

Adaptive Multi-Factor Authentication

Sécurité intelligente pour vos terminaux, applications et infrastructure

Les temps ont changé. Les intrusions ont cédé la place aux usurpations d'identité. L'augmentation des attaques basées sur l'identité atteste la nécessité de sécuriser tous les points d'entrée à votre entreprise, qu'il s'agisse de vos applications cloud et on-premise ou de votre infrastructure. Sans oublier les accès aux applications utilisées par vos clients et les clients de vos clients. Les produits d'authentification adaptative d'Okta tels qu'Adaptive Multi-Factor Authentication et Adaptive Single Sign-On protègent votre entreprise contre les brèches de données en appliquant une gestion des accès contextualisée. Grâce à une approche axée sur les risques, qui prend en compte des éléments contextuels tels que le terminal, l'utilisateur, le comportement ou l'emplacement, les produits d'authentification adaptative d'Okta sécurisent l'ensemble des points d'accès aux ressources d'entreprise.

Les atouts d'Okta Adaptive MFA

Flexibilité des mesures de protection

Okta protège l'accès à vos données où qu'elles résident, indépendamment de l'emplacement des utilisateurs ou des terminaux utilisés. Conçue pour s'adapter à tous les environnements, Okta Adaptive MFA sécurise non seulement vos ressources dans le cloud, mais aussi vos actifs on-premise dans le cadre des connexions VPN, RDP et SSH, sans oublier les applications web et mobiles créées sur mesure auxquelles vos collaborateurs, partenaires, clients et utilisateurs ont accès.

Adaptive MFA

La solution Adaptive MFA répond aux enjeux de déploiement d'une solution multifacteur avec les fonctionnalités suivantes :

1. Solution universelle adaptée à tous les types d'utilisateurs – Okta répond à tous vos besoins en matière d'authentification multifacteur et de politiques adaptatives pour vos collaborateurs, fournisseurs, prestataires, clients ou utilisateurs. Il est possible d'appliquer des règles à toute application web ou mobile native, et même d'utiliser Okta en tant que fournisseur d'authentification pour vos applications créées sur mesure.
2. Réponse dynamique en fonction du contexte de connexion – L'authentification multifacteur n'est pas adaptée si vous êtes limité à un contexte binaire de type oui/non. Okta applique l'authentification renforcée lorsque cela s'avère pertinent en fonction du contexte historique de l'utilisateur en association avec le terminal, l'emplacement, l'adresse IP et divers autres paramètres de connexion.
3. Minimisation de l'importance des mots de passe – Même lorsque des politiques de mots de passe rigoureuses sont en place, les utilisateurs restent le maillon faible de la sécurité. Permettez à vos utilisateurs de bénéficier d'une expérience de connexion simple et fluide tout en renforçant votre sécurité, en remplaçant les mots de passe par des facteurs d'authentification forts comme Okta Verify, les données biométriques et les jetons FIDO2.

Avantages



Sélection des facteurs les mieux adaptés à votre entreprise

Okta met à votre disposition une large gamme de méthodes d'authentification multifacteur prêtes à l'emploi et vous offre la possibilité d'utiliser n'importe quel fournisseur d'authentification SAML ou OIDC en tant que facteur.



Connexion sécurisée sans mot de passe à tous types de terminaux

Appliquez la technologie Device Trust pour évaluer la fiabilité des terminaux et mettez à profit des facteurs d'authentification forte tels qu'Okta Verify et FIDO2 comme mode d'authentification principale, en lieu et place des mots de passe.



Authentification basée sur les risques pour identifier les anomalies de connexion

Okta utilise un modèle de machine learning pour hiérarchiser les anomalies selon différents niveaux de risque (haut, moyen, bas). Utilisez l'authentification basée sur les risques pour associer à un niveau de risque le facteur approprié.



Prévention des attaques d'usurpation d'identité à grande échelle grâce à Okta ThreatInsight

Le réseau d'Okta capture des milliards de connexions de ses clients. Grâce à Okta ThreatInsight, les administrateurs peuvent bloquer l'accès de préauthentification d'adresses IP suspectes, empêchant ainsi le piratage de comptes et le verrouillage de comptes pour vos collaborateurs, clients et utilisateurs.

À propos d'Okta

Okta est le leader indépendant des services de gestion des identités et des accès. Okta Identity Cloud permet aux organisations de connecter aux technologies pertinentes les individus adéquats, au moment opportun. Grâce à plus de 7 000 pré-intégrations avec des applications et fournisseurs d'infrastructures, les clients d'Okta peuvent utiliser les technologies dont ils ont besoin pour mener à bien leurs activités, et ce de façon simple et sécurisée. Plus de 13 050 organisations à travers le monde – dont Engie, JetBlue, Nordstrom, Siemens, Slack, T-Mobile, Takeda, ou encore Twilio – font confiance à Okta pour protéger les identités de leurs personnel et clients.