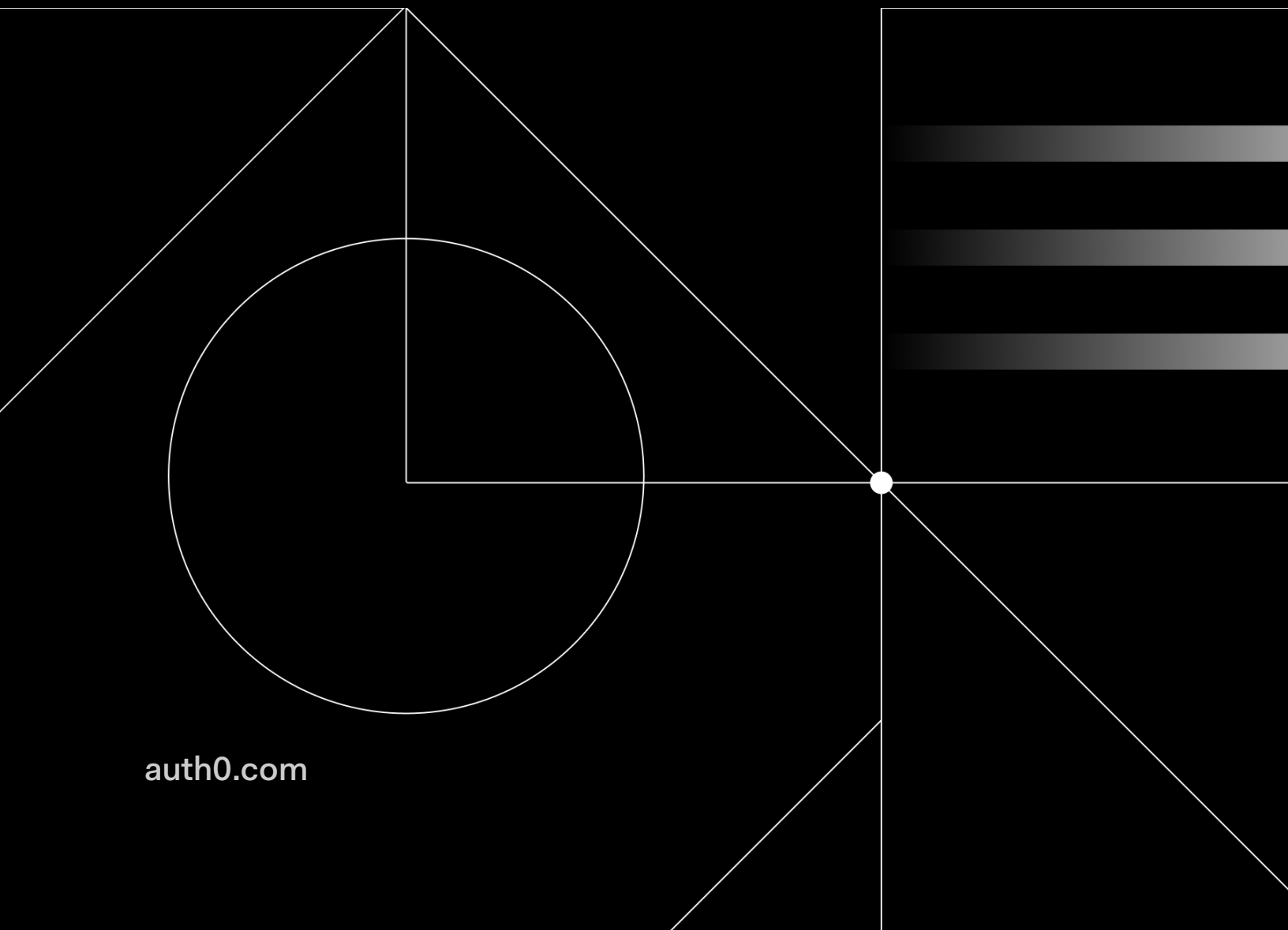
Auth0

To Build or to Buy

Evaluating B2B Identity Management Solutions



auth0.com

What is IAM?

Identity and access management (IAM) is a service or platform that verifies users' identities and controls their access to digital resources. In other words, IAM allows the right people to access the right resources at the right time. IAM is crucial for protecting your data assets, catalyzing digital transformation efforts, and delivering a frictionless experience for users (whether customers, employees, or partners).

IAM encompasses both **authentication** (verifying the identity of a user) and **authorization** (granting access to data based on that identity). A modern IAM platform like Auth0 enables you to control authorization from a central user dashboard via APIs, bolstering your security posture and allowing you to devote more resources to your core service offerings — rather than supporting an expensive in-house identity solution.

Identity management is a continually evolving field, constantly adapting to address new features of the digital landscape. In today's environment, companies need to be able to provide secure access to their users regardless of where they are or what device they're using. That means they need to protect identity across a wide range of devices and platforms. In recent years, modern identity management concepts like multi-factor authentication (MFA) and single sign-on (SSO) have become the gold standard for managing identity across distributed systems.

IAM for B2B

B2B companies operate on a wide array of customized technology stacks and are subject to significant fines under data privacy regulations and revenue loss in the event of a data breach. And a data breach is not a vague or remote threat: In the first half of 2019 alone, data breaches exposed 4.1 billion records, according to Forbes. Cybercrime has spiked in 2020 as bad actors exploit the confusion and new vulnerabilities created by the COVID-19 pandemic and associated social and economic disruption.

The good news is that investing in IAM goes a long way toward protecting your data against attack while empowering you to work more effectively and deliver more value to your customers.

In-house identity solutions, built from scratch over time to accommodate evolving requirements, often struggle to scale with today's business needs, such as onboarding multiple enterprise customers. Homegrown identity solutions supported by in-house developers can also prove prohibitively expensive — in terms of both time and cost — to maintain and improve. This is why startups often shift to third-party IAM platforms when they begin to move upmarket: They must be able to federate identity quickly with any provider on any tech stack.

It's not just startups, however; increasingly, larger and more mature companies are federating identity with a third-party IAM provider to strengthen security posture, improve efficiency, and gain an advantage over the competition.

What is Federated Identity?

Federated identity management involves one company providing federated identity services to another, such as Slack allowing you to use your enterprise credentials to log onto its platform. Supporting federated identity is a baseline requirement for B2B identity management, for reasons we're about to explore.

For one thing, federated identity is a more secure authentication method than username/password combinations. Many enterprises require federated identity in order to meet their security and governance standards. Federated identity enables SSO, which in turn enables a frictionless customer experience that helps keep churn to a minimum. Crucially, federated identity also reduces the volume of help desk calls because users encounter far fewer problems logging in when they can use existing credentials.

The Cost of Not Offering Federated Identity

The inability to offer federated identity via an IAM platform like Auth0 blocks growth. Enterprise customers expect the ease and security of federated identity, and if you can't deliver, they may take their business elsewhere. Investing in a third-party IAM solution to enable federated identity and other premium offerings for the enterprise is a cost — but don't forget to consider the costs of not offering these value-adds.

- **Lower adoption rates:** Certain customers simply won't work with you if you don't offer federated identity. You must be able to support any type of enterprise federation your customers ask for.
- **Lost revenue:** In addition to revenue loss due to lower adoption rates, not offering federated identity costs you opportunities to generate more revenue through upsells and premium offerings.
- **Missed standards:** Without the security and governance requirements that enterprise buyers look for, you'll have trouble increasing adoption rates.
- **Poor user experience:** Without federated identity, users have the pain of remembering a username/password combination — which isn't the most secure way of authenticating identity anyway. Supporting SSO increases security and reduces friction for customers.
- **Additional support costs:** Handling authentication questions and resolving customer issues places a heavy burden on your support team. The conventional wisdom is that you save $70 for every help desk call you avoid — and those costs add up quickly.

The Business Value of a Third-Party IAM Solution

When it comes to B2B identity management, there are many reasons to go with a third-party solution rather than building your own. Let's unpack the business benefits you can realize by entrusting identity to the experts.

Reduce Engineering Costs

The process of implementing a third-party IAM solution is straightforward and enabling powerful features can be as easy as clicking. This means that hundreds or even thousands of development hours can be directed back to core functions, rather than being devoted to authentication and authorization. With a third-party IAM solution, the time-consuming work of integrating and mapping identity providers is already done. The right IAM platform should also offer software development kits (SDKs) for popular development stacks, further reducing the coding work necessary. This way, your engineering team can focus on configuration, rather than coding and customization.

Improve Security Posture

Data is your organization's most valuable asset and storing that data with a third-party IAM provider who adheres to security compliance policies and certifications can make it safer. IAM platforms like Auth0 take on the responsibility of storing and transporting your data securely, so you can rest easy. Moreover, federated identity means your users won't be tempted to reuse the same credentials across multiple services, leaving you vulnerable to credential stuffing attacks and other fraudulent activity.

Encourage Enterprise Adoption

As we've said, the right IAM solution offers robust enterprise federation by enabling users to connect through Microsoft Active Directory (including Azure AD), LDAP, ADFS, SAML, Google Apps, and more. Enterprise federation increases adoption by allowing users to log in with existing credentials rather than having to create new usernames and passwords. This smooths friction and reduces churn, especially during hectic M&A activity and other transitions where federated identity can make the difference between success and failure.

Streamline Sales and Onboarding

A centralized IAM platform allows organizations to use their internal credentials with an external platform or service while ensuring that security requirements are met. Because there's no need to introduce users to an unfamiliar login process or make them remember yet another password, implementing IAM can speed up sales cycles and expedite partner onboarding.

Signs you need to move your B2B SaaS app from a DIY to an IAM solution

How do you know when it's time for your organization to shift from handling identity in-house to investing in a third-party solution?

This checklist can help you reach a decision:

- You need a standards-based solution, such as OpenID Connect, SAML, WS-Federation, and/or OAuth.
- Your users authenticate with various identity providers but lack a way to link their accounts.
- Your applications are hosted on different domains, requiring users to log in separately for each.
- Your development team spends too much time building and maintaining your identity solution, rather than focusing on core business applications.
- Your organization has experienced any kind of a data breach, or you're concerned about a data breach.
- Your customers want to use their enterprise credentials to log onto your platform.
- You want to support enterprise federation with multiple identity providers, like Active Directory, in addition to a username/password option.
- You're being asked for industry certifications like SOC 2, HIPAA, and ISO 27001 that you haven't considered or addressed.
- You can't delegate user management to your customer's service desk.

If these scenarios sound familiar, it's time to think about investing in an identity solution to help you meet not just the business needs you're encountering today, but also those you might encounter six months, a year, and five years from now.

Three Ways IAM Fuels B2B Growth

Investing in an IAM solution not only protects you from data breaches and fines; it also accelerates revenue growth and helps you deliver more value to your customers. Let's explore three ways identity management drives revenue growth.

1. IAM Shortens the Sales Cycle

The right IAM solution accelerates implementation, so prospects can be up and running in a day. Building enterprise federation from scratch takes, at minimum, weeks for each identity provider integration — whereas a robust third-party IAM solution can take hours, or even less, to perform these integrations.

What's more, modern, flexible IAM solutions can be quickly tailored to meet the specific needs of any customer. With the right IAM platform, engineering teams can deliver in days, if not hours, driving sales wins and generating more revenue with upsell opportunities.

Enterprise prospects usually have certification and industry standard requirements. An IAM solution ensures compliance with standards such as SOC 2, HIPAA/BAA, OIDC, and more. When systems are compliant immediately upon implementation, the sales cycle is much faster. With a certified IAM platform, sales teams can breeze through security reviews with an email instead of an audit.

"Most Fortune 500 companies won't sign deals if you don't have the applicable certifications," points out Adam Nunn, Auth0 Senior Director of Governance, Risk, and Compliance. "Yearly tooling costs can vary from organization to organization, ranging from $25,000 to multi-millions, depending on the size of the org."

2. IAM Speeds Innovation by Refocusing Engineering Resources

It's faster and easier to implement a third-party IAM solution than it is to build a DIY solution over time. By taking identity management off engineering's plate, you free up valuable development hours. Instead of building and maintaining your identity solution, your developers can focus on crafting business logic and enhancing the value of your core offerings.

Every enterprise has its own identity provider and infrastructure. With an IAM platform in place, you can integrate with any provider in an hour or less. By recovering thousands of hours of engineering time, you can increase focus on your core competencies, which accelerates the pace of innovation and enables you to create more value for your customers.

3. IAM Unlocks New Revenue Streams via Premium Offerings

A third-party IAM solution allows SaaS companies to offer premium security to customers, which unlocks new revenue streams. For example, Slack and Trello both offer enterprise features and enhanced security in their higher-tier subscription plans. Essentially, SaaS companies can leverage their IAM solutions to offer higher-priced services that deliver more value to customers via stronger security measures and a superior customer experience.

To Build or to Buy: How Three Companies Made the Call

To understand how real companies have made the decision to buy a third-party solution rather than build their own, let's look at three stories from Auth0 customers.

A Cloud Guru

A Cloud Guru is dedicated to educating engineers on cloud services. Over 800,000 students are currently enrolled in courses covering major cloud providers like Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and others. As cloud services become increasingly ubiquitous across industries, A Cloud Guru can help both individuals and organizations quickly gain the skills they need to thrive in an ever-changing technical landscape.

With more than 800,000 users ranging from individuals to teams at major companies, A Cloud Guru needs to keep user data secure without compromising experience. Auth0 provides A Cloud Guru with SSO services to enable unified login credentials and a secure, seamless experience.

One of the most important reasons A Cloud Guru chose to work with Auth0 was our ability to build a reliable authentication solution that would be ready to hit the market in less than a month. John McKim, VP of Product and Technology, explained,

"When Sam Kroonenburg, one of the founders of A Cloud Guru, picked Auth0, it was because he built the first version of the platform in the space of three weeks. He needed to get something out to market as quickly as possible, and you cannot build your own identity platform within that time period. Adopting Auth0 was a really good way to really rapidly get to market."

Even if the pressure to get to market had been less intense, McKim noted, the time and money necessary to handle identity in-house would still have been prohibitive.

"It would potentially be a team of maybe four to five people," he said, explaining that each member of the team would lose at least one week of productivity per month just to maintain the system. "That team would approximately cost, I'm going to say, $550,000 AUD a year. It's often, I think, underestimated how much does go into identity and some of those parts of the platform."

Autotrader

Cox Automotive, the world's largest automotive service organization, owns Autotrader, a transparent, customer-centric marketplace for car buyers and sellers. To expand into the competitive Australian market, Autotrader needed an edge that would get them to market quickly, protect users against fraud, and deliver a more customized experience. These needs meant outsourcing identity to a trusted third party: Auth0.

"[Auth0] enables the teams to move at speed," said Jeremy Gupta, CTO. "That gives the teams more focus on things that we can solve and things that we have in our own destiny. The second [reason we went with Auth0] is the premium consumer experience that we can get through an identity platform like Auth0."

That premium experience allows Autotrader users to shortlist a car or save search results they want to see again. A wall between the user's ability to shortlist and save searches could lead to dropouts they expect to avoid thanks to Auth0's flexible registration, said Gupta.

Auth0 also allows Autotrader to offer protection against fraud, verifying mobile and email using out-of-the-box flows plus customization. "We also get some really strong moderation through the Auth0 platform, which allows our customer service team to jump on fraudulent users ahead of time," said Gupta.

Estimating that it would have needed a team of six people and several months to build an effective identity solution, Autotrader saved potentially $255,000 AUD at launch by investing in Auth0, with additional savings to accrue through avoidance of future maintenance costs.

Topcoder

Topcoder is a global talent network and crowdsourcing platform with more than a million designers, developers, data scientists, and testers.

At first, Topcoder opted to handle identity management in-house — until they realized that they were outgrowing their homemade solution faster than their team could keep up. Security concerns and constant maintenance were in danger of stunting the growth of a platform that prides itself on staying ahead of the curve. To achieve balanced growth, Topcoder decided to invest in a third-party identity solution.

For Topcoder's first decade, working on identity cost them an estimated six months of developer time every year. Building and maintaining their own identity solution was taking their attention away from what was really important: working on their own product and providing more value to customers.

As Topcoder began offloading more of their identity management needs to Auth0's platform, they quickly saw how Auth0's features could unlock strategic advantages. For example, Auth0's machine-to-machine (M2M) token capabilities let financial institutions collaborate without worrying about data being

compromised. Topcoder no longer had to worry about staying on top of evolving industry standards, and customers felt more secure entrusting their data to Topcoder. As Dave Messinger, CTO, put it, “Auth0’s credentials add an air of credibility.”

Messinger reported that with Auth0, Topcoder cut the amount of developer time spent on identity from a work year to a work month. Furthermore, since making the switch, “our complaints are dramatically down.”

IAM Supports Future Growth

Embracing a third-party IAM solution helps B2B companies be more successful. Here are the business-specific metrics that can help you assess the positive impact of your IAM solution:

- Increased enterprise adoption
- Increased revenue from enterprise customers
- Faster sales cycle
- Faster implementation and onboarding for new users
- Reduced churn
- Increased user NPS (Net Promoter Score)

Enterprise customers can bring enterprise-level growth to your company, but only if your identity solution includes the seamless SSO, high availability, and premium support your enterprise users expect.

Learn more about how Auth0 enables B2B identity management by watching this live demo.

Top Considerations for Evaluating an IAM Solution for B2B

When weighing a purchasing decision, keep in mind the following business requirements:

Flexible deployment options: Look for the ability to host anywhere. The right IAM solution gives you the option to deploy to the solution's cloud, your cloud, or your own data center.

Ease of integration: One of the foremost advantages to using a third-party IAM solution is the development time you save. Look for a solution that offers SDKs, robust documentation, powerful APIs, and features that are simple and straightforward to configure and enable.

Support for all identity providers: Your identity management solution should support widely used B2B identity sources, including Microsoft Active Directory, SAML, ADFS, Google Apps, Office 365, and more.

Extensibility: Your business doesn't remain static, so your identity management solution shouldn't, either. The right IAM platform allows for easy customization of the authentication and authorization pipeline. Ideally, you should be able to customize the product to fit your needs from the dashboard, without needing to contact support or buy a custom package. Extensibility also allows you to extend the functionality of your IAM solution to support future business requirements, so you can tackle whatever identity challenges the future holds.

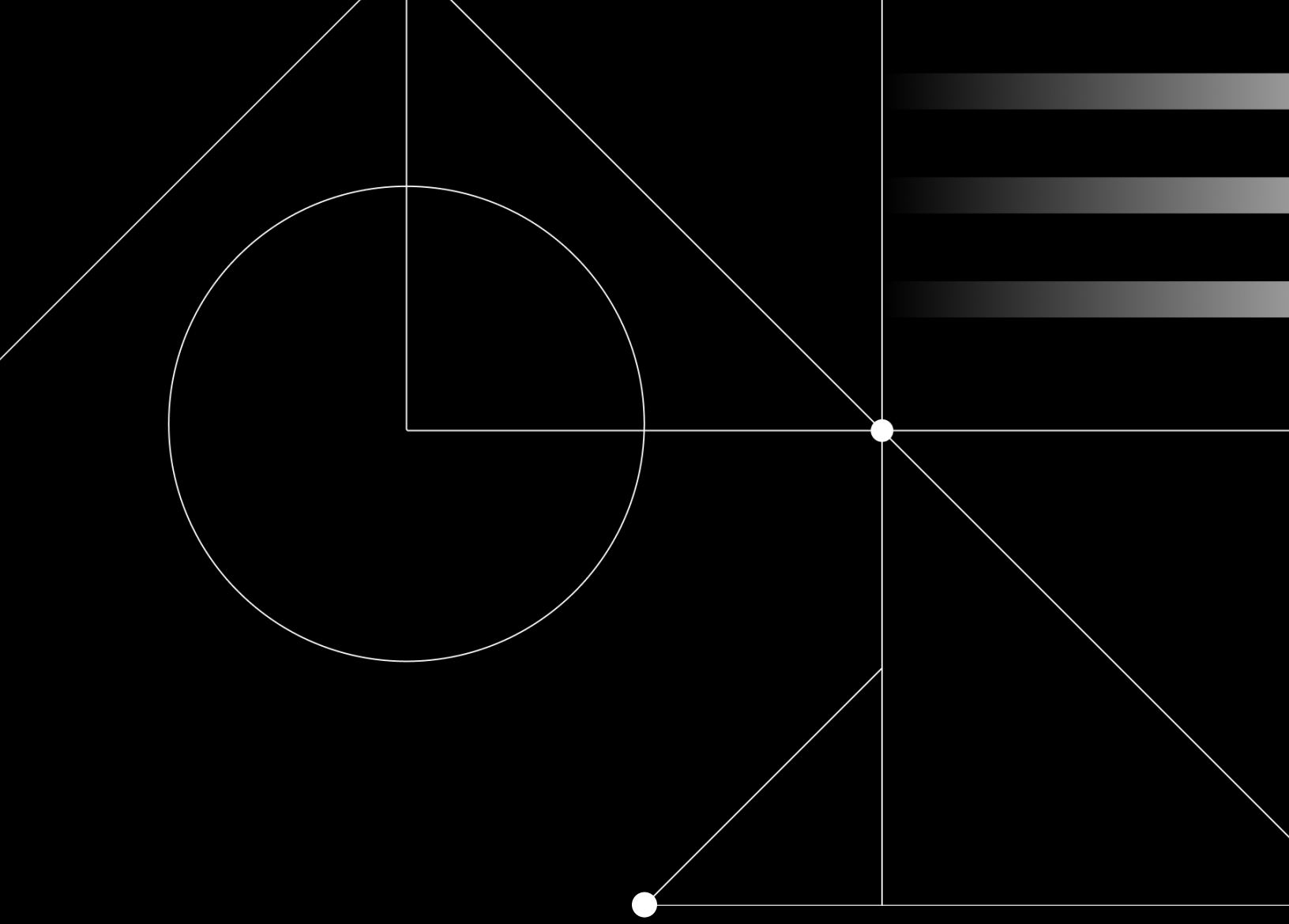
Best-in-class security features: Your IAM selection should be peer-reviewed by international security experts and in compliance with standards such as SAML, OAuth, and WS-Federation and certifications like OpenID Connect, SOC 2, and HIPAA. Look for features that protect against data breaches, like breached password detection and brute force protection.

Ease of migration: Your IAM solution should support unrestricted movement to and from the platform. Be sure there's no vendor lock-in agreement in place that could inhibit migrating users out of the system in the future. Also, look for a solution that connects to any user store you already use, and that doesn't require users to manually reset their passwords when they migrate to the new solution.

Fast, reliable support from security experts: Your IAM solution should come with a customer support team, including security experts, ready to help with any problem 24/7. The support team should also include senior engineers with extensive hands-on experience implementing IAM solutions.

In addition to these requirements, look for an IAM solution that:

- Is stack-agnostic, so you can develop on any stack and for any device.
- Offers a turnkey, customizable branded login widget and home realm discovery.
- Supports delegated administration, so your customers can own simplified user management.
- Supports code reuse across projects.
- Offers auditing and reporting to support data-driven decisions.



Auth0

About Auth0

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and development teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit www.auth0.com or follow @auth0 on Twitter.