Comment bénéficier d'une visibilité sur toutes les menaces d'identité et d'une remédiation en temps réel

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 améliorent les résultats à tous les niveaux de l'activité. Par contre, elles vous exposent également à certains risques.

Trop souvent, à mesure que les entreprises évoluent et grandissent, leurs équipes IT et sécurité ont du mal à s'adapter et à suivre le rythme. Cela donne lieu à des **environnements IT fragmentés** au sein desquels les identités et ressources essentielles sont dispersées entre différents systèmes et infrastructures.

Le résultat ? Un manque de visibilité sur la posture de sécurité de l'entreprise et un risque élevé de brèche qui pourrait lui coûter très cher.

L'identité est devenue le premier vecteur d'attaque pour les cybercriminels

80 % des brèches de données ont commencé par le vol d'identifiants et/ou des attaques de phishing

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

Verizon, 2024 Data Breach Investigations Report

Une sécurité des identités unifiée pour une visibilité accrue

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. Elle expose votre entreprise et vos clients à des risques incontrôlables, dans un paysage des menaces toujours plus sophistiqué.

Pour mieux gérer ces risques, les processus et systèmes d'identité doivent être unifiés au sein d'une seule plateforme 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.

Des résultats concrets avec Okta

Okta Platform vous offre la possibilité 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 propose 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 visant l'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, cela permet de protéger 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.

Avec Okta

En unifiant l'orchestration de l'identité, Okta offre une visibilité incomparable sur les signaux et politiques dans vos environnements IT, sécurité et clients, et dote vos équipes d'outils puissants pour détecter et répondre aux menaces en temps réel.

Identity Threat Protection avec Okta AI

- Bénéficiez d'une visibilité en temps réel sur les menaces dans l'ensemble de vos systèmes, terminaux et types d'utilisateurs afin de profiter d'une posture de sécurité proactive.
- Tirez parti des signaux tiers et des données first-party d'Okta pour avoir accès à des informations plus pertinentes et accélérer la détection des menaces.
- Répondez rapidement aux menaces avec des actions automatisées personnalisables, par exemple le déclenchement d'un MFA ou la déconnexion des utilisateurs compromis.

Okta FastPass

- Déployez une authentification passwordless résistante au phishing pour offrir une expérience utilisateur fluide et sûre.
- Vérifiez la posture de sécurité des terminaux au cours de l'authentification pour respecter les impératifs de conformité.
- Avertissez les utilisateurs et les administrateurs en cas de tentatives de phishing et consignez les attaques dans des logs pour améliorer la visibilité.
- Bloquez les applications non fiables avant qu'elles puissent exploiter les processus d'authentification.

Onboarding sécurisé des applications

- Faites en sorte que les nouveaux utilisateurs (collaborateurs ou clients) disposent dès le premier jour des autorisations appropriées pour accéder aux principales applications et ressources.
- Modifiez l'accès des utilisateurs finaux à partir d'une seule plateforme centralisée.
- Intégrez l'onboarding avec les logiciels et annuaires RH pour disposer d'une gestion consolidée des informations et des autorisations des collaborateurs, et connectez-le à des systèmes de gestion des identités clients pour gérer et sécuriser les comptes clients à grande échelle.
- Révoquez automatiquement l'accès lors du départ des collaborateurs pour renforcer la sécurité et réduire les coûts.
- Simplifiez la gestion des comptes clients pour qu'ils disposent d'un accès sûr et à jour, en accord avec leurs activités et leurs préférences.

Identity Security Posture Management

- Identifiez et priorisez les risques cachés liés à l'identité pour l'ensemble de vos fournisseurs d'identité, applications SaaS et infrastructure cloud grâce à une surveillance continue et à une analyse optimisée par l'IA.
- Réduisez la surface d'attaque de façon proactive en identifiant les vulnérabilités critiques telles que le contournement du MFA, la multiplication des administrateurs, les utilisateurs à l'offboarding partiel et les risques liés aux identités non humaines, avant qu'elles puissent être exploitées.
- Simplifiez la validation de la conformité grâce à des frameworks et standards tels que le NIST, le CIS, les normes ISO et le PCI-DSS au moyen d'une surveillance et d'un reporting continus et automatisés des contrôles.
- Améliorez la productivité de l'équipe sécurité en offrant un contexte de l'identité consolidé pour l'ensemble des systèmes ainsi qu'une visualisation graphique des relations d'identité complexes pour permettre à l'équipe de comprendre et de gérer rapidement la posture de sécurité.

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.

Vous souhaitez en savoir plus sur l'unification de votre stratégie de sécurité à l'aide d'une solution d'identité moderne ? Prenez contact avec notre équipe et découvrez Okta Platform en action.