Whitepaper

AI-driven innovation

Balancing challenges and seizing opportunities

Contents

A time of breakthrough transformations

Artificial intelligence (AI) has emerged as one of the most transformative technological advancements of our generation. This breakthrough technology has the potential to revolutionize every aspect of business.

AI adoption has grown steadily in the last few years. But the unprecedented growth of generative AI (GenAI) and large language models (LLMs) took the world by storm — uncovering exciting new possibilities. Adoption of this technology has nearly doubled in just 10 months, with 65% of organizations reporting regular use. Gartner hailed GenAI as “the most disruptive set of technologies and capabilities to hit the global market in decades.” We’re only at the cusp of understanding the game-changing opportunities of GenAI for organizations of all sizes.

10X

IDC forecasts that spending in GenAI will increase at an annual compound growth rate of 59% between 2024 and 2028, outpacing the growth of AI overall. Embracing this shift is paramount to your ability to continue innovating.

The growth of this nascent technology will maintain its meteoric pace. IDC forecasts that spending in GenAI will increase at an annual compound growth rate of 59% between 2024 and 2028, outpacing the growth of AI overall. Embracing this shift is paramount to your ability to continue innovating.

As AI datasets grow bigger and more complex and the ecosystem of interconnected AI programs expands, security and customer experience remain paramount. To unlock the full potential of GenAI, developers must find ways to integrate AI into their applications and products securely while product teams need to streamline customer onboarding without throttling time to market — all while meeting employee and customer expectations.

Since the IT environment is evolving as well, it becomes more complicated. This evolution brings new data security and privacy risks, stemming from factors such as:

- An expanded attack surface
- A growing number of connection points
- Massive amounts of valuable data that's being collected and processed
- Increased reliance on the cloud, along with more complex and dynamic workloads

If your AI systems are not secure, risks such as data compromise, operational disruption, reputational damage, financial losses, and regulatory noncompliance become an even bigger challenge. Any one of these outcomes could cause setbacks to your AI initiatives, threatening your ability to maintain a competitive advantage.

Digital identities — those of the customers and employees — play a central role in the AI era. Strong and secure authentication is the foundation of successful AI adoption, whether you're integrating it into internal systems or your products. Since digital identities control access to all your data, applications, and services, managing identities effectively and protecting your organizations against identity-centric threats take on new urgency.

By rethinking your approach to identity, you can embrace the disruptive opportunities of AI — accelerating time to market while maintaining secure access to applications and meeting customer expectations.

The complexities and risks of data management in the world of AI

58%

An Okta survey of executives across different industries found that 58% view AI as "a positive force in the world," with 31% describing it as very positive.

While some organizations have yet to embrace AI, most have an optimistic view of its impact. An Okta survey of executives across different industries found that 58% view AI as "a positive force in the world," with 31% describing it as very positive.

Those who have begun harnessing this technology are seeing meaningful results:

- 54% of small-business owners and executives say AI contributes to business growth and 48% believe it boosts profits.
- 77% of organizations investing in AI note operational efficiencies, while 74% report improved employee productivity and 72% report an increase in customer satisfaction.
- 69% of organizations are using AI and machine learning (ML) to develop new revenue drivers and create value vs. simply saving costs.

The explosive growth of data, performance-heavy workloads, and analytics required by AI models pushes you to reevaluate your data infrastructure. Data management is one of the biggest barriers to AI/ML implementation, especially since these workloads are deployed across multiple locations — from data centers to public and private clouds and the edge. According to the Okta survey, insufficient data infrastructure is the second biggest reason why organizations believe they're behind their competitors in adopting and leveraging AI.

Impact on application and product development

To incorporate AI into your applications and products successfully, you need to keep up with customer and market requirements, ranging from data privacy and customer experience to cutting costs and improving efficiencies.

As one example, chatbots can help enhance customer engagement while delivering a more personalized experience. The AI agents that facilitate these interactions rely on APIs for connecting different data sources, applications, and systems. To ensure AI-ready APIs, developers need to implement processes for preventing data leakage and driving fast performance without creating friction for customers.

74%

Okta's survey shows that 74% and 71% of executives, respectively, cite concerns that data privacy and security cause the biggest AI trepidations.

Implications to data privacy and security

Data privacy and security, by far, cause the biggest AI trepidations. Okta's survey shows that 74% and 71% of executives, respectively, cite these concerns. Their worries are not unfounded. As with any technology that sees rapid adoption, the rush to embrace AI outpaces organizations' understanding of security risks, not to mention their ability to evolve security controls.

In addition to being tough to manage, complex AI data environments demand more sophisticated data protection. Maintaining strict security and access is especially challenging as you manage data and analytics integrations between vendors, platforms, and tools in the fragmented AI market.

The exponential growth in data and the expanded attack surface in AI environments significantly impact the three pillars of information security:

- **Data confidentiality:** AI systems process massive amounts of sensitive data that may include intellectual property and private customer information. These systems are also connecting to and authenticating more data sources and applications. Unauthorized access could lead to data breaches and leaks, whether they're caused by attackers or unwitting employees.
- **Data integrity:** Accurate, high-quality, and reliable data is essential to AI models. If datasets that are used to make critical decisions are compromised and manipulated, the results could prove catastrophic. Biased and inaccurate results also have ethical implications, which could be compounded due to AI's ability to distribute content at scale.
- **Data availability:** One of the competitive advantages that stem from AI is the capacity to process and analyze massive quantities of data in real-time. A major incident like a cyberattack that disrupts access to this data can severely impact your operations or ability to react quickly to changes in the market or customer demands.

67%

Small and midsized businesses are particularly vulnerable to AI-powered attacks because they have limited resources — and 67% don't even have dedicated cybersecurity specialists.

Threat actors could also target AI systems to deny service to your customers or create inaccurate predictions. As the technology matures and adoption reaches the mainstream, cybercriminals will see an increased return on investment (ROI) from attacking AI systems.

Besides existing risks that are compounded by AI deployment — such as supply chain attacks and cloud vulnerabilities — you must prepare for AI-specific threats. Emerging threats such as data poisoning, model theft, and prompt injections can compromise personally identifiable information (PII) or intellectual property in the LLMs to harm your business.

AI's double-edged sword

Forward-thinking businesses are not the only ones leveraging AI. Cybercriminals are looking for efficiencies and innovating their capabilities as well, and GenAI is the latest tool that can help them scale. Small and midsized businesses are particularly vulnerable to AI-powered attacks because they have limited resources — and 67% don't even have dedicated cybersecurity specialists.

Managing non-human users like AI agents

When integrating AI into your own applications, one aspect to consider is how you're managing the identities of non-human users such as AI agents and bots, service accounts, and automated software systems. Just like people, non-human users are associated with digital identities that enable them to become authenticated and authorized to access data and systems. Managing non-human identities and their access is important to maintaining strong security. Recommended best practices include:

- Assigning permissions and access types based on the identity's function
- Using the principles of least privilege
- Changing default vendor passwords
- Restricting credential sharing
- Logging and monitoring user activities

60%

Security researchers observed a nearly 60% year-over-year increase in phishing attacks globally in 2023.

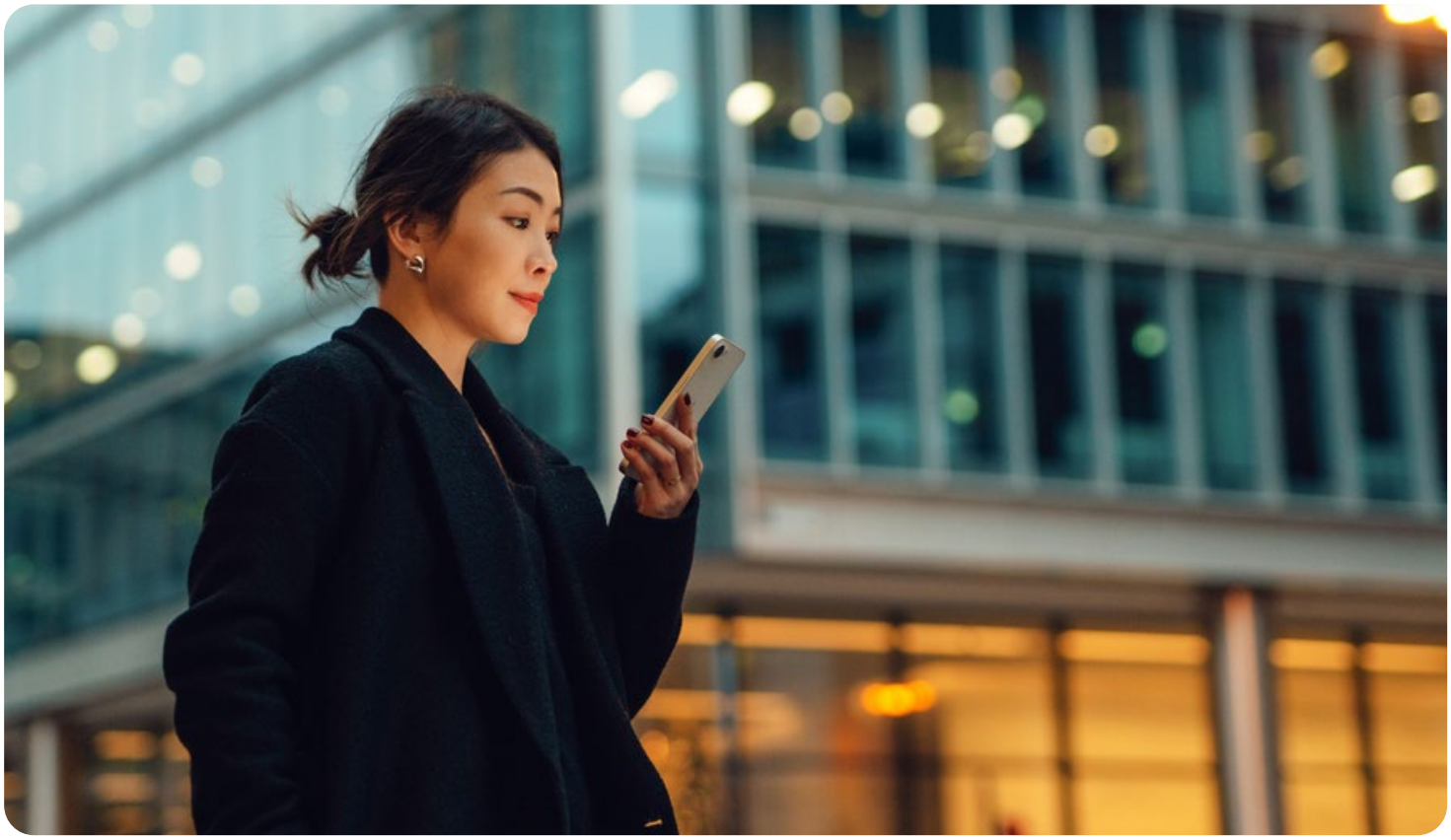
AI-powered threats to watch for include:

- **Phishing:** GenAI can help malicious actors craft flawless phishing messages that are more difficult to spot, generate convincing images, and mimic voices through deepfakes, as well as quickly deploy large infrastructure such as phishing websites. Security researchers observed a nearly 60% year-over-year increase in phishing attacks globally in 2023, driven in part by proliferation of GenAI tools. In a recent warning about this escalating threat, the FBI also noted that cybercriminals are using both "publicly available and custom-made AI tools to orchestrate highly targeted phishing campaigns."
- **Synthetic identities:** Combining fake and real information to create a new identity, synthetic identity fraud is fueled in part by the abundance of personally identifiable data available in the criminal underground. Synthetic fraud is even more difficult to track than traditional fraud because the fictitious data enables the pieced-together identity to pass through security checks and the crimes build slowly while the scammer cultivates trust with the organizations. A global data analysis found that synthetic identity fraud was the fastest growing type of digital fraud in 2023. AI can help fraudsters create synthetic identities in the blink of an eye, as well as automate and scale attacks.
- **Password cracking:** Brute-force attacks such as password cracking are the second most common type of hacking action in data breaches involving basic web application attacks (surpassed only by the use of stolen credentials). Malicious actors have long used automated tools to crack passwords, but AI takes that to a new level. With LLMs, they can scour public sources such as social media at speed and scale for personal information that people commonly use in passwords.

The impact on regulatory compliance

Only 11% of organizations surveyed in 2024 were not required to report a data breach, and noncompliance is one of the top factors contributing to the cost of a breach. Given the increased data usage and access, organizations across all sizes and sectors must comply with a range of complex and often inconsistent regulations. In addition to complying with mandatory requirements, adopting frameworks that provide best practices and standards for information security, such as the NIST Cybersecurity Framework, ISO 27001, and SOC 2, can be critical for organizations adopting AI.

AI's extensive data access, collection, and processing capabilities are also raising new scrutiny from regulatory bodies. As one example, the European Union introduced the AI Act in 2024, which focuses on responsible AI development and deployment. Several US states have enacted or are considering AI privacy regulations as well. The evolving nature of AI regulations makes it even more challenging to keep up with compliance.



The role of identity in AI environments

Identity is the enabler of your modern business, shaping the way your customers engage with your services and how your employees get their work done. In an AI-powered environment, identity becomes even more important because every digital interaction starts with it:

- Employees, vendors, and partners need seamless and secure access to your digital resources and systems from anywhere.
- Customers want convenient and frictionless access, and as you onboard them to your AI-enabled products and services, they expect personalized experiences and options like managing their own users.

As you adopt AI and digital identities control access to even more applications, systems, and services, managing and protecting identities becomes mission critical.

Addressing customer expectations and concerns

The modern customer journey is an omnichannel experience that spans through the interaction with your core services, enrollment, authentication, and self-services. Ensuring a seamless, reliable, and convenient experience throughout this journey while enhancing the user experience is critical to your ability to gain new customers, reduce churn, and drive growth. Nearly 90% of surveyed consumers and business buyers say that the experience provided by a company is “as important as its products and services.”

Trust is also increasingly important to customers, with 71% saying that it’s more important today than in the past to trust the brands they do business with. Whether you’re developing consumer apps or enterprise solutions, you need to ensure your customer identities are protected and meet compliance requirements. Yet Okta’s “AI at Work” survey found that security is the top priority identified by executives in the context of AI adoption.

90%

Nearly 90% of surveyed consumers and business buyers say that the experience provided by a company is “as important as its products and services.”

71%

71% of customers are saying that it’s more important today than in the past to trust the brands they do business with.

Staying ahead of and proactively mitigating and remediating identity threats can help you:

- Scale AI projects securely
- Build customer and employee trust
- Protect your brand reputation
- Remove barriers to innovation
- Boost productivity
- Save costs and increase revenue

Strong security helps to ensure only authorized and authenticated users can access data and other resources in your AI-powered applications and products. To provide customers and employees with seamless, convenient, and frictionless access, it's important to balance security with user experience. Since this is not a one-size-fits-all approach, a flexible framework is best for meeting you where you are.

The challenge for small development teams is that building a robust authentication solution from scratch — especially one that satisfies the requirements of enterprise customers — is time-consuming. Steps like learning the nuances of SSO protocols and integrating third-party apps into identity workflows divert engineering resources from developing core product features while delaying the product launch. Additional challenges arise as you move upmarket and need to quickly scale, as well as maintain the growing number of identities.

A pre-built, SaaS digital identity solution can solve these challenges by allowing product and development teams to offload identity. A purpose-built identity solution can:

- Significantly reduce developer time and engineering costs and maintenance costs.
- Easily integrate with your current or future technology stack.
- Scale efficiently as you grow your customer base or expand into new markets.

24%

24% of login attempts met our criteria for credential stuffing.

14%

14% of attempted account registrations met our criteria for a sign-up attack.

13%

13% of MFA attempts met our criteria for being malicious.

Detecting and proactively responding to threats at the point of access

As identity grows into the primary entry point into consumer and workforce applications, the most critical aspect of modern security is to secure that point of access — before, at, and after "the login box."

Okta data shows that the login box is a treasure chest for malicious actors:

- 24% of login attempts met our criteria for credential stuffing
- 14% of attempted account registrations met our criteria for a sign-up attack
- 13% of MFA attempts met our criteria for being malicious

These findings illustrate that you need to deploy security across the entire journey:

- **Before the login box** to filter out as many malicious actions as possible and prevent human or machine entities from accessing the login interface. Defenses must be applied at the hosting, platform, and application layers to detect and block threats like bots, suspicious IP addresses, and distributed-denial-of-service (DDoS) attacks.
- **At the login box** to prevent threat actors who had made it through by submitting fraudulent registrations or taking over existing accounts. You can mitigate the risk through techniques like offering logins through a social network provider's single sign-on (SSO), using additional verifications like knowledge-based identification for identity proofing, and adopting passkeys to prevent brute-force password attacks.
- **After the login box** to help ensure identities are protected for the life of the entire user session. Measures like authenticating continuously and lowering maximum session time can prevent bad actors from using stolen cookies for session hijacking.

As you deploy and scale AI initiatives, you have to manage more vendors, platforms, and tools. Cross-platform compatibility and integration can quickly become a challenge when you're trying to maintain strict security and access across all these systems. As you're evaluating security solutions, look for controls that can integrate into your entire technology stack and provide consistent visibility, policy enforcement, and threat mitigation.

Deploying enhanced controls to manage identities and security

Advanced threats and complex customer needs require advanced techniques. Continuously maturing your identity approach and moving beyond foundational steps help ensure you can protect data and scale your identity controls as your AI needs and the complexity of your environment grow.

Recommended advanced controls for managing identities and security include:

- **Privileged access management (PAM):** PAM protects privileged accounts and users, such as data scientists and AI/ML engineers, with additional security layers. Stricter controls for users with elevated access rights include techniques like storing their credentials in a separate vault and automatically rotating credentials (changing passwords).
- **Enhanced access controls:** Methods such as role-based access control (RBAC), attribute-based access control, and policy-based access control restrict access to your sensitive data and systems based on factors such as job function and role, data sensitivity, access location, and a set of predefined policies. These models can scale to meet the growing data demands of AI models.
- **Advanced MFA:** MFA protocols with phishing-resistant capabilities provide protection against phishing-related credential theft. SMS authentication is vulnerable to interception, and using factors such as biometric authentication or hardware security keys provides one of the best protections while balancing security with the user experience.
- **Adaptive MFA:** Another advanced technique, adaptive MFA takes into consideration changes in context, such as prompting for MFA less frequently for users logging in through SSO or on a managed device. Conversely, when a higher risk is present, such as a login attempt from a new device or an attempt to access critical resources, additional or more secure authentication can be prompted.

Strengthening AI integration through smarter user management

A trailblazing business needs innovative user management and security. In a modern, AI-powered environment, a robust identity and access management (IAM) program is essential. More than three-quarters of executives surveyed by Okta agreed that IAM is important or very important for AI adoption and integration.

IAM helps to ensure that only the right individuals — whether that's your employees, customers, or partners — can access AI resources at the right time and for the right reasons without sacrificing productivity or user experience.

IAM is a set of policies, standards, protocols, and tools that support data confidentiality, integrity, and availability so you can mitigate unauthorized access and digital fraud. In short, an IAM framework helps you govern your corporate network users and which services and resources they can access and how. Your IAM framework guides your identity approach, including your PAM, RBAC, SSO, and other advanced practices that are instrumental to AI adoption and integration.

The benefits of IAM go beyond securing access to your AI ecosystem, including:

- **Centralized management:** A centralized platform for managing customer identities can help you reduce launch timelines for new AI-powered products and services so you can respond to the changing market and customer demands with more agility.
- **Operational efficiency:** Automating provisioning and de-provisioning and integrating SSO helps streamline IT operations and cut costs while providing users with easy access to your AI resources from anywhere.
- **Improved compliance:** IAM helps simplify governance and compliance through capabilities such as centrally managing policies and roles, securing access to PII with MFA and other advanced authentication, and simplifying auditing and reporting.

How IAM can help you scale AI initiatives

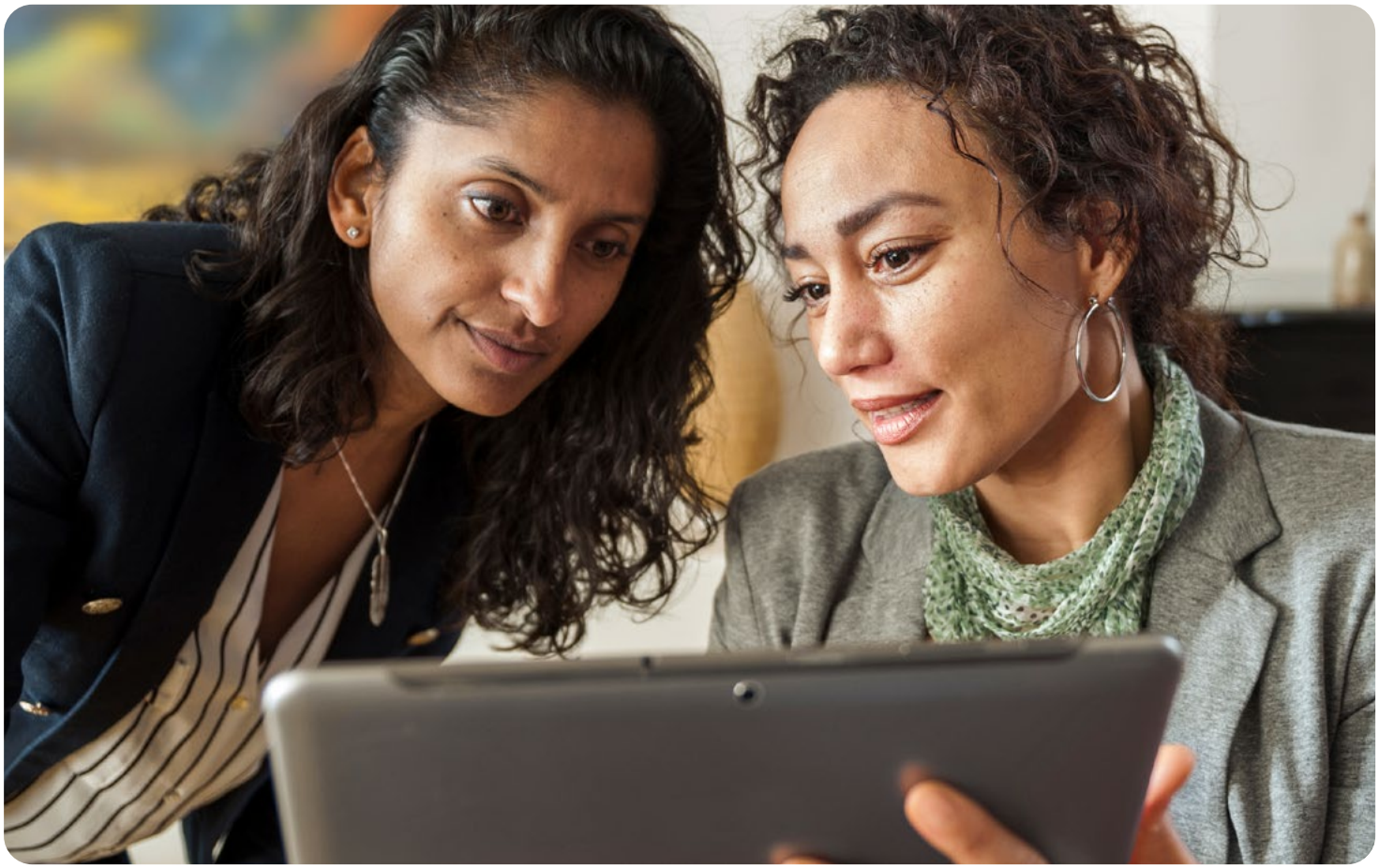
A robust, scalable identity platform is a core part of your IAM program and helps you effectively authenticate customers and employees, centralize identity management, personalize customer experiences, detect and respond to identity-based attacks, and secure your data.

The best IAM solutions deliver:

- Seamless integration across your technology stack, including your multicloud infrastructure and AI systems
- A vendor-neutral platform that connects to any apps you use today or may adopt in the future
- Comprehensive workflows that you can customize to your organization's needs
- Automated, no-code processes that make the solution easy to deploy and manage
- A central admin console for managing all your policies, users, and apps in one place
- An enhanced, streamlined user experience that eliminates friction for your customers and employees
- Advanced monitoring and analytics so you can manage your cybersecurity risks
- Support for a Zero Trust architecture
- AI-powered functionalities for enhancing threat detection and mitigation, productivity, and more

Taking a DIY approach to IAM can be overwhelming, especially for organizations that have limited resources or struggle with talent recruitment and retention. Turn-key, purpose-built solutions that allow you to build and maintain identity with less effort can free up developer time, reduce engineering costs, and improve productivity.

Enterprise customers have thousands of choices for SaaS products, and competing in this landscape requires an agile response to market conditions and customer demands. An Okta survey shows that 88% of organizations using third-party authentication reduced their time to market in the past year. By offloading identity to a cutting-edge platform, you can also reduce your time and money spent managing employee and customer identities and access — removing the barriers to AI innovation. These platforms scale as your needs grow and become more complex, ensuring you can continue to explore new opportunities.



How IAM connects to broader business goals

Forward-looking organizations are adopting IAM to grow their businesses with AI by securely managing their users and apps, offering frictionless onboarding and access to customers, and saving costs with a modern solution. Here are some of their success stories.

Hypotenuse.ai

Hypotenuse AI is a startup whose artificial intelligence platform helps organizations optimize their business processes by reducing manual labor and automating tedious, time-consuming tasks. The company wanted to serve enterprise customers as well as offer a self-service option. The development team needed a fast, secure, reliable, and customizable authentication solution.

To offer product subscriptions, Hypotenuse AI deployed secure authentication with Auth0 by Okta. As demand grew, the company used Auth0 Actions and Flows functionalities to automate the majority of user onboarding steps, saving time and effort by adding pre-user registration validation processes.

> "Overall, Auth0 has allowed us to significantly enhance the performance of our login UX and streamline our user onboarding."
>
> **Low Lin-Hui**
> Founder, Hypotenuse.ai

200K

During six months, the team of four senior engineers oversaw 200,000 new user signups.

Browse AI

The mission of startup Browse AI is to democratize access to information on the internet by empowering their customers to make data-driven decisions and maintain competitiveness. The company's no-code web data extraction platform allows nontechnical individuals to turn a website into a data pipeline or spreadsheets in minutes by training custom AI bots. Understanding that building user authentication would require extensive engineering resources, Browse AI chose to implement a trusted, purpose-built solution instead.

With Auth0 by Okta, the lean engineering team was able to support rapid growth in the customer base. During six months, the team of four senior engineers oversaw 200,000 new user signups. Since then, the team saved another four to five months of engineering time thanks to their ability to scale authentication reliably.

> "We used Auth0 from day one to be able to spend our limited time on innovating and creating new user experiences rather than building another user authentication system."
>
> **Ardy Naghshineh**
> CEO, Browse AI

What's next

Your approach to identity needs to evolve in step with our changing world. Cutting-edge identity solutions that adapt to market, customer, and employee expectations while enabling highly secure AI adoption and integration can safeguard your technological innovations and drive business growth.

Don't let potential security risks and complicated identity needs prevent you from taking the leap toward the next frontier of digital breakthroughs. Okta can help you find the right customer or workforce identity solution so you can harness the promise of AI.

To learn more about Okta and AI, please visit okta.com/products/okta-ai/ or contact us at okta.com/contact-sales.