Whitepaper

Okta & AI

How artificial intelligence is reshaping Identity and Access Management (IAM)

Contents

Summary

Artificial intelligence (AI) in general is reshaping how organizations operate and is powering innovative products and services by commoditizing optimization, data analysis, anomaly detection, and other prediction-based applications. For the most part, such functionality isn't new; rather, what's new is that cost reductions and performance improvements have made it practical to integrate such capabilities into — well, almost anything.

What is new is the seemingly overnight arrival of generative AI, due to rapid advances in the Large Language Models (LLMs) at the core of applications such as OpenAI's ChatGPT and DALL-E, Google's Bard, and Meta's Code Llama.

In fact, we believe that generative AI represents a true, once-in-a-generation paradigm shift, the impacts of which are only just beginning to be felt, let alone understood.

And few domains are as well-suited to the application of AI as Identity. Not only is Identity complex — so there's lots of opportunity for AI to improve things — but Identity flows and transactions produce vast quantities of data, which is essentially the fuel of AI engines. While we aspire to leverage data network effects across the entire Identity domain, in the short term we're focusing our research and development investments on:

- Strengthening security
- Enhancing productivity
- Improving user experiences

Crucially, AI is not new to the Okta team, and we are proud to have already embraced the power of AI in several key areas. For example:

- The Okta Workforce Identity Cloud (WIC) incorporates AI into ThreatInsight, Adaptive Multi-factor Authentication (Adaptive MFA), and our Anti-Toll Fraud safeguards
- The Okta Customer Identity Cloud (CIC) relies upon AI within the Bot Detection feature (and the related Identity Threat Level, or ITL), and Adaptive MFA

And at Oktane 2023, we announced a number of new AI-driven features. Okta AI debuted four new WIC capabilities to:

- Strengthen security: Identity Threat Protection
- Assist with governance: Governance Analyzer
- Simplify administration: Log Investigator, Policy Recommender

The CIC received six new features to:

- Strengthen tenant security: Security Recommendations
- Improve the customer experience and grow revenue: Funnel Conversion Recommendations, Brand Customization
- Simplify administration: Co-Pilot, Action Selection and Development, Personalized Tenant Configuration Summary

Additionally, we foster an innovation-centric culture which is on display during two company-wide hackathons a year. Many of the ideas explored in these hackathons evolve into patents and product proof of concepts and, ultimately, make it to market in one form or another. Notably, during a recent hack, 25% of the projects focused on AI experimentation — and we're excited by their potential.

In recognition both of the importance of AI and of the excitement it's generating within the wider developer ranks, we also scheduled our first-ever dedicated AI hackathon.

We have also helped our customers produce inspiring and elegant experiences with LLMs, and the wider Okta ecosystem — Okta Ventures, the Okta Integration Network, Auth0 for Startups, and the Auth0 Marketplace — offers a broad network of AI solutions that integrate with our Okta offerings.

The future will not be without challenges — cybercriminals are already leveraging AI in general, and LLMs in particular to explore new attack vectors and to make existing attacks more dangerous. Nevertheless, we remain optimistic that AI can and will be a force for good.

Today, digital identities control access to an ever-growing number of applications and services, impacting — and to some degree governing — many aspects of modern living. Tomorrow, their impacts will be even larger, making authentication, authorization, and Identity in general vital to preserving trust and security, as well as providing the foundation of delightful user experiences.

And we're committed to harnessing the power of AI to strengthen the connections between people, technology, and community.

Introduction

In recent months, technology and mainstream news alike have published countless articles on breakthroughs in artificial intelligence (AI) and the applications — some expected, others unforeseen — that these breakthroughs enable.

As Andy Grove famously stated, "Only the paranoid survive," so it should come as no surprise that businesses large and small, in a wide range of industries, are racing to harness AI to improve existing solutions, power new ones, and deepen the metaphorical moats that provide advantage over the competition.

To a large extent, our investment in emerging AI represents business as usual for us. AI already powers a number of important products and features within our portfolio. In particular, machine learning (ML) is at the heart of much of our dynamic risk assessment and risk-based authentication intelligence.

Having learned from years of hands-on experience, we don't regard AI as a single module or capability — something that can simply be bolted on or added to our platform. Rather, we recognize that AI is a general purpose technology (or, more accurately, a collection of general purpose technologies) best applied when embedded within and integrated with Identity infrastructure.

In this whitepaper, we aim to pull back the curtain on Okta's relationship with AI, by exploring:

- Why AI offers such promise to disrupt and reshape practically any digital domain
- Why Identity is especially well-positioned to benefit from AI
- The leading value propositions we see for AI in the immediate future
- How we have already employed AI within the Okta Workforce Identity Cloud (WIC) and Okta Customer Identity Cloud (CIC)
- How we're leveraging Okta AI in new WIC and CIC capabilities

Why AI?

On a basic level, artificial intelligence can be understood as a decision made by a computer where its "smartness" is indistinguishable from a human-made decision — no matter how the decision is made.

While the concept of AI was formally introduced at the Dartmouth Workshop, the original premise traces to 1943, when logician Walter Pitts and neuroscientist Warren McCulloch tried to create a mathematical representation of the neurons in a human brain. These contemporary advances built on a long history of progress in the Theory of Computation, from Ada Lovelace in the nineteenth century to Alan Turing.

Since the 1960s, AI has evolved into a very large collection of algorithms, including the detection and recognition of patterns — which is usually performed by machine learning (ML). The ML field has advanced dramatically in the last 15 years, leading to the emergence of practical and economic deep learning.

Generative AI is a once-in-a-generation paradigm shift

The AI development that has taken the wider world by storm is the incredible — and many would say shocking — arrival and rapid evolution of generative AI, driven mainly by remarkable advances in Large Language Models (LLMs).

Powered by LLMs, applications like OpenAI's ChatGPT and DALL-E brought AI into the mainstream, partly due to their human-mimicking capabilities and partly due to the absence of transparency regarding the data ingested by the model (and shaping its behavior).

Suddenly, writing prose and creating complex (and lifelike, if that's the intention) images are no longer the sole domain of humans. And what's more, because LLMs are so adept at writing, programming is a form of writing, and so many things are now controlled by software, LLMs are behind unexpected breakthroughs and advances in a wide range of domains.

Clearly, we have entered a more modern era of AI. As such, it's only natural to wonder how to put its capabilities — old, new, and still emerging — to use.

What can AI do?

In their book Prediction Machines, economists Ajay Agrawal, Joshua Gans, and Avi Goldfarb recast the rise of AI as a drop in the cost of prediction, which they define as taking information that's available and using it to generate new information.

Because prediction "is at the heart of making decisions under uncertainty" and "our business and personal lives are riddled with such decisions," lowering the cost of prediction brings with it extraordinary potential. To offer just a few examples, prediction is an essential component of:

- Optimization: Using context and past observations to predict an optimal path, response, configuration, user interface design, etc.
- Behavioral analysis: Observing real-time behavior in the context of historical actions to predict a user's intentions
- Data mining: Predicting what data and insights best satisfy a user's query or prompt (and it's worth noting that prediction is also at the heart of LLMs and generative AI.)

Like classical computing, AI (in all its forms) is a general-purpose technology that promises to disrupt and reshape existing industries — and we are particularly bullish about its potential to power the evolution of Identity.

AI and Identity

A digital Identity is the set of attributes that define a particular user in the context of a function that is delivered by a particular application. Today, digital identities control access to an ever-growing number of applications and services, impacting — and to some degree governing — many aspects of modern living. Tomorrow, their impacts will be even larger, making authentication, authorization, and Identity in general vital to preserving trust and security, as well as providing the foundation of delightful user experiences.

As a result, IAM services are cornerstones of our connected world, ensuring that only authorized users — employees, contractors, partners, customers — can access particular resources. Conceptually, IAM is very simple: a user proves their Identity and is permitted access to a resource to which they are entitled. In practice, however, several factors introduce complexity:

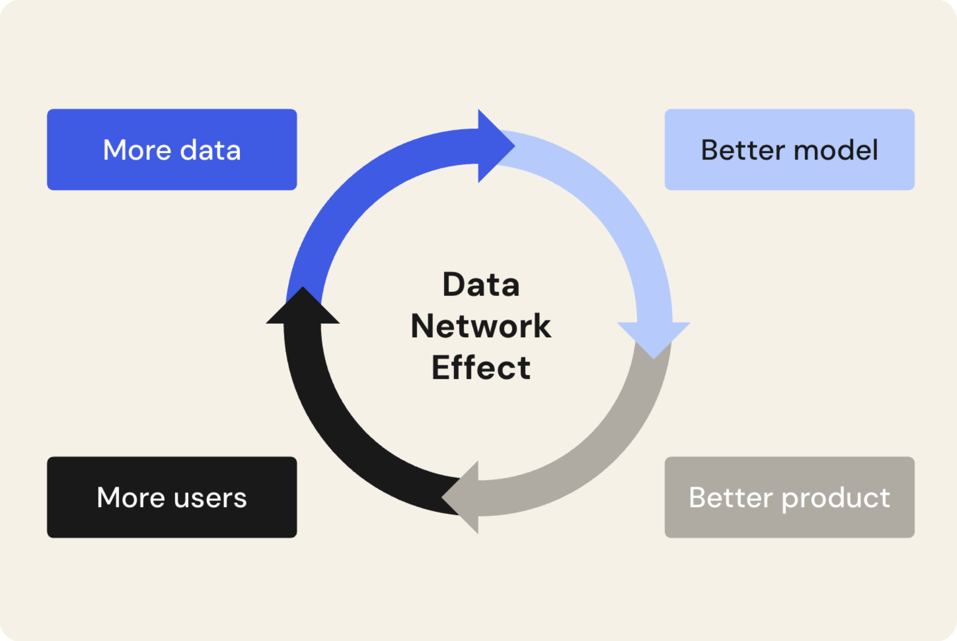
- Today's digital world includes many users, an individual user may have many digital identities, and there are countless ways to express a digital Identity
- Different digital identities have different rights and authorizations with respect to resources — and these rights and authorizations are increasingly dynamic
- As security perimeters dissolve, attackers are focusing efforts on Identity

As we've seen, AI is eminently capable of dealing with complexity and uncertainty — provided there's enough data available.

Fortunately, the Identity domain has plenty of data to offer, because Identity itself has evolved from a static, one-dimensional attribute to a dynamic, ongoing interaction, reshaping itself with every new data point. This evolution would not have been possible without the cloud transformation in the past, and will continue thanks to the AI transformation happening currently.

Leveraging data network effects

One important consequence of this evolution is that it enables a virtuous cycle of data network effects: the higher the volume and quality of data to which an AI model has access, the faster it can learn and the more accurate its predictions or decisions become; this, in turn, makes the product or service more valuable to its users, which attracts more users, who then generate more data, which can be fed back into the model in a virtuous cycle:



1. **More Data:** The more a product or service is used, the more data is generated through user interactions, transactions, feedback, etc.
2. **Better Model:** This data is used to refine the underlying AI model. The higher the volume and quality of data, the more accurate the model's predictions or decisions become.
3. **Better Product:** As the AI model improves, so too does the product or service.
4. **Attract More Users or Usage:** The improved product or service attracts more users, who generate even more data, continuing the cycle.

This self-reinforcing loop can be a powerful driver of innovation and competitive differentiation.

Strengthening security

By now, it's well understood that AI can:

- Make existing Identity attacks like credential stuffing and phishing more dangerous (e.g., harder to detect, more effective/destructive)
- Enable entirely new types of Identity attack, many of which will only become apparent once they're spotted in the wild
- Overcome some existing security measures (e.g., solving CAPTCHAs, tricking voice biometric systems)

Plus, the coding and scripting abilities of generative AI makes it easier for threat actors of any skill level (i.e., with or without coding abilities) to launch attacks, in general, potentially drawing more participants into the cybercrime ecosystem and improving operational efficiencies.

This changing threat landscape prompted Gartner to warn that **"Through 2025, attacks leveraging generative AI will force security-conscious organizations to lower thresholds for detecting suspicious activity, generating more false alerts, and thus requiring more — not less — human response."**

But while AI will undoubtedly aid attackers, it also serves as a 'power-up' for defenders.

Okta already leads the industry with FastPass' phishing-resistant authentication — on any platform for both managed and unmanaged devices — and making it easier for developers to adopt user-friendly and phishing-resistant FIDO2 authentication. However, we also recognize the need to use AI to:

- **Further secure Okta by design**: Just as threat actors can use AI to probe for vulnerabilities and security gaps, so too can organizations like Okta. Our advantage is that we can employ AI to harden software and systems before they're released.
- **Automate threat detection:** Contextual and behavioral analysis is already capable of informing intelligent risk assessments and detecting advanced Identity threats, and advances in AI will only improve our ability to perform these functions and introduce new ones.
- **Mitigate risk on behalf of our customers:** Whether automating defensive measures (e.g., containment actions, blocking malicious activities), combining an alert with a recommended playbook, or supporting governance, risk management, and compliance (GRC) initiatives, AI will be invaluable in proactively mitigating risk and responding to attacks.

Fortunately, we already have a wealth of experience integrating AI-driven security features into both our Workforce Identity Cloud and Customer Identity Cloud.

[1] Gartner, 4 Ways Generative AI Will Impact CISOs and Their Teams, Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook, 29 June 2023) GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S and internationally and is used herein with permission. All rights reserved.

Enhancing productivity

One of the main findings of Okta's How Development Teams Purchase SaaS — 2023 Report is that there are basically two types of development organizations: those that already use AI in product engineering (52% of survey respondents), and those that will within the next 12 months (45%).

In pursuit of a range of benefits — particularly agility, new capabilities, cost reduction, time savings — organizations are integrating AI tools for data analytics, quality assurance, machine learning, automation, and much more.

We share this optimistic outlook of the potential of AI to enhance productivity within our own engineering organization.

At the same time, we recognize that AI's impact should extend much farther: to every member of the workforce in practically every customer organization regardless of size or industry.

A modern and mature workforce Identity infrastructure:

- Enables employees, contractors, and business partners to work from anywhere, with seamless and secure access to critical tools and resources
- Provides a convenient user experience, increases operational efficiencies, and decreases administrative burdens — freeing up time and energy to focus on growth, innovation, and other priorities
- Enables the organization to scale and improves its agility at every size
- Helps to safeguard against disruptions caused by malicious actors

Embedded throughout an Identity infrastructure, AI can boost all of these benefits — and no doubt introduce new ones.

Improving user experiences

Let's focus, for a moment, on friction.

For consumer businesses, friction — i.e., anything that slows down a person's interactions with your service — is a major obstacle to conversions and, by extension, to revenue. Okta's Customer Identity Trends Report revealed that nearly 60% of survey respondents indicated that they would be more likely to spend money when services offered a simple, secure, and frictionless login process. This finding is consistent across all sectors/industries, suggesting that users crave convenience in every interaction.

Of course, some amount of friction is necessary to establish trust and provide security controls, but lowering friction wherever practical — in any and every consumer interaction — can increase conversion rates and, accordingly, grow revenue in both the short and long term.

Where does AI fit in? Three obvious places are:

- Providing continuous risk assessment to enable passwordless and loginless experiences
- Optimizing Identity flows for user convenience
- Improving user interface design (i.e., during Identity transactions) for user convenience

Within the workplace, friction can be thought of as anything that prevents or slows down getting things done. While Identity can't (by itself) start a meeting on time or encourage a colleague to respond sooner to an inquiry, a mature Identity infrastructure contributes in other ways, including:

- Ensuring users can access the right resources (e.g., data, systems, applications), with the right privileges, at the right time
- Powering self-service capabilities (e.g., requesting access to resources, altering profiles, enrolling security factors, etc.)
- Automating existing processes (e.g., access reviews and certifications, secure offboarding, etc.)

Again, AI can supercharge these existing capabilities while also unlocking new ones. For example, AI can analyze reams of Identity deployments and performance metrics to determine the most efficient and effective configurations, and use this intelligence to provide recommendations that are personalized to each organization or department. And AI can help administrators quickly locate needed information within an otherwise overwhelming volume of operational and logging data.

Plus, the natural language capabilities of LLMs means that even more Identity-related functions can become accessible to non-coders. Okta Workflows already enables no-code Identity automation and orchestration through a drag-and-drop interface; it's not a stretch to imagine a solution that takes natural language instructions.

AI in the Workforce Identity Cloud (WIC)

While previously regarded as only a utility service managing usernames and passwords, Identity has become both a necessity for, and an enabler of, any modern business. As a result, Identity infrastructure is an interconnected and foundational layer within the broader IT environment, connecting users and other entities with systems, data, and resources both on-premises and in the cloud.

Consequently, securing Identity is a foundational element of a strong security posture — one that can help combat abuse from insider threats and from intruders abusing stolen credentials

In addition to helping to safeguard workforce Identity infrastructure from threats, AI is also highly capable of supporting governance activities, in particular by examining huge volumes of configuration data to identify risks, recommend corrective actions, and even automate many common and important tasks.

Similarly, AI's ability to analyze information and surface insights makes it well-suited to interpret vast quantities of logs.

Coupling these capabilities with natural language processing and generative AI is already transforming how administrators manage their ever-growing Identity infrastructure.

In their 2022 Trends in Securing Digital Identities report, based on a survey of more than 500 IAM or security professionals, the Identity Defined Security Alliance (of which Okta is a member) revealed that:

- **84%** of respondents said their company experienced an Identity-related breach in the previous year
- **78%** cited direct business impacts resulting from a breach
- **64%** indicated that effectively managing and security digital identities is either the top security priority (16%) or a top-3 priority (48%)

ThreatInsight

AI's role: Predicts whether or not requests are originating from a malicious source, based upon observations and automated feedback from attacks and authentication requests across the broad Okta customer base

ThreatInsight is a baseline security capability that detects and mitigates high-volume credential-based attacks (password spraying, credential stuffing, and similar brute-force attacks) directed at Okta endpoints. A customer simply selects block mode in the Okta Admin Console to automatically deny requests predicted as malicious before attackers attempt to authenticate, or log mode to audit malicious traffic.

Harnessing the network effect of the many millions of authentication requests made to thousands of Okta organizations on any given day, ThreatInsight employs a combination of heuristics (static rules) and machine learning to observe and derive intelligence from credential-based attacks.

For every known malicious IP blocked at the edge layer, Okta sees many more suspicious events coming from IP addresses that cannot be confirmed malicious with 100% certainty. There could be a legitimate use case for multiple failed logins depending on the scenario, such as when a hotel hosts a large conference. In these scenarios, it isn't unreasonable to have dozens, hundreds, or even thousands of login failures across multiple accounts in multiple Okta organizations — all of which appear to come from the same source (i.e., the hotel's network). Blocking those IP addresses could actually block legitimate authentication attempts, which would ultimately be just as bad as falling victim to a DDoS attack.

To avoid such false positives, suspicious IP addresses are defined as IPs involved in Identity attacks across Okta's full customer base — in other words, only IPs that are known to be participants in attacks are added to the ThreatInsight database, to the benefit of all Okta customers.

Importantly, ThreatInsight uses a rolling window, and suspicious IP addresses which stop exhibiting suspicious activity by the next evaluation are removed from the database.

Adaptive MFA

AI's role: Provides contextual intelligence to pair with an appropriate authentication method by predicting risk associated with authentication events (e.g., logging in) and post-authentication actions (e.g., accessing a particular resource)

Adaptive Multi-factor Authentication (AMFA) introduces additional intelligence into Identity flows by taking into account the ever-changing context in which an authentication request is made. By dynamically adapting security and authentication policies, adaptive MFA can simultaneously improve an organization's security posture and the user experience.

For example, an adaptive MFA policy can reduce friction for users by prompting for MFA less frequently when users sign in through SSO or through a managed or known device. However, the same adaptive MFA solution can prompt for an additional or more secure authentication factor when the risk associated with a request is assessed to be higher — such as a login attempt made at an unusual time of day or from a new device, or if a logged-in user is attempting to access particularly sensitive resources or information.

The degree of flexibility and control provided by an adaptive MFA solution largely depends upon the MFA factors available and the richness of the contextual intelligence incorporated into the risk assessment.

Within Adaptive MFA, an intelligent agent examines a range of risk signals — including user ID, device, network, location, travel, IP, and external data from third parties and endpoint security integrations — to categorize anomalies and apply risk-based authentication at each step of the authentication process, and even after the user has logged in (e.g., for step-up authentication).

Anti-Toll Fraud

AI's role: Detects anomalies and categorizes risk associated with attempted telephony transactions based upon a range of inputs (e.g., IP, phone prefix, country)

International revenue share fraud (IRSF), also known as toll fraud, is a type of fraud where fraudsters artificially generate a high volume of international calls/SMS on expensive routes. Due to the high costs associated with long-range international telephony transactions, toll fraud can bear a significant financial impact on the businesses that use phone calls and/or texts as part of the MFA flow.

The Anti-Toll Fraud capability protects customers while still providing reliable telephony service, and does so by leveraging complementary detection mechanisms: a heuristic engine and multiple ML engines.

Broadly speaking, each transaction is assigned a risk marker, and transactions deemed higher risk are subject to stricter rate limits (for details on how these components operate, and how the Anti-Toll Fraud capability incorporates them, please see this blog)

Notably, the introduction of the machine learning components resulted in a 20% improvement in effectively detecting fraudulent transactions.

Identity Threat Protection with Okta AI

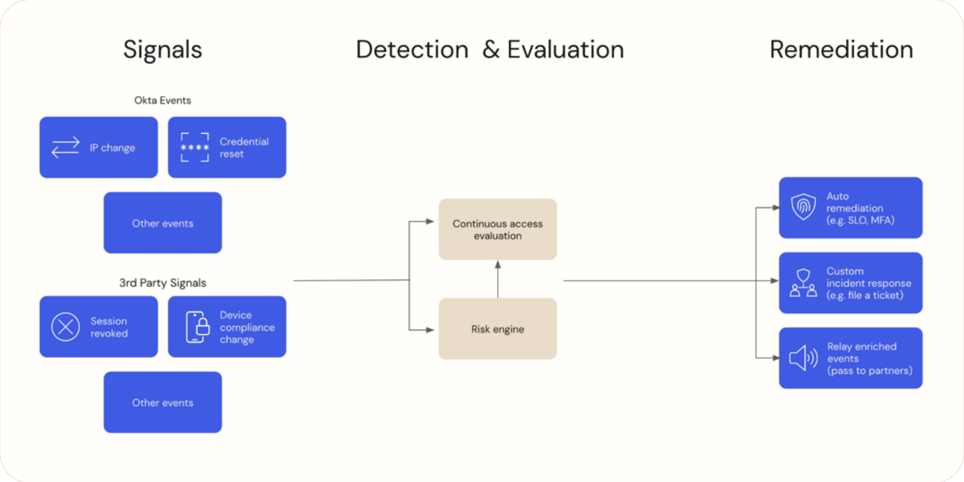
Limited Early Access Q1 2024

AI's role: ML model automatically adapts risk scoring to different contexts, providing more accurate and nuanced assessments suitable for dynamic environments

Defending against today's Identity threats requires a layered approach that begins before a user authenticates and that continues throughout the life of the session. In particular, continuous authentication is expected to grow in importance as stronger authentication techniques gain wider adoption, and threat actors respond by directing more resources at bypassing MFA and hijacking active sessions.

Identity Threat Protection with Okta AI helps to safeguard against advanced Identity threats with three critical capabilities:

1. **Continuous Risk Evaluation** leverages AI to enforce security policies both at login and during an active user session, reducing the potential for unauthorized access and post authentication threats like session hijacking.
2. **Shared Signals Pipeline** amplifies threat visibility across the tech ecosystem, enabling security teams to detect and respond to emerging threats between various security technologies, including Mobile Device Management (MDM), Cloud Access Security Broker (CASB), network security, Endpoint Detection & Response (EDR) solutions, and more
3. **Adaptive Actions** responds to real-time threats by enabling targeted actions such as Universal Logout from supported applications with the feature enabled, prompting users for on-demand multi-factor authentication, and executing automated workflows to address emerging risks.



Governance Analyzer with Okta AI

Limited Early Access Q2 2024

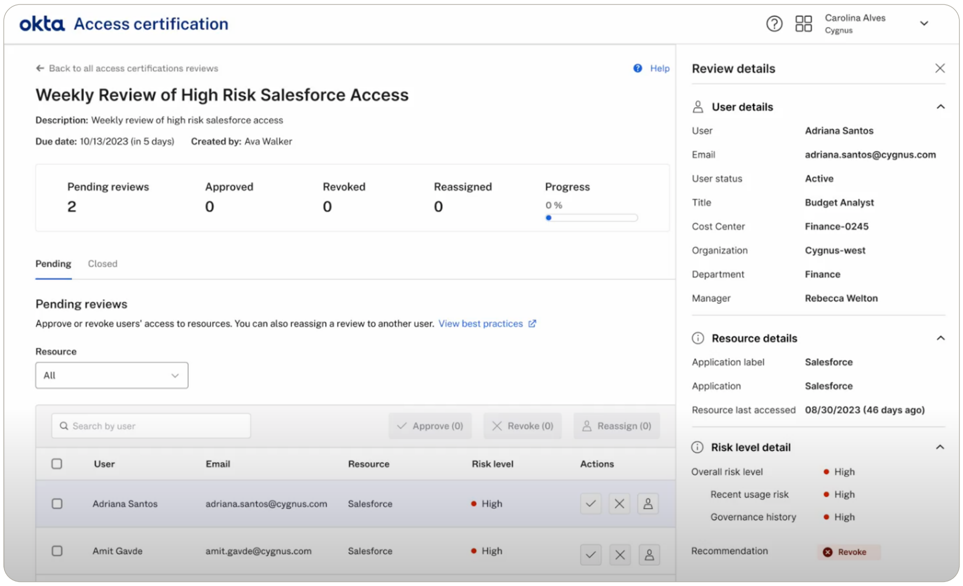
AI's role: Ingests a broad range of device access signals, user access signals, and other critical contextual signals to deliver actionable Identity governance insights

- Identity Governance and Administration (IGA) is a policy-based approach to Identity management and access control that combines:
- Identity governance: Processes and policies that cover the separation of duties, role management, logging, access reviews, analytics, and reporting
- Identity administration: Account and credential administration, user and device provisioning and deprovisioning, and entitlement management

Okta's position as a unified platform for IAM, IGA, and Privileged Access Management (PAM) provides a uniquely vast Identity dataset that can be leveraged to help organizations meet compliance requirements, satisfy the information needs of audits, improve process efficiency, and enable increased workforce productivity.

Governance Analyzer with Okta AI supports these goals by leveraging machine learning, device access signals, and user access signals to:

- Reduce the cognitive burden on decision makers in governance processes
- Deliver non-trivial insights into the risk of user-resource combinations
- Leverage the breadth of Okta data to deliver insights other vendors cannot



Weekly Review of High Risk Salesforce Access

Description: Weekly review of high risk salesforce access

Due date: 10/13/2023 (in 5 days) **Created by:** Ava Walker

Pending reviews	Approved	Revoked	Reassigned	Progress
2	0	0	0	0 %

Pending reviews

Approve or revoke users' access to resources. You can also reassign a review to another user. View best practices

Resource: All

□	User	Email	Resource	Risk level	Actions
□	Adriana Santos	adriana.santos@cygnus.com	Salesforce	● High	✓ ✕
□	Amit Gavde	amit.gavde@cygnus.com	Salesforce	● High	✓ ✕

Review details

User details

User	Adriana Santos
Email	adriana.santos@cygnus.com
User status	Active
Title	Budget Analyst
Cost Center	Finance-0245
Organization	Cygnus-west
Department	Finance
Manager	Rebecca Welton

Resource details

Application label	Salesforce
Application	Salesforce
Resource last accessed	08/30/2023 (46 days ago)

Risk level detail

Overall risk level	● High
Recent usage risk	● High
Governance history	● High
Recommendation	Revoke

For example, potential applications of Governance Analyzer include:

- Informing a decision about whether or not a user's access should be approved (e.g., in a request) or extended (e.g., in a certification)
- Determining who can request access to a given resource (e.g., only users below a certain risk threshold have the ability to request access)
- Setting the scope of whose access is reviewed in a campaign (e.g., any user above a specified risk level is automatically reviewed or reviewed more frequently)
- Taking automated action to approve or deny access, in either a request or certification campaign
- Recommending appropriate governance configurations to ensure that critical resources have the requisite approvals to gain access and that access is reviewed frequently

Log Investigator with Okta AI

Limited Early Access Q3 2024

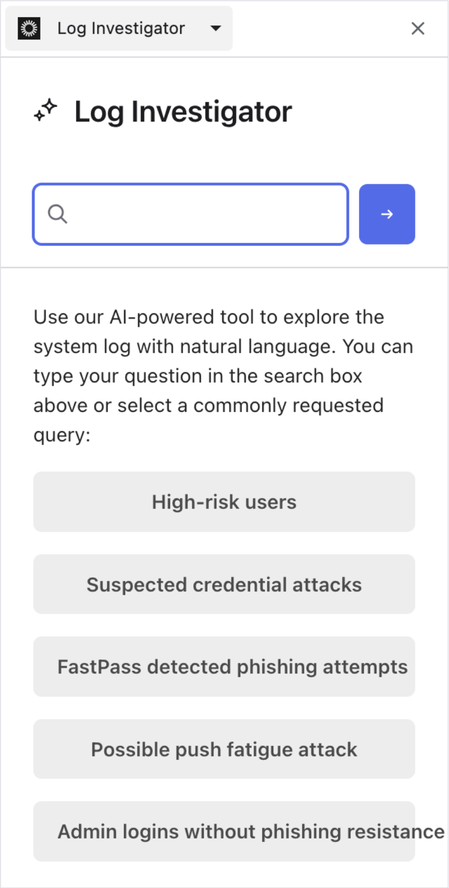
AI's role: Powers a natural-language log and API search tool that makes it easy for IT personnel to quickly find information and insights from Okta's vast dataset

Since the advent of computing, logs have served as an invaluable information resource to determine what happened, what's happening, and why. But as digital technologies came to control ever-more aspects of business operations and the granularity of such control increased, the volume of logs has soared and the insights they hold have become more difficult to extract. In many IT systems, finding the answers to even simple questions often requires carefully constructed queries and/or substantial manual effort to comb through hundreds of results — consuming time and resources when both are in short supply.

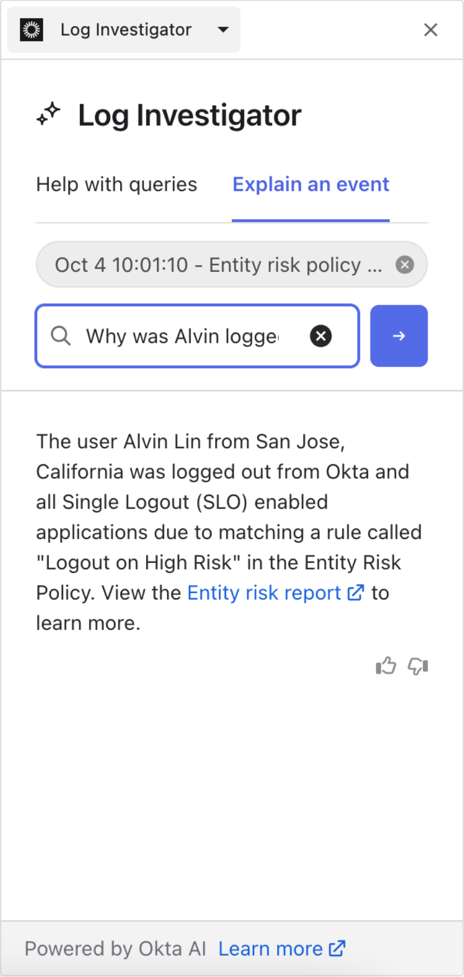
Fortunately, generative AI is transforming how people interact with datasets to extract useful information.

Log Investigator with Okta AI is a natural language log and API search utility that allows IT personnel to easily and quickly navigate Okta's vast dataset, helping to answer Identity-related questions like:

- "Have we seen any suspicious logins this week?"
- "Which of these were from unmanaged devices"
- "Were any of these from a new location?"


Log Investigator
Log Investigator
High-risk users
Suspected credential attacks
FastPass detected phishing attempts
Possible push fatigue attack
Admin logins without phishing resistance

Use our AI-powered tool to explore the system log with natural language. You can type your question in the search box above or select a commonly requested query:



Oct 4 10:01:10 - Entity risk policy ...

Why was Alvin logge

The user Alvin Lin from San Jose, California was logged out from Okta and all Single Logout (SLO) enabled applications due to matching a rule called "Logout on High Risk" in the Entity Risk Policy. View the Entity risk report to learn more.

Policy Recommender with Okta AI

Limited Early Access Q1 2024

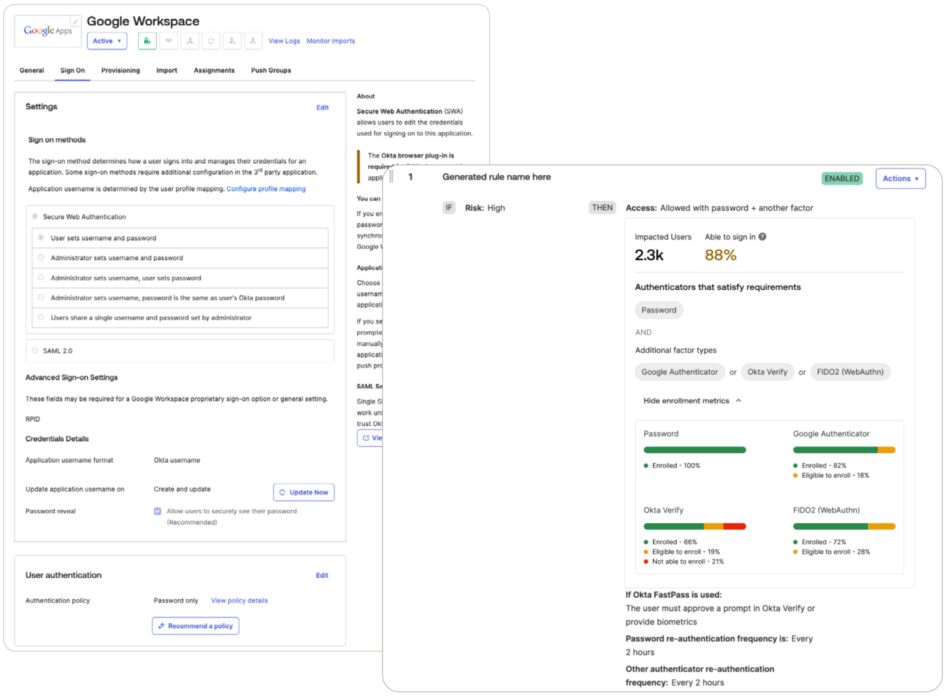
AI's role: Examines policy configuration data from Okta's customer base to extract best practices and generate machine-readable policies that can be directly applied within Okta environments

Identity infrastructure forms a vast interconnected web spanning an organization's entire IT environment — and even beyond to third-party applications. Consequently, configuring and managing such an extensive system is a complex undertaking that can consume time, energy, and expertise.

At the same time, different organizations encounter and address many of the same administration scenarios, especially across the most common applications like Slack, Salesforce, and GitHub — and these shared experiences create an opportunity to leverage the wisdom of the crowd.

Policy Recommender with Okta AI leverages anonymized, aggregated insights from across Okta's customer base to equip administrators with policy recommendations and insights (e.g., how many users will be impacted by a policy change, previewing the impact of a policy before applying) for managing Okta Integration Network (OIN) apps, allowing admins to:

- Better understand and more easily resolve any issues they encounter
- Apply the right configuration and settings for the right features with confidence
- Ultimately, improve security, efficiency, and workforce productivity



Google Workspace

Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

● Secure Web Authentication

● User sets username and password
○ Administrator sets username and password
○ Administrator sets username, user sets password
○ Administrator sets username, password is the same as user's Okta password
○ Users share a single username and password set by administrator

○ SAML 2.0

Advanced Sign-on Settings

These fields may be required for a Google Workspace proprietary sign-on option or general setting.

RPID

Credentials Details

Application username format	Okta username
Update application username on	Create and update
Password reveal	☑ Allow users to securely see their password (Recommended)

User authentication

Authentication policy: Password only

About

Secure Web Authentication (SWA) allows users to edit the credentials used for signing on to this application.

The **Okta browser plug-in is**

1 Generated rule name here

IF **Risk:** High THEN **Access:** Allowed with password + another factor

Impacted Users 2.3k

Able to sign in 88%

Authenticators that satisfy requirements

Password

AND

Additional factor types

Google Authenticator or Okta Verify or FIDO2 (WebAuthn)

Password
- ● Enrolled - 100%

Google Authenticator
- ● Enrolled - 82%
- ● Eligible to enroll - 18%

Okta Verify
- ● Enrolled - 66%
- ● Eligible to enroll - 19%
- ● Not able to enroll - 21%

FIDO2 (WebAuthn)
- ● Enrolled - 72%
- ● Eligible to enroll - 28%

If Okta FastPass is used: The user must approve a prompt in Okta Verify or provide biometrics

Password re-authentication frequency is: Every 2 hours

Other authenticator re-authentication frequency: Every 2 hours

AI in the Customer Identity Cloud (CIC)

While the literal definition of Customer Identity and Access Management (CIAM) has remained consistent, its true meaning — in terms of what use cases it enables, using what functional components, for what types of organizations — has evolved, especially in recent years. Today, CIAM is essential for:

- Serving consumer customers: In the business-to-consumer (B2C) world, an effective CIAM implementation enables companies to offer highly personalized promotions and recommendations that drive additional revenue and create more value for customers — all while ensuring a convenient user experience across multiple digital channels.
- Empowering business customers: Countless organizations rely on business-to-business (B2B) SaaS applications as essential enablers. However, different users within each organization need different levels of access to different resources, and creating a convenient and secure experience requires precisely managing Identity and access privileges. CIAM provides the answer by empowering B2B SaaS customers to self-manage Identity.

Okta's initial adoption of AI in the Customer Identity Cloud focused on security, for the straightforward reason that customer-facing applications face a wide range of threats. However, the same approaches that can help to secure workforce Identity aren't always applicable to the world of customer Identity. In an enterprise environment, security often trumps convenience, so administrators can impose controls with comparatively little regard for the user experience.

In contrast, customer Identity management must maintain security and privacy while minimizing friction — which requires engineering defenses that can withstand sophisticated threats while remaining nearly invisible to users.

Fortunately, AI has proven very adept at distinguishing threat actors masquerading as legitimate users from the legitimate users themselves.

In addition to new Okta AI security features, other recent capabilities make use of machine learning and generative AI to enhance the customer experience, increase conversions, and simplify administration.

Accenture's Technology Vision 2023 report notes that, **"The ability to authenticate customers' identities online seems to be a top priority for executives — 85% said it is "becoming a strategic business imperative," and three in four respondents said that customer authentication issues have negatively impacted their company's bottom line in the form of abandoned transactions, user frustration, and more."**

Bot Detection

AI's role: Examines 60+ signals to predict when an authentication request is coming from a bot, rather than the legitimate account holder

As a vital part of the Attack Protection add-on in the Customer Identity Cloud, the Bot Detection feature mitigates scripted attacks (e.g., credential stuffing attacks or list validation attacks) against native applications, passwordless flows, and custom login pages.

By analyzing more than 60 data sources — like past events associated with an IP address, recent login history, IP reputation data, and an assortment of other factors — Bot Detection predicts when an Identity request is likely to be coming from a bot. Above a certain prediction/confidence threshold, the authentication flow presents a countermeasure, such as a CAPTCHA.

Bot detection is an example of how AI can improve upon prior techniques:

- The first version, introduced in February 2021, was rules-based and detected 18% of bots
- Version two, which debuted in August 2021, employed machine learning for behavioral analysis; this AI-driven approach more than doubled the effectiveness, detecting 45% of bots
- The most recent version, launched in June 2022, detected 79% of bots — the highest performance yet, despite threat actors continually refining their own techniques

Importantly, these improved defensive capabilities were achieved without introducing unnecessary user friction. Carefully training and continually tuning the AI at the heart of the Bot Detection feature helps to ensure that human users are rarely presented with a CAPTCHA.

Plus, a detailed internal study examining the before-and-after effects of Bot Detection has revealed a strong deterrent effect:

- On average, customers in the study who enabled Bot Detection saw a reduction in malicious traffic of more than 40%
- Some larger customers in the study saw bot traffic drop by nearly 90%!

Building on Bot Detection: Identity Threat Level (ITL)

In April 2023, we provided a sneak peek into our Identity Threat Level (ITL) initiative. Being at the 'front door' of applications with a CIAM solution that secures billions of login transactions per month provides us with a unique vantage point from which to monitor Identity threats.

This powerful perspective was the genesis of the ITL: a score from 0 to 10 that reveals the inferred level of bot activity by representing the probability that traffic will fail a CAPTCHA. A score of 0 means there's practically no bot activity to speak of, while a score of 10 means almost all traffic is likely attributable to bots.

By aggregating (anonymously, of course!) observations across our customer base, we can calculate an ITL for different industries and geographies, with the option of introducing additional slicing and dicing on other common attributes. For instance, the ITL can show:

- How likely malicious traffic to CIC customers in various industries or operating regions has changed over time
- How levels of likely malicious traffic to CIC customers compares across different industries or operating regions

Tracking historical trends and daily shifts has the potential to inform of elevated risks to CIAM login and sign-up flows, enabling app providers to increase their own monitoring, proactively tighten thresholds, implement additional defenses — or respond in any other way they see fit.

And it's all built upon the foundation of Bot Detection.

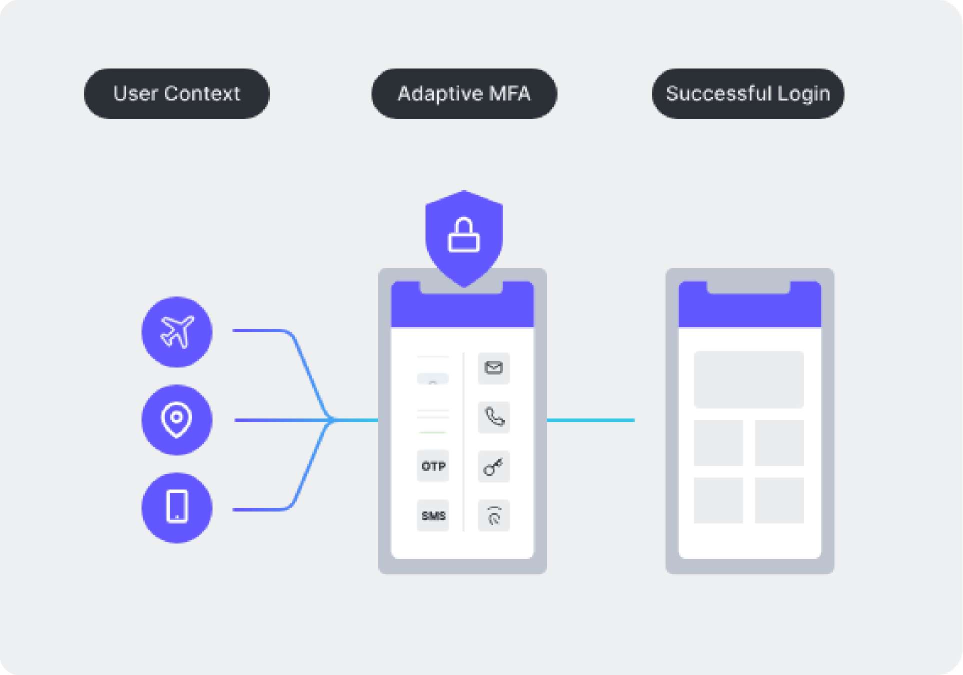
Adaptive MFA

AI's role: Provides crucial risk context by analyzing a broad set of Identity signals to predict whether an authentication attempt is from the legitimate user or from a threat actor masquerading as such.

Adaptive MFA provides intelligent access that fits a business' needs while adapting its customers' login behaviors.

While MFA is a proven defense against account takeovers, many companies — especially in B2C — shy away from its use out of concern that the added friction will undermine the user experience.

Adaptive MFA provides a compelling alternative, by only presenting an MFA challenge when a login is deemed risky — and preserving a seamless experience at all other times.



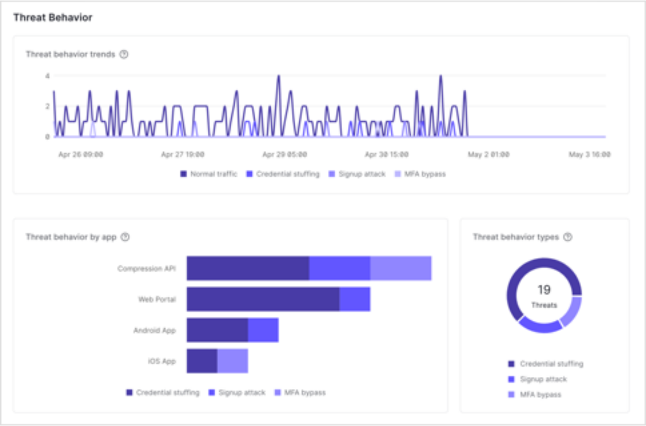
Security Recommendations

Coming soon

AI's role: Powers intelligent recommendations that enable organizations to improve their tenant's security posture

Security Center allows IT and security personnel to see potential attack trends and quickly respond to them in real-time, by providing:

- A streamlined view of authentication events, potential incidents, and threat response efficacy
- Real-time notifications of anomaly detection metrics
- Visualizations of potential attack trends (e.g., credential stuffing, signup attacks, MFA bypass attempts)
- Insights into the user experience impacts of Attack Protection features (e.g., rate limiting, CAPTCHA)



These capabilities will now be extended with intelligent, ML-driven security recommendations delivered through security snapshot alerts and dashboard notifications.

Identity Flow Optimizer with Okta AI

Limited Early Access Q4 2024

AI's role: Analyzes authentication data to suggest ways to provide a better customer experience and to increase conversions

In a customer-facing business, friction refers to anything that slows down a person's interactions with a service. These interactions may include (but are not limited to) a user:

- signing up for your service
- logging in to their existing account
- updating their information and preferences
- recovering lost account data
- checking out (i.e., completing a purchase)

The more friction there is, the lower an organization's conversion rates and the less revenue gained over both the short and long term. However, manually optimizing customer flows can be very challenging, due to the vast quantities of data involved and the highly personal preferences of different users.

Plus, securing Identity flows must always be a priority, but remains a difficult endeavor for experts, let alone developers who are new to Identity.

To address these challenges, Identity Flow Optimizer provides developers with inline recommendations on the identity configurations and actions they can add to boost conversions, improve security, and build their apps faster.

Brand Customizer with Okta AI

Limited Early Access Q4 2024

AI's role: Automatically builds or populates design templates with an organization's branding

Brands have strict design guidelines for a reason: to deliver a consistent user experience that positively reinforces the brand's carefully curated Identity.

The Brand Customizer can design a one-page template and adapt the design to all the other required templates. A developer can also provide a screenshot or logo, and the AI then builds the templates, with the developer customizing them as needed.

Not only does this approach create a consistent look and feel for end users, but it also speeds time-to-value by making it easier and faster for developers to build superior customer experiences, innovate rapidly, and contribute to business scale.

Guide with Okta AI

Limited Early Access Q4 2024

AI's role: Interprets plain-language prompts and provides contextual assistance to help users effectively and efficiently work with the Customer Identity Cloud

The Customer Identity Cloud is powerful, feature-rich, and highly extensible — but the full breadth and depth of its capabilities can be intimidating for new users, and even experts might not be familiar with every detail or be able to keep up with new capabilities.

To help new users onboard quickly and to help any user get the most out of the CIC, Guide:

- Offers comprehensive onboarding assistance and intuitively maps out the best steps for users to take, seamlessly steering them toward the most valuable workflows from simple English prompts
- Can explain any setting or jargon in the platform into easily understandable language and also enrich the experience with contextual assistance and curated links to relevant documentation

Actions Navigator with Okta AI

Limited Early Access Q2 2024

AI's role: Enables plain-language search to more easily find appropriate integrations, and helps users to develop brand new integrations as needed

Extensibility is a core capability of the Customer Identity Cloud, and the Auth0 Marketplace aims to simplify development processes by providing a straightforward way to add an integration to Identity applications.

But with hundreds of integrations, it can sometimes be difficult to find exactly what's needed.

Actions Navigator allows developers to discover and implement marketplace integrations or write an Action (a function that is used to customize and extend CIC capabilities) by simply asking for it in a search prompt. Code generation is one of the most transformative uses of generative AI and this feature unlocks new capabilities both for developers and for those who don’t have experience writing their own code.

Tenant Security Manager with Okta AI

Limited Early Access Q2 2024

AI’s role: Develops plain-language summary descriptions of complex Identity configurations

Many organizations have subject matter experts who have valuable institutional knowledge about particular systems, including Identity.

When these experts are unavailable — e.g., whether moving to a new department or leaving the company — it can be very difficult for others to understand the state of the system and the details of its configuration.

Tenant Security manager enriches Okta’s Attack Protection capabilities with intelligent security recommendations through security snapshot alerts and dashboard notifications to improve the customer tenant’s security posture.

Conclusion

The sudden arrival of ChatGPT, and the rapid debut of a long list of similarly impressive tools in response, shows the state of the art is changing so quickly, and the ripple effects are so varied, that making specific predictions about AI and its impacts is a bit of a fool’s errand.

However, some things are clear. For instance, when it comes to the ramifications of AI — and especially of generative AI — the headline of a Forrester press release really tells the story: Ignoring Generative AI Will Be A Costly Mistake For Enterprises.

Another way of looking at the subject: while you may not know exactly where your investments in AI will take you, you can be confident that not making investments will lead to a competitive disadvantage, at best, and potentially irrelevance. The paradigm shift really is that significant.

By directing a meaningful portion of our research and development dollars toward AI, and by leveraging our enormous IAM dataset, Okta will continue to deliver innovative AI-driven capabilities to strengthen security, enhance productivity, and improve user experiences — within both our Workforce Identity Cloud and Customer Identity Cloud.

And while we don’t know exactly what fruit our own investments will bear, we’re confident that we will look back upon today’s capabilities and those in our pipeline as only the first steps of a transformative journey.

Disclaimer

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.

Any products, features or functionality referenced in this material that are not currently generally available may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.