Une sécurité axée sur l'identité bien implémentée prend en charge un écosystème ouvert qui permet de créer et d'utiliser en toute simplicité et sécurité n'importe quels outils, applications ou systèmes, en veillant à ce que ceux-ci soient sécurisés et faciles à gérer.

Fini les identités cloisonnées. Fini les intégrations personnalisées chronophages et coûteuses. Fini les failles de sécurité et la visibilité lacunaire sur les environnements IT et clients. Pour cela, adoptez une pile technologique ultraperformante, sécurisée par défaut et conçue pour privilégier la fluidité.

Le nouveau standard de sécurité des identités

Le groupe de travail *Interoperability Profile for Secure Identity in the Enterprise* (IPSIE) de l'OpenID Foundation est la dernière initiative lancée pour faire de cet idéal une réalité.



Premier standard de sécurité unifié en matière d'identité, l'IPSIE proposera un parcours complet vers un écosystème totalement intégré, adapté au paysage moderne et capable de vous rendre le contrôle de votre sécurité.

Comment parvenir à la maturité en matière d'identité :

Modèle de maturité de l'identité Okta

La modernisation de votre identité et l'unification de votre stratégie de sécurité représentent une tâche considérable pour les équipes IT et sécurité. De plus, il ne s'agit pas de conditions binaires. Au contraire, la création d'une stratégie moderne en matière d'identité doit être une campagne continue d'amélioration progressive.

C'est pourquoi Okta a développé son modèle de maturité de l'identité : il offre aux entreprises de tous les secteurs un framework, reposant sur l'apport d'experts et une évaluation comparative, qui peut vous aider à gérer la complexité et à faire progresser votre entreprise en toute confiance.

Les entreprises sont confrontées à différents défis en fonction du stade atteint en matière de maturité de l'identité. Le modèle de maturité de l'identité prend tous ces éléments en compte et offre des lignes directrices précises à chaque stade du processus. Il s'agit d'une ressource incontournable lorsqu'il s'agit d'identifier les priorités, de mesurer les progrès accomplis et d'atteindre les objectifs métier voulus.

Sécuriser l'identité pour tout protéger

On ne saurait trop le souligner : la sécurité passe par l'identité. Pour garder une longueur d'avance sur les acteurs malveillants et renforcer la sécurité et la résilience des entreprises, les responsables IT et sécurité doivent prendre les mesures qui s'imposent pour moderniser leur solution d'identité et exploiter pleinement tout son potentiel.

Lorsque vous sécurisez l'identité, vous sécurisez l'avenir de votre organisation : vous la protégez contre la vague croissante de menaces toujours plus sophistiquées et les nouvelles méthodes d'attaque basées sur l'IA. De plus, vous bénéficiez de l'avantage concurrentiel que vous offrent des environnements clients, IT et de sécurité harmonieux, optimisés par l'automatisation.

Pour vous lancer dans votre parcours de maturité de l'identité et bénéficier de recommandations ciblées d'experts Okta, consultez la page suivante ou prenez contact avec notre équipe.

okta

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie – France

+33 01 85 64 08 80