

# Okta AI

Chaque jour, l'intelligence artificielle (IA) devient de plus en plus performante. Pour les entreprises, l'IA représente un saut technologique majeur offrant de nouvelles opportunités en termes d'efficacité et d'agilité, tout en accélérant le rythme de l'innovation.

Mais la promesse de l'IA n'est pas passée inaperçue auprès des cybercriminels. L'intelligence artificielle a donné un nouveau souffle à d'anciennes tactiques telles que le phishing. Les entreprises font face à deux grands défis : elles doivent trouver de nouveaux moyens créatifs d'exploiter l'IA, tout en se protégeant contre ces nouveaux cybercriminels qui en tirent parti, eux aussi.

En tant qu'éditeur spécialisé dans l'identité, Okta possède une connaissance approfondie de ces enjeux. L'IA joue un rôle de plus en plus déterminant dans notre secteur. Elle est intégrée aux outils qui améliorent l'agilité des développeurs et réduisent les délais de lancement, ainsi qu'aux solutions conçues pour bloquer les menaces, qu'elles soient courantes ou émergentes.

Cette fiche produit présente les nombreuses fonctionnalités basées sur l'IA disponibles dans Workforce Identity Cloud et Customer Identity Cloud. Vous découvrirez également la philosophie fondamentale d'Okta en matière d'IA. Notre point de vue est optimiste : nous pensons que l'IA est une technologie transformationnelle, capable de combattre les nouvelles menaces de sécurité qu'elle contribue à générer.

## Comment les acteurs malveillants utilisent l'IA

### Phishing à grande échelle

Les outils d'IA générative peuvent servir à créer des e-mails de phishing convaincants d'apparence professionnelle en quelques secondes seulement, dont le contenu est souvent personnalisé en fonction de l'individu ciblé.

### Profil synthétiques

Les cybercriminels peuvent avoir recours à l'IA pour créer des portraits réalistes leur permettant d'établir des profils crédibles pour des attaques de phishing.

### Imitation

Certains outils d'IA peuvent imiter la voix d'une personne avec une exactitude surprenante, ce qui permet aux acteurs malveillants d'usurper l'identité de dirigeants dans le cadre d'attaques de phishing (phishing vocal).

### Code personnalisé

Les capacités d'écriture de code de l'IA générative peuvent permettre à un cybercriminel de créer des exploits en quelques minutes seulement.

### Contournement des CAPTCHA

L'IA peut contourner les CAPTCHA conçus pour faire la distinction entre les utilisateurs humains et automatisés.

# Comment Okta utilise l'intelligence artificielle

## Fonctionnalités de Workforce Identity Cloud optimisées par Okta AI

### Telephony Anti-Toll Fraud System

À l'aide d'un modèle de machine learning (ML) personnalisé, Okta peut détecter l'emploi abusif de numéros surtaxés dans les flux MFA, ce qui protège votre entreprise contre la fraude et les frais téléphoniques excessifs.

### ThreatInsight

Utilise les données de notre réseau de clients, d'administrateurs et d'utilisateurs finaux pour protéger vos collaborateurs contre les attaques basées sur les identifiants. Le modèle de machine learning propriétaire d'Okta détecte si une entreprise fait l'objet d'une attaque et signale les adresses IP malveillantes à vitesse record.

### Adaptive Multi-Factor Authentication

Fournit des renseignements supplémentaires sur les flux d'identité en tenant compte du contexte en constante évolution dans lequel une demande d'authentification est effectuée. En adaptant dynamiquement les politiques de sécurité et d'authentification, la fonction Adaptive MFA peut améliorer simultanément la posture de sécurité et l'expérience utilisateur d'une entreprise.

### Policy Recommender

**Disponible en Early Access au T1 2024**

Fournit des recommandations et modèles personnalisés basés sur les renseignements agrégés provenant de l'écosystème étendu d'Okta ainsi que sur les bonnes pratiques de sécurité. Cela simplifie la configuration des processus d'authentification sécurisée, tels que les vérifications du niveau de sécurité des terminaux et les authentificateurs résistants au phishing.

### Log Investigator

**Disponible en Early Access au T3 2024**

Grâce à la technologie de traitement en langage naturel, les administrateurs peuvent poser des questions sur les données Okta en termes simples, et obtenir des informations sur le contexte historique de leur posture d'identité. Cela facilite l'identification des activités anormales ou suspectes.

### Identity Threat Protection

**Disponible en Early Access au T1 2024**

Utilise l'IA pour l'évaluation continue des risques afin d'appliquer des politiques de sécurité au moment de la connexion et au cours d'une session utilisateur active, ce qui réduit le risque d'accès non autorisés et de menaces post-authentification telles que le détournement de session.

### Governance Analyzer

**Disponible en Early Access au T2 2024**

Fournit aux décideurs un contexte pertinent et des recommandations dans les évaluations et les demandes, ce qui leur permet de prendre des décisions éclairées en matière de gouvernance, sans augmenter leur charge cognitive.

## Fonctionnalités de Customer Identity Cloud optimisées par Okta AI

### Bot Detection

Utilise un modèle de machine learning qui ingère plus de 60 entrées pour faire la distinction entre les utilisateurs humains et les utilisateurs automatisés, bloquant jusqu'à 79 % des tentatives de connexion de bots en préservant au maximum la fluidité des activités légitimes.

### Identity Threat Level (ITL)

D'après les observations agrégées et anonymisées et les modèles de données de notre base de clients, nous calculons un score Identity Threat Level pour indiquer le niveau d'activité de bots détecté dans tous les flux de connexion clients CIAM. Les visiteurs du microsite peuvent saisir leurs informations et recevoir un score propre à leur secteur d'activité et à leur région géographique. Ils ont également accès à des filtres d'attributs et peuvent télécharger un rapport détaillé.

### Tenant Security Manager

**Disponible en Early Access au T2 2024**

Enrichit nos fonctionnalités Attack Protection avec des recommandations de sécurité intelligentes sous la forme d'alertes et de notifications affichées sur le tableau de bord, dans le but d'améliorer la posture de sécurité de votre tenant.

### Guide

**Disponible en Early Access au T4 2024**

Conçue pour être votre guide aguerri d'Okta Customer Identity Cloud, cette fonctionnalité offre une assistance complète à l'onboarding et identifie intuitivement les étapes à suivre par les utilisateurs, en les orientant vers les workflows les plus pertinents grâce à des invites simples.

### Actions Navigator

**Disponible en Early Access au T2 2024**

Profitez de fonctionnalités de recherche intelligente. Trouvez les intégrations de marketplace adaptées à vos besoins, même si vos mots clés de recherche ne figurent pas dans le titre ou la description des intégrations. Par ailleurs, si l'action ou l'intégration souhaitée n'existe pas, notre outil d'IA peut vous aider à écrire une action en fonction de la recherche de l'utilisateur, puis y ajouter des conditions ou corriger la logique métier.

### Brand Customizer

**Disponible en Early Access au T4 2024**

Pour personnaliser le branding, créez des modèles d'une page pour adapter le design à tous les autres modèles requis. Vous pouvez également fournir une capture d'écran ou un logo qui seront utilisés dans les modèles à personnaliser.

### Identity Flow Optimizer

**Disponible en Early Access au T4 2024**

L'outil d'IA Funnel Analytics analyse toutes les données d'authentification d'un tenant et fournit des suggestions pour améliorer l'expérience client, le flux d'inscription, etc.

## Statistiques clés

# 79 %

L'IA aide Okta à bloquer 79 % des tentatives de connexion automatisées et peut réduire le trafic de bots de 90 % en 90 jours.

# 20 %

Amélioration de la détection des transactions frauduleuses par SMS ou appel vocal grâce au modèle de machine learning d'Okta permettant de lutter contre la fraude au numéro surtaxé.

## Point de vue d'Okta

Notre conviction est que nous sommes en train de vivre une nouvelle révolution technologique. L'IA sera bientôt aussi importante que le smartphone ou le cloud. Elle permettra la création de logiciels plus performants et intelligents, et l'introduction de fonctionnalités avancées en un temps record.

Bien que nous ne soyons qu'à l'aube de cette transition, l'IA a déjà changé la manière dont Okta protège les utilisateurs avec ses solutions Workforce Identity Cloud et Customer Identity Cloud, tout en optimisant les expériences utilisateurs et l'agilité des développeurs. Nous pensons également que l'IA permettra à d'autres entreprises de profiter d'avantages similaires.

Il est bien établi que les cybercriminels utilisent et continueront à utiliser l'IA pour optimiser leurs opérations et lancer des attaques plus personnalisées (et donc plus efficaces). Mais le défaitisme n'est pas de mise : Okta exploite elle aussi l'IA pour créer des contre-mesures efficaces qui protègent les utilisateurs et les entreprises.

Pour en savoir plus, consultez cet [article](#) de Todd McKinnon, fondateur et CEO d'Okta, sur la façon dont vous pouvez tirer parti du potentiel de l'IA et vous protéger contre les risques que pose la technologie grâce à Okta AI.

\* Tous les produits, fonctions et fonctionnalités mentionnés ici qui ne sont pas encore disponibles pourraient être distribués plus tard qu'aux dates annoncées ou annulés. Les roadmaps produits ne représentent en rien un engagement, une obligation ou une promesse d'offre de produit ou fonctionnalité, et les clients ne doivent pas se baser sur ces plans pour prendre leur décision d'achat.

Source :

1. [Battling Bots: Introducing the Identity Threat Level \(ITL\)](#)
2. [How Okta uses machine learning to automatically detect and mitigate toll fraud](#)

### À propos d'Okta

Okta est le leader indépendant des solutions de gestion des identités. Okta Identity Cloud permet aux entreprises de connecter en toute sécurité les bonnes personnes aux bonnes technologies au bon moment. Nous fournissons des accès fluides et sécurisés aux personnes et aux entreprises, où qu'elles se trouvent, leur donnant la confiance nécessaire pour réaliser leur plein potentiel. Pour en savoir plus, consultez notre site [okta.com/fr](https://okta.com/fr).