Whitepaper

Okta en AI

Hoe artificiële intelligentie Identity and Access Management (IAM) opnieuw definieert

Inhoud

Samenvatting

In het algemeen kan worden gesteld dat artificiële intelligentie (AI) een nieuwe definitie geeft aan de manier waarop organisaties opereren en aanzet tot innovatieve producten en services door optimalisering, data-analyse, detectie van onregelmatigheden en andere op voorspellingen gebaseerde applicaties te veralgemeniseren. Dergelijke functionaliteit is voor het merendeel niets nieuws. Wat wel nieuw is, is dat het door kostenbesparingen en prestatieverbeteringen gemakkelijker is geworden om zulke mogelijkheden te integreren in eigenlijk alles wat u maar wilt.

Ook nieuw is de ogenschijnlijk plotselinge komst van generatieve AI, vanwege de snelle vooruitgang in Large Language Models (LLM's) in de kern van applicaties zoals ChatGPT en DALL-E van OpenAI, Bard van Google en Code Llama van Meta.

In onze ogen staat generatieve AI voor een onvervalste paradigma-verschuiving die eens per generatie voorkomt en waarvan de impact nog maar net te merken, laat staan te begrijpen is.

En er zijn maar weinig domeinen die zo geschikt zijn voor de toepassing van AI als Identity. Identity is niet alleen complex (zodat er met AI heel wat kan worden verbeterd), maar Identity-flows en -transacties produceren ook gigantische hoeveelheden data, wat precies de brandstof vormt voor AI-engines. Hoewel we ernaar streven datanetwerkeffecten toe te passen in het gehele Identity-domein, zetten we op de korte termijn onze investeringen in onderzoek en ontwikkeling in voor het volgende:

- Security versterken
- Productiviteit vergroten
- User experiences verbeteren

AI is niets nieuws voor het Okta-team en we hebben de mogelijkheden ervan al toegepast op diverse cruciale gebieden. Enkele voorbeelden:

- De Okta Workforce Identity Cloud (WIC) past AI toe in ThreatInsight, Adaptieve multi-factor authenticatie (Adaptieve MFA) en in onze maatregelen tegen Anti-Toll Fraud
- De Okta Customer Identity Cloud (CIC) werkt met AI in de Bot Detection-functie (en het bijbehorende Identity Threat Level, ofwel ITL) en in Adaptieve MFA

Bovendien hebben we tijdens Oktane 2023 een aantal nieuwe AI-gestuurde functies aangekondigd. Okta AI kwam met vier nieuwe WIC-mogelijkheden voor de volgende toepassingen:

- Security versterken Bescherming tegen identitybedreigingen
- Ondersteuning voor governance: Governance Analyzer
- Beheer vereenvoudigen: Log Investigator, Policy Recommender

De CIC kreeg zes nieuwe functies voor deze toepassingen:

- Tenantsecurity versterken: Securityaanbevelingen
- Customer experience verbeteren en omzet vergroten: Funnel Conversion Recommendations, Brand Customization
- Beheer vereenvoudigen: Co-Pilot, Action Selection and Development, Personalized Tenant Configuration Summary

Daarnaast stimuleren we een op innovatie gerichte cultuur, die tot uitdrukking komt tijdens twee hackathons per jaar waar de hele organisatie aan meedoet. Veel van de ideeën die tijdens deze hackathons naar boven komen, worden uitgewerkt tot patenten en proof-of-concepts voor producten en komen uiteindelijk in de een of andere vorm op de markt terecht. Tijdens een recente hackathon experimenteerde 25% van de projecten met AI en we zijn enthousiast over wat daaruit is voortgekomen.

Gelet op zowel het belang van AI als de opwinding die het teweegbrengt onder developers hebben we voor het eerst een op AI toegespitste hackathon gepland.

Ook hebben we onze klanten geholpen bij het opzetten van inspirerende en elegante ervaringen met LLM's. Verder biedt het bredere Okta-ecosysteem – denk daarbij aan Okta Ventures, het Okta Integration Network, Auth0 for Startups en de Auth0 Marketplace – een uitgebreid netwerk aan AI-oplossingen die kunnen worden geïntegreerd met onze Okta-producten.

De toekomst zal ongetwijfeld de nodige uitdagingen met zich meebrengen. Zo maken cybercriminelen nu al gebruik van AI in het algemeen en van LLM's in het bijzonder om nieuwe aanvalsvectoren uit te proberen en om bestaande aanvallen nog gevaarlijker te maken. Desondanks blijven we optimistisch dat AI een kracht ten goede kan en zal zijn.

Tegenwoordig beheren digitale identities de toegang tot steeds meer applicaties en services, en zijn daarmee van invloed op – en bepalen in zekere mate – tal van aspecten van het moderne leven. In de toekomst wordt die invloed alleen maar groter en worden authenticatie, autorisatie en Identity in het algemeen van vitaal belang voor het behoud van vertrouwen en security, en vormen digitale identities de basis van geweldige user experiences.

Wij streven ernaar om de kracht van AI in te zetten om de verbinding tussen mensen, technologie en gemeenschap te versterken.

Inleiding

De afgelopen maanden zijn in de tech- en nieuwsmedia tal van artikelen verschenen over doorbraken in artificiële intelligentie (AI) en de toepassingen, waarvan er sommige wel en andere niet te verwachten waren, die daardoor mogelijk werden.

Andy Grove van Intel wist het bondig te formuleren: "Je moet paranoïde zijn om te overleven". Het zou dan ook niet verrassend moeten zijn dat grote en kleine organisaties in allerlei sectoren zich haasten om AI in te zetten om bestaande oplossingen te verbeteren, nieuwe oplossingen te ondersteunen en de metaforische kloof te verbreden om de concurrentie op afstand te houden.

Voor een groot deel is onze investering in opkomende AI business as usual. AI stuurt al een aantal belangrijke producten en tools in ons portfolio aan. Met name machine learning (ML) vormt de kern van een groot deel van onze dynamische risicobeoordeling en op risico gebaseerde authenticatie.

We hebben geleerd van jaren praktische ervaring en beschouwen AI dan ook niet als een afzonderlijke module of functionaliteit, als iets dat simpelweg aan ons platform kan worden gekoppeld of toegevoegd. We gaan er liever vanuit dat AI een technologie voor algemeen gebruik is (of beter gezegd, een verzameling technologieën voor algemeen gebruik) die het meest effectief is wanneer deze is ingebed binnen en geïntegreerd met een Identity-infrastructuur.

In deze whitepaper willen we wat meer achtergrondinformatie geven over de relatie van Okta met AI, en wel aan de hand van de volgende punten:

- Waarom AI de belofte inhoudt om praktisch elk digitaal domein te transformeren en te hervormen
- Waarom Identity zo geschikt is om te profiteren van AI
- De leidende waardeproposities die we voor AI in de directe toekomst zien
- Hoe wij AI al in de Okta Workforce Identity Cloud (WIC) en Okta Customer Identity Cloud (CIC) toepassen
- Hoe wij Okta AI inzetten voor nieuwe WIC- en CIC-functionaliteiten

Waarom AI?

Op elementair niveau kan artificiële intelligentie worden beschouwd als een beslissing van een computer waarbij de "slimheid" van de computer niet te onderscheiden is van een door mensen genomen beslissing, ongeacht hoe die beslissing wordt genomen.

Hoewel het concept van AI formeel werd geïntroduceerd tijdens de Dartmouth Workshop in 1956, dateert het oorspronkelijke uitgangspunt van 1943, toen logicus Walter Pitts en neurowetenschapper Warren McCulloch een wiskundige weergave van de neuronen in het menselijk brein probeerden te maken. Deze hedendaagse ontwikkelingen berusten op een lange historie van vooruitgang in de berekenbaarheidstheorie, vanaf Ada Lovelace in de negentiende eeuw tot Alan Turing in de vorige eeuw.

Sinds de jaren 60 van de vorige eeuw heeft AI zich ontwikkeld tot een grote verzameling algoritmen, waaronder de detectie en herkenning van patronen, die doorgaans wordt uitgevoerd door machine learning (ML). ML heeft zich de laatste 15 jaar zeer sterk ontwikkeld, met de opkomst van praktische en rendabele deep learning.

Generatieve AI is een paradigmaverschuiving die eens per generatie voorkomt

De ontwikkeling in AI die de wereld stormenderhand wist te veroveren is de ongelooflijke – en velen zouden zeggen, de verbijsterende – komst en razendsnelle evolutie van generatieve AI, die voornamelijk het gevolg is van een opmerkelijke vooruitgang in Large Language Models (LLM's).

Door applicaties op basis van LLM's, zoals ChatGPT en DALL-E van OpenAI, werd AI gangbaar, deels vanwege het vermogen om mensen na te bootsen en deels vanwege het ontbreken van transparantie wat betreft de door het model opgenomen data (waardoor het model vorm wordt gegeven).

Plotseling zijn het schrijven van teksten en het creëren van complexe (en levensechte, als dat de bedoeling is) afbeeldingen niet langer uitsluitend het domein van mensen. Omdat LLM's zo bedreven zijn in schrijven, en programmeren een manier van schrijven is, worden nu veel dingen geregeld door software en zijn LLM's dus de motor achter onverwachte doorbraken en ontwikkelingen in een scala van domeinen.

Het is duidelijk dat we een nieuw tijdperk in AI betreden. Het is dan ook niet vreemd om ons af te vragen hoe de mogelijkheden ervan – oude, nieuwe en andere die we nog niet kennen – benut moeten worden.

Wat kan AI allemaal?

In hun boek Prediction Machines beschouwen economen Ajay Agrawal, Joshua Gans en Avi Goldfarb de opkomst van AI als het verlagen van de kosten voor voorspelling, die zij definiëren als het gebruikmaken van beschikbare informatie om nieuwe informatie te genereren.

Omdat voorspelling "de kern vormt van besluitvorming bij onzekerheid (decision making under uncertainty)" en "ons zakelijk leven en ons privéleven vol zitten met zulke besluiten", biedt het verlagen van de kosten voor voorspelling een buitengewoon potentieel. Hier zijn enkele voorbeelden die laten zien dat voorspelling een essentieel onderdeel is van:

- Optimalisering: het gebruik van context en eerdere observaties om optimale paden, reacties, configuraties, UI-ontwerpen, enzovoort te voorspellen.
- Gedragsanalyse: het observeren van realtime gedrag in de context van eerdere acties om de intentie van een gebruiker te voorspellen.
- Datamining: het voorspellen welke data en inzichten het beste voldoen aan de vraag of melding van een gebruiker (we wijzen er in dit verband nog maar eens op dat voorspelling ook de kern vormt van LLM's en generatieve AI).

Net zoals klassieke computermodellen is AI (in al zijn vormen) een technologie voor algemeen gebruik die de belofte inhoudt om bestaande sectoren te transformeren en te hervormen, en we zijn met name optimistisch over het potentieel van AI om de verdere ontwikkeling van Identity een boost te geven.

AI en Identity

Een digitale identity bestaat uit de reeks attributen waarmee een bepaalde gebruiker wordt gedefinieerd binnen de context van een functie die door een bepaalde applicatie wordt geleverd. Tegenwoordig beheren digitale identities de toegang tot steeds meer applicaties en services, en zijn daarmee van invloed op – en bepalen in zekere mate – tal van aspecten van het moderne leven. In de toekomst wordt die invloed alleen maar groter en worden authenticatie, autorisatie en Identity in het algemeen van vitaal belang voor het behoud van vertrouwen en security, en vormen digitale identities de basis van geweldige user experiences.

Dat maakt IAM-services tot de hoekstenen van onze digitale wereld door ervoor te zorgen dat alleen bevoegde gebruikers, zoals werknemers, externen, partners en klanten, toegang hebben tot bepaalde resources. Conceptueel ziet IAM er heel eenvoudig uit: gebruikers bewijzen hun identiteit en krijgen toegang tot een resource waartoe ze gerechtigd zijn. Maar in de praktijk zijn er diverse factoren die het ingewikkeld maken:

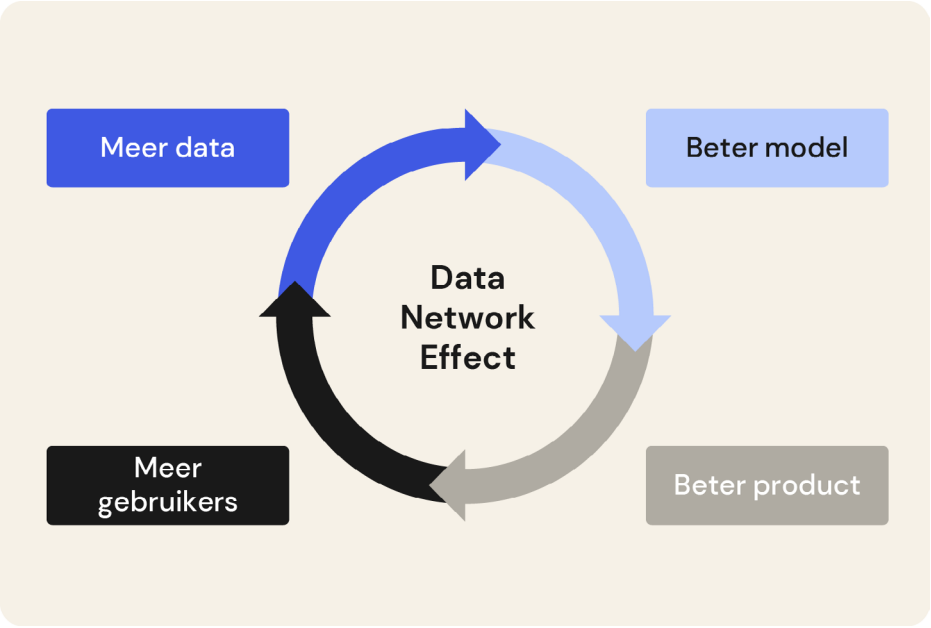
- De digitale wereld van vandaag kent vele gebruikers. Iedere gebruiker kan vele digitale identiteiten aannemen en er zijn talloze manieren om uitdrukking te geven aan een digitale identiteit.
- Verschillende digitale identiteiten hebben verschillende rechten en autorisaties wat betreft resources, en deze rechten en autorisaties worden steeds dynamischer.
- Nu securityperimeters steeds meer vervagen, richten aanvallers zich op Identity.

Zoals we hebben gezien, is AI uitermate geschikt om om te gaan met complexiteit en onzekerheid, gesteld dat er voldoende data beschikbaar is.

Gelukkig beschikt het Identity-domein over voldoende data, omdat Identity zelf zich heeft ontwikkeld van een statisch, eendimensionaal attribuut tot dynamische, continue interactie, waarbij het zichzelf opnieuw definieert met elk nieuw datapunt. Deze ontwikkeling zou niet mogelijk zijn geweest zonder de eerdere cloudtransformatie en de ontwikkeling blijft alleen maar doorgaan dankzij de huidige transformatie door AI.

Datanetwerkeffecten

Een belangrijke consequentie van deze ontwikkeling is dat er een virtuele cyclus van datanetwerkeffecten ontstaat: hoe groter het volume en hoe hoger de kwaliteit van data waartoe een AI-model toegang heeft, des te sneller het kan leren en des te nauwkeuriger de voorspellingen of beslissingen worden. Daardoor krijgt het product of de service meer waarde voor zijn gebruikers, wat weer meer gebruikers aantrekt, die op hun beurt meer data genereren, die vervolgens aan het model worden toegevoegd, waardoor er een virtuele cyclus ontstaat:



1. **Meer data:** hoe vaker een product of service wordt gebruikt, hoe meer data wordt gegenereerd met interacties, transacties, feedback, enzovoort, van gebruikers.
2. **Beter model:** deze data wordt gebruikt om het onderliggende AI-model te verfijnen. Hoe groter het volume en hoe hoger de kwaliteit van de data, hoe nauwkeuriger de voorspellingen of beslissingen van het model.
3. **Beter product:** naarmate het AI-model beter wordt, geldt dat ook voor het product of de service.
4. **Meer gebruikers of gebruik:** het verbeterde product of de verbeterde service trekken meer gebruikers aan, die nog meer data genereren en zo de cyclus voortzetten.

Deze zichzelf versterkende cyclus kan een sterke kracht achter innovatie en competitieve differentiatie zijn.

Security versterken

Het is inmiddels wel duidelijk dat met AI het volgende kan gebeuren:

- Bestaande aanvallen op Identity, zoals credential stuffing en phishing, worden gevaarlijker (bijvoorbeeld moeilijker te detecteren, effectiever/destructiever)
- Er ontstaan totaal nieuwe typen aanvallen op Identity, waarvan er vele pas worden opgemerkt nadat ze hebben toegeslagen
- Sommige bestaande beveiligingsmaatregelen worden overwonnen (zoals het oplossen van CAPTCHA's, het misleiden van biometrische spraaksystemen)

Daar komt bij dat door de coderings- en scriptingmogelijkheden van generatieve AI allerlei criminelen, of ze nu wel of niet kunnen coderen, gemakkelijker aanvallen kunnen opzetten, waardoor er mogelijk nog meer mensen zich aangetrokken voelen tot het cybercriminele ecosysteem en de aanvallen nog effectiever worden.

Maar hoewel AI ongetwijfeld door aanvallers gebruikt zal worden, fungeert het ook als een krachtig beschermingsmiddel.

Okta is al toonaangevend in de sector met de phishingbestendige FastPass-authenticatie, geschikt voor elk platform voor zowel beheerde als niet beheerde devices, waardoor developers gemakkelijker gebruikersvriendelijke en phishingbestendige FIDO2-authenticatie kunnen toepassen. Maar we zien ook in dat AI gebruikt moet worden voor het volgende:

- **Verdere beveiliging van Okta by design**: net zoals criminelen AI kunnen gebruiken om kwetsbaarheden en beveiligingshiaten op te sporen, doen organisaties zoals Okta dat ook. Wij hebben als voordeel dat we met AI software en systemen veiliger kunnen maken nog voordat die uitgebracht worden.
- **Detectie van bedreigingen automatiseren:** contextuele en gedragsanalyse is al in staat intelligente risicobeoordelingen te maken en geavanceerde aanvallen op Identity te detecteren. En door de verdere ontwikkeling van AI zijn we beter in staat deze functies te verbeteren en nieuwe te introduceren.
- **Risico's beperken namens onze klanten:** of het nu gaat om het automatiseren van defensieve maatregelen (zoals inperkingsacties en het blokkeren van schadelijke activiteiten), het combineren van een alarm met een aanbevolen playbook of het ondersteunen van GRC-initiatieven (governance, risicobeheer en compliance), AI gaat onmisbaar worden in het proactief verkleinen van risico's en het reageren op aanvallen.

Gelukkig beschikken we al over een schat aan ervaring met het integreren van AI-gestuurde securityfuncties in onze Workforce Identity Cloud en Customer Identity Cloud.

Dit veranderende bedreigingslandschap bracht Gartner tot de volgende waarschuwing: **"Tot in 2025 zullen aanvallen die gebruikmaken van generatieve AI, beveiligingsbewuste organisaties ertoe dwingen de drempels voor het detecteren van verdachte activiteiten te verlagen, waardoor er vaker sprake is van vals alarm en er dus vaker, en niet minder vaak, een reactie van mensen vereist is."**

[1] Gartner, 4 Ways Generative AI Will Impact CISOs and Their Teams, Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook, 29 juni 2023) GARTNER is een gedeponeerd handelsmerk en servicemerk van Gartner, Inc. en/of haar dochterondernemingen in de Verenigde Staten en andere landen en wordt met toestemming gebruikt. Alle rechten voorbehouden.

Productiviteit vergroten

Een van de voornaamste bevindingen van ons How Development Teams Purchase SaaS — 2023 Report is dat er in wezen twee typen ontwikkelingsorganisaties zijn: organisaties die AI al gebruiken voor productengineering (52% van de respondenten) en organisaties die dat binnen een jaar gaan doen (45%).

Op zoek naar een heel pakket aan voordelen, en dan met name flexibiliteit, nieuwe mogelijkheden, kostenbesparing en tijdsbesparing, integreren organisaties AI-tools voor data-analyse, kwaliteitsborging, machine learning, automatisering en tal van andere toepassingen.

Wij delen dit optimistische vooruitzicht van het potentieel van AI om de productiviteit binnen onze eigen engineeringorganisatie te vergroten.

Tegelijkertijd erkennen we dat de toepassing van AI nog veel verder moet gaan, en wel naar alle partijen van praktisch elke klantorganisatie, ongeacht grootte of sector.

Een moderne en volwassen Identity-infrastructuur voor organisaties heeft de volgende kenmerken:

- Het stelt medewerkers, externen en zakelijke partners met frictieloze en veilige toegang tot cruciale tools en resources in staat om vanaf elke gewenste locatie te werken.
- Het biedt een praktische user experience, vergroot de operationele efficiëntie en vermindert de administratieve lasten, zodat er tijd en energie vrijkomt om meer aandacht te geven aan groei, innovatie en andere prioriteiten.
- Het stelt de organisatie in staat om op te schalen en de flexibiliteit voortdurend te verbeteren.
- Het helpt te beschermen tegen verstoringen veroorzaakt door kwaadwillenden.

Door AI volledig te integreren in een Identity-infrastructuur, kunnen al deze voordelen worden verwezenlijkt en zullen er ongetwijfeld nieuwe bijkomen.

User experiences verbeteren

Laten we ook eens kijken naar frictie.

Voor klantenorganisaties is frictie, dat wil zeggen alles wat de interactie van een persoon met uw service tegenwerkt, een groot obstakel bij het genereren van conversies en, bijgevolg, voor de omzet. Het Rapport Customer Identity-trends van Okta liet zien dat bijna 60% van de respondenten aangaf dat ze waarschijnlijk meer zouden uitgeven wanneer services een eenvoudig, veilig en frictieloos loginproces zouden hebben. Dit geldt voor alle branches en sectoren en maakt duidelijk dat gebruikers bij elke interactie vragen om gebruiksgemak.

Uiteraard is enige mate van frictie noodzakelijk voor het vertrouwen en om beveiligingsmaatregelen in te stellen, maar door de frictie waar mogelijk te verminderen voor elke klantinteractie, kan het conversiepercentage toenemen en als gevolg de omzet worden vergroot op zowel de korte als de lange termijn.

Waar kan AI worden toegepast? Drie voor de hand liggende toepassingen:

- Het leveren van constante risicobeoordelingen voor passwordless en loginless experiences
- Het optimaliseren van Identity-flows voor het gemak van de gebruiker
- Het verbeteren van UI-ontwerpen (tijdens Identity-transacties) voor het gemak van de gebruiker

Binnen de context van de werkplek kan frictie worden gezien als alles wat het voltooien van een taak tegengaat of vertraagt. Hoewel Identity (op zichzelf) een vergadering niet op tijd kan laten beginnen of een collega kan aansporen eerder op een vraag te reageren, kan een volwassen Identity-infrastructuur wel op andere manieren een bijdrage leveren, zoals:

- Ervoor zorgen dat gebruikers toegang hebben tot de juiste resources (zoals data, systemen, applicaties), met de juiste toegangsrechten en op het juiste moment.
- Het ondersteunen van selfservicemogelijkheden (zoals toegang vragen tot resources, profielen aanpassen, securityfactoren inschrijven, enz.).
- Het automatiseren van bestaande processen (zoals toegang tot reviews en certificeringen, veilige offboarding, enz.).

Ook hier geldt dat AI deze bestaande mogelijkheden kan versterken, maar ook nieuwe mogelijkheden kan ontsluiten. AI kan bijvoorbeeld hele reeksen Identity-implementaties en prestatiestatistieken analyseren om te bepalen wat de meest efficiënte en effectieve configuraties zijn en deze informatie vervolgens gebruiken voor aanbevelingen die specifiek zijn afgestemd op elke organisatie of afdeling. AI kan ook admins helpen om snel de benodigde informatie te lokaliseren binnen een hoeveelheid operationele en logindata die anders veel te groot zou zijn.

Daar komt bij dat door het gebruik van natuurlijke taal in LLM's nog meer Identity-gerelateerde functies toegankelijk worden voor gebruikers die zelf niet kunnen programmeren. Okta Workflows werkt al met no-code Identity-automatisering en -orkestratie middels een drag-and-drop interface. Het is dan ook niet zo moeilijk om je een oplossing voor te stellen die instructies in natuurlijke taal accepteert.

AI in de Workforce Identity Cloud (WIC)

Waar Identity voorheen alleen werd beschouwd als een hulpmiddel voor het beheren van gebruikersnamen en wachtwoorden, is het nu een vereiste, en facilitator, voor elke moderne organisatie geworden. Dat maakt van de Identity-infrastructuur een basislaag die onderling verbonden is binnen de bredere IT-omgeving en gebruikers en andere entiteiten verbindt met systemen, data en resources zowel on-prem als in de cloud.

Dat maakt het beveiligen van Identity tot een fundamenteel element van een krachtige beveiligingsstatus, waarmee misbruik van binnenuit en van buitenaf met gestolen inloggegevens kan worden voorkomen.

Niet alleen beschermt de Identity-infrastructuur tegen bedreigingen, AI is ook bij uitstek geschikt voor de ondersteuning van governanceactiviteiten, met name door het onderzoeken van grote hoeveelheden configuratiedata om risico's te identificeren, corrigerende maatregelen aan te bevelen en zelfs tal van algemene en belangrijke taken te automatiseren.

Omdat AI goed is in het analyseren van gegevens en het naar boven halen van inzichten, is het ook zeer geschikt voor het interpreteren van grote hoeveelheden logboeken.

Door deze functionaliteiten te koppelen aan de verwerking van natuurlijke taal en generatieve AI kunnen admins nu al op een effectievere manier die alsmaar uitdijende Identity-infrastructuur beheren.

In hun rapport over 2022, Trends in Securing Digital Identities, gebaseerd op een onderzoek onder meer dan 500 IAM- en securityprofessionals, meldt de Identity Defined Security Alliance (waarvan Okta lid is) het volgende:

- **84%** van de respondenten gaf aan dat hun organisatie het afgelopen jaar te maken heeft gehad met een Identity-gerelateerd lek
- **78%** meldde een rechtstreekse impact op hun zakelijke activiteiten als gevolg van een lek
- **64%** gaf te kennen dat het effectief beheren en beveiligen van digitale identiteiten hun topprioriteit voor security is (16%) of tot de top-3 behoort (48%)

ThreatInsight

De rol van AI: voorspelt op basis van observaties en geautomatiseerde feedback van aanvallen en authenticatieverzoeken in het klantenbestand van Okta of verzoeken wel of niet van een schadelijke bron afkomstig zijn

ThreatInsight is een elementaire securityfunctie voor het detecteren en afslaan van grote hoeveelheden aanvallen op basis van inloggegevens (password spraying, credential stuffing en soortgelijke brute-force-aanvallen) gericht tegen Okta-endpoints. Een klant hoeft alleen maar de blokkeringsmodus in de Okta Admin Console te selecteren om automatisch verzoeken te weigeren waarvan wordt voorspeld dat ze schadelijk zijn nog voordat aanvallers proberen te authenticeren, of de logboekmodus om schadelijk verkeer vast te leggen.

Om elke dag weer de effecten op het netwerk van de vele miljoenen authenticatieverzoeken aan duizenden Okta-organisaties aan te kunnen, hanteert ThreatInsight een combinatie van heuristiek (statische regels) en machine learning om informatie uit aanvallen met inloggegevens te observeren en af te leiden.

Voor elk bekend schadelijk IP-adres dat op de perimeter wordt geblokkeerd ziet Okta veel meer verdachte gebeurtenissen afkomstig van IP-adressen die niet met 100 procent zekerheid als schadelijk kunnen worden aangemerkt. Er kan sprake zijn van een legitieme use case voor meerdere mislukte logins afhankelijk van het scenario, bijvoorbeeld wanneer een hotel een grote conferentie organiseert. In dergelijke scenario's is het niet zo gek als er tientallen, honderden of zelfs duizenden loginfouten optreden voor meerdere accounts in verschillende Okta-organisaties, en die dan allemaal van dezelfde bron blijken te komen: het netwerk van het hotel zelf. Door die IP-adressen te blokkeren kunnen ook legitieme authenticatiepogingen worden geblokkeerd, wat uiteindelijk net zo erg kan zijn als slachtoffer worden van een DDoS-aanval.

Om zulke vals-positieven te voorkomen, worden verdachte IP-adressen gedefinieerd als IP-adressen die betrokken zijn bij Identity-aanvallen op het gehele klantenbestand van Okta. Met andere woorden, alleen IP-adressen waarvan bekend is dat ze deelnemen aan aanvallen worden toegevoegd aan de ThreatInsight-database, en dat is in het voordeel van alle Okta-klanten.

Het is belangrijk te weten dat ThreatInsight werkt met een 'rolling window', waardoor verdachte IP-adressen die bij de volgende evaluatie geen verdachte activiteiten meer vertonen, uit de database worden verwijderd.

Adaptieve MFA

De rol van AI: biedt contextuele informatie die wordt gekoppeld aan een geschikte authenticatiemethode door risico's te voorspellen die verbonden zijn aan authenticatiegebeurtenissen (zoals inloggen) en acties die plaatsvinden na authenticatie (zoals toegang vragen tot een bepaalde resource)

Adaptieve multi-factor authenticatie (AMFA) biedt aanvullende informatie over Identity-flows door rekening te houden met de voortdurend veranderende context waarbinnen een authenticatieverzoek wordt gedaan. Door de security- en authenticatiepolicy dynamisch aan te passen kan adaptieve MFA zowel de beveiligingsstatus als de user experience van een organisatie verbeteren.

Een policy met adaptieve MFA kan bijvoorbeeld de frictie voor gebruikers verminderen door minder vaak om MFA te vragen wanneer gebruikers zich aanmelden via SSO of via een beheerd of bekend device. Maar dezelfde oplossing met adaptieve MFA kan ook vragen naar een extra of veiligere authenticatiefactor wanneer het aan een verzoek gekoppelde risico hoger wordt ingeschat, zoals een loginpoging op een ongebruikelijk tijdstip of vanaf een nieuw device, of als een ingelogde gebruiker bijzonder gevoelige resources of informatiebronnen probeert te openen.

De mate van flexibiliteit en controle die wordt geboden door een oplossing met adaptieve MFA is in hoge mate afhankelijk van de beschikbare MFA-factoren en de hoeveelheid contextuele informatie die in de risicobeoordeling is opgenomen.

Binnen adaptieve MFA onderzoekt een intelligente agent een scala van risicosignalen – zoals data over gebruikers-ID's, device, netwerk, locatie, reisgedrag en IP-adres, en externe data afkomstig van derden en integraties voor endpointsecurity – om afwijkingen te categoriseren en om op risico's gebaseerde authenticatie toe te passen bij elke stap van het authenticatieproces, zelfs nog nadat de gebruiker is ingelogd (bijvoorbeeld voor step-up authenticatie).

Anti-Toll Fraud

De rol van AI: detecteert afwijkingen en categoriseert risico's gekoppeld aan telefonische transacties op basis van een reeks inputs (bijvoorbeeld IP-adres, netnummer, land)

International revenue share fraud (IRSF), ook wel bekend als frauduleus telefoongebruik, is een type fraude waarbij fraudeurs kunstmatig een grote hoeveelheid internationale gesprekken/sms-berichten over dure routes genereren. Vanwege de hoge kosten die gepaard gaan met internationale telefonische transacties, kan frauduleus telefoongebruik aanzienlijke financiële gevolgen hebben voor organisaties die telefoongesprekken of sms-berichten in hun MFA-proces gebruiken.

Het Anti-Toll Fraud-systeem beschermt klanten en biedt tegelijkertijd een betrouwbaar telefoongebruik door gebruik te maken van aanvullende detectiemechanismen in de vorm van een heuristiekengine en meerdere ML-engines.

In grote lijnen komt het erop neer dat aan elke transactie een risicomarker wordt toegewezen. Transacties met een hogere risicofactor krijgen striktere limieten toegewezen (ga naar deze blog voor meer informatie over hoe deze componenten werken en hoe ze worden opgenomen in het Anti Toll Fraud-systeem).

Het is opvallend dat de introductie van de ML-componenten leidde tot een verbetering van 20% in het effectief detecteren van frauduleuze transacties.

Identity Threat Protection met Okta AI

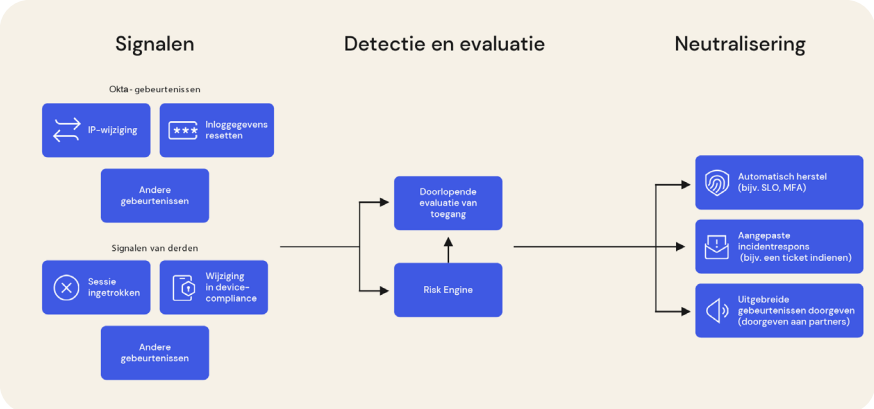
Beperkte early access Q1 2024

De rol van AI: het ML-model past risicoscores automatisch aan verschillende contexten aan voor een nauwkeurigere en genuanceerdere beoordeling die geschikt is voor dynamische omgevingen

Bescherming tegen moderne Identity-bedreiging vereist een gelaagde aanpak die al begint voordat een gebruiker authenticatie uitvoert en die doorgaat gedurende de hele sessie. Met name van continue authenticatie wordt verwacht dat deze belangrijker wordt, omdat krachtigere authenticatietechnieken steeds meer worden toegepast en criminelen daarop reageren door nog meer resources MFA te laten omzeilen en actieve sessies te kapen.

Identity Threat Protection met Okta AI biedt bescherming tegen geavanceerde Identity-bedreigingen met drie cruciale functies:

1. **Continuous Risk Evaluation** gebruikt AI 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.
2. **Shared Signals Pipeline** verbetert de zichtbaarheid van bedreigingen in het tech-ecosysteem, zodat securityteams bedreigingen tussen verschillende securitytechnologieën, waaronder oplossingen voor Mobile Device Management (MDM), Cloud Access Security Broker (CASB), netwerksecurity en Endpoint Detection & Response (EDR), kunnen detecteren en erop kunnen reageren.
3. **Adaptive Actions** reageert op realtime bedreigingen door gebruik te maken van gerichte acties zoals Universal Logout vanuit ondersteunde applicaties met de functie ingeschakeld, door gebruikers te vragen om on-demand multi-factor authenticatie in te schakelen en geautomatiseerde workflows uit te voeren om opkomende bedreigingen aan te pakken.



Governance Analyzer met Okta AI

Beperkte early access Q2 2024

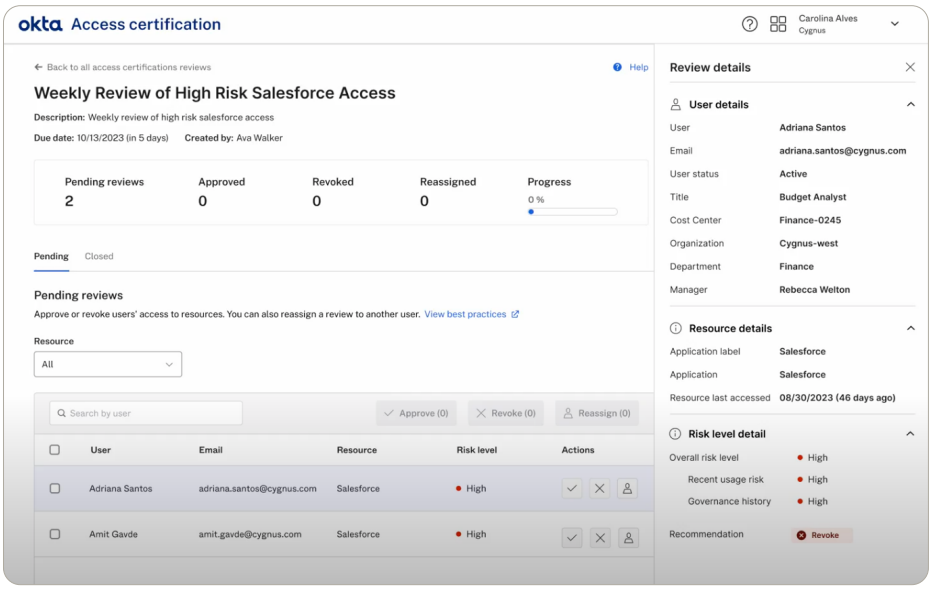
De rol van AI: gebruikt een breed scala aan signalen van devicetoegang, signalen van gebruikerstoegang en andere kritische contextuele signalen om praktische inzichten in Identity-governance te bieden

- Identity Governance and Administration (IGA) is een op policies gebaseerde aanpak van identity management en toegangscontrole waarin het volgende is gecombineerd:
- Identity-governance: processen en policies die betrekking hebben op de scheiding van functies, rol management, inloggen, herziening van toegangsrechten, analytics en rapportage
- Identity-beheer: account- en inloggegevensbeheer, provisioning en deprovisioning van gebruikers en devices, en toewijzing van rechten

Okta's positie als geconsolideerd platform voor IAM, IGA en Privileged Access Management (PAM) biedt een ongekend omvangrijke Identity-dataset waarmee organisaties kunnen voldoen aan compliancevereisten en de informatiebehoefte voor audits, de efficiëntie van processen kunnen verbeteren en voor een hogere productiviteit van medewerkers kunnen zorgen.

Governance Analyzer met Okta AI ondersteunt deze doelen om met behulp van machine learning, signalen van devicetoegang en signalen van gebruikerstoegang het volgende te bewerkstelligen:

- Minder noodzaak voor aanvullend onderzoek door besluitvormers in governanceprocedures
- Niet-triviale inzichten in de risico's van de combinatie gebruiker-resource
- Met de reikwijdte van Okta-data inzichten bieden waartoe andere leveranciers niet in staat zijn



Dit zijn bijvoorbeeld enkele mogelijke toepassingen van Governance Analyzer:

- Onderbouwen van een beslissing of een gebruiker wel of geen toegangsrechten krijgt (bijvoorbeeld in een verzoek) of dat toegangsrechten moeten worden uitgebreid (bijvoorbeeld in een certificering)
- Vaststellen wie toegang kan aanvragen tot een bepaalde resource (bijvoorbeeld alleen gebruikers onder een bepaalde risicodrempel kunnen toegang aanvragen)
- Instellen van wie de toegang wordt beoordeeld in een campagne (bijvoorbeeld alle gebruikers boven een bepaalde risicodrempel worden automatisch of vaker gecontroleerd)
- Automatisch actie ondernemen om wel of geen toegang te verlenen, hetzij in een verzoek, hetzij in een certificeringscampagne
- De juiste governanceconfiguraties aanbevelen om ervoor te zorgen dat cruciale resources over de vereiste goedkeuring beschikken om toegang te krijgen en dat de toegang regelmatig wordt gecontroleerd

Log Investigator met Okta AI

Beperkte early access Q3 2024

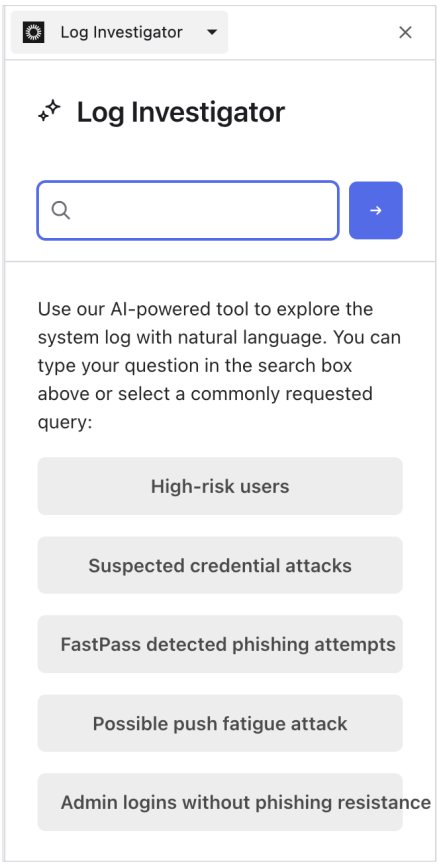
De rol van AI: ondersteuning bieden voor een logboek- en API-zoekfunctie met natuurlijke taal zodat IT-medewerkers snel en gemakkelijk informatie en inzichten kunnen vinden in de enorme dataset van Okta

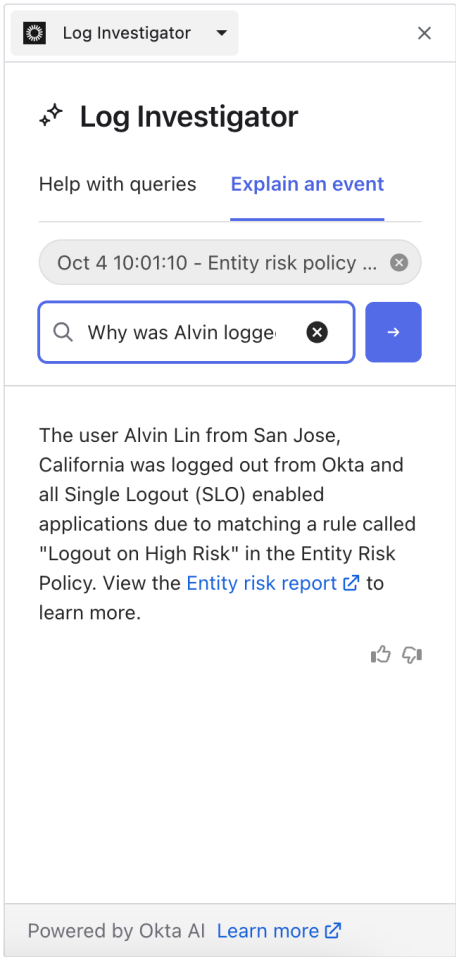
AI sinds de komst van de computer hebben logboeken gediend als waardevolle informatiebronnen om te bepalen wat er is gebeurd, en waarom. Maar sinds digitale technologieën steeds meer aspecten van de activiteiten van organisaties gingen controleren en die controle steeds gedetailleerder werd, is het volume van logboeken gigantisch toegenomen en werd het steeds moeilijker de daarin opgenomen inzichten eruit te halen. In veel IT-systemen vergt het vinden van een antwoord op zelfs de eenvoudigste vragen vaak zorgvuldig samengestelde query's en/of aanzienlijke handmatige inspanningen om honderden resultaten uit te kammen, wat de nodige tijd en middelen in beslag neemt die toch al schaars zijn.

Maar gelukkig transformeert generatieve AI de manier waarop mensen werken met datasets om daar bruikbare informatie uit te halen.

Log Investigator met Okta AI is een logboek- en API-zoekfunctie met natuurlijke taal waarmee IT-medewerkers snel en gemakkelijk de omvangrijke dataset van Okta kunnen doorspitten om Identity-gerelateerde vragen te beantwoorden zoals:

- "Hebben er deze week verdachte logins plaatsgevonden?"
- "Welke daarvan waren afkomstig van onbeheerde devices?"
- "Waren er ook bij die afkomstig waren van een nieuwe locatie?"





Policy Recommender met Okta AI

Beperkte early access Q1 2024

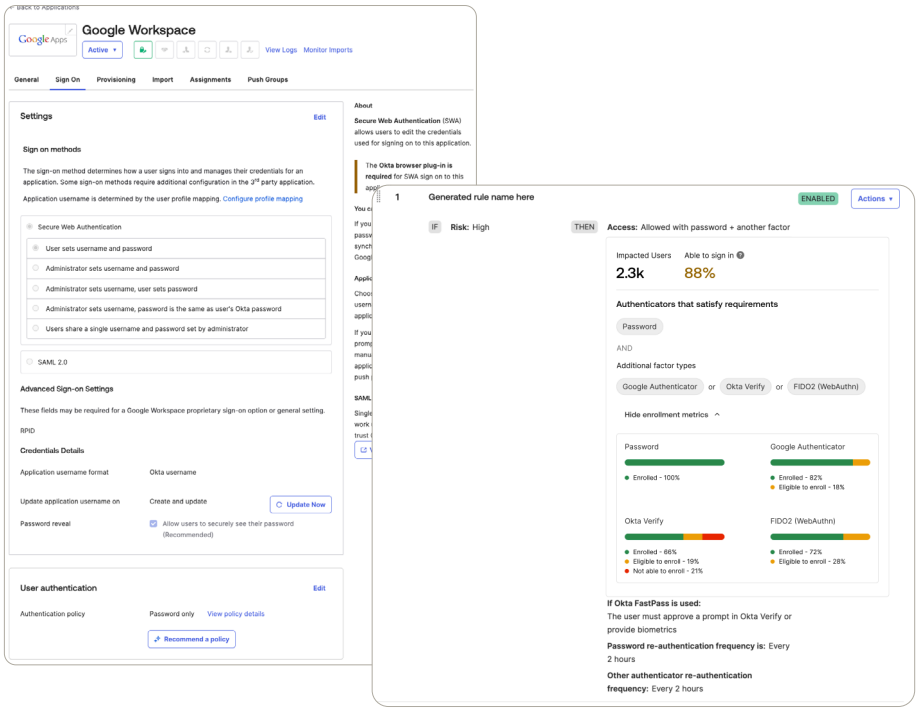
De rol van AI: onderzoekt data van policyconfiguratie afkomstig uit het klantenbestand van Okta om best practices op te halen en machine-leesbare beleidsregels te genereren die rechtstreeks kunnen worden toegepast binnen Okta-omgevingen

Identity-infrastructuur vormt een uitgebreid onderling verbonden web dat niet alleen de gehele IT-omgeving van een organisatie omvat, maar ook applicaties van derden. Dat maakt het configureren en beheren van zo'n uitgebreid systeem tot een complexe aangelegenheid die tijd, energie en expertise kan vergen.

Tegelijkertijd moeten verschillende organisaties veel van dezelfde beheerscenario's aanpakken, met name bij veelgebruikte applicaties als Slack, Salesforce en GitHub. Dat biedt de mogelijkheid om alle gezamenlijk opgeslagen kennis te benutten.

Policy Recommender met Okta AI gebruikt geanonimiseerde, verzamelde inzichten uit het klantenbestand van Okta om admins te voorzien van policyaanbevelingen en -inzichten (bijvoorbeeld hoeveel gebruikers te maken krijgen met een policywijziging of de impact van een policy bekijken voordat deze wordt toegepast) om apps van het Okta Integration Network (OIN) te beheren, zodat admins:

- Problemen die ze tegenkomen beter begrijpen en gemakkelijker kunnen oplossen
- De juiste configuratie en instellingen voor de juiste functies kunnen toepassen
- De security, efficiëntie en productiviteit kunnen verbeteren



AI in de Customer Identity Cloud (CIC)

Het rapport Technology Vision 2023 van Accenture vermeldt het volgende: **"De mogelijkheid om de identities van klanten te authenticeren schijnt een topprioriteit te zijn voor executives: 85% gaf aan dat "het een strategische zakelijke vereiste" is en drie van de vier respondenten meldde dat problemen met de authenticatie van klanten een negatieve invloed hebben gehad op het bedrijfsresultaat in de vorm van afgebroken transacties, frustratie van gebruikers enzovoort."**

Ook al is de letterlijke definitie van Customer Identity and Access Management (CIAM) hetzelfde gebleven, de ware betekenis – in termen van de use cases die het mogelijk maakt welke functionele componenten voor welke typen organisaties worden gebruikt – heeft zich met name de laatste jaren verder ontwikkeld. Tegenwoordig is CIAM essentieel voor:

- Het bedienen van consumenten: in de B2C-wereld (business-to-consumer) kunnen organisaties met een effectieve CIAM-implementatie zorgen voor sterk gepersonaliseerde promoties en aanbevelingen om extra omzet te genereren en meer waarde voor klanten te creëren, en dat alles met een prettige user experience in meerdere digitale kanalen.
- Het ondersteunen van zakelijke klanten: voor veel organisaties zijn business-to-business (B2B) SaaS-applicaties van essentieel belang. Maar in elke organisatie hebben allerlei gebruikers hun eigen toegangsniveau tot uiteenlopende resources nodig. En het creëren van een gebruiksvriendelijke en veilige experience vereist een zeer zorgvuldig beheer van Identity en toegangsrechten. CIAM biedt de oplossing door B2B SaaS-klanten de identities zelf te laten beheren.

Okta's eerste toepassing van AI in de Customer Identity Cloud was gericht op security om de voor de hand liggende reden dat klantgerichte applicaties met een scala van bedreigingen te maken hebben. Maar de aanpak die de identity van medewerkers kan beveiligen werkt niet altijd voor de identity van klanten. In een zakelijke omgeving heeft security vaak meer prioriteit dan gebruiksgemak, waardoor admins controles kunnen instellen die niet altijd rekening houden met de user experience.

Anderzijds moet Identity management van klanten uitgaan van security en privacy met minimale frictie. Dat vergt het instellen van beveiligingsmaatregelen die geavanceerde bedreigingen kunnen weerstaan en toch nauwelijks merkbaar zijn voor gebruikers.

Gelukkig blijkt AI heel bedreven te zijn in het herkennen van criminelen die zich voordoen als legitieme gebruikers.

Naast de nieuwe securityfuncties van Okta AI maken andere recent ontwikkelde functies gebruik van machine learning en generatieve AI om de customer experience te verbeteren, meer conversies te genereren en het beheer te vereenvoudigen.

Bot Detection

De rol van AI: onderzoekt meer dan 60 signalen om te voorspellen wanneer een authenticatieverzoek afkomstig is van een bot en niet van een legitiem account

Als vitaal onderdeel van de add-on Attack Protection in de Customer Identity Cloud vermindert de Bot Detection-functie aanvallen met scripts (zoals aanvallen via credential stuffing of via lijstvalidatie) op native applicaties, passwordless flows en pagina's met aangepast inloggen.

Door meer dan 60 databronnen te analyseren, zoals eerdere gebeurtenissen gekoppeld aan een IP-adres, recente inloggeschiedenis, data over IP-reputatie en tal van andere factoren, voorspelt Bot Detection wanneer een Identity-verzoek waarschijnlijk afkomstig is van een bot. Boven een bepaald prognose-/betrouwbaarheidsniveau komt de authenticatieflow met een tegenmaatregel, zoals een CAPTCHA.

De werking van Bot Detection is een voorbeeld van hoe AI eerdere technieken kan verbeteren:

- De eerste versie van februari 2021 was op regels gebaseerd en herkende 18% van de bots
- Versie twee van augustus 2021 gebruikte machine learning voor gedragsanalyse; deze AI-gestuurde aanpak was meer dan twee keer zo effectief met 45% van bots die werden herkend
- De meest recente versie, van juni 2022, herkende 79% van de bots en dat is de beste prestatie tot op heden, hoewel criminelen hun eigen technieken steeds verfijnder maken

Belangrijk daarbij is dat deze verbeterde beveiliging werd gerealiseerd zonder dat dit gepaard ging met meer frictie voor de gebruiker. Door zorgvuldig te trainen en AI voortdurend af te stemmen op de kern van de functionaliteiten van Bot Detection krijgen menselijke gebruikers nog maar zelden een CAPTCHA voorgeschoteld.

Bovendien is uit gedetailleerd onderzoek van de effecten voor en na gebleken dat Bot Detection een sterk afschrikkend effect heeft:

- Gemiddeld zagen klanten in het onderzoek die Bot Detection hadden ingeschakeld, een afname van meer dan 40% van schadelijk verkeer
- Enkele grotere klanten in het onderzoek zagen zelfs een afname van het botverkeer van bijna 90%!

Voortbouwend op Bot Detection: Identity Threat Level (ITL)

In april 2023 gaven we een voorproefje van ons Identity Threat Level-initiatief (ITL). Omdat we ons bij de 'voordeur' bevinden van applicaties met een CIAM-oplossing die miljarden logintransacties per maand beveiligt, beschikken we over een uniek uitkijkpunt van waaruit we Identity-bedreigingen in de gaten kunnen houden.

Dat krachtige perspectief heeft geleid tot het ontstaan van het ITL: een score van 0 tot 10 die het afgeleide niveau van botactiviteit laat zien door aan te geven hoe waarschijnlijk het is dat verkeer een CAPTCHA niet doorstaat. Een score van 0 betekent dat er nauwelijks sprake is van enige botactiviteit, terwijl een score van 10 aangeeft dat bijna alle verkeer afkomstig is van bots.

Door observaties in ons klantenbestand samen te voegen (uiteraard anoniem!), kunnen we een ITL voor verschillende sectoren en regio's berekenen, met de mogelijkheid om andere algemene attributen aan te passen. ITL kan bijvoorbeeld dit laten zien:

- Hoe vermoedelijk schadelijk verkeer naar CIC-klanten in diverse sectoren of regio's in de loop van de tijd is veranderd
- Hoe de mate van vermoedelijk schadelijk verkeer naar CIC-klanten zich verhoudt tussen diverse sectoren of regio's

Aan de hand van historische trends en dagelijkse veranderingen kunnen verhoogde risico's voor CIAM-login- en aanmeldingsflows worden vastgesteld. Aan de hand daarvan kunnen app-leveranciers hun eigen monitoring verbeteren, drempelwaarden proactief verhogen, extra maatregelen treffen of op elke andere gewenste manier reageren.

En dat allemaal met Bot Detection als basis.

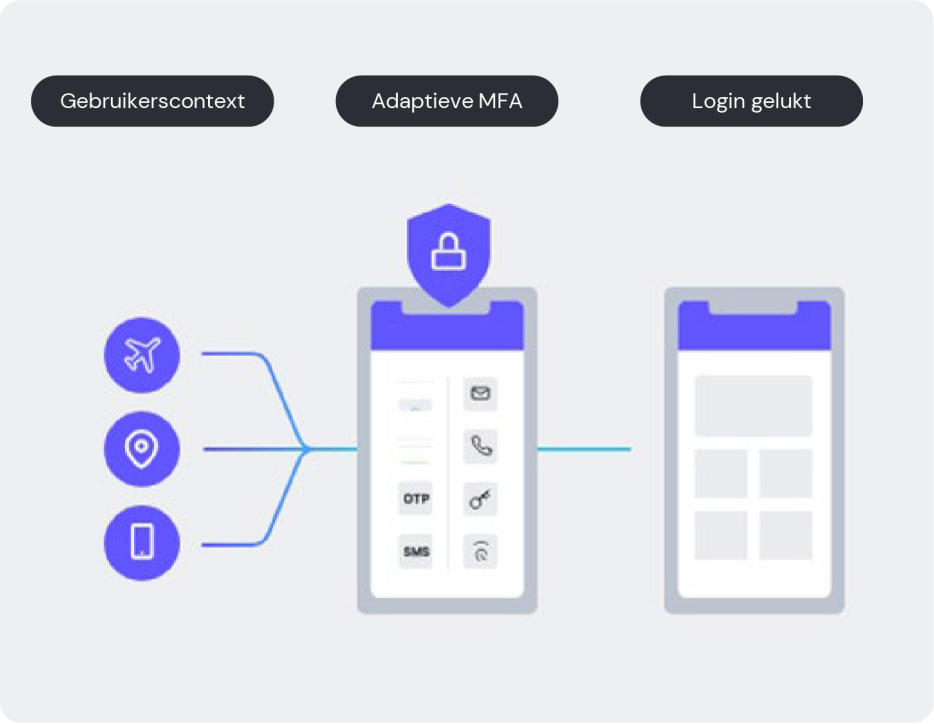
Adaptieve MFA

De rol van AI: biedt cruciale risicocontext door een breed scala van Identity-signalen te analyseren om te voorspellen of een authenticatiepoging afkomstig is van een legitieme gebruiker of van een crimineel die zich als legitieme gebruiker voordoet

Adaptieve MFA maakt intelligente toegang mogelijk, afgestemd op de behoeften van een organisatie en het inloggedrag van klanten.

Hoewel MFA zich heeft bewezen als verdediging tegen account takeovers, schrikken veel organisaties, met name in B2C, terug voor het gebruik ervan, omdat ze bang zijn dat de daarmee gepaard gaande extra frictie nadelig is voor de user experience.

Adaptieve MFA biedt dan een overtuigend alternatief door een MFA-uitdaging alleen te tonen wanneer een login als risicovol wordt bestempeld, waardoor altijd een naadloze user experiences gewaarborgd is.



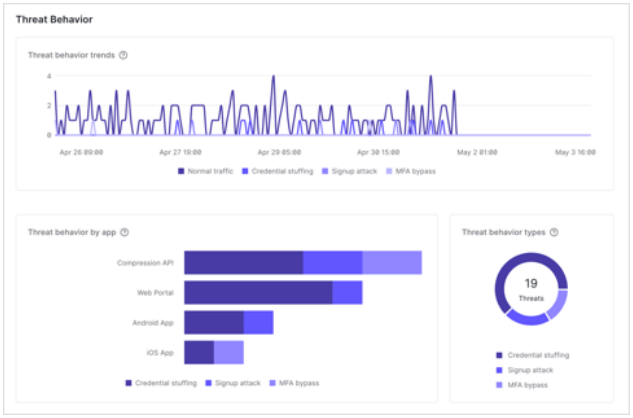
Securityaanbevelingen

Binnenkort

De rol van AI: doet intelligente aanbevelingen aan de hand waarvan organisaties de beveiligingsstatus van hun tenant kunnen verbeteren

Met behulp van Security Center kunnen IT- en securitymedewerkers trends in potentiële aanvallen zien en daar snel, in real time op reageren met:

- Een gestroomlijnde weergave van authenticatiegebeurtenissen, potentiële incidenten en effectieve reacties op bedreigingen
- Realtime meldingen van detectie van onregelmatigheden
- Visualisaties van potentiële trends in aanvallen (bijvoorbeeld credential stuffing, aanvallen bij aanmelding, pogingen om MFA te omzeilen)
- Inzicht in de gevolgen voor de user experience van Attack Protection-functies (zoals rate limiting, CAPTCHA)



Deze mogelijkheden worden nu uitgebreid met intelligente, ML-gestuurde securityaanbevelingen via snapshotwaarschuwingen en dashboardmeldingen.

Identity Flow Optimizer met Okta AI

Beperkte early access Q4 2024

De rol van AI: analyseert authenticatiedata om manieren voor te stellen om een betere customer experience te bieden en om het aantal conversies te vergroten

Met klanten als uitgangspunt verwijst "frictie" naar alles wat een remmende werking heeft op de interacties tussen een gebruiker en een service. Het kan hierbij onder meer gaan om interacties waarbij gebruikers:

- registreren bij een service
- inloggen bij een account
- gegevens en voorkeuren bijwerken
- verloren accountgegevens herstellen
- afrekenen (een aankoop afronden)

Hoe meer frictie er is, des te lager het conversiepercentage – en dus ook de omzet – op zowel de korte als de lange termijn. Het handmatig optimaliseren van customer flows kan echter zeer uitdagend zijn vanwege de gigantische hoeveelheden data en de zeer persoonlijke voorkeuren van verschillende gebruikers.

Daarnaast moet het beveiligen van Identity-flows altijd prioriteit hebben, maar dat blijft een hele uitdaging voor experts, laat staan voor developers die nog niet vertrouwd zijn met Identity.

Om dat aan te kunnen pakken, biedt Identity Flow Optimizer developers inline aanbevelingen over de Identity-configuraties en -acties die ze kunnen toevoegen om meer conversies te genereren, de security te verbeteren en sneller apps te bouwen.

Brand Customizer met Okta AI

Beperkte early access Q4 2024

De rol van AI: stelt ontwerptemplates automatisch samen of vult deze automatisch in met de branding van een organisatie

Merken hanteren strikte ontwerprichtlijnen om te zorgen voor een consistente user experience die de zorgvuldig samengestelde Identity van het merk ondersteunt.

Brand Customizer kan een template van één pagina ontwerpen en past het ontwerp aan alle andere vereiste templates aan. Een developer levert een screenshot of logo, aan de hand waarvan AI de templates samenstelt en de developer die waar nodig aanpast.

Dat zorgt niet alleen voor een consistente look-and-feel voor eindgebruikers, maar het versnelt ook de time-to-value doordat developers sneller en gemakkelijker superieure customer experiences kunnen produceren, snel kunnen innoveren en kunnen bijdragen aan het opschalen van de organisatie.

Guide met Okta AI

Beperkte early access Q4 2024

De rol van AI: interpreteert prompts in gewone taal en biedt contextuele hulp zodat gebruikers effectief en efficiënt kunnen werken met de Customer Identity Cloud

De Customer Identity Cloud is krachtig, biedt een groot aantal functies en kan sterk worden uitgebreid. AI die mogelijkheden kunnen wel intimiderend zijn voor nieuwe gebruikers, en zelfs experts zijn misschien niet bekend met elk detail of zijn niet in staat om al die nieuwe functies bij te houden.

Om nieuwe gebruikers te helpen snel aan de slag te gaan en om te zorgen dat iedere mogelijke gebruiker alles uit de CIC kan halen, biedt de Guide het volgende:

- Uitgebreide hulp bij de onboarding en intuïtieve selectie van de beste stappen die gebruikers kunnen nemen, zodat ze soepel de workflows met de meeste waarde kunnen volgen met behulp van eenvoudige aanwijzingen in het Engels.
- Uitleg bij elke instelling of elke vakterm op het platform in begrijpelijke taal, plus contextuele hulp en geselecteerde links naar relevante documentatie.

Actions Navigator met Okta AI

Beperkte early access Q2 2024

De rol van AI: zoeken met opdrachten in gewone taal om eenvoudiger de juiste integraties te vinden en hulp voor gebruikers om waar nodig geheel nieuwe integraties te ontwikkelen

Uitbreidbaarheid is een kernfunctie van Customer Identity Cloud, en de Auth0 Marketplace is bedoeld om ontwikkelingsprocessen te vereenvoudigen door op een duidelijke manier een integratie toe te voegen aan Identity-applicaties.

Maar met honderden integraties is het soms moeilijk om precies dat te vinden wat nodig is.

Met Actions Navigator kunnen developers marktintegraties vinden en implementeren of een Action schrijven (een functie om CIC-mogelijkheden aan te passen en uit te breiden) door er gewoon naar te vragen in een zoekopdracht. Het genereren van code is een van de meest transformatieve toepassingen van generatieve AI en deze functie biedt nieuwe mogelijkheden voor zowel developers als gebruikers die geen ervaring hebben met het schrijven van eigen code.

Tenant Security Manager met Okta AI

Beperkte early access Q2 2024

De rol van AI: ontwikkelt samenvattingen van complexe Identity-configuraties in gewone taal

Veel organisaties beschikken over experts met waardevolle institutionele kennis over specifieke systemen, zoals Identity.

Zijn deze experts niet beschikbaar, omdat ze bijvoorbeeld verplaatst zijn naar een andere afdeling of de organisatie hebben verlaten, dan kan het voor anderen bijzonder moeilijk zijn om de staat van het systeem en de details van de configuratie te begrijpen.

Tenant Security Manager vult de functionaliteit van Attack Protection van Okta aan met intelligente securityaanbevelingen door middel van snapshotwaarschuwingen en dashboardmeldingen om de beveiligingsstatus van uw tenant te verbeteren.

Conclusie

Het plotselinge verschijnen van ChatGPT, en als reactie daarop het snelle begin van een hele lijst aan soortgelijke krachtige tools, laat zien dat de veranderingen razendsnel gaan en het domino-effect is zo gevarieerd dat het doen van specifieke voorspellingen over AI op gekkenwerk lijkt.

Toch zijn sommige zaken wel duidelijk. Wat betreft de gevolgen van AI, en dan met name van generatieve AI, laat deze kop van een persbericht van Forrester precies zien waar het om gaat: Het negeren van generatieve AI is een kostbare vergissing voor enterprises.

Een andere manier om naar AI te kijken: ook al weet u niet precies wat uw investeringen in AI zullen opleveren, u kunt ervan op aan dat niet investeren op zijn minst uw concurrentiepositie zal verzwakken, maar u ook tot een irrelevante speler kan maken. Zo belangrijk is deze paradigmaverschuiving.

Door een belangrijk deel van onze uitgaven aan onderzoek en ontwikkeling in te zetten voor AI en door gebruik te maken van onze enorme IAM-dataset, blijft Okta innovatieve AI-gestuurde mogelijkheden leveren om de security te versterken, de productiviteit te verhogen en user experiences te verbeteren, zowel binnen onze Workforce Identity Cloud als de Customer Identity Cloud.

En ook al weten we niet precies wat onze investeringen gaan opleveren, we hebben er alle vertrouwen in dat als we later terugkijken op onze huidige mogelijkheden én de mogelijkheden die nog in de pijplijn zitten, dit de eerste stappen van een transformatief traject bleken te zijn.

Disclaimer

Dit materiaal en alle daarin opgenomen aanbevelingen vormen geen advies op juridisch, privacy-, security-, compliance- of zakelijk gebied. Dit materiaal is alleen bedoeld voor algemene doeleinden en vormt wellicht geen afspiegeling van de meest recente ontwikkelingen in security, privacy en wetgeving, noch van alle relevante problemen. U bent zelf verantwoordelijk voor het inwinnen van advies op juridisch, privacy-, security-, compliance- of zakelijk gebied bij uw eigen jurist of andere professionele adviseur en u kunt zich niet beroepen op de hier gedane aanbevelingen. Okta is tegenover u niet aansprakelijk voor verlies of schade die het gevolg kunnen zijn van uw implementatie van de aanbevelingen in dit materiaal. Okta geeft geen verklaringen, garanties of andere waarborgen met betrekking tot de inhoud van dit materiaal. Informatie over de contractuele waarborgen die Okta zijn klanten beidt, is te vinden op okta.com/agreements.

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 dan ook niet op vertrouwen bij uw aankoopbesluiten.