Whitepaper

Okta och AI

Så här påverkar artificiell intelligens identitets- och åtkomsthantering (IAM)

Innehåll

Sammanfattning

Artificiell intelligens (AI) i allmänhet påverkar organisationers verksamhet och driver innovativa produkter och tjänster med hjälp av optimering, dataanalys, avvikelseidentifiering och andra förutsägelsebaserade tillämpningar. Större delen av dessa funktioner är inte nya, men minskade kostnader och ökad prestanda innebär att det nu är praktiskt att integrera dessa funktioner i så gott som vad som helst.

Generativ AI verkar ha dykt upp över en natt, tack vare snabba framsteg i stora språkmodeller (LLM) som utgör grunden för program såsom OpenAI:s ChatGPT och DALL-E, Googles Bard och Metas Code Llama.

Vi anser att generativ AI utgör ett verkligt, sällsynt paradigmskifte vars effekter vårt samhälle bara har börjat att upptäcka, för att inte tala om förstå.

Och få domäner lämpar sig lika bra för tillämpningen av AI som identitet. Identitet är komplicerad, så det finns många saker som AI kan förbättra, och identitetsflöden och transaktioner producerar enorma mängder data, vilket är bränslet för AI-motorer. Vi strävar efter att utnyttja datanätverkseffekter i hela identitetsdomänen, men på kort sikt fokuserar vi våra forsknings- och utvecklingsinvesteringar på att

- stärka säkerheten
- förbättra produktiviteten
- förbättra användarupplevelser.

Okta-teamet är bekanta med AI och vi är stolta över att redan ha använt AI i flera viktiga områden. Till exempel:

- Oktas Workforce Identity Cloud (WIC) införlivar AI i ThreatInsight, Adaptive Multi-factor Authentication (Adaptive MFA) och våra skydd mot Anti-Toll Fraud.
- Oktas Customer Identity Cloud (CIC) använder AI i funktionen Bot Detection (och relaterade Identity Threat Level, eller ITL) och Adaptive MFA.

Och på Oktane 2023 presenterade vi ett antal nya AI-drivna funktioner. Okta AI har fyra nya WIC-funktioner för följande syften:

- Stärka säkerheten: Identity Threat Protection
- Hjälpa till med styrningen: Governance Analyzer
- Förenkla administrationen: Log Investigator, Policy Recommender

CIC har fått sex nya funktioner för följande syften:

- Stärka klientorganisationens säkerhet: Security Recommendations
- Förbättra kundupplevelsen och öka intäkterna: Funnel Conversion Recommendations, Brand Customization
- Förenkla administrationen: Co-Pilot, Action Selection and Development, Personalized Tenant Configuration Summary

Dessutom främjar vi en innovationsfokuserad kultur som vi lyfter fram under två hackatons för hela företaget varje år. Många av de idéer som utforskas på dessa hackatons utvecklas till patent och produktkoncepttester och når slutligen marknaden på ett eller annat sätt. Under en av våra senaste hackatons fokuserade 25 % av projekten på AI-experimentering – och vi tycker att de har bra potential.

På grund av vikten av AI och den spänning den orsakar bland utvecklare i allmänhet har vi även schemalagt vårt allra första AI-fokuserade hackaton.

Vi har även hjälpt våra kunder att producera inspirerande och eleganta upplevelser med LLM:er, och Oktas övergripande ekosystem – Okta Ventures, Okta Integration Network, Auth0 for Startups och Auth0 Marketplace – erbjuder ett stort nätverk av AI-lösningar som integreras med våra Okta-erbjudanden.

Vi kommer att ställas inför utmaningar – cyberbrottslingar utnyttjar redan AI i allmänhet och LLM:er i synnerhet för att upptäcka nya attackvektorer och göra befintliga attacker farligare. Men vi är optimistiska och anser att AI kan och kommer att leda till bra saker.

I nuläget styr digitala identiteter åtkomsten till ett ständigt växande antal program och tjänster, vilket påverkar, och till viss del styr, många aspekter av vår moderna livsstil. I framtiden kommer de att ha ännu större påverkan, vilket innebär att autentisering, auktorisering och identitet i allmänhet är avgörande för att bevara förtroendet och säkerheten samt tillhandahålla grunden för bra användarupplevelser.

Och vi strävar efter att utnyttja kraften hos AI för att stärka kopplingarna mellan människor, teknik och samhälle.

Inledning

Under de senaste månaderna har både teknologifokuserade och vanliga nyheter publicerat otaliga artiklar om genombrott inom artificiell intelligens (AI) och de tillämpningar, både förväntade och oförutsedda, som dessa genombrott möjliggör.

Som Andy Grove sa: ”Endast de paranoida överlever.” Så det är knappast överraskande att såväl stora som små företag inom en rad olika branscher strävar efter att utnyttja AI för att förbättra befintliga lösningar, driva nya lösningar och fördjupa de metaforiska vallgravar som ger dem övertaget över konkurrenterna.

I hög grad är vår investering i ny AI inget nytt för oss – AI driver redan ett antal viktiga produkter och funktioner i vår portfölj. I synnerhet är maskininlärning (ML) själva kärnan för mycket av vår dynamiska riskbedömning och riskbaserade autentiseringsintelligens.

Vi har lärt oss av många års praktisk erfarenhet och ser inte AI som en enskild modul eller funktion – något som kan skruvas fast eller läggas till på vår plattform. I stället är vi medvetna om att AI är en allmän teknik (eller snarare en samling allmänna tekniker) som ger bäst resultat när den är inbäddad i och integrerad med infrastrukturen för identitet.

I detta whitepaper försöker vi förklara Oktas relation till AI genom att utforska

- varför AI verkar så lovande för att ändra och omforma praktiskt taget alla digitala domäner
- varför identitet är särskilt lämpad för att dra nytta av AI
- de ledande värdeerbjudanden som vi ser för AI inom den närmaste framtiden
- hur vi redan har använt AI inom Oktas Workforce Identity Cloud (WIC) och Customer Identity Cloud (CIC)
- hur vi utnyttjar Okta AI i nya WIC- och CIC-funktioner.

Varför använda AI?

I grunden kan artificiell intelligens ses som ett beslut som fattas av en dator där det inte går att skilja mellan dess ”smarthet” och en människas beslut – oavsett hur beslutet fattas.

AI-konceptet introducerades formellt på Dartmouth-konferensen, men den ursprungliga premissen går tillbaka till 1943, då logikern Walter Pitts och neuroforskaren Warren McCulloch försökte skapa en matematisk representation av neuronerna i människans hjärna. Dessa moderna framsteg byggde vidare på en lång historia av framsteg inom beräkningsteorin, från Ada Lovelace på 1800-talet till Alan Turing.

Sedan 1960-talet har AI utvecklats till en mycket stor samling algoritmer, inklusive identifiering och igenkänning av mönster – som vanligtvis utförs med maskininlärning (ML). Det har gjorts stora framsteg inom ML-fältet de senaste 15 åren, vilket har lett till framväxten av praktisk och ekonomisk djupinlärning.

Generativ AI är ett sällsynt paradigmskifte

AI-utvecklingen som har tagit världen med storm är den otroliga och, enligt många, chockerande ankomsten och snabba utvecklingen av generativ AI, som främst drivs av anmärkningsvärda framsteg inom stora språkmodeller (LLM:er).

Program såsom OpenAI:s ChatGPT och DALL-E drivs av LLM:er och har gjort AI mainstream, delvis på grund av deras förmåga att imitera människor och delvis på grund av bristande transparens när det gäller de data som modellen tar in (och som formar dess beteende).

Plötsligt är det inte bara människor som kan skriva prosa och skapa komplicerade (och verklighetstrogna, om det är avsikten) bilder. Eftersom LLM:er är duktiga på att skriva (och programmering är en form av skrift) och många saker styrs av programvara, ligger LLM:er bakom oväntade genombrott och framsteg inom en rad olika domäner.

Det här är helt klart en modernare era för AI:n, så det är naturligt att undra hur vi kan använda dess funktioner – gamla, nya och kommande.

Vad kan AI göra?

I boken Prediction Machines beskriver ekonomerna Ajay Agrawal, Joshua Gans och Avi Goldfarb framväxten av AI som en minskad kostnad för förutsägelser, som de definierar som att ta tillgänglig information och använda den för att generera ny information.

Eftersom förutsägelser ”är själva kärnan för att fatta beslut i osäkra situationer” och ”våra arbetsliv och privatliv är översållade med sådana beslut” medför minskade kostnader för förutsägelser enastående potential. Förutsägelser är till exempel en avgörande komponent för följande:

- Optimering: Använda sammanhang och tidigare observationer för att förutsäga bästa sökväg, svar, konfiguration, utformning för användargränssnitt osv.
- Beteendeanalys: Observera beteende i realtid med hänsyn till tidigare handlingar för att förutsäga en användares avsikter.
- Datautvinning: Förutsäga vilka data och insikter som bäst tillgodoser en användares fråga eller uppmaning (och det är värt att notera att förutsägelser även är grundläggande för LLM:er och generativ AI).

Precis som klassisk beräkning är AI (i alla dess former) en allmän teknik som har potential att ändra och omforma befintliga branscher – och vi är särskilt optimistiska när det gäller dess potential att driva utvecklingen av identitet.

AI och identitet

En digital identitet är den uppsättning attribut som definierar en viss användare när det gäller en funktion som levereras av ett visst program. I nuläget styr digitala identiteter åtkomsten till ett ständigt växande antal program och tjänster, vilket påverkar, och till viss del styr, många aspekter av vår moderna livsstil. I framtiden kommer de att ha ännu större påverkan, vilket innebär att autentisering, auktorisering och identitet i allmänhet är avgörande för att bevara förtroendet och säkerheten samt tillhandahålla grunden för bra användarupplevelser.

Därför är IAM-tjänster hörnstenar i vår uppkopplade värld, som säkerställer att endast behöriga användare, såsom medarbetare, leverantörer, partner och kunder, kan få åtkomst till vissa resurser. IAM-konceptet är mycket enkelt: en användare bevisar sin identitet och får åtkomst till en resurs som den har behörighet för. Men i praktiken kan flera faktorer komplicera det hela:

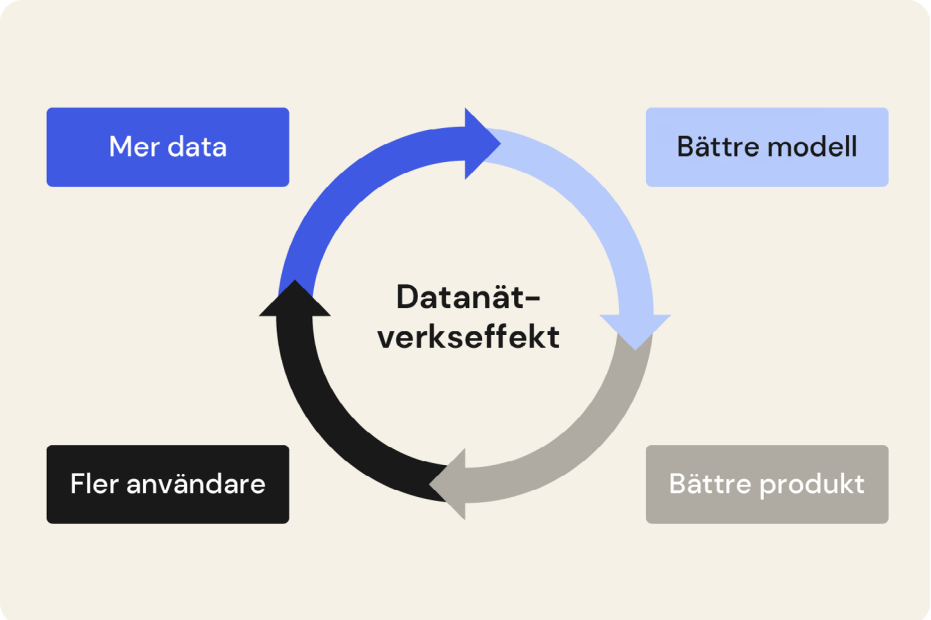
- Dagens digitala värld omfattar många användare, en enskild användare kan ha många digitala identiteter och det finns otaliga sätt att uttrycka en digital identitet.
- Olika digitala identiteter har olika rättigheter och behörigheter när det gäller resurser – och dessa rättigheter och behörigheter blir alltmer dynamiska.
- När säkerhetsparametrar löses upp fokuserar angripare på identitet.

Som vi har sett kan AI hantera komplicerade situationer och osäkerheter – förutsatt att det finns tillräckligt med tillgängliga data.

Som tur är har identitetsdomänen gott om data att erbjuda, eftersom själva identiteten har utvecklats från ett statiskt, endimensionellt attribut till en dynamisk, fortlöpande interaktion som omformas med varje ny datapunkt. Den här utvecklingen skulle inte ha varit möjlig utan den tidigare molnomvandlingen och kommer att fortsätta tack vare den nuvarande AI-omvandlingen.

Utnyttja datanätverkseffekter

En viktig konsekvens av denna utveckling är att den möjliggör en god cykel av datanätverkseffekter: Ju högre datavolym och kvalitet som en AI-modell har åtkomst till, desto snabbare kan den lära sig och desto exaktare blir dess förutsägelser eller beslut. Detta gör i sin tur produkten eller tjänsten värdefullare för dess användare, vilket lockar fler användare som sedan genererar mer data, som kan matas in i modellen i en god cykel:



1. **Mer data:** Ju mer en produkt eller tjänst används, desto mer data genereras genom användarnas interaktioner, transaktioner, feedback osv.
2. **Bättre modell:** Dessa data används för att förfina den underliggande AI-modellen. Ju högre datavolym och -kvalitet, desto exaktare blir modellens förutsägelser eller beslut.
3. **Bättre produkt:** I takt med att AI-modellen förbättras blir även produkten eller tjänsten bättre.
4. **Locka fler användare eller användning:** Den förbättrade produkten eller tjänsten lockar fler användare som genererar ännu mer data och fortsätter cykeln.

Denna självförstärkande slinga kan vara en kraftfull drivkraft för innovation och övertag över konkurrenterna.

Stärka säkerheten

Vid det här laget är det vida känt att AI kan

- göra befintliga identitetsattacker såsom stulna inloggningsattacker och nätfiske farligare (t.ex. svårare att identifiera, effektivare/destruktivare)
- möjliggöra helt nya typer av identitetsattacker, varav många inte blir uppenbara förrän de inträffar
- övervinna vissa befintliga säkerhetsåtgärder (t.ex. lösa CAPTCHA-tester, lura röstbiometrisystem).

Och eftersom generativ AI kan koda och skapa skript blir det enklare i allmänhet för hotaktörer att lansera attacker oavsett färdighetsnivå (dvs. med eller utan kodningsförmåga), vilket kan leda till fler cyberbrottslingar och göra dem effektivare.

Denna förändrade hotbild ledde till en varning från Gartner: **”Under 2025 kommer attacker som utnyttjar generativ AI att tvinga säkerhetsmedvetna organisationer att sänka tröskelvärdena för identifiering av misstänkt aktivitet, vilket kommer att leda till fler falsklarm och kräva fler, inte färre, ingrepp från människor.”**

AI kommer utan tvekan att vara till hjälp för angripare, men den hjälper även försvaret.

Okta är redan branschledande med FastPass nätfiskebeständiga autentisering, på alla plattformar för både hanterade och ohanterade enheter, och gör det enklare för utvecklare att använda användarvänlig och nätfiskebeständig FIDO2-autentisering. Vi inser dock även att AI måste användas för följande:

- **Ytterligare inbyggd Okta-säkerhet**: Hotaktörer kan använda AI för att undersöka sårbarheter och säkerhetsluckor, men det kan även organisationer som Okta. Och vi kan använda AI för att stärka programvara och system innan de lanseras.
- **Automatiserad hotidentifiering:** Sammanhangsbaserad analys och beteendeanalys kan redan informera intelligenta riskbedömningar och identifiera avancerade identitetshot, och framsteg inom AI kommer bara att förbättra vår förmåga att göra detta och leda till nya funktioner.
- **Minskad risk för våra kunders räkning:** Oavsett om du vill automatisera försvarsåtgärder (t.ex. inneslutning, blockering av skadliga aktiviteter), kombinera en avisering med en rekommenderad spelbok eller stödja initiativ för styrning, riskhantering och efterlevnad (GRC) kommer AI att vara ovärderlig för att proaktivt minska riskerna och reagera på attacker.

Som tur är har vi redan gott om erfarenhet av att integrera AI-drivna säkerhetsfunktioner i både vårt Workforce Identity Cloud och vårt Customer Identity Cloud.

[1] Gartner, 4 Ways Generative AI Will Impact CISOs and Their Teams, Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook, 29 juni 2023. GARTNER är ett registrerat varumärke och tjänstmärke som tillhör Gartner Inc. och/eller dess dotterbolag i USA och andra länder och används med tillstånd här. Med ensamrätt.

Förbättra produktiviteten

En av de främsta slutsatserna i Oktas rapport om hur team köper SaaS 2023 är att det i grunden finns två typer av utvecklingsorganisationer: de som redan använder AI inom produktteknik (52 % av de som deltog i undersökningen) och de som kommer att göra det inom de kommande 12 månaderna (45 %).

Organisationer är ute efter en rad fördelar, särskilt smidighet, nya funktioner, minskad kostnad och tidsbesparingar, och integrerar AI-verktyg för dataanalys, kvalitetskontroll, maskininlärning, automatisering och mycket mer.

Vi delar den optimistiska synen på AI:ns potential att öka produktiviteten inom vår egen teknikorganisation.

Samtidigt inser vi att AI:ns påverkan bör sträcka sig mycket längre: till alla medarbetare i praktiskt taget alla kundorganisationer, oavsett storlek eller bransch.

Fördelar med en modern och mogen infrastruktur för arbetsstyrkans identitet:

- Medarbetare, leverantörer och affärspartner kan arbeta var som helst, med smidig och säker åtkomst till viktiga verktyg och resurser.
- Användare får en smidig användarupplevelse, verksamhetens effektivitet ökar och administrationen minskar, vilket frigör tid och energi som kan läggas på tillväxt, innovation och andra prioriteringar.
- Organisationer kan skala upp och förbättra sin smidighet oavsett storlek.
- Skydd mot störningar som orsakas av skadliga aktörer.

När AI är inbäddad i identitetsinfrastrukturer kan den främja alla dessa fördelar, och utan tvekan leda till ännu fler.

Förbättra användarupplevelser

Nu ska vi fokusera på friktion.

För konsumentföretag är friktion, dvs. allt som saktar ner en persons interaktion med din tjänst, ett stort hinder för konverteringar och därmed intäkterna. Enligt Oktas rapport om kundidentitetstrender angav nästan 60 % av dem som deltog i undersökningen att det är mer sannolikt att de spenderar pengar när tjänster erbjuder en enkel, säker och friktionsfri inloggningsprocess. Detta gäller för alla sektorer/branscher, vilket antyder att användare vill att alla interaktioner ska vara smidiga.

Det krävs en viss friktion för att skapa tillit och tillhandahålla säkerhetskontroller, men minskad friktion där det är praktiskt, i alla konsumentinteraktioner, kan öka konverteringstakten och därmed öka intäkterna på både kort och lång sikt.

Var passar AI in? Tre uppenbara platser:

- Kontinuerlig riskbedömning för att möjliggöra lösenordsfria och inloggningsfria upplevelser.
- Optimerade identitetsflöden för smidiga användarupplevelser.
- Förbättrad utformning av användargränssnitt (t.ex. under identitetstransaktioner) för smidiga användarupplevelser.

På arbetsplatsen är friktion allt som hindrar eller saktar ner saker och ting. Identitet kan inte (på egen hand) starta ett möte i tid eller uppmuntra en kollega att svara snabbare på en förfrågan, men en mogen identitetsinfrastruktur bidrar på andra sätt, inklusive genom att

- säkerställa att användare har åtkomst till rätt resurser (t.ex. data, system, program) med rätt behörighet vid rätt tillfälle
- driva självbetjäningsfunktioner (t.ex. begära åtkomst till resurser, ändra profiler, registrera säkerhetsfaktorer osv.)
- automatisera befintliga processer (t.ex. åtkomstgranskningar och certifieringar, säker avregistrering osv.).

Återigen kan AI maximera dessa befintliga funktioner och leda till nya. AI kan till exempel analysera stora mängder identitetsdistributioner och prestandavärden för att fastställa de effektivaste konfigurationerna och använda denna information för att ge rekommendationer som är anpassade till varje organisation eller avdelning. Och AI kan hjälpa administratörer att snabbt hitta information som behövs utan att överväldigas av volymen av drifts- och loggningsdata.

Dessutom har LLM:er funktioner för naturligt språk, vilket ger användare som inte kan koda åtkomst till ännu fler identitetsrelaterade funktioner. Okta Workflows möjliggör redan identitetsautomatisering och -orkestrering utan kodning via ett Drag & Drop-gränssnitt, så det är lätt att föreställa sig en lösning som tar instruktioner på naturligt språk.

AI i Workforce Identity Cloud (WIC)

Tidigare ansågs identiteten bara vara en tjänst för att hantera användarnamn och lösenord, men numera är den nödvändig för alla moderna verksamheter, som inte skulle fungera utan den. Därför är infrastrukturen för identitet ett sammankopplat och grundläggande lager i den generella IT-miljön, som kopplar samman användare och andra enheter med system, data och resurser både lokalt och i molnet.

Därför är identitetsskyddet en grundläggande del av en stark säkerhetssits och kan hjälpa till att bekämpa missbruk från interna hot och från inkräktare som missbrukar stulna inloggningsdata.

Förutom att bidra till att skydda infrastrukturen för arbetsstyrkans identitet mot hot kan AI även stödja styrningsaktiviteter, i synnerhet genom att undersöka stora volymer av konfigurationsdata för att identifiera risker, rekommendera korrigerande åtgärder och till och med automatisera många vanliga och viktiga uppgifter.

Och AI:ns förmåga att analysera information och lyfta fram insikter innebär att den lämpar sig väl för att tolka stora mängder loggar.

Dessa funktioner tillsammans med bearbetning med naturligt språk och generativ AI omvandlar redan hur administratörer hanterar ständigt växande infrastrukturer för identitet.

I rapporten om trender inom skydd av digitala identiteter från 2022, baserad på en undersökning med fler än 500 IAM- eller säkerhetsexperter, visade Identity Defined Security Alliance (som Okta är medlem av) följande:

- **84 %** av de som deltog uppgav att deras företag hade upplevt ett identitetsrelaterat intrång under det föregående året.
- **78 %** angav direkta affärseffekter till följd av ett intrång.
- **64 %** angav att effektiv hantering av och säkerhet för digitala identiteter antingen är den högsta säkerhetsprioriteringen (16 %) eller bland de tre främsta prioriteringarna (48 %).

ThreatInsight

AI:ns roll: Förutsäger huruvida förfrågningar kommer från en skadlig källa, baserat på observationer och automatiserad feedback från attacker och autentiseringsförfrågningar från den stora Okta-kundbasen.

ThreatInsight är en grundläggande säkerhetsfunktion som identifierar och minskar attacker med hög volym som involverar inloggningsdata (lösenordssprutning, stulna inloggningsattacker och liknande råstyrkeattacker) som riktas mot Okta-slutpunkter. En kund väljer helt enkelt blockeringsläget i Oktas administratörskonsol för att automatiskt neka förfrågningar som förutsägs vara skadliga innan angripare försöker autentisera, eller loggningsläget för att granska skadlig trafik.

ThreatInsight utnyttjar nätverkseffekten av de miljontals autentiserings-förfrågningar som görs till tusentals Okta-organisationer varje dag och använder en kombination av heuristik (statiska regler) och maskininlärning för att observera och härleda information från attacker som involverar inloggningsdata.

För varje känd skadlig IP-adress som blockeras vid kantlagret ser Okta många fler misstänkta händelser som kommer från IP-adresser som inte kan bekräftas vara skadliga med 100 % visshet. Det finns situationer då det kan uppstå flera misslyckade inloggningar, till exempel vid en stor konferens på ett hotell. I dessa situationer är det inte orimligt med dussintals, hundratals eller till och med tusentals misslyckade inloggningar för flera konton i flera Okta-organisationer, som alla verkar komma från samma källa (dvs. hotellets nätverk). Om du blockerar dessa IP-adresser kan du blockera legitima inloggningsförsök, vilket i slutändan vore lika illa som att drabbas av en DDoS-attack.

För att undvika sådana falsklarm definieras misstänkta IP-adresser som IP-adresser som är inblandade i identitetsattacker i Oktas fullständiga kundbas, med andra ord läggs endast IP-adresser som vi vet har deltagit i attacker till i ThreatInsight-databasen, till förmån för alla Okta-kunder.

ThreatInsight använder ett glidande fönster och misstänkta IP-adresser som har slutat uppvisa misstänkt aktivitet vid nästa utvärdering tas bort från databasen.

Adaptive MFA

AI:ns roll: Ger sammanhangsbaserad information som kan kombineras med en lämplig autentiseringsmetod genom att förutsäga risken för autentiseringshändelser (t.ex. inloggning) och åtgärder efter autentisering (t.ex. åtkomst till en viss resurs).

Adaptive Multi-Factor Authentication (AMFA) introducerar ytterligare information i identitetsflöden genom att ta hänsyn till det ständigt föränderliga sammanhanget där en autentiseringsförfrågan görs. Genom att dynamiskt anpassa säkerhets- och autentiseringspolicyer kan Adaptive MFA både förbättra en organisations säkerhetssits och användarupplevelse.

En Adaptive MFA-policy kan till exempel minska friktionen för användare genom att inte fråga efter MFA så ofta när användare loggar in via SSO eller via en hanterad eller känd enhet. Samma Adaptive MFA-lösning kan dock be om en ytterligare eller säkrare autentiseringsfaktor när risken som är förknippad med en förfrågan bedöms vara högre, t.ex. ett inloggningsförsök vid en ovanlig tidpunkt eller från en ny enhet, eller om en inloggad användare försöker komma åt särskilt känsliga resurser eller information.

Flexibiliteten och kontrollen som tillhandahålls av en Adaptive MFA-lösning beror till stor del på de tillgängliga MFA-faktorerna och hur mycket sammanhangsbaserad information som inkluderas i riskbedömningen.

Inom Adaptive MFA undersöker en intelligent agent en rad risksignaler, inklusive användar-ID, enhet, nätverk, plats, resor, IP-adress och externa data från tredje parter och slutpunktssäkerhetsintegreringar, för att kategorisera avvikelser och tillämpa riskbaserad autentisering vid varje steg i autentiseringsprocessen, även efter att användaren har loggat in (t.ex. för autentiseringstillägg).

Anti-Toll Fraud

AI:ns roll: Identifierar avvikelser och kategoriserar risker i samband med försök till telefonitransaktioner baserat på en rad indata (t.ex. IP-adress, telefonprefix, land).

International Revenue Share Fraud (IRSF), som även kallas Toll Fraud, är en typ av bedrägeri där bedragare på konstgjort sätt genererar en stor mängd internationella samtal/SMS till dyra nummer. Internationella långdistanstelefonitransaktioner är dyra, så dessa bedrägerier kan ha en avsevärd ekonomisk påverkan på verksamheter som använder telefonsamtal och/eller SMS som en del av MFA-flödet.

Anti-Toll Fraud-funktionen skyddar kunderna och tillhandahåller tillförlitlig telefonitjänst genom att utnyttja kompletterande identifieringsmekanismer: en heuristisk motor och flera ML-motorer.

I stort sett tilldelas varje transaktion en riskmarkör och transaktioner som bedöms ha högre risk omfattas av striktare prisgränser. (Det finns mer information om hur dessa komponenter fungerar och hur Anti-Toll Fraud-funktionen använder dem i det här blogginlägget.)

Införandet av maskininlärningskomponenterna ledde till 20 % effektivare identifiering av bedrägliga transaktioner.

Identity Threat Protection med Okta AI

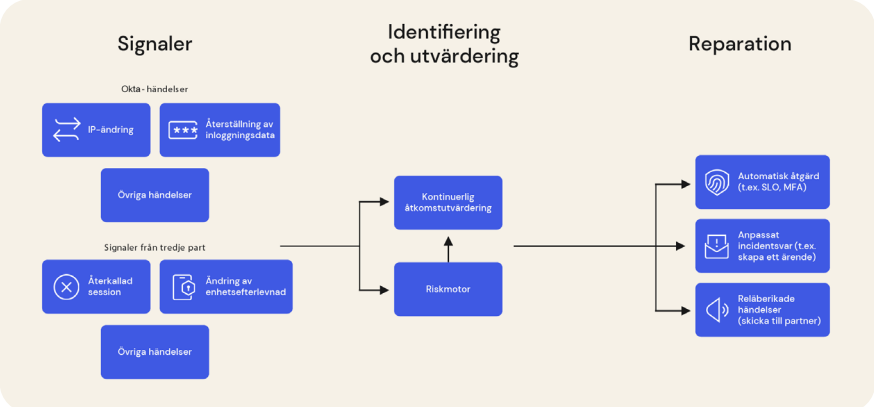
Begränsad tidig åtkomst första kvartalet 2024

AI:ns roll: ML-modellen anpassar automatiskt riskbedömningen till olika sammanhang, vilket ger exaktare och mer nyanserade bedömningar som lämpar sig för dynamiska miljöer.

Du behöver flera skyddslager för att skydda dig mot dagens identitetshot, som börjar redan innan användaren autentiseras och fortsätter under hela sessionen. I synnerhet förväntas kontinuerlig autentisering bli viktigare när starkare autentiseringstekniker blir vanligare och hotaktörer reagerar genom att använda fler resurser till att kringgå MFA och kapa aktiva sessioner.

Identity Threat Protection med Okta AI hjälper till att skydda mot avancerade identitetshot med tre viktiga funktioner:

1. **Kontinuerlig riskutvärdering** utnyttjar AI för att tillämpa säkerhetspolicyer både vid inloggning och under en aktiv användarsession, vilket minskar risken för obehörig åtkomst och hot efter autentisering såsom sessionskapning.
2. **Delad signalpipeline** gör hoten tydligare i hela teknikekosystemet, så att säkerhetsteam kan identifiera och reagera på framväxande hot mellan olika säkerhetstekniker, inklusive hantering av mobilenheter (MDM), säkerhetförmedling för molnåtkomst (CASB), nätverkssäkerhet, slutpunktsidentifiering och svar (EDR) med mera.
3. **Adaptiva åtgärder** reagerar på hot i realtid genom att möjliggöra riktade åtgärder såsom universell utloggning från program som stöds där funktionen är aktiverad, uppmana användare att utföra multifaktorautentisering på begäran och utföra automatiserade arbetsflöden för att hantera nya risker.



Governance Analyzer med Okta AI

Begränsad tidig åtkomst andra kvartalet 2024

AI:ns roll: Tar emot många olika enhetsåtkomstsignaler, användaråtkomstsignaler och andra viktiga sammanhangsbaserade signaler för att tillhandahålla handlingsbara insikter om identitetsstyrning.

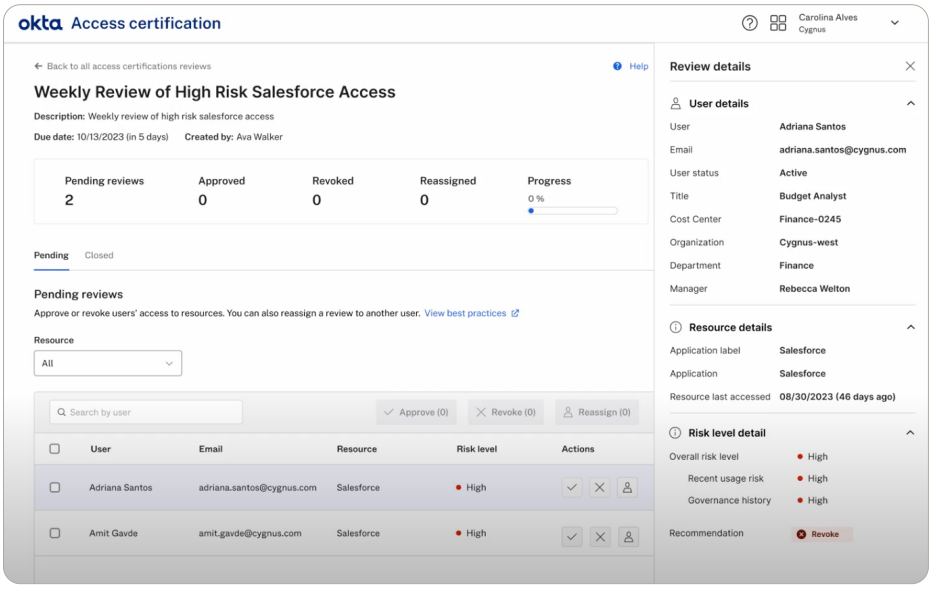
Identity Governance and Administration (IGA) är en policybaserad metod för identitetshantering och åtkomstkontroll som kombinerar följande:

- Identitetsstyrning: Processer och policyer som omfattar separeringen av uppgifter, rollhantering, loggning, åtkomstgranskningar, analyser och rapportering.
- Identitetsadministration: Administration av konto- och inloggningsdata, provisionering och deprovisionering av användare och enheter samt berättigandehantering.

Oktas position som en enhetlig plattform för IAM, IGA och privilegierad åtkomsthantering (PAM) ger en unikt omfattande identitetsdatauppsättning som kan utnyttjas för att hjälpa organisationer att uppfylla efterlevnadskraven, få den information som behövs för granskningar, effektivisera processer och göra arbetsstyrkan produktivare.

Governance Analyzer med Okta AI stöttar dessa mål genom att utnyttja maskininlärning, enhetsåtkomstsignaler och användaråtkomstsignaler för att

- minska den kognitiva bördan för beslutsfattare i styrningsprocesser
- ge betydelsefulla insikter om risken för kombinationer av användare och resurser
- utnyttja Oktas omfattande data för att tillhandahålla insikter som andra leverantörer inte kan tillhandahålla.



Potentiella tillämpningar för Governance Analyzer:

- Informera beslut om huruvida en användares åtkomst ska godkännas (t.ex. vid en förfrågan) eller förlängas (t.ex. vid en certifiering).
- Fastställa vem som kan begära åtkomst till en viss resurs (t.ex. endast användare under en viss risknivå kan begära åtkomst).
- Ange omfattningen för vems åtkomst som granskas i en kampanj (t.ex. alla användare över en angiven risknivå granskas automatiskt eller oftare).
- Vidta automatiska åtgärder för att godkänna eller neka åtkomst vid en begäran eller en certifieringskampanj.
- Rekommendera lämpliga styrningskonfigurationer för att säkerställa att viktiga resurser har nödvändiga godkännanden för att få åtkomst och att åtkomsten granskas ofta.

Log Investigator med Okta AI

Begränsad tidig åtkomst tredje kvartalet 2024

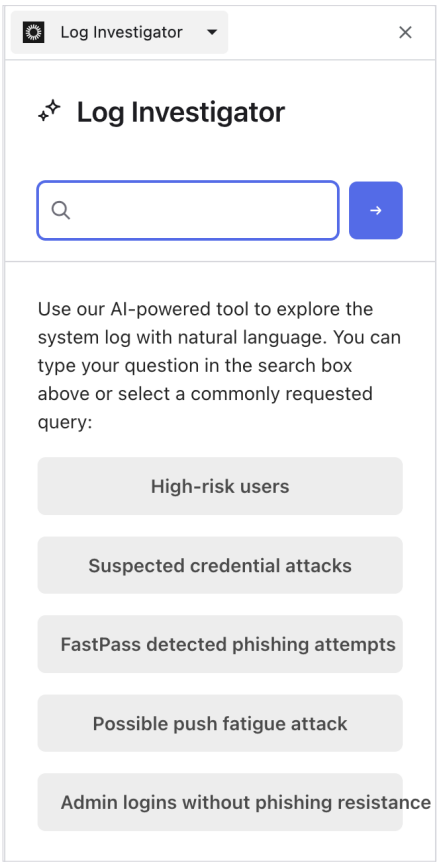
AI:ns roll: Driver en logg och ett API-sökverktyg på naturligt språk så att IT-medarbetare snabbt och enkelt kan hitta information och insikter från Oktas stora datauppsättning.

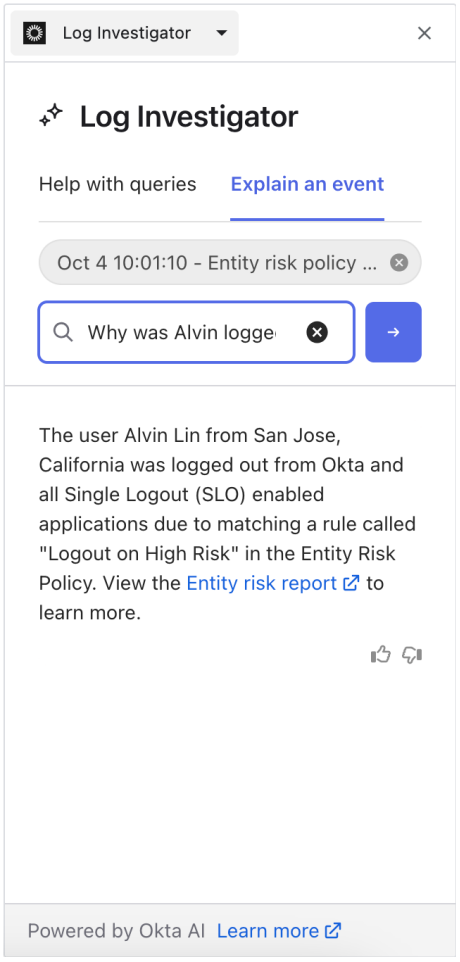
Sedan beräkningens gryning har loggar varit en ovärderlig informationsresurs för att avgöra vad som har hänt, vad som händer och varför. Men i takt med att digitala tekniker styr allt fler aspekter av verksamheter och kontrollen blir finkornigare har volymen loggar skjutit i taket och det har blivit svårare att extrahera insikter från dem. I många IT-system krävs det ofta noggrant utformade frågor och/eller manuell genomgång av hundratals resultat för att hitta svar även på enkla frågor, vilket tar upp tid och resurser som skulle kunna läggas på annat.

Som tur är ändrar generativ AI hur människor interagerar med datauppsättningar för att extrahera användbar information.

Log Investigator med Okta AI är en logg och ett API-sökverktyg med naturligt språk som IT-medarbetare kan använda för att snabbt och enkelt navigera i Oktas stora datauppsättning så att de kan få svar på identitetsfrågor:

- ”Har vi haft några misstänkta inloggningar den här veckan?”
- ”Vilka av dem kom från ohanterade enheter?”
- ”Kom någon av dem från en ny plats?”





Policy Recommender med Okta AI

Begränsad tidig åtkomst första kvartalet 2024

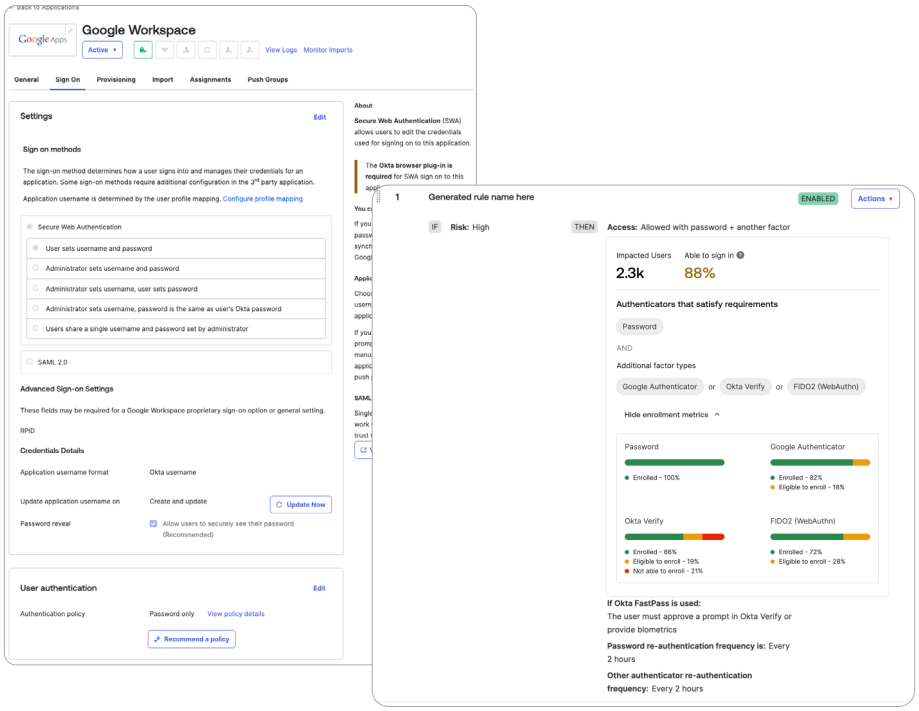
AI:ns roll: Undersöker policykonfigurationsdata från Oktas kundbas för att extrahera bästa praxis och generera policyer som kan läsas av maskiner som kan tillämpas direkt i Okta-miljöer.

Identitetsinfrastrukturen utgör ett enormt sammankopplat nät som omfattar hela organisationens IT-miljö – och till och med program från tredje parter. Det betyder att det är komplicerat att konfigurera och hantera detta omfattande system, och det kan ta tid och kräva energi och expertis.

Samtidigt stöter olika organisationer på och bemöter många liknande administrationssituationer, särskilt i de vanligaste programmen såsom Slack, Salesforce och GitHub – och dessa delade erfarenheter är en chans att dra nytta av varandras kunskap.

Policy Recommender med Okta AI utnyttjar anonymiserade, aggregerade insikter från Oktas kundbas för att ge administratörer policyrekommendationer och insikter (t.ex. hur många användare som påverkas av en policyändring, förhandsgranskning av effekten av en policy innan den tillämpas) för hantering av Okta Integration Network-appar (OIN), så att administratörer kan

- förstå problem som de stöter på och lösa dem lättare
- tillämpa rätt konfiguration och inställningar för rätt funktioner utan bekymmer
- förbättra säkerheten, effektiviteten och arbetsstyrkans produktivitet.



AI i Customer Identity Cloud (CIC)

Enligt Accentures Technology Vision 2023-rapport: **”Förmågan att autentisera kundernas identitet online verkar vara en prioritet för chefer – 85 % av dem sa att det börjar bli ett strategiskt kärnvärde, och tre fjärdedelar av deltagarna sa att problem med kundautentisering har haft en negativ påverkan på företagets resultat på grund av avbrutna transaktioner, frustrerade användare med mera.”**

Den bokstavliga definitionen av identitets- och åtkomsthantering för kunder (CIAM) har inte förändrats, men dess verkliga betydelse, när det gäller de exempel på användning den möjliggör, med vilka funktionella komponenter och för vilka typer av organisationer, har utvecklats, särskilt de senaste åren. Nu är CIAM avgörande för följande:

- Betjäna konsumentkunder: När det gäller business-to-consumer (B2C) gör en effektiv implementering av CIAM det möjligt för företag att erbjuda mycket personliga kampanjer och rekommendationer som ökar intäkterna och skapar mervärde för kunderna – samtidigt som de säkerställer en smidig användarupplevelse i flera digitala kanaler.
- Stärka företagskunder: Oräkneliga organisationer förlitar sig på SaaS-program för business-to-business (B2B). Olika användare inom varje organisation behöver dock olika åtkomstnivåer till olika resurser, och identitets- och åtkomstbehörigheter måste hanteras exakt för att möjliggöra en smidig och säker upplevelse. CIAM är lösningen eftersom den hjälper B2B SaaS-kunder att hantera identiteten själva.

Oktas inledande implementering av AI i Customer Identity Cloud fokuserade på säkerheten, av den enkla anledningen att det finns många olika hot mot program som används av kunder. Men tillvägagångssätt som kan användas för att skydda arbetsstyrkans identitet kan inte alltid användas för kundidentiteten. I företagsmiljöer är det ofta viktigare att upplevelser är säkra än att de är smidiga, så administratörer kan implementera kontroller utan att ta så mycket hänsyn till användarupplevelsen.

Men hantering av kundidentiteten måste bibehålla säkerheten och sekretessen med minimal friktion, vilket kräver försvar som kan stå emot sofistikerade hot utan att användare lägger märke till dem.

Som tur är har AI visat sig vara mycket bra på att skilja mellan hotaktörer som låtsas vara legitima användare och faktiska legitima användare.

Utöver nya Okta AI-säkerhetsfunktioner använder även andra nya funktioner maskininlärning och generativ AI för att förbättra kundupplevelsen, öka antalet konverteringar och förenkla administrationen.

Bot Detection

AI:ns roll: Undersöker över 60 signaler för att förutsäga när en autentiseringsförfrågan kommer från en bott, snarare än den legitima kontoinnehavaren.

Som en viktig del av tillägget Attack Protection i Customer Identity Cloud minskar Bot Detection-funktionen skriptade attacker (t.ex. stulna inloggningsattacker eller listvalideringsattacker) mot inbyggda program, lösenordsfria flöden och anpassade inloggningssidor.

Genom att analysera fler än 60 datakällor, såsom tidigare händelser kopplade till en IP-adress, den senaste inloggningshistoriken, en IP-adress rykte och diverse andra faktorer, förutsäger Bot Detection när en identitetsförfrågan sannolikt kommer från en bott. Över en viss förutsägelse-/relevansnivå tillämpar autentiseringsflödet en motåtgärd, t.ex. ett CAPTCHA-test.

Bot Detection är ett exempel på hur AI kan förbättra tidigare tekniker:

- Den första versionen, som introducerades i februari 2021, var regelbaserad och identifierade 18 % av bottarna.
- Den andra versionen, som lanserades i augusti 2021, använde maskininlärning för beteendeanalys. Denna AI-drivna metod mer än fördubblade effektiviteten och identifierade 45 % av bottarna.
- Den senaste versionen, som lanserades i juni 2022, identifierar 79 % av bottarna – det bästa resultatet hittills, trots att hotaktörer ständigt finslipar sina tekniker.

Viktigast av allt är att dessa nya försvarsfunktioner har uppnåtts utan onödig friktion för användare. Noggrann träning och kontinuerlig finjustering av AI:n som är själva kärnan av Bot Detection-funktionen hjälper till att se till att mänskliga användare sällan ser CAPTCHA-test.

Dessutom har en detaljerad intern studie som undersökte effekterna före och efter Bot Detection visat en stark avskräckande effekt:

- I genomsnitt minskade den skadliga trafiken med mer än 40 % för kunderna i studien som aktiverade Bot Detection.
- Bottrafiken minskade med nästan 90 % för vissa av de större kunderna i studien!

Bygga vidare på Bot Detection: Identity Threat Level (ITL)

I april 2023 gav vi en smygtitt på vårt initiativ för Identity Threat Level (ITL). Genom att vara vid programmens ”ytterdörr” med en CIAM-lösning som skyddar flera miljarder inloggningstransaktioner varje månad får vi en unik position för att övervaka identitetshot.

Detta mäktiga perspektiv ledde till ITL: en poäng från 0 till 10 som avslöjar den härledda bottaktivitetsnivån genom att representera sannolikheten att trafiken misslyckas med ett CAPTCHA-test. Ett betyg på 0 innebär att det praktiskt taget inte finns någon bottaktivitet, och ett betyg på 10 innebär att nästan all trafik sannolikt kommer från bottar.

Genom att aggregera (anonymt, så klart!) observationer i vår kundbas kan vi beräkna en ITL för olika branscher och geografiska områden, med möjlighet att införa ytterligare justeringar för andra gemensamma attribut. Exempel på vad ITL kan visa:

- Hur troligt skadlig trafik till CIC-kunder i olika branscher eller verksamhetsregioner har förändrats med tiden.
- Hur nivåer av troligt skadlig trafik till CIC-kunder jämförs mellan olika branscher eller verksamhetsregioner.

Spårning av tidigare trender och dagliga förändringar kan informera om förhöjda risker vid CIAM-flöden för inloggning och registrering, så att appleverantörer kan öka sin egen övervakning, proaktivt minska gränserna eller implementera ytterligare försvar, eller vidta andra åtgärder som de tycker krävs.

Och allt detta bygger på Bot Detection.

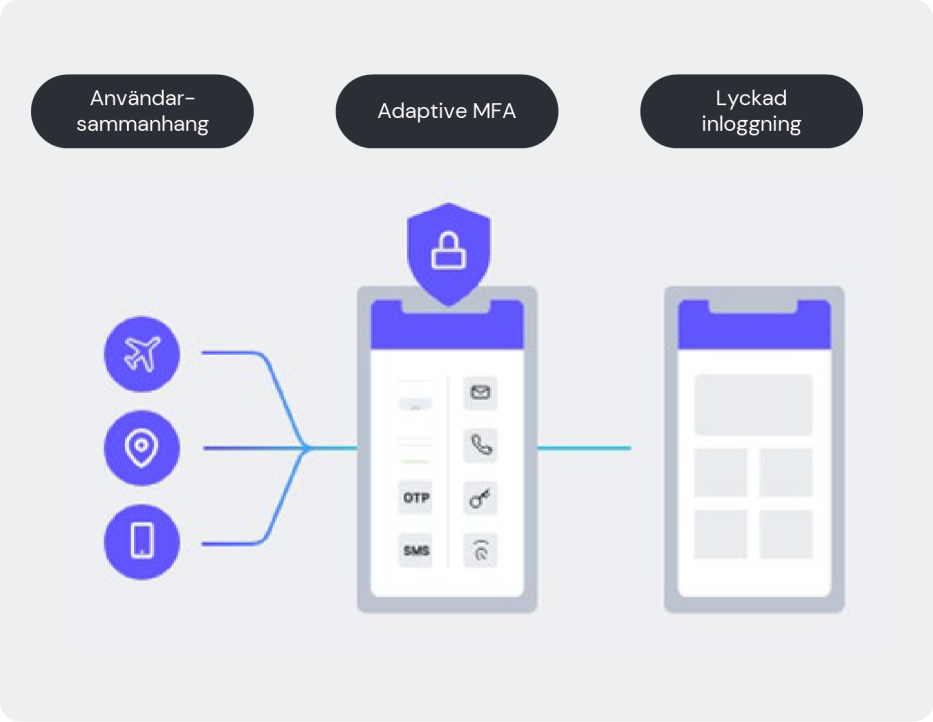
Adaptive MFA

AI:ns roll: Ger avgörande risksammanhang genom att analysera en stor uppsättning identitetssignaler för att förutsäga om ett autentiseringsförsök kommer från den legitima användaren eller från en hotaktör som låtsas vara en användare.

Adaptive MFA ger intelligent åtkomst som passar företagets behov och anpassar kundernas inloggningsbeteenden.

MFA är ett beprövat skydd mot kontokapning, men många företag, särskilt inom B2C, är tveksamma till att använda den eftersom de är oroliga att friktionen påverkar användarupplevelsen negativt.

Adaptive MFA är ett bra alternativ eftersom den bara visar en MFA-utmaning när en inloggning anses vara riskabel – och bevarar en smidig upplevelse resten av tiden.



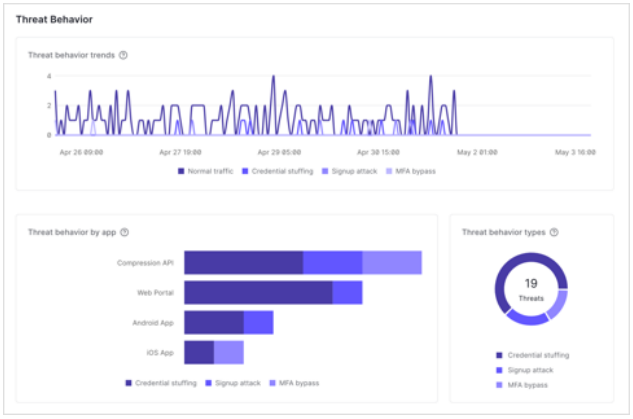
Security Recommendations

Kommer snart

AI:ns roll: Driver intelligenta rekommendationer som organisationer kan använda för att förbättra klientorganisationens säkerhetssits.

Med Säkerhetscenter kan IT- och säkerhetsmedarbetare se trender för potentiella attacker och snabbt reagera på dem i realtid genom att tillhandahålla följande:

- En enkel vy med autentiseringshändelser, potentiella incidenter och effektiviteten för hotrespons.
- Aviseringar i realtid om värden för avvikelseidentifiering.
- Visualiseringar av trender för potentiella attacker (t.ex. stulna inloggningsattacker, registreringsattacker, försök att kringgå MFA).
- Insikter om hur användarupplevelsen påverkas av Attack Protection-funktioner (t.ex. hastighetsbegränsning, CAPTCHA).



Dessa funktioner kommer nu att utökas med intelligenta, ML-drivna säkerhetsrekommendationer som tillhandahålls via säkerhetsrelaterade ögonblicksbildsaviseringar och kontrollpanelsaviseringar.

Identity Flow Optimizer med Okta AI

Begränsad tidig åtkomst fjärde kvartalet 2024

AI:ns roll: Analyserar autentiseringsdata för att föreslå sätt att förbättra kundupplevelsen och öka antalet konverteringar.

Inom kundriktade verksamheter innebär friktion allt som saktar ner interaktioner med en tjänst. Dessa interaktioner kan omfatta (men är inte begränsade till) en användare som

- registrerar sig för din tjänst
- loggar in på sitt befintliga konto
- uppdaterar sin information och sina inställningar
- återställer förlorade kontodata
- betalar i kassan (dvs. slutför ett köp).

Ju mer friktion det finns, desto lägre är en organisations konverteringstakt och desto mindre blir intäkterna på både kort och lång sikt. Men det kan vara väldigt svårt att optimera kundflöden manuellt, på grund av de enorma mängderna data och det faktum att alla användare har olika preferenser.

Dessutom måste identitetsflöden vara säkra, och det kan vara svårt även för experter, för att inte tala om nybörjare.

För att hantera dessa utmaningar ger Identity Flow Optimizer utvecklare infogade rekommendationer om identitetskonfigurationer och åtgärder de kan lägga till för att öka antalet konverteringar, förbättra säkerheten och bygga sina appar snabbare.

Brand Customizer med Okta AI

Begränsad tidig åtkomst fjärde kvartalet 2024

AI:ns roll: Skapar eller fyller automatiskt i utformningsmallar med en organisations varumärke.

Det finns en anledning till att utformningsriktlinjerna för varumärken är strikta: För att tillhandahålla en konsekvent användarupplevelse som förstärker varumärkets noggrant genomtänkta identitet.

Brand Customizer kan utforma en mall på en sida och anpassa utformningen till alla andra obligatoriska mallar. En utvecklare kan även tillhandahålla en skärmbild eller logotyp, så skapar AI:n mallarna och utvecklaren kan anpassa dem efter behov.

Den här metoden skapar ett sammanhängande intryck och känsla för slutanvändarna, och skapar värde snabbare eftersom det är enklare och går snabbare för utvecklare att skapa överlägsna kundupplevelser, innovera och bidra till företagets skala.

Guide med Okta AI

Begränsad tidig åtkomst fjärde kvartalet 2024

AI:ns roll: Tolkar uppmaningar på naturligt språk och ger sammanhangsbaserad hjälp för att hjälpa användare att arbeta effektivt med Customer Identity Cloud.

Customer Identity Cloud är kraftfullt, har många funktioner och är mycket utbyggbart men det stora utbudet av funktioner kan avskräcka nya användare, och inte ens experter har nödvändigtvis koll på alla detaljer och nya funktioner.

Så här hjälper Guide nya användare att komma igång snabbt och alla användare att få ut mesta möjliga av CIC:

- Omfattande onboardinghjälp och intuitiv kartläggning av de bästa stegen för användare, så att de smidigt styrs mot de bästa arbetsflödena från enkla uppmaningar på naturligt språk.
- Kan förklara vilken inställning eller jargong som helst på plattformen på ett lättförståeligt sätt och även berika upplevelsen med sammanhangsbaserad hjälp och sammanställda länkar till relevant dokumentation.

Actions Navigator med Okta AI

Begränsad tidig åtkomst andra kvartalet 2024

AI:ns roll: Möjliggör sökning på naturligt språk så att det är enklare att hitta rätt integreringar, och hjälper användare att utveckla helt nya integreringar efter behov.

Utbyggbarhet är en huvudfunktion i Customer Identity Cloud och Auth0 Marketplace strävar efter att förenkla utvecklingsprocesser genom att tillhandahålla ett enkelt sätt att lägga till en integrering i identitetsprogram.

Men det finns hundratals integreringar, så det kan vara svårt att hitta exakt det man behöver.

Med Actions Navigator kan utvecklare upptäcka och implementera marknadsplatsintegreringar eller skriva en åtgärd (en funktion som används för att anpassa och utöka CIC-funktioner) genom att helt enkelt be om den i en sökfråga. Kodgenerering är ett av de mest omvandlande användningsområdena för generativ AI, som leder till nya funktioner både för utvecklare och för dem som inte kan skriva kod.

Tenant Security Manager med Okta AI

Begränsad tidig åtkomst andra kvartalet 2024

AI:ns roll: Utvecklar sammanfattningsbeskrivningar på naturligt språk för komplicerade identitetskonfigurationer.

Många organisationer har ämnesexperter som har värdefull institutionell kunskap om vissa system, inklusive identitet.

När dessa experter inte är tillgängliga, t.ex. om de flyttar till en ny avdelning eller lämnar företaget, kan det vara mycket svårt för andra att förstå systemet och detaljerna i dess konfiguration.

Tenant Security Manager förbättrar Oktas Attack Protection-funktioner med intelligenta säkerhetsrekommendationer genom säkerhetsrelaterade ögonblicksbildsaviseringar och kontrollpanelsaviseringar för att förbättra klientorganisationens säkerhetssits.

Sammanfattning

ChatGPT:s plötsliga ankomst, och den snabba lanseringen av en lång rad lika imponerande verktyg, visar att den senaste tekniken förändras så snabbt, med så många olika konsekvenser, att det vore dåraktigt att försöka göra specifika förutsägelser om AI och dess påverkan.

Vissa saker är dock tydliga. Rubriken i ett pressmeddelande från Forrester säger allt om konsekvenserna av AI, och särskilt generativ AI: Det vore ett dyrt misstag för företag att ignorera generativ AI.

Eller se det så här: Du kanske inte vet exakt vart dina investeringar i AI leder, men du kan vara säker på att om du inte gör några investeringar hamnar du efter konkurrenterna, eller blir irrelevant i värsta fall.
Så avgörande är det här paradigmskiftet.

Genom att använda en avsevärd del av vår forsknings- och utvecklingsbudget för AI, och genom att utnyttja vår enorma IAM-datauppsättning, kommer Okta att fortsätta att tillhandahålla innovativa AI-drivna funktioner för att stärka säkerheten, öka produktiviteten och förbättra användarupplevelser – både inom Workforce Identity Cloud och Customer Identity Cloud.

Vi vet inte exakt vad våra investeringar kommer att leda till, men vi är säkra på att vi i framtiden kommer att se dagens funktioner och de funktioner vi utvecklar som de första stegen på en omvälvande resa.

Ansvarsfriskrivning

Detta material och eventuella rekommendationer häri utgör inte rådgivning gällande juridisk information, sekretess, säkerhet, efterlevnad eller affärsverksamhet. Detta material är endast avsett för allmänna informationssyften och kanske inte återspeglar de senaste säkerhets-, sekretess- och lagstiftningsutvecklingarna eller alla relevanta ämnen. Du ansvarar för att erhålla rådgivning gällande juridisk information, säkerhet, sekretess, efterlevnad eller affärsverksamhet från din egen advokat eller annan professionell rådgivare och bör inte förlita dig på rekommendationerna häri. Okta ansvarar inte för eventuella förluster eller skador som kan uppstå till följd av att du följer rekommendationer i detta material. Okta ger inga utfästelser, garantier eller andra försäkringar gällande innehållet i detta material. Det finns information om Oktas avtalsförpliktelser gentemot dess kunder på okta.com/agreements.

Produkter, funktioner eller funktionaliteter som nämns i det här materialet och som inte är allmänt tillgängliga i nuläget kanske inte kan levereras i tid eller inte alls. Produktöversikter ska inte likställas med några utfästelser, skyldigheter eller löften om att leverera produkter, funktioner eller funktionaliteter, och du bör inte förlita dig på dem när du fattar inköpsbeslut.