okta

Une visibilité optimale pour une sécurité efficace

Comment détecter chaque menace et bloquer les attaques en temps réel grâce à une stratégie de sécurité moderne, axée sur l'identité

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

Lorsque les entreprises évoluent et prennent de l'ampleur, leurs piles technologiques font de même. Trop souvent, les équipes IT et sécurité ont du mal à s'adapter et à suivre le rythme.

Cela donne lieu à des environnements IT fragmentés, aux ressources et aux identités dispersées.

Le résultat ? Un manque de visibilité et un risque accru de brèches au coût élevé.

Les acteurs malveillants savent reconnaître une opportunité lorsqu'elle se présente. C'est pourquoi l'identité est devenue leur premier vecteur d'attaque.

80 %

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

(Verizon)

Et bon nombre d'entreprises restent mal préparées pour répondre aux menaces.

180 %

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

(Okta)

290 jours

Il faut en moyenne 290 jours à une entreprise pour circonscrire une brèche.

(Verizon)

4,8 Mio $

En 2024, le coût moyen d'une brèche de données était estimé à 4,88 millions de dollars.

(IBM)

La fragmentation des identités expose les entreprises aux risques, dans la mesure où il leur est impossible d'identifier les principales vulnérabilités de leur environnement.

- Détection et réponse aux menaces plus lentes
- Masse ingérable de données sur les risques désorganisées
- Risque incontrôlable dans un paysage des menaces toujours plus sophistiqué

Question :

Comment les entreprises évoluées peuvent-elles éliminer les risques liés à la fragmentation des identités ?

Réponse :

Grâce à une approche unifiée de sécurité axée sur l'identité.

Okta relève le défi.

Avec l'orchestration de l'identité, Okta offre une visibilité accrue sur les signaux, les politiques et les activités des utilisateurs dans l'ensemble de vos environnements IT, sécurité et clients, pour bénéficier d'une détection et réponse aux menaces plus proactives.

Identity Threat Protection avec Okta AI

Réponses pilotées par l'automatisation pour chaque type de menaces visant l'identité

- Synthétisez et priorisez les signaux de risques générés pour l'ensemble de vos systèmes, terminaux et types d'utilisateurs afin de conserver une posture de sécurité proactive.
- Tirez parti des signaux tiers et first-party pour détecter et gérer les activités suspectes et les identifiants compromis en temps réel.
- 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 avec résistance 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.

Okta Identity Security Posture Management

Bénéficiez d'une visibilité complète sur les lacunes de sécurité des identités dans toute l'entreprise.

- Profitez d'une visibilité complète sur les failles en matière de gestion des identités à l'échelle de l'entreprise.
- Détectez les vulnérabilités critiques telles que le contournement du MFA, la multiplication des administrateurs et les utilisateurs à l'offboarding incomplet.
- Surveillez les identités non humaines et identifiez les risques tels que les clés API non renouvelées et les comptes de services à privilèges excessifs.

Okta vous offre un onboarding des applications plus sûr

Une bonne visibilité sur les identités est essentielle pour sécuriser chaque étape de l'accès, y compris l'onboarding des applications. Avec Okta, vous bénéficiez d'informations en temps réel sur l'activité des utilisateurs et les signaux de risques, ce qui offre une intégration fluide mais sécurisée des nouvelles applications en cinq étapes simples.

1. Veillez à ce que les nouveaux utilisateurs disposent des autorisations d'accès appropriées dès le premier jour.
2. Modifiez l'accès des utilisateurs finaux à partir d'une seule plateforme centralisée.
3. Intégrez l'onboarding avec les logiciels et les annuaires RH pour bénéficier d'une gestion consolidée des informations.
4. Révoquez automatiquement l'accès lors du départ des collaborateurs.
5. Gérez les comptes clients grâce à un accès sûr et à jour, basé sur leurs activités.

Prêt à découvrir comment unifier votre stratégie de sécurité avec des solutions d'identité modernes ?

Contactez notre équipe et découvrez Okta Platform en action.

Contactez-nous

okta