okta

# Okta AI

Artificiële intelligentie (AI) wordt met de dag krachtiger. Voor organisaties betekent AI een nieuwe stap met nieuwe mogelijkheden wat betreft efficiëntie en flexibiliteit, maar ook snellere innovatie.

Maar de belofte die AI inhoudt is niet ongezien voorbijgegaan aan kwaadwillenden. Artificiële intelligentie heeft oude tactieken, zoals phishing, nieuw leven ingeblazen. Organisaties hebben te maken met twee verschillende uitdagingen: nieuwe en creatieve manieren vinden om AI in te zetten en tegelijkertijd zichzelf beschermen tegen deze nieuwe kwaadwillenden die werken met AI.

Als Identity-bedrijf kent Okta deze uitdaging maar al te goed. AI neemt een steeds prominentere plaats in binnen onze activiteiten. AI versterkt tools die flexibiliteit in het ontwikkelen en de time-to-market versnellen, maar ook tools die bedoeld zijn als bescherming tegen zowel algemene als nieuwe securitybedreigingen.

In deze datasheet laten we u kennismaken met de vele AI-gestuurde functies in Workforce Identity- en Customer Identity-clouds. We gaan het ook hebben over Okta's kernfilosofie achter AI. We bekijken de ontwikkelingen vanuit een positief perspectief. We geloven niet alleen dat AI een technologie is die transformaties tot stand brengt, maar dat het ook elke nieuwe securitybedreiging aankan die door AI zelf wordt gecreëerd.

### Hoe aanvallers gebruikmaken van AI

**Phishing op grote schaal**
Tools voor generatieve AI kunnen in luttele seconden overtuigende, professioneel uitziende e-mails opstellen, waarvan de inhoud vaak is toegespitst op het individuele doelwit.

**Synthetische profielen**
Aanvallers kunnen met behulp van AI fotorealistische gezichten genereren, waardoor ze ogenschijnlijk geloofwaardige profielen kunnen opstellen voor gebruik in phishingaanvallen.

**Imitatie**
Sommige AI-tools kunnen de stem van een persoon met verbluffende nauwkeurigheid nabootsen, waardoor aanvallers zich kunnen voordoen als topmensen uit het bedrijfsleven bij het uitvoeren van aanvallen via vishing (voice phishing).

**Aangepaste code**
Met de mogelijkheden die generatieve AI biedt voor het schrijven van software kan een aanvaller in enkele minuten tijd snel en effectief exploits fabriceren.

**Omzeiling van CAPTCHA**
AI kan CAPTCHA-puzzels omzeilen die bedoeld zijn om onderscheid te maken tussen menselijke en geautomatiseerde gebruikers.

# Hoe Okta artificiële intelligentie gebruikt

## Functies in Workforce Identity Cloud met Okta AI

### Telephony Anti-Toll Fraud System

Met een zelf ontwikkeld ML-model (machine learning) kan Okta pogingen detecteren van kwaadwillenden die speciale telefoonnummers gebruiken bij multi-factor authenticatie (MFA), waardoor uw organisatie wordt beschermd tegen fraude en torenhoge telefoonkosten.

### ThreatInsight

Gebruikt data uit ons klantennetwerk en van admins en eindgebruikers om uw medewerkers te beschermen tegen aanvallen op basis van inloggegevens. Okta's eigen ML-model detecteert of een organisatie wordt aangevallen en signaleert schadelijke IP-adressen sneller dan ooit tevoren.

### Adaptive Multi-Factor Authentication

Biedt aanvullende informatie over Identity-flows door rekening te houden met de voortdurend veranderende context waarbinnen een authenticatieverzoek wordt uitgevoerd. Door de security- en authenticatiepolicy dynamisch aan te passen kan adaptieve MFA zowel de beveiligingsstatus als de user experience van een organisatie verbeteren.

### Policy Recommender

**Beperkte early access Q1 2024**

Biedt gepersonaliseerde aanbevelingen en templates op basis van informatie die is verzameld uit het omvangrijke ecosysteem van Okta naast best practices op securitygebied. Dat stroomlijnt het instellen van veilige authenticatieprocedures, waaronder checks van de devicestatus en phishing-bestendige authenticators.

### Log Investigator

**Beperkte early access Q3 2024**

Met behulp van NLP-technologieën (natural language processing) biedt Okta admins de mogelijkheid vragen over Okta-data te stellen in natuurlijke taal en inzicht te krijgen in de historische context van hun Identity-status. Dat maakt het gemakkelijker om schadelijke of verdachte activiteiten te identificeren.

### Identity Threat Protection

**Beperkte early access Q1 2024**

Gebruik AI voor doorlopende risico-evaluatie om beveiligingspolicies zowel tijdens het inloggen als tijdens een actieve gebruikerssessie af te dwingen om daarmee ongeautoriseerde toegang en bedreigingen na de authenticatie, zoals het kapen van sessies, te verminderen.

### Governance Analyzer

**Beperkte early access Q2 2024**

Biedt besluitvormers waardevolle context en aanbevelingen bij beoordelingen en aanvragen, met als gevolg governancebeslissingen van de hoogste kwaliteit zonder dat er aanvullend onderzoek nodig is.

okta

## Functies in Customer Identity Cloud met Okta AI

### Bot Detection

Gebruikt een machine learning-model dat werkt met meer dan 60 inputs om menselijke gebruikers te onderscheiden van geautomatiseerde gebruikers. Daarmee wordt 79% van de inlogpogingen door bots geblokkeerd, met minimale verstoring van legitieme activiteiten.

### Identity Threat Level (ITL)

Op basis van verzamelde en geanonimiseerde waarnemingen en datapatronen in ons klantenbestand berekenen we een Identity Threat Level-score om de mate van botactiviteiten in alle CIAM-loginprocedures van klanten aan te geven. Bezoekers van de microsite kunnen hun informatie invoeren en een score ontvangen die specifiek geldt voor hun sector en regio, met aanvullende filtering van kenmerken en de mogelijkheid om een gedetailleerd rapport te downloaden.

### Tenant Security Manager

**Beperkte early access Q2 2024**

Verbetert de mogelijkheden van onze Attack Protection met "intelligente" securityaanbevelingen door middel van snapshotwaarschuwingen en dashboardmeldingen om de beveiligingsstatus van uw tenant te verbeteren.

### Guide

**Beperkte early access Q4 2024**

Deze handige gids voor Okta Customer Identity Cloud biedt uitgebreide hulp bij de onboarding en zet op intuïtieve wijze de best mogelijke stappen voor gebruikers uiteen om tot een optimale workflow te komen – en dat alles op basis van aanwijzingen in eenvoudige, alledaagse taal.

### Actions Navigator

**Beperkte early access Q2 2024**

Intelligent zoeken is binnen handbereik. Vind de juiste marktintegraties op basis van datgene waarnaar u op zoek bent, zelfs als de trefwoorden waarop u zoekt afwijken van wat er is opgenomen in de titel of beschrijving van de integratie. En mocht die actie of integratie niet bestaan, dan kan onze handige AI-tool u helpen bij het schrijven van een actie op basis van de zoekopdracht of prompt en daaraan voor verder gebruik voorwaarden of de juiste bedrijfslogica toevoegen.

### Brand Customizer

**Beperkte early access Q4 2024**

U kunt de branding aanpassen door templates van één pagina te ontwerpen en die toe te passen op alle andere vereiste templates. Of geef alleen maar een screenshot of logo op, waarna de templates automatisch worden gegenereerd en door u verder kunnen worden aangepast.

### Identity Flow Optimizer

**Beperkte early access Q4 2024**

De Funnel Analytics AI-tool analyseert alle authenticatiedata van een tenant en geeft suggesties voor het verbeteren van de customer experience, het aanmeldproces en meer.

okta

# Belangrijkste cijfers

**79%**

AI helpt Okta 79% van de geautomatiseerde inlogpogingen te blokkeren en kan in 90 dagen tijd botverkeer verminderen met 90%.

**20%**

verbetering bij het detecteren van frauduleuze spraak- of sms-transacties met Okta's ML-model om misbruik van telefoonnummers te voorkomen.

# Het perspectief van Okta

Volgens ons zitten we midden in een nieuwe technologische revolutie. AI wordt net zo belangrijk als de smartphone of de cloud. Het zorgt voor betere, slimmere software met meer mogelijkheden, waardoor engineers razendsnel geavanceerde functionaliteit kunnen genereren.

Hoewel we ons nog maar net aan het begin van dit nieuwe tijdperk bevinden, heeft AI nu al de manier veranderd waarop Okta gebruikers in zijn Workforce Identity- en Customer Identity-producten beveiligt, en zijn bovendien de user experience en de mogelijkheden van developers verbeterd. We denken ook dat andere organisaties dankzij AI soortgelijke voordelen kunnen behalen.

We zien daarnaast in dat kwaadwillenden artificiële intelligentie gebruiken – en zullen blijven gebruiken – om hun activiteiten op te schalen en aanvallen uit te voeren die nog meer op de persoon gericht zijn en daardoor nog effectiever zullen zijn. Maar we gaan niet bij de pakken neerzitten. Okta gaat AI inzetten om effectieve tegenmaatregelen te treffen ter bescherming van gebruikers en organisaties.

U kunt meer informatie vinden in dit artikel van Okta-oprichter en CEO Todd McKinnon over hoe u de toekomst van AI vorm kunt geven en hoe u zich met Okta AI kunt beschermen tegen de risico's die de technologie met zich meebrengt.

*Producten, functies of functionaliteit waarnaar in dit document wordt verwezen en die momenteel niet algemeen beschikbaar zijn, worden mogelijk niet op tijd of in het geheel niet geleverd. Productroadmaps houden geen toezegging, verplichting of belofte in tot het leveren van een product, functie of functionaliteit, en u moet daar niet op vertrouwen bij uw aankoopbesluiten.

Bron:

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

**Over Okta**

Okta is de toonaangevende onafhankelijke Identity-provider. De Okta Identity Cloud stelt organisaties in staat om de juiste mensen op het juiste moment veilig te verbinden met de juiste technologieën. Het is ons doel om mensen en organisaties over de hele wereld eenvoudig en veilig toegang te bieden, zodat ze hun potentieel volledig kunnen benutten. Ga voor meer informatie naar **okta.com/nl**