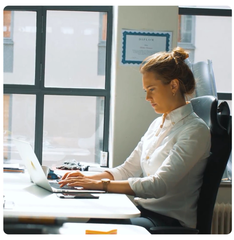
Comment l'identité dans le cloud protège vos clients

Pour mieux protéger les données de leurs clients et renforcer la confiance à chaque interaction, de nombreuses entreprises se tournent vers l'identité client. Cinq raisons expliquent ce choix :

Cinq raisons d'adopter une stratégie Zero Trust axée sur l'identité

1. Elle empêche les cybercriminels de s'inscrire ou se connecter à l'aide d'identifiants volés.

Détectez automatiquement les mots de passe compromis et informez vos clients lorsque leurs données ont été divulguées à un tiers.



80 %

des brèches associées à des attaques d'applications web sont imputables à des identifiants volés.

Source : Verizon, Data Breach Investigations Report 2022

2. Elle permet une vérification sécurisée et sans mot de passe.

Remplacez l'authentification traditionnelle à l'aide d'un nom d'utilisateur et d'un mot de passe par des applications de vérification sécurisées et ajoutez une couche de sécurité supplémentaire grâce à l'authentification multifacteur (MFA).

90 %

des clients s'inquiètent de la vulnérabilité des mots de passe.

Source : Avast, Cybersecurity : Reality Check

---

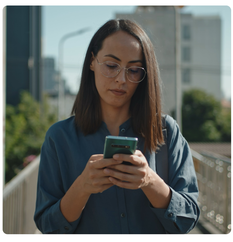
3. Elle offre le juste équilibre entre praticité et sécurité.

Offrez à vos clients un moyen plus simple et sûr de s'inscrire et d'accéder à votre site web ou à votre application à l'aide des identifiants existants d'un réseau social tel que Facebook, Twitter ou Google.

50 %

des clients préfèrent utiliser la connexion via les réseaux sociaux lors de leurs interactions en ligne avec une marque.

Source : Okta Customer Identity Trends Report 2023



4. Elle permet de détecter les demandes susceptibles de provenir d'un bot.

Identifiez instantanément les modèles de trafic irréguliers et bloquez les requêtes automatisées des bots malveillants avant qu'ils ne compromettent les comptes de vos clients.

27,7 %

du trafic Internet est généré par des bots malveillants.

Source : 2022 Imperva Bad Bot Report

---

5. Elle bloque le trafic provenant d'adresses IP qui effectuent des tentatives de connexion répétées dans un laps de temps réduit.

Utilisez la limitation des adresses IP suspectes pour protéger vos applications orientées client contre les attaques à grande vitesse qui ciblent plusieurs comptes simultanément.

Plus de 15 millions

d'adresses IP infectées sont actuellement utilisées dans le monde entier dans le cadre d'attaques DDoS.

Source : A10, 2022 A10 Networks DDoS Threat Report

Protégez les données de vos clients grâce à l'identité.

Pour découvrir comment l'identité client peut protéger les données de vos clients, éliminer les points de friction et renforcer la confiance à chaque interaction numérique, consultez l'eBook **Sécurité vs facilité d'utilisation : renforcer la confiance, pas les tensions**.

Pour découvrir comment l'identité client permet aux entreprises à travers l'Europe d'offrir les expériences numériques fluides, confidentielles et sécurisées auxquelles vos clients aspirent, consultez le rapport **Okta Customer Identity Trends Report 2023**.