Whitepaper

Okta & AI

Wie künstliche Intelligenz das Identity and Access Management (IAM) verändert

Inhalt

Zusammen-fassung

Künstliche Intelligenz (KI) verändert die Art und Weise, wie Unternehmen arbeiten – und treibt mithilfe von Optimierungsanalysen, Datenauswertungen, Anomalie-Erkennungen und anderen auf die Zukunft ausgerichteten Ansätzen die Entwicklung innovativer Produkte und Services voran. Die meisten dieser Features sind nicht neu. Neu ist vielmehr, dass Kostensenkungen und Leistungssteigerungen die Integration solche Features in, nun ja, so ziemlich alles möglich gemacht haben.

Neu ist, dass die generative KI dank der rasanten Fortschritte bei den Large Language Models (LLMs), die den Kern von Anwendungen wie ChatGPT und DALL-E von OpenAI, Bard von Google und Code Llama von Meta bilden, scheinbar über Nacht Einzug gehalten hat.

Wir glauben, dass die generative KI einen echten und einzigartigen Paradigmenwechsel darstellt, dessen Auswirkungen wir gerade erst zu spüren – und zu verstehen – beginnen.

Und nur wenige Bereiche eignen sich so gut für die Anwendung von KI wie Identity. Der Bereich Identity ist nicht nur komplex – es gibt also viele Möglichkeiten für KI, die Dinge zu verbessern –, sondern Identity-Prozesse und -Transaktionen generieren auch riesige Datenmengen, die KI-Engines im Grunde antreiben. Während wir Datennetzwerkeffekte im gesamten Bereich Identity nutzen möchten, konzentrieren wir unsere R&D-Investitionen kurzfristig auf:

- Verbesserung der Sicherheit
- Steigerung der Produktivität
- Hochwertige User Experiences

Entscheidend ist, dass KI für das Okta Team kein Neuland ist, und wir sind stolz darauf, ihr Potenzial bereits in mehreren Schlüsselbereichen zu nutzen. Zum Beispiel:

- Die Okta Workforce Identity Cloud (WIC) integriert KI in ThreatInsight, Adaptive Multi-Faktor-Authentifizierung (Adaptive MFA) und unsere Anti-Toll Fraud-Schutzmaßnahmen
- Die Okta Customer Identity Cloud (CIC) greift bei der Bot Detection (und dem damit verbundenen Identity Threat Level, oder ITL) und der Adaptive MFA auf KI zurück

Und auf der Oktane 2023 haben wir eine Reihe neuer KI-gestützter Features angekündigt. Okta AI stellte vier neue WIC-Features vor, um:

- die Sicherheit zu verbessern: Identity Threat Protection
- die Governance zu unterstützen: Governance Analyzer
- die Administration zu vereinfachen: Log Investigator, Policy Recommender

Die CIC wurde mit sechs neuen Features ausgestattet, um:

- die Tenant-Sicherheit zu verbessern: Security Recommendations
- die Customer Experience zu verbessern und den Umsatz zu steigern: Funnel Conversion Recommendations, Brand Customization
- die Administration zu vereinfachen: Co-Pilot, Action Selection and Development, Personalized Tenant Configuration Summary

Darüber hinaus fördern wir eine innovationsorientierte Kultur, die in zwei unternehmensweiten Hackathons pro Jahr ihren Ausdruck findet. Viele der Ideen, die bei diesen Hackathons entwickelt werden, führen zu Patenten und Produkt-PoCs und kommen schließlich in der einen oder anderen Form auf den Markt. Bei einem der letzten Hackathons konzentrierten sich 25 % der Projekte auf KI-Experimente — und wir sind begeistert von ihrem Potenzial.

Um der Bedeutung von KI und der Begeisterung, die sie bei Entwicklern hervorruft, Rechnung zu tragen, haben wir darüber hinaus unseren allerersten dedizierten KI-Hackathon geplant.

Wir haben auch unsere Kunden dabei unterstützt, spannende und elegante Erfahrungen mit LLMs zu schaffen, und das erweiterte Ökosystem von Okta – Okta Ventures, das Okta Integration Network, Auth0 for Startups und den Auth0 Marketplace – bietet eine breite Palette an KI-Lösungen, die sich mit unseren Angeboten integrieren lassen.

Die Zukunft hält ohne Frage Herausforderungen bereit – Cyberkriminelle nutzen KI, und insbesondere LLMs, bereits, um neue Angriffsvektoren auszuloten und bestehenden Angriffen noch mehr Wucht zu verleihen. Dennoch bleiben wir optimistisch, dass KI eine Kraft für das Gute sein kann und wird.

Digitale Identitäten regeln heute den Zugang zu immer mehr Anwendungen und Diensten – und beeinflussen und steuern damit viele Aspekte des modernen Lebens. In Zukunft wird die Tragweite noch wesentlich größer sein. Authentifizierung, Autorisierung und Identity werden unverzichtbar sein, um Vertrauen, Sicherheit und eine hochwertige User Experience zu gewährleisten.

Wir haben es uns auf die Fahnen geschrieben, das Potenzial der KI zu nutzen, um die Menschen, die Technologie und die Gesellschaft noch enger zusammenzubringen.

Einführung

In den letzten Monaten wurde sowohl in den Tech- als auch in den Mainstream-Medien viel über Durchbrüche im Bereich der künstlichen Intelligenz (KI) und die – teils erwarteten, teils unerwarteten – Anwendungen berichtet, die durch diese Durchbrüche möglich gemacht werden.

Wie es Andy Grove einmal formulierte: „Nur die Paranoiden überleben." Es sollte daher nicht überraschen, dass sich Unternehmen unterschiedlichster Größen und Branchen darum bemühen, KI zu nutzen, um bestehende Lösungen zu verbessern, neue Lösungen zu entwickeln und den Vorsprung auf den Wettbewerb auszubauen.

In innovative KI-Technologien zu investieren, ist für uns selbstverständlich. KI unterstützt bereits eine Reihe wichtiger Produkte und Features in unserem Portfolio. Insbesondere Machine Learning (ML) ist fest mit einem Großteil unserer Dynamic-Risk-Assessment- und Risk-Based-Authentication-Intelligence-Lösungen verankert.

Als Resultat jahrelanger praktischer Erfahrung betrachten wir KI nicht als isoliertes Modul oder Funktionalität – etwas, das sich einfach an unsere Plattform anflanschen ließe. Vielmehr betrachten wir KI als eine universelle Technologie (oder besser, eine Sammlung von Universaltechnologien), die es mit der Identity-Infrastruktur zu verflechten und zu integrieren gilt.

In unserem Whitepaper schauen wir hinter die Kulissen – und verraten Ihnen, wie Okta das Thema AI angeht:

- Warum KI das Potenzial besitzt, praktisch jeden digitalen Bereich zu revolutionieren
- Warum Identity besonders von KI profitiert
- Den wichtigsten Mehrwert, den wir in KI in naher Zukunft sehen
- Wie wir KI bereits in der Okta Workforce Identity Cloud (WIC) und der Okta Customer Identity Cloud (CIC) einsetzen
- Wie wir Okta AI in neuen WIC- und CIC-Features einsetzen

Warum AI?

Auf einer grundlegenden Ebene kann Künstliche Intelligenz als eine von einem Computer getroffene Entscheidung verstanden werden, deren „Intelligenz“ sich nicht von einer von einem Menschen getroffenen Entscheidung unterscheidet – unabhängig davon, wie die Entscheidung zustande kommt.

Obwohl das Konzept der KI offiziell auf dem Dartmouth Workshop vorgestellt wurde, geht die ursprüngliche Prämisse auf das Jahr 1943 zurück, als der Logiker Walter Pitts und der Neurowissenschaftler Warren McCulloch versuchten, eine mathematische Darstellung der Neuronen im menschlichen Gehirn zu erstellen. Diese zeitgenössischen Fortschritte bauten auf einer langen Geschichte von Fortschritten in der Theoretischen Informatik auf, von Ada Lovelace im 19. Jahrhundert bis zu Alan Turing.

Seit den 1960er Jahren hat sich die KI zu einer riesigen Sammlung von Algorithmen entwickelt, die unter anderem zum Entdecken und Erkennen von Mustern dienen – in der Regel mithilfe von Machine Learning. Der ML-Bereich hat sich in den letzten 15 Jahren rasant entwickelt, was zur Entstehung des praktischen und wirtschaftlichen Deep Learnings geführt hat.

Generative KI stellt einen einzigartigen Paradigmenwechsel dar

Die KI-Entwicklung, die die Welt im Sturm erobert hat, ist der unglaubliche – und viele würden sagen schockierende – Siegeszug und die rasante Entwicklung der generativen KI, die vor allem durch bemerkenswerte Fortschritte bei den Large Language Models (LLMs) vorangetrieben wird.

Anwendungen wie ChatGPT und DALL-E von OpenAI, die auf LLMs basieren, haben KI Mainstream-tauglich gemacht; zum Teil aufgrund ihrer Fähigkeit, Menschen zu imitieren, zum Teil aufgrund mangelnder Transparenz über die vom Modell verarbeiteten (und dessen Verhalten beeinflussenden) Daten.

Plötzlich sind das Schreiben von Prosa und das Entwerfen komplexer (und lebendiger, sofern das denn die Intention ist) Bilder nicht mehr die alleinige Domäne des Menschen. Weil LLMs so gut schreiben – und auch Programmieren ist letztlich ja schreiben – und so vieles heute von Software gesteuert wird, sind LLMs für unerwartete Durchbrüche und Fortschritte in einer Vielzahl von Bereichen verantwortlich.

Ganz offensichtlich ist ein modernes KI-Zeitalter angebrochen. Es ist daher nur natürlich, sich zu fragen, wie man ihre Fähigkeiten – alte, neue und noch in der Entwicklung befindliche – nutzen kann.

Was kann KI leisten?

In ihrem Buch „Prediction Machines“ beschreiben die Wirtschafts-wissenschaftler Ajay Agrawal, Joshua Gans und Avi Goldfarb den Aufstieg der KI als Senkung der Kosten für Prognosen, die sie wiederum als Nutzung vorhandener Informationen zur Generierung neuer Informationen definieren.

Da Prognosen „das Herzstück von mit Unsicherheit behafteten Entscheidungen bilden“ und „unser Berufs- und Privatleben von solchen Entscheidungen durchsetzt ist“, birgt die Senkung der Kosten für Prognosen ein außerordentliches Potenzial. Prognosen sind etwa wesentlicher Bestandteil von:

- Optimierung: Nutzung des Kontexts und früherer Beobachtungen zur Prognose eines optimalen Pfads, einer optimalen Reaktion, einer optimalen Konfiguration, eines optimalen UI-Designs usw.
- Verhaltensanalyse: Beobachtung des Echtzeitverhaltens im Kontext früherer Aktionen zur Prognose der Absichten eines Users
- Data Mining: Prognose, welche Daten und Erkenntnisse am besten zur Anfrage oder Aufforderung eines Users passen (nebenbei bemerkt, bilden Prognosen auch das Herzstück von LLMs und generativer KI)

Wie die klassische Informatik ist KI (in all ihren Formen) eine Universal-technologie, die verspricht, bestehende Branchen zu revolutionieren – und wir sind besonders optimistisch, was ihr Potenzial zur Weiterentwicklung von Identity angeht.

KI und Identity

Eine digitale Identität ist eine Reihe von Attributen, die einen bestimmten User im Kontext einer von einer bestimmten Anwendung bereitgestellten Funktion definieren. Digitale Identitäten regeln heute den Zugang zu immer mehr Anwendungen und Diensten – und beeinflussen und steuern damit viele Aspekte des modernen Lebens. In Zukunft wird die Tragweite noch wesentlich größer sein. Authentifizierung, Autorisierung und Identity werden unverzichtbar sein, um Vertrauen, Sicherheit und eine hochwertige User Experience zu gewährleisten.

IAM-Services bilden daher die Eckpfeiler unserer vernetzten Welt und stellen sicher, dass nur autorisierte User – Mitarbeiter, Lieferanten, Partner, Kunden – auf bestimmte Ressourcen zugreifen können. Konzeptionell gesehen, ist IAM sehr einfach: Ein User bestätigt seine Identität und erhält Zugriff auf eine Ressource, für die er berechtigt ist. Die Praxis wird jedoch durch mehrere Faktoren verkompliziert:

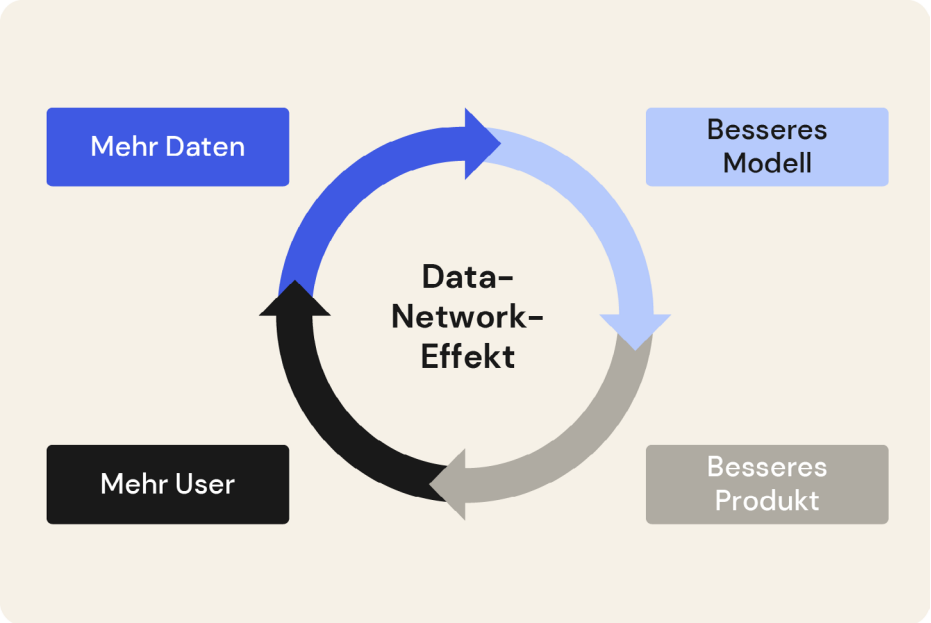
- In der heutigen digitalen Welt gibt es viele User, ein einzelner User kann mehrere digitale Identitäten besitzen, und es gibt unzählige Möglichkeiten, eine digitale Identität zum Ausdruck zu bringen
- Unterschiedliche digitale Identitäten haben unterschiedliche Rechte und Befugnisse in Bezug auf Ressourcen – und diese Rechte und Befugnisse sind zunehmend dynamisch
- Mit dem Ende des klassischen Perimeters satteln Bedrohungsakteure auf identitätsbasierte Angriffe um

Wie wir gesehen haben, kann KI sehr gut mit Komplexität und Unsicherheit umgehen – vorausgesetzt, es stehen genügend Daten zur Verfügung.

Glücklicherweise gibt es im Identity-Bereich reichlich Daten, denn Identity selbst hat sich von einem statischen, eindimensionalen Attribut zu einer dynamischen, fortlaufenden Interaktion entwickelt, die sich mit jedem neuen Datenpunkt verändert. Diese Entwicklung wäre ohne die Cloud-Transformation in der Vergangenheit nicht möglich gewesen und wird sich dank der derzeit stattfindenden KI-Transformation fortsetzen.

Nutzung von Datennetzwerkeffekten

Eine wichtige Folge dieser Entwicklung ist, dass sie einen positiven Kreislauf von Datennetzwerkeffekten ermöglicht: Je mehr und je bessere Daten einem KI-Modell zur Verfügung stehen, desto schneller kann es lernen und desto genauer werden seine Prognosen oder Entscheidungen; dies wiederum macht das Produkt oder den Service für seine User wertvoller, was wiederum mehr User anzieht, die wiederum mehr Daten generieren, die in einem positiven Kreislauf wieder in das Modell eingespeist werden können:



1. **Mehr Daten:** Je stärker ein Produkt oder ein Service genutzt wird, desto mehr Daten werden durch User-Interaktionen, -Transaktionen, -Feedback usw. generiert.
2. **Besseres Modell:** Diese Daten werden verwendet, um das zugrundeliegende KI-Modell zu verfeinern. Je größer die Menge und je höher die Qualität der Daten, desto genauer die Prognosen oder Entscheidungen des Modells.
3. **Besseres Produkt:** Mit dem KI-Modell verbessert sich auch das Produkt oder der Service.
4. **Mehr User:** Das verbesserte Produkt oder der verbesserte Service zieht weitere User an, die noch mehr Daten generieren, wodurch sich der Kreislauf fortsetzt.

Dieser sich selbst verstärkende Kreislauf kann ein starker Motor für Innovation und Wettbewerbsdifferenzierung sein.

Angesichts der dynamischen Bedrohungslandschaft warnt Gartner davor, dass **„Angriffe, die generative KI nutzen, sicherheitsbewusste Unternehmen bis 2025 dazu zwingen werden, die Schwellenwerte für die Erkennung verdächtiger Aktivitäten zu senken, was zu mehr Fehlalarmen und damit zu mehr – nicht weniger – menschlicher Intervention führen wird."**

[1] Gartner, 4 Ways Generative AI Will Impact CISOs and Their Teams, Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook, 29. Juni 2023) GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seinen Tochtergesellschaften in den Vereinigten Staaten und international und wird hier mit Genehmigung verwendet. Alle Rechte vorbehalten.

Verbesserung der Sicherheit

Es ist inzwischen kein Geheimnis mehr, dass KI:

- bestehende identitätsbasierte Angriffe, wie Credential Stuffing und Phishing, gefährlicher (sprich schwieriger zu erkennen, effektiver/zerstörerischer) machen kann
- völlig neue Arten von identitätsbasierten Angriffen ermöglichen kann, auf die man größtenteils erst dann aufmerksam wird, wenn sie in freier Wildbahn auftauchen
- einige bestehende Schutzmaßnahmen aushebeln (z. B. CAPTCHAs lösen, Sprachbiometrie überlisten) kann

Darüber hinaus machen es die Programmier- und Skripting-Fähigkeiten der generativen KI für Bedrohungsakteure aller Qualifikationsstufen (d. h., mit oder ohne Programmierfähigkeiten) einfacher, Angriffe zu lancieren, was potenziell mehr Teilnehmer in das Cybercrime-Ökosystem lockt und die Effizienz verbessert.

Zwar wird KI zweifellos viele Angriffe flankieren, sie dient aber auch den Security-Teams als „Power-up".

Okta ist mit FastPass im Bereich der Phishing-resistenten Authentisierung – auf jeder Plattform für gemanagte und nicht gemanagte Geräte – bereits branchenführend und erleichtert Entwicklern die Implementierung der benutzerfreundlichen und Phishing-resistenten FIDO2-Authentisierung. Wir sind uns jedoch auch der Notwendigkeit bewusst, KI einzusetzen, um:

- **Okta von Grund auf noch sicherer zu machen**: So wie Bedrohungsakteure KI nutzen können, um nach Schwachstellen und Sicherheitslücken zu suchen, können dies auch Unternehmen wie Okta. Unser Vorteil ist, dass wir KI einsetzen können, um Software und Systeme bereits vor Release zu härten.
- **Die Threat-Erkennung zu automatisieren:** Kontext- und Verhaltensanalysen sind bereits in der Lage, intelligente Risikobewertungen durchzuführen und mehrstufige Identity Threats zu erkennen, und Fortschritte in der KI werden diese Features weiter verbessern und neue hervorbringen.
- **Risiken für unsere Kunden zu minimieren:** Egal, ob es um die Automatisierung von Schutzmaßnahmen (z. B. Eindämmung, Blockieren bösartiger Aktivitäten), um die Kombination eines Alerts mit einem empfohlenen Playbook oder um die Unterstützung von Governance, Risikomanagement und Compliance (GRC) geht – KI wird bei der proaktiven Risikominimierung und der Reaktion auf Angriffe von unschätzbarem Wert sein.

Glücklicherweise verfügen wir bereits über umfangreiche Erfahrungen bei der Integration von KI-gestützten Security-Features in unsere Workforce Identity Cloud und Customer Identity Cloud.

Steigerung der Produktivität

Eine der wichtigsten Erkenntnisse des Reports „How Development Teams Purchase SaaS – 2023“ von Okta ist, dass es im Wesentlichen zwei Arten von Unternehmen gibt: diejenigen, die KI bereits in der Produktentwicklung einsetzen (52 % der Befragten), und diejenigen, die dies in den nächsten 12 Monaten tun werden (45 %).

Immer mehr Unternehmen integrieren KI-gestützte Tools für Datenanalysen, Qualitätssicherung, Machine Learning, Automatisierung und mehr, weil sie sich davon viele Vorteile versprechen – von höherer Agilität über neue Funktionalitäten bis hin zu Kosten- und Zeitersparnis.

Wir teilen diesen Optimismus und nutzen das produktivitätssteigernde Potenzial von KI in unseren eigenen Entwicklungsprozessen.

Gleichzeitig sind wir uns bewusst, dass die Vorteile von KI viel weiter reichen sollten: bis zu jedem einzelnen Mitarbeiter in praktisch jedem Kundenunternehmen, unabhängig von Größe und Branche.

Eine moderne und ausgereifte Workforce-Identity-Infrastruktur:

- ermöglicht es Mitarbeitern, Lieferanten und Partnern, bei der Arbeit von überall aus sicher auf kritische Tools und Ressourcen zuzugreifen
- bietet eine komfortable User Experience, steigert die betriebliche Effizienz und reduziert den Verwaltungsaufwand – sodass mehr Zeit und Energie für Wachstum, Innovation und andere Prioritäten zur Verfügung steht
- ermöglicht die Skalierung des Unternehmens und verbessert seine Agilität unabhängig von der Größe
- schützt vor Geschäftsunterbrechungen durch böswillige Akteure

Eingebettet in eine Identity-Infrastruktur kann KI all diese Vorteile verstärken – und zweifellos neue hervorbringen.

Hochwertige User Experiences

Konzentrieren wir uns für einen Moment auf das Thema Reibungsverluste.

Im Privatkundengeschäft ist Mehraufwand – sprich: alles, was die Interaktion des Anwenders mit Ihrem Service verlangsamt – ein großes Hindernis für Konversionen und somit für den Umsatz. Der Okta Customer Identity Trends Report ergab, dass fast 60 Prozent der Befragten eher dazu bereit wären, Geld auszugeben, wenn Services einen einfachen, sicheren und reibungslosen Login-Prozess bieten würden. Diese Erkenntnis gilt dabei über alle Segmente und Branchen hinweg. Eine unkomplizierte und komfortable Interaktion ist also allen Kunden gleichermaßen wichtig.

Natürlich ist ein gewisses Maß an Reibungsverlust notwendig, um Vertrauen zu schaffen und Sicherheit zu bieten. Allerdings kann die Reduzierung von Reibungsverlusten, wo immer dies möglich ist – bei jeder Kundeninteraktion –, die Konversionsraten erhöhen und somit den Umsatz sowohl kurz- als auch langfristig steigern.

Wo kommt KI ins Spiel? Drei naheliegende Anwendungsbereiche sind:

- Kontinuierliches Risk Assessment, um Erfahrungen ohne Passwort und Login zu ermöglichen
- Optimierung von Identitäts-Prozessen für eine bessere Usability
- Verbesserung des UI-Designs (z. B. während Identity-Transaktionen) für eine bessere Usability

Am Arbeitsplatz können Reibungsverluste als alles verstanden werden, was die Erledigung von Aufgaben verhindert oder verlangsamt. Obwohl Identity (allein) nicht dafür sorgen kann, dass ein Meeting pünktlich beginnt oder ein Kollege schneller auf eine Anfrage antwortet, kann eine ausgereifte Identity-Infrastruktur anderweitig unterstützen, etwa:

- sicherstellen, dass User zur richtigen Zeit mit den richtigen Privilegien auf die richtigen Ressourcen (z. B. Daten, Systeme, Anwendungen) zugreifen können
- Self-Service-Features (z. B. Zugriffsanforderung auf Ressourcen, Profiländerung, Aktivierung von Sicherheitsfaktoren usw.) ermöglichen
- bestehende Prozesse (z. B. Zugriffsüberprüfung und -zertifizierung, sicheres Offboarding etc.) automatisieren

Auch hier kann KI diese bestehenden Fähigkeiten verbessern und gleichzeitig neue erschließen. Beispielsweise kann KI große Mengen von Identity-Implementierungen und Performance-Indikatoren analysieren, um die effizientesten und effektivsten Konfigurationen zu ermitteln, und diese Erkenntnisse nutzen, um Empfehlungen auszusprechen, die auf das jeweilige Unternehmen oder die jeweilige Abteilung zugeschnitten sind. Darüber hinaus kann KI Administratoren dabei unterstützen, schnell die benötigten Informationen in einer ansonsten überwältigenden Menge an Betriebs- und Log-Daten zu finden.

Dank der Fähigkeit von LLMs, natürliche Sprache zu verarbeiten, werden mehr und mehr identitätsbezogene Funktionen auch für Nicht-Programmierer zugänglich. Okta Workflows ermöglicht bereits No-Code-Identity-Automatisierung und -Orchestrierung über eine Drag-and-Drop-Schnittstelle – eine Lösung, die Anweisungen in natürlicher Sprache verarbeitet, ist also gar nicht so weit hergeholt.

KI in der Workforce Identity Cloud (WIC)

Während Identity früher nur als ein Service für das Management von Usernamen und Passwörtern angesehen wurde, ist sie heute eine Notwendigkeit und ein Innvationsmotor für jedes moderne Unternehmen. Infolgedessen ist die Identity-Infrastruktur eine vernetzte und grundlegende Schicht innerhalb der weiteren IT-Umgebung, die User und andere Entitäten mit Systemen, Daten und Ressourcen sowohl On-Prem als auch in der Cloud verbindet.

Daher ist Identity Security ein grundlegendes Element eines starken Security-Standings – und unterstützt bei der Bekämpfung von Insider-Threats sowie Credential-basierten Bedrohungen von außen.

KI trägt nicht nur dazu bei, die Workforce-Identity-Infrastruktur vor Bedrohungen zu schützen, sondern ist auch besonders gut dafür geeignet, Governance-Aktivitäten zu unterstützen – insbesondere durch die Analyse großer Mengen an Konfigurationsdaten, um Risiken zu identifizieren, Korrekturmaßnahmen zu empfehlen und sogar viele gängige und wichtige Aufgaben zu automatisieren.

Aufgrund ihrer Fähigkeit, Informationen zu analysieren und Erkenntnisse zu gewinnen, ist KI auch hervorragend für die Interpretation großer Mengen an Logs geeignet.

Die Kombination dieser Fähigkeiten mit der Verarbeitung natürlicher Sprache und generativer KI verändert bereits die Art und Weise, wie Administratoren ihre ständig wachsenden Identity-Infrastrukturen managen.

Laut dem auf einer Umfrage unter mehr als 500 IAM- oder Security-Experten basierenden Report „Trends in Securing Digital Identities 2022“ der Identity Defined Security Alliance (zu der Okta gehört) gaben:

- **84 %** der Befragten an, dass ihr Unternehmen im vergangenen Jahr einem identitätsbezogenen Breach zum Opfer gefallen ist
- **78 %** an, dass ein Breach direkte Auswirkungen auf das Business hatte
- **64 %** an, dass das effektive Management und die Sicherheit digitaler Identitäten entweder höchste Priorität hat (16 %) oder unter den Top 3 rangiert (48 %)

ThreatInsight

Die Rolle der KI: Sie prognostiziert, ob Requests aus einer bösartigen Quelle stammen oder nicht, basierend auf Beobachtungen und automatisiertem Feedback von Angriffen und Authentisierungs-Requests aus dem Okta Kundenstamm

ThreatInsight ist ein zentrales Security-Feature, das groß angelegte Credential-basierte Angriffe (Passwort-Spraying, Credential Stuffing und ähnliche Brute-Force-Angriffe) auf Okta-Endpunkte erkennt und eindämmt. Der Kunde wählt in der Okta-Admin-Konsole einfach den Block-Modus, um als bösartig eingestufte Requests automatisch zu verweigern, bevor Angreifer versuchen, sich zu authentisieren, oder den Log-Modus, um bösartigen Traffic zu überwachen.

ThreatInsight nutzt den Netzwerkeffekt von Millionen von Authentisierungs-Requests, die täglich bei Tausenden von Okta Unternehmen eingehen, und verwendet eine Kombination aus Heuristik (statischen Regeln) und Machine Learning, um Credential-basierte Angriffe zu beobachten und daraus Erkenntnisse abzuleiten.

Für jede bekannte bösartige IP, die am Edge blockiert wird, verzeichnet Okta viele andere verdächtige Ereignisse, die von IP-Adressen stammen, die nicht mit 100-prozentiger Sicherheit als bösartig bestätigt werden können. Je nach Szenario kann es einen legitimen Use Case für mehrere fehlgeschlagene Logins geben, z. B. wenn ein Hotel eine große Konferenz ausrichtet. In solchen Szenarien ist es nicht abwegig, Dutzende, Hunderte oder sogar Tausende von fehlgeschlagenen Logins über mehrere Accounts in mehreren Okta Unternehmen zu verzeichnen – die alle aus derselben Quelle (sprich dem Hotelnetzwerk) zu stammen scheinen. Das Blockieren dieser IP-Adressen könnte in der Tat legitime Authentisierungsversuche blockieren, was letztlich genauso schlimm wäre, wie Opfer eines DDoS-Angriffs zu werden.

Um solche False Positives zu vermeiden, werden verdächtige IP-Adressen als IPs definiert, die Teil von Identity-Angriffen gegen den Okta Kundenstamm waren. In anderen Worten: Es werden nur IPs in die ThreatInsight Datenbank aufgenommen, die bekanntermaßen an Angriffen beteiligt waren – zum Vorteil aller Okta Kunden.

Wichtige Anmerkung: ThreatInsight aktualisiert sich automatisch – IP-Adressen, über die in der Vergangenheit verdächtige Aktivitäten registriert wurden, werden aus der Datenbank entfernt, wenn bis zur nächsten Auswertung keine Auffälligkeiten mehr festgestellt werden.

Adaptive MFA

Die Rolle der KI: Liefert kontextbezogene Intelligenz und ermittelt eine geeignete Authentifizierungsmethode, indem sie das Risiko im Zusammenhang mit Authentifizierungsaktionen (z. B. Logins) und dem Verhalten nach der Authentifizierung (z. B. auf welche Ressourcen zugegriffen wird) einschätzt

Adaptive Multi-Faktor-Authentifizierung reichert den Identity Flow mit dem dynamischen Kontext der Authentifizierungs-Requests an. Durch die dynamische Anpassung der Security- und Authentisierungs-Policies kann Adaptive MFA sowohl das Security-Standing als auch die User Experience nachhaltig verbessern.

Eine adaptive MFA-Policy kann u. a. Reibungspunkte für die User beseitigen, indem eine MFA nicht mehr so häufig eingefordert wird – beispielsweise, wenn User sich über SSO oder ein bereits bekanntes Gerät einloggen. Allerdings kann adaptive MFA auch einen zusätzlichen Faktor für die Authentifizierung einfordern, wenn das geschätzte Risiko bei einer Anfrage besonders hoch ausfällt. Das betrifft z. B. Login-Versuche zu unüblichen Tageszeiten, von unbekannten Geräten aus oder für den Fall, dass der User versucht, auf eine besonders kritische Ressource oder Information zuzugreifen.

Das Maß an Flexibilität und Kontrolle, das adaptive MFA bietet, hängt dabei maßgeblich von den verfügbaren MFA-Faktoren und vom Umfang der Informationen ab, die für eine Risikobewertung herangezogen werden.

Die adaptive MFA wird wie folgt durchgeführt: Ein intelligenter Agent untersucht verschiedene Risikoanzeichen, beispielsweise Benutzer-ID, Gerät, Netzwerk, Standort, Bewegungen, IP, externe Third-Party-Daten und Endpoint-Security-Integrationen. So werden nach und nach Anomalien bestimmten Kategorien zugewiesen. Aufsetzend auf die Erkenntnisse kann risikobasierte Authentifizierung angewandt werden – für jeden Schritt des Prozesses und sogar nach bereits erfolgtem Login (z. B. bei der Step-up-Authentifizierung).

Anti-Toll Fraud

Die Rolle der KI: Erkennt Anomalien und schätzt daraufhin das Risiko ein, das im Zusammenhang mit bestimmten Aktionen und Gegebenheiten besteht (z. B. IP, Telefonvorwahl, Land)

Beim sogenannten International Revenue Share Fraud (IRSF), auch bekannt als Toll-Fraud, initiieren Betrüger eine Vielzahl an fingierten Anrufen/SMS aus dem Ausland, die dementsprechend kostspielig sind. Aufgrund der hohen Kosten, die mit internationalen Ferngesprächen verbunden sind, kann Toll-Fraud schnell zur Kostenfalle für Unternehmen, die Anrufe und/oder SMS als Authentifizierungsfaktor in ihren MFA-Flow aufnehmen, werden.

Die Anti-Toll-Fraud-Funktion schützt Kunden vor diesem Angriff und gewährleistet einen einwandfreien Telefonbetrieb, indem ein mehrschichtiger Erkennungsmechanismus – bestehend aus einer heuristischen Engine und mehreren ML-Engines – zum Einsatz kommt.

Jede Transaktion erhält einen bestimmten Risikomarker – und die Transaktionen, die als besonders risikoreich eingestuft wurden, werden mit einer strengeren Kostenobergrenze versehen (weitere Informationen zum Thema Anti-Toll-Fraud-Funktion erhalten Sie in unserem Blog).

Zum Verständnis: Die Einführung der ML-Engines hat die Erkennungsrate für betrügerische Aktionen um 20 % gesteigert.

Identity Threat Protection mit Okta AI

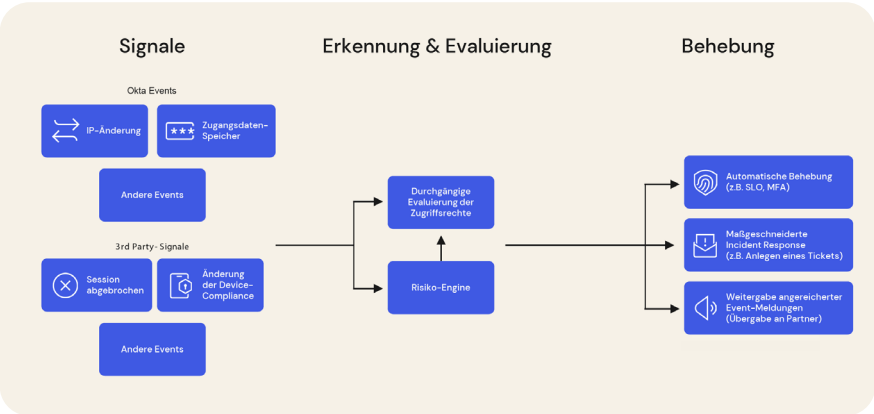
Limitierter Early Access ab Q1 2024

Die Rolle der KI: Mit dem ML-Modell erfolgt die Risikoeinschätzung automatisch auf Grundlage des individuellen Kontexts und liefert so genauere und differenzierte Bewertungen, die ideal für dynamische Umgebungen sind

Der Schutz vor Angriffen auf Identities erfordert einen mehrschichtigen Ansatz: Der Schutz muss bereits vor der Authentifizierung des Users gewährleistet sein und über die gesamte Dauer der Session hinweg aufrechterhalten werden. Die fortlaufende Authentifizierung wird in Zukunft sogar eine noch wichtigere Rolle einnehmen: Es ist absehbar, dass sich immer stärkere Authentifizierungs-Techniken durchsetzen, auf die feindliche Akteure wiederum reagieren müssen. Als Antwort darauf werden sie mehr Ressourcen aufwenden, um die MFA zu umgehen oder aktive Sitzungen zu hacken.

Identity Threat Protection mit Okta AI liefert drei wichtige Funktionen, um Identities zuverlässig vor raffinierten Bedrohungen zu schützen:

1. **Continuous Risk Evaluation** definiert KI-gestützte Security-Policies, die sowohl beim Login als auch während der gesamten aktiven Sitzung eines Users angewendet werden. So wird die Wahrscheinlichkeit eines feindlichen Übergriffs bei oder nach erfolgter Authentifizierung (Stichwort: Session Hijacking) deutlich reduziert.
2. **Shared Signals Pipeline** verbessert die Threat-Visibilität für Security-Teams über das gesamte Technologie-Ökosystem hinweg. So können sie mithilfe moderner Security-Technologien (Mobile Device Management (MDM), Cloud Access Security Broker (CASB), Netzwerk-Security oder Endpoint Detection & Response (EDR)-Lösungen) neue Bedrohungen schneller erkennen und zeitnah stoppen.
3. **Adaptive Actions** reagiert auf Bedrohungen in Echtzeit, etwa mit einem Universal Logout – vorausgesetzt, die betroffene Anwendung unterstützt dieses Feature und es wurde in den Einstellungen aktiviert. Zusätzlich werden die Anwender bei Bedarf zur MFA aufgefordert. Automatisierte Workflows bieten Schutz vor neuen Risiken.



Governance Analyzer mit Okta AI

Limitierter Early Access ab Q2 2024

Die Rolle der KI: Sie erfasst unterschiedlichste Signale – beispielsweise im Rahmen von Device Access, User Access oder auch in anderem kritischen Kontext relevante Signale – und trägt so zur besseren Identity Governance bei

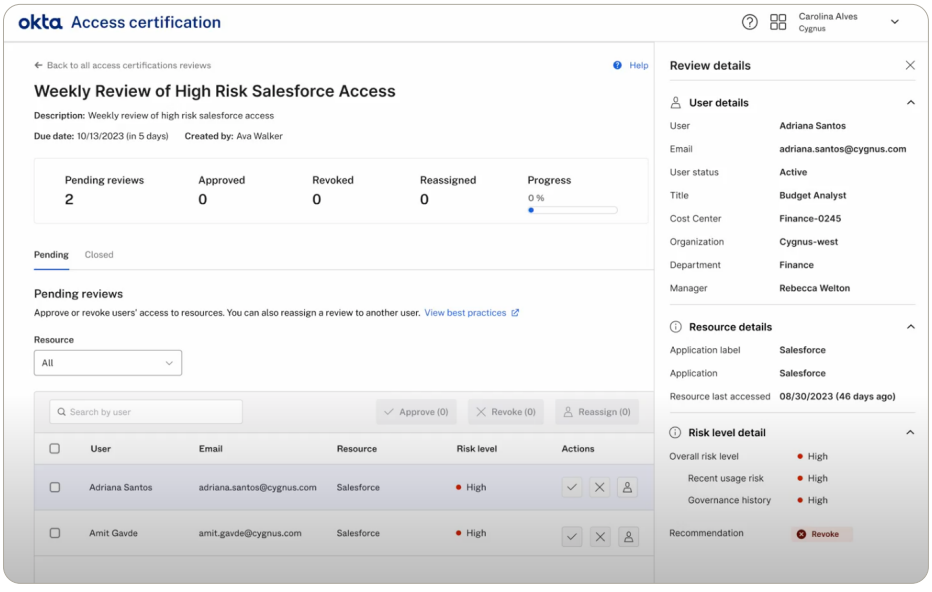
Identity Governance and Administration (IGA)-Ansatz ist richtlinienbasiert und wird im Rahmen des Identity-Managements und der Zugriffskontrolle angewandt. Die Lösung unterstützt folgende Komponenten:

- Identity Governance Abläufe und Policies, die die Trennung der Aufgabenbereiche, das Management unterschiedlicher Rollen, die Registrierung, die Access-Reviews, die Analysen und das Reporting betreffen
- Identity Administration: Verwaltung von Accounts und Login-Credentials sowie die Provisionierung und De-Provisionierung von User-Konten und Geräten und das Management von Zugriffsrechten

Okta bietet eine holistische Plattform für IAM, IGA und Privileged Access Management (PAM), die eine Vielzahl an identitätsbezogenen Daten bereitstellt. Dies hilft Unternehmen, Compliance-Anforderungen gerecht zu werden, alle nötigen Informationen für anstehende Audits zusammenzutragen, die Effizienz der betrieblichen Prozesse zu maximieren und die Produktivität der Workforce zu steigern.

Governance Analyzer mit Okta AI unterstützt diese Ziele und verwendet ML, Device-Access-Signale und User-Access-Signale, um:

- Entscheidern einen Großteil des Aufwands beim Management der Governance-Prozesse abzunehmen
- komplexe Einblicke in die Risiken der individuellen User-Ressourcen-Beziehungen zu gewähren
- Erkenntnisse auf Grundlage umfangreicher Daten bereitzustellen, die andere Anbieter nicht bereitstellen können



Der Governance Analyzer im Überblick:

- Die Lösung entscheidet, ob ein User Zugang erhält (z. B. im Rahmen einer Zugriffsanfrage) oder ob ein bestehender Zugang für den User verlängert werden soll (z. B. im Rahmen einer Zertifizierung)
- Sie legt fest, wer – unter Berücksichtigung der individuellen Risikoeinschätzung – für bestimmte Ressourcen einen Zugang anfordern kann
- Sie definiert, mit welchen Maßnahmen Anwender, die einen Zugang besitzen, überprüft werden (Beispiel: User mit einer hohen Risikoeinschätzung werden automatisch häufiger überprüft)
- Sie genehmigt oder verweigert voll automatisiert den Zugang, wenn ein User einen Zugriff anfragt oder eine Zertifizierung erhalten möchte
- Sie empfiehlt geeignete Governance-Konfigurationen, um sicherzustellen, dass sensible Ressourcen besser geschützt und der Zugriff darauf regelmäßig überprüft wird

Log Investigator mit Okta AI

Limitierter Early Access ab Q3 2024

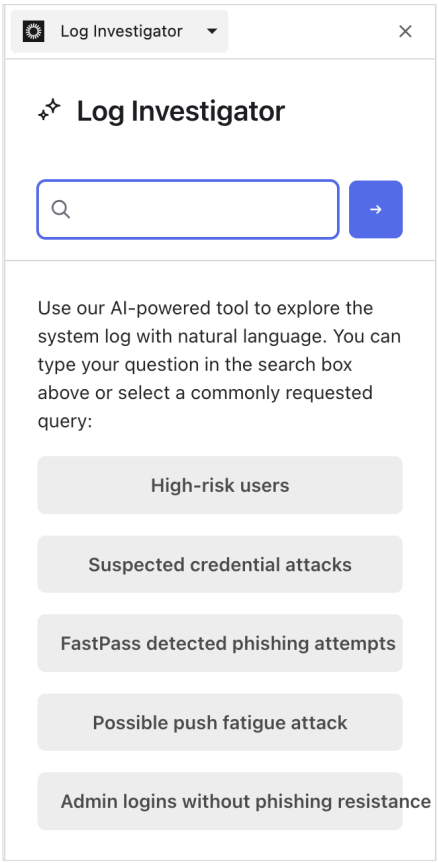
Die Rolle der KI: Sie unterstützt Log- & API-Suchen in natürlicher Sprache, die es für IT-Verantwortliche leichter machen, Informationen und Erkenntnisse im umfangreichen Datenbestand von Okta zu finden

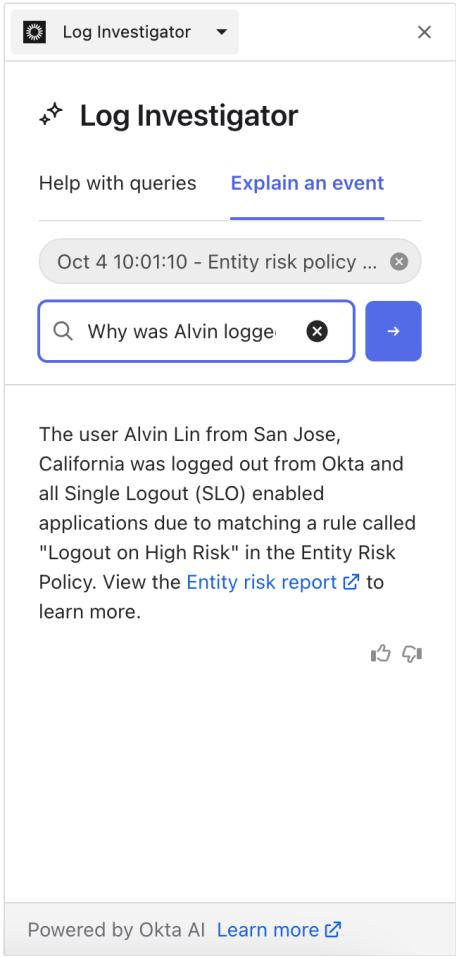
Seit es Computer gibt, sind Protokolle eine unerlässliche Informationsquelle – denn sie halten fest, was bereits passiert ist, was gerade passiert und warum etwas passiert. Mittlerweile kontrollieren digitale Technologien aber auch viele Aspekte des Geschäftsbetriebes, was eine steigende Granularität zur Folge hat. Das Resultat: Die Protokolle sind so umfangreich, dass es schwer ist einzelne Erkenntnisse gezielt herauszuziehen. Da Hunderte von Ergebnissen gesichtet werden müssen, erfordert oft auch die Suche nach Antworten auf einfache Fragen komplexe Suchanfragen und/oder manuelle Eingriffe. Das bindet Zeit und Ressourcen.

Durch die generative KI hat sich bereits viel geändert – die Art, wie Menschen mit Daten interagieren, um daraus nützliche Informationen zu ziehen, ist eine ganz andere.

Mit Log Investigator mit Okta AI lassen sich Log- und API-Suchen in natürlicher Sprache durchführen. So finden sich IT-Teams besser in den riesigen Datenbeständen von Okta zurecht und können Identity-bezogene Fragen zuverlässig und effizienter beantworten. Wie zum Beispiel:

- „Gab es in dieser Woche verdächtige Login-Versuche?“
- „Welche dieser Versuche wurden über ein unbekanntes Gerät unternommen?“
- „Wurden diese Versuche von einem ungewöhnlichen Standort aus unternommen?“





Policy Recommender mit Okta AI

Limitierter Early Access ab Q1 2024

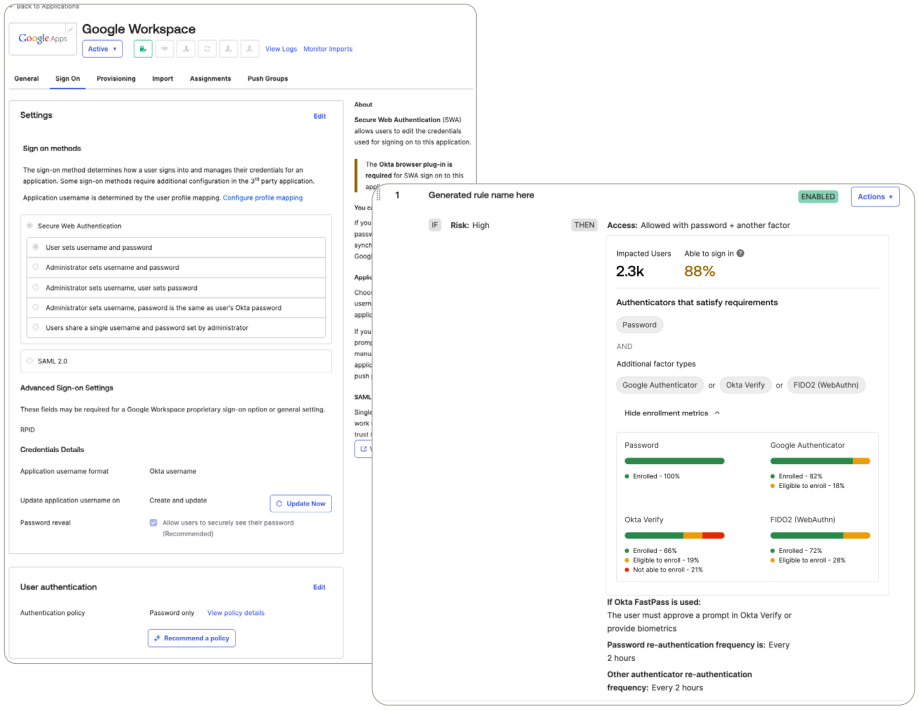
Die Rolle der KI: Die Lösung analysiert Policy-Konfigurationen von Okta-Kunden, um daraus Best Practices abzuleiten und generiert automatisch Richtlinien, die auf die komplette Okta-Umgebung angewandt werden können

Die Identity-Infrastruktur durchzieht die gesamte IT-Umgebung eines Unternehmens – und reicht mitunter sogar darüber hinaus, wenn man Anwendungen von Third-Parties mitberücksichtigt. Folglich sind die Konfiguration und das Management eines solchen Systems sehr komplex, und erfordern Zeit, Energie und Knowhow.

Allerdings ähneln sich die Management-Prozesse – besonders für gängige Anwendungen wie Slack, Salesforce und GitHub – in vielen Unternehmen. Das bedeutet, dass die Anwender ihr Wissen theoretisch bündeln könnten und so alle davon profitieren würden.

Policy Recommender mit Okta AI nutzt die gesammelten und anonymisierten Erkenntnisse aus der gesamten Okta-Kundenbasis, um Admins konkrete Empfehlungen für die Policy-Erstellung an die Hand zu geben. Admins können diese Erkenntnisse (z. B. wie User von einer Änderung der Policies betroffen wären und welche Auswirkungen das potenziell hätte) auch für das Management der Okta Integration Network (OIN)-Anwendungen nutzen. Das Resultat:

- Sie verstehen Probleme und lösen sie so leichter
- Sie managen zuverlässig Konfigurationen und Einstellungen der einzelnen Features
- Sie verbessern Sicherheit, Effizienz und Produktivität der gesamten Workforce



KI in der Customer Identity Cloud (CIC)

Während die wörtliche Definition von Customer Identity & Access Management (CIAM) gleichgeblieben ist, hat sich seine Bedeutung in der Praxis – in Bezug darauf, welche Use Cases es mit welchen funktionalen Komponenten für welche Arten von Unternehmen ermöglicht – vor allem in den letzten Jahren weiterentwickelt. Heute ist CIAM unverzichtbar für:

- Optimale Betreuung Ihrer Consumer-Kunden: In der Business-to-Consumer-Welt (B2C) ermöglicht eine effektive CIAM-Implementierung hochgradig personalisierte Angebote und Empfehlungen, die zusätzliche Umsätze generieren und Mehrwert für Kunden schaffen – während sie gleichzeitig eine komfortable User Experience über alle digitalen Kanäle hinweg gewährleistet.
- Geschäftskunden: Unzählige Unternehmen setzen heute auf B2B-SaaS-Anwendungen, um effizienter und produktiver zu arbeiten. Doch in jedem Unternehmen gibt es unterschiedliche Anwender, die auch unterschiedliche Zugriffsrechte auf unterschiedliche Ressourcen benötigen. Wenn Sie ihnen eine hochwertige und sichere User Experience bieten möchten, müssen Sie die Identities und die Zugriffsrechte sorgfältig managen. CIAM bietet die Lösung, indem es B2B-SaaS-Kunden ermöglicht, Identitäten selbst zu managen.

Okta entschied sich für den Einsatz von KI in der Customer Identity Cloud ursprünglich, um die Sicherheit für Kunden zu verbessern – denn kundenseitige Anwendungen sind immer einer Vielzahl von unterschiedlichen Bedrohungen ausgesetzt. Allerdings sind die Maßnahmen, die ergriffen werden, um Workforce-Identities zuverlässig zu schützen, nicht immer 1:1 auf den Schutz von Kunden-Identities anwendbar.
In einer Enterprise-Umgebung nimmt die Sicherheit oftmals einen höheren Stellenwert als die Benutzerfreundlichkeit ein. Daher führen Admins häufig Sicherheitsmechanismen ein, ohne dabei darauf zu schauen, ob sie die User Experience signifikant beeinträchtigen.

Beim Customer-Identity-Management hingegen wird der Fokus auf beide Seiten gelegt: Sicherheit und Datenschutz müssen gewahrt, parallel dazu aber auch Reibungspunkte minimiert werden. Dazu braucht es zuverlässige Schutzmechanismen vor raffinierten Bedrohungen, von denen die User jedoch nahezu unberührt bleiben.

Es ist längst bekannt, dass man sich auf die KI verlassen kann, wenn es darum geht, Hacker – die sich als legitime User ausgeben – von tatsächlich legitimen Usern zu unterscheiden.

Ergänzend zu den neuen KI-basierten Security-Features von Okta, fußen auch viele weitere Funktionen auf Machine Learning und generativer KI, um die Customer Experience auf einen neuen Level zu heben, die Konversionsrate zu erhöhen und Management-Prozesse zu vereinfachen.

Der Accenture Technology Vision 2023 Report stellt fest, dass **„[...] die Möglichkeit, Kunden online zu authentifizieren, für Führungskräfte höchste Priorität hat – 85 % der Befragten gaben an, dass dies ‚zunehmend zur strategischen Notwendigkeit für ein Business wird'. Drei von vier Befragten gaben zudem an, dass sich Probleme bei der Kundenauthentifizierung negativ auf das Unternehmen ausgewirkt hätten. Das äußerte sich beispielsweise durch abgebrochene Käufe und wachsende Frustration unter den Usern."**

Bot Detection

Die Rolle der KI: Die Lösung überprüft mehr als 60 Signale, um festzustellen, ob die Authentifizierungsanfrage von einem legitimen Kontoinhaber gestellt wurde – oder von einem Bot

Als wesentlicher Bestandteil des Attack Protection-Add-ons der Customer Identity Cloud, minimiert das Bot Detection Feature das Schadenspotenzial geskripteter Angriffe z. B. Credential-Stuffing- oder List-Validation-Attacken) gegen native Anwendungen, passwortlose Flows und benutzerdefinierte Login-Pages.

Durch die Analyse von mehr als 60 Datenquellen – wie frühere Ereignisse im Zusammenhang mit einer IP-Adresse, die jüngste Login-Historie, IP-Reputationsdaten und eine Reihe anderer Faktoren – prognostiziert Bot Detection, wann ein Identity Request wahrscheinlich von einem Bot stammt. Ab einem bestimmten Schwellenwert wird eine Gegenmaßnahme, z. B. ein CAPTCHA, ausgelöst.

Bot Detection ist ein gutes Beispiel dafür, wie KI ältere Techniken verbessern kann:

- Die erste Version, die im Februar 2021 gelauncht wurde, war regelbasiert und erkannte 18 % der Bots
- Die zweite Version, die im August 2021 gelauncht wurde, nutzte Machine Learning zur Verhaltensanalyse. Dieser KI-gestützte Ansatz verdoppelte die Effizienz und erkannte 45 % der Bots
- Die jüngste Version, die im Juni 2022 auf den Markt kam, erkannte 79 % der Bots — die bisher beste Performance, und das, obwohl die Bedrohungsakteure ihre eigenen Techniken ständig verfeinern

Es ist wichtig hervorzuheben, dass diese verbesserten Security-Features keine unnötigen Reibungspunkte für die User nach sich gezogen haben. Durch konstante Optimierung der KI-Technologie, die den Kern des Bot-Detection-Features darstellt, sinkt die Wahrscheinlichkeit, dass ein CAPTCHA bei einem legitimen User ausgelöst wird.

Darüber hinaus hat eine detaillierte interne Studie, in der die Vorher-Nachher-Effekte der Bot Detection untersucht wurden, einen starken Abschreckungseffekt gezeigt:

- Im Durchschnitt stellten die Kunden, die Bot Detection aktiviert hatten, einen Rückgang des bösartigen Traffics um mehr als 40 % fest
- Bei einigen größeren Kunden in der Studie ging der Bot-Traffic um fast 90 % zurück!

Aufsetzend auf die Bot Detection: Identity Threat Level (ITL)

Im April 2023 gaben wir bereits einen kleinen Ausblick auf unser Identity-Threat-Level-(ITL-)Projekt. Die Tatsache, dass unsere CIAM-Lösung als Gatekeeper monatlich Milliarden von Login-Transaktionen prüft und schützt, bietet uns einzigartige Einblicke, die uns helfen, Identity-Threats zuverlässig zu erkennen.

Diese Perspektive war der Ausgangspunkt für ITL: eine Skala von 0 bis 10, auf der der Bot-Traffic angegeben wird, gemessen anhand der Wahrscheinlichkeit, dass der Traffic den CAPTCHA nicht besteht. Ein Wert von 0 impliziert, dass kein nennenswerter Bot-Traffic festgestellt werden konnte – die 10 hingegen bedeutet, dass fast der gesamte Traffic auf Bots zurückzuführen ist.

Wir nehmen unsere (zuvor anonymisierte!) Kundenbasis genau unter die Lupe – und können so einen ITL für verschiedene Branchen und Regionen ermitteln, mit der Option den Wert noch einmal für weitere übliche Merkmale aufzusplitten. Anhand des ITL kann z. B. festgestellt werden:

- Wie sich mutmaßlicher Bot-Traffic bei CIC-Kunden in verschiedenen Branchen und Regionen im Laufe der Zeit geändert hat
- Wie sich die Level des mutmaßlichen Bot-Traffics bei den unterschiedlichen CIC-Kunden unterscheiden (je nach Branche oder Region)

Und weil wir auch vergangene Trends und tägliche Veränderungen im Auge behalten, lassen sich auch erhöhte Risiken bei den Login- und Signup-Flows im CIAM schnell erkennen. Das wiederum ermöglicht es Providern, angemessen auf das Risiko zu reagieren, beispielsweise indem sie ihr Monitoring verstärken, proaktiv Grenzwerte senken oder weitere Schutzmaßnahmen implementieren.

Für all das bildet Bot Detection die Grundlage.

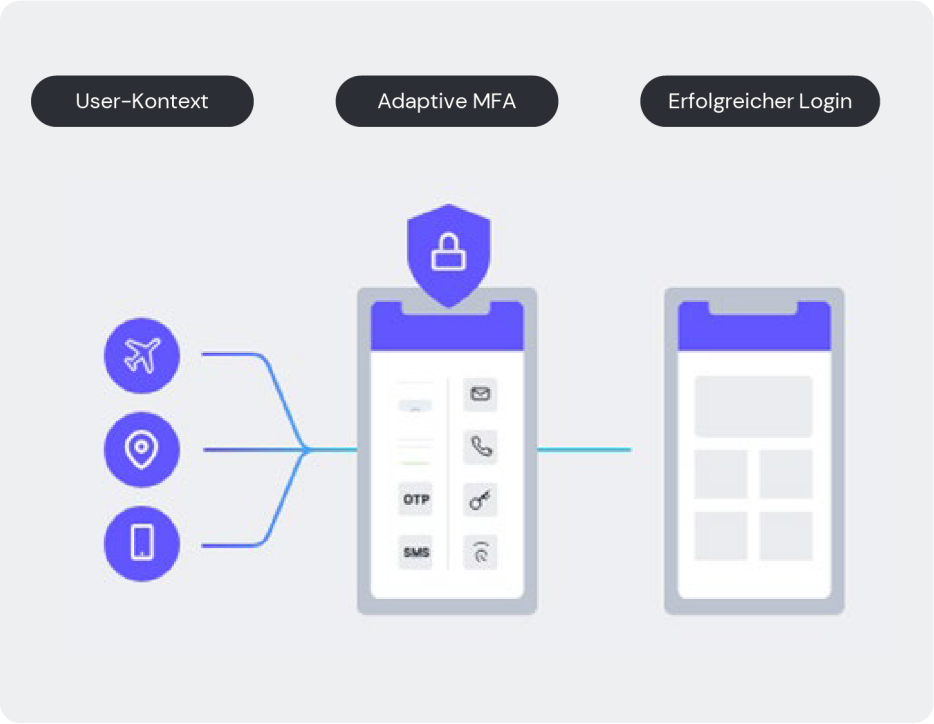
Adaptive MFA

Die Rolle der KI: Die Lösung liefert wichtigen Risiko-Kontext, indem sie eine Vielzahl identitätsbezogener Signale analysiert und eine Prognose darüber abgibt, ob ein Authentifizierungsversuch von einem legitimen User ausgeht – oder von einem Angreifer, der sich als legitimer User ausgibt.

Adaptive MFA richtet die Zugriffe der Anwender intelligent am Kontext des Logins und an den Business-Zielen aus.

Obwohl die MFA bekanntlich eine bewährte Methode ist, um Accounts vor einer feindlichen Übernahme zu schützen, scheuen viele Unternehmen – primär im B2C-Bereich – davor zurück. Sie fürchten, dass zusätzliche Reibungspunkte die User Experience zu stark beeinträchtigen.

Adaptive MFA stellt eine attraktive Alternative dar: Eine MFA ist nur dann erforderlich, wenn die Risikoeinschätzung bei einem Login besonders hoch ausfällt. Wenn das nicht der Fall ist, erhält der User eine lückenlose Experience.



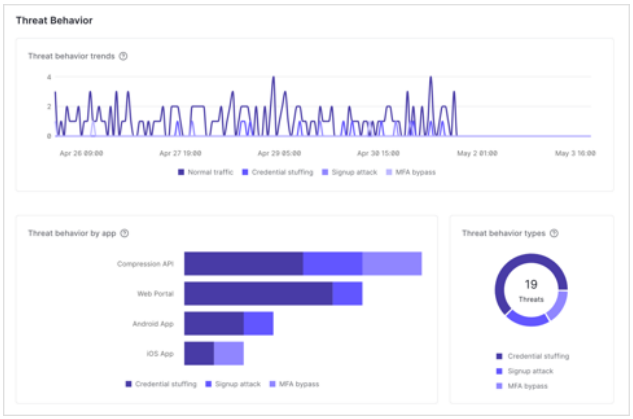
Security Recommendations

Demnächst verfügbar

Die Rolle der KI: Die Lösung liefert intelligente Handlungsempfehlungen, die es Unternehmen ermöglichen, das Security-Standing ihrer Tenants zu optimieren

Security Center unterstützen IT-Abteilungen und Security-Verantwortliche dabei, potenzielle Angriffs-Trends im Auge zu behalten und im Ernstfall in Echtzeit zu reagieren. Das Center bietet:

- einen einheitlichen Blick auf alle Authentifizierungsvorgänge, potenzielle Vorfälle und die Wirksamkeit der aktuellen Threat Response
- Echtzeit-Benachrichtigungen über anomale Muster
- Darstellungen von potenziellen Angriffs-Trends (z. B. Credential Stuffing, Signup-Angriffe und versuchte MFA-Umschiffung)
- Einblicke in die Auswirkungen von Schutz-Features (z. B. Rate-Limits und CAPTCHA) auf die User Experience



Diese Funktionen werden aktuell um intelligente und ML-basierte Security Recommendations erweitert, welche mithilfe von Security-Snapshot-Alerts und Dashboard-Benachrichtigungen übermittelt werden.

Identity Threat Protection mit Okta AI

Limitierter Early Access ab Q4 2024

Die Rolle der KI: Die Lösung wertet Authentifizierungsdaten aus, um Vorschläge abzugeben, wie die Customer Experience verbessert und die Konversionsrate gesteigert werden kann

In klassischen Consumer-Szenarien dient CIAM vor allem zur Reduzierung des Aufwands bei der Interaktion mit Ihrem Unternehmen: Diese Interaktionen umfassen beispielsweise (aber nicht ausschließlich)

- Anwender, die sich für Ihre Services anmelden
- Anwender, die sich an bestehenden Accounts einloggen
- Anwender, die Daten und Einstellungen aktualisieren
- Anwender, die Daten aus verlorenen Accounts wiederherstellen
- Anwender, die auschecken (also einen Kauf abschließen)

Je höher der Aufwand für die Kunden ist, desto niedriger ist die Konversionsrate, und desto weniger Umsatz macht das Unternehmen kurz- und langfristig. Customer-Flows zu optimieren, kann jedoch mitunter eine große Herausforderung darstellen, da oftmals große Datenmengen vorliegen und verschiedene User sehr persönliche Präferenzen haben.

Darüber hinaus muss auch die Sicherheit der Identity-Flows priorisiert werden, was selbst für Identity-Experten schwierig ist – ganz zu schweigen von Entwicklern, die mit der Materie „Identität“ keine nennenswerten Berührungspunkte haben.

Um diesen Herausforderungen zu begegnen, gibt der Identity Flow Optimizer den Entwicklern konkrete Handlungsempfehlungen an die Hand, wie sie mit der richtigen Konfiguration der Identities und neuen Actions die Konversionsrate erhöhen, die Sicherheit verbessern und ihre Anwendungen schneller entwickeln können.

Brand Customizer mit Okta AI

Limitierter Early Access ab Q4 2024

Die Rolle der KI: Die Lösung erstellt automatisch Design-Templates mit dem Branding des jeweiligen Unternehmens

Unternehmen haben nicht umsonst strenge CI-Guides: Sie sollen eine einheitliche User Experience gewährleisten, die die sorgsam konzipierte Identity einer Marke unterstreichen soll.

Der Brand Customizer entwirft One-Pager-Templates, deren Design nach Belieben auf andere Templates übertragen werden kann. Entwickler können z. B. auch einen Screenshot oder ein Logo bereitstellen, auf deren Grundlage die KI ein Template erstellt. Das kann daraufhin von Entwicklern individuell angepasst werden.

Das Tool trägt jedoch nicht nur dazu bei, ein einheitliches Erscheinungsbild für den End-User zu schaffen. Es verkürzt auch die Time-to-Value, indem es Entwicklern wertvolle Arbeit abnimmt und so hilft, schnellstmöglich eine erstklassige Customer Experience zu schaffen, Innovationen umzusetzen und das Unternehmen zu skalieren.

Guide mit Okta AI

Limitierter Early Access ab Q4 2024

Die Rolle der KI: Die Lösung interpretiert Abfragen in natürlicher Sprache und bietet kontextbezogene Unterstützung an, damit User effektiv und effizient mit der Customer Identity Cloud arbeiten können

Die Customer Identity Cloud ist leistungsfähig, bietet ein breites Feature-Set und ist hochgradig skalierbar. Allerdings kann der breite Leistungsumfang auch einschüchternd wirken. Sogar Experten haben mitunter Schwierigkeiten, über die neuesten Funktionen auf dem Laufenden zu bleiben und über jedes Detail informiert zu sein.

Um neuen Usern das Onboarding zu erleichtern und allen Usern die optimale Nutzung der CIC zu ermöglichen:

- bietet der neue Guide umfassende Onboarding-Unterstützung, die jedem Benutzer intuitiv die besten nächsten Schritte aufzeigt, um mit einfachen Prompts in natürlicher englischer Sprache die besten Ergebnisse zu erzielen
- erklärt er jede Einstellung oder jeden Fachbegriff auf der Plattform in natürlicher Sprache und verbessert die Experience, indem er kontextbezogene Unterstützung und ausgewählte Links zu relevanten Aufzeichnungen bereitstellt

Actions Navigator mit Okta AI

Limitierter Early Access ab Q2 2024

Die Rolle der KI: Ermöglicht die Suche in natürlicher Sprache, um schneller geeignete Integrationen zu finden oder bei Bedarf ganz neue Integrationen zu entwickeln

Eine der größten Stärken der Customer Identity Cloud ist ihre Erweiterbarkeit. Der Auth0 Marketplace vereinfacht Ihre Entwicklungsprozesse nachhaltig, indem er eine unkomplizierte Möglichkeit bietet, Identity-Anwendungen um weitere Integrationen zu erweitern.

Allerdings kann es bei der Vielzahl an Integrationen, die zur Verfügung stehen, mitunter schwierig sein, auf Anhieb das zu finden, was man braucht.

Mithilfe des Action Navigators können Entwickler Integrationen im Marketplace finden und implementieren, oder eine Action schreiben (eine Funktion, die die CIC-Features erweitert und je nach Bedürfnis anpasst) – und das nur über eine simple Suchabfrage. Die Möglichkeit, Code zu schreiben, ist vermutlich die revolutionärste Fähigkeit generativer KI – und diese Funktion eröffnet Entwicklern und Laien, die selbst noch keine Erfahrung im Schreiben von Codes haben, ganz neue Optionen.

Tenant Security Manager mit Okta AI

Limitierter Early Access ab Q2 2024

Die Rolle der KI: Die Lösung erstellt Zusammenfassungen komplexer Identity-Konfigurationen in natürlicher Sprache

In vielen Unternehmen gibt es versierte Fachleute, die über wertvolles Knowhow verfügen – auch im Bereich Identity.

Sollte sich jedoch die personellen Situation ändern und diese Fachleute nicht mehr zur Verfügung stehen, kann es für andere mitunter zur Herausforderung werden, den Systemstatus und die Details der Konfiguration nachzuvollziehen.

Der Tenant Security Manager erweitert die Okta Attack Protection um intelligente Security-Empfehlungen in Form von Sicherheitswarnungen und Dashboard-Nachrichten, um das Security-Standing der Kunden-Tenants zu verbessern.

Fazit

Der Siegeszug von Chat GPT – und die lange Liste ähnlich beeindruckender Tools, die als Antwort auf die Innovation auf der Bildfläche aufgetaucht sind – haben gezeigt, dass sich der Stand der Technik von heute auf morgen schlagartig ändern kann. Über die Zukunft und die Tragweite der KI lässt sich also allenfalls vage spekulieren.

Einige Sachen sind jedoch klar. Die Überschrift einer aktuellen Forrester-Pressemitteilung über KI (speziell generative KI) und ihre Folgen bringt es auf den Punkt: Generative KI zu ignorieren, kann für Unternehmen zum kostspieligen Fehler werden.

Man kann es auch aus einem anderen Blickwinkel betrachten: Es kann gut sein, dass Unternehmen den Wert der Investitionen in KI jetzt noch nicht begreifen – aber nicht zu investieren, führt über kurz oder lang zu einem Wettbewerbsnachteil, der Unternehmen möglicherweise ins Aus befördert. Ja, der Paradigmenwechsel ist wirklich so signifikant.

Schon heute fließt ein Großteil unserer Forschungs- und Entwicklungsetats bereits in KI-Technologien – wir können also mit Gewissheit sagen, dass Okta auch in Zukunft innovative KI-gestützte Features auf den Weg bringen wird. Diese Features werden Ihnen helfen, die Sicherheit zu verbessern, die Produktivität zu steigern und die User Experience zu optimieren – sowohl in der Workforce Identity Cloud als auch in der Customer Identity Cloud.

Auch wenn wir noch nicht wissen, wie diese Innovationen aussehen werden, sind wir zuversichtlich, dass die Funktionen, die wir aktuell auf den Weg bringen, und die, die wir bereits jetzt in der Pipeline haben, nur die ersten Schritte auf einer transformativen Reise sind.

Disclaimer:

Diese Informationen und die darin enthaltenen Empfehlungen stellen keine Rechts-, Datenschutz-, Sicherheits-, Compliance- oder Geschäftsberatung dar. Dieses Dokument dient nur zu allgemeinen Informationszwecken und gibt womöglich nicht den aktuellen Stand aller relevanten Fragen wieder. Es liegt in Ihrer Verantwortung sich mit Blick auf die Rechtslage, den Datenschutz, die Security, die Compliance und das Business beraten zu lassen. Stützen Sie sich nicht allein auf die enthaltenen Empfehlungen. Okta übernimmt keine Haftung für Verluste oder Schäden, die sich potenziell aus der Umsetzung der Empfehlungen in diesem Report ergeben haben. Okta gibt keine Zusicherungen, Garantien oder sonstige Zusicherungen in Bezug auf den Inhalt dieser Materialien. Informationen zu den vertraglichen Zusicherungen von Okta an seine Kunden finden Sie unter okta.com/agreements.

Alle Produkte, Merkmale oder Funktionen, auf die hier verwiesen wird und die derzeit noch nicht in der Breite verfügbar sind, werden möglicherweise nicht zum angekündigten Zeitpunkt oder überhaupt nicht bereitgestellt. Produkt-Roadmaps stellen keine Zusage, keine Verpflichtung und kein Versprechen dar, ein Produkt, ein Feature oder eine Funktionalität bereitzustellen. Sie sollten sich bei Ihren Kaufentscheidungen nicht auf sie verlassen.