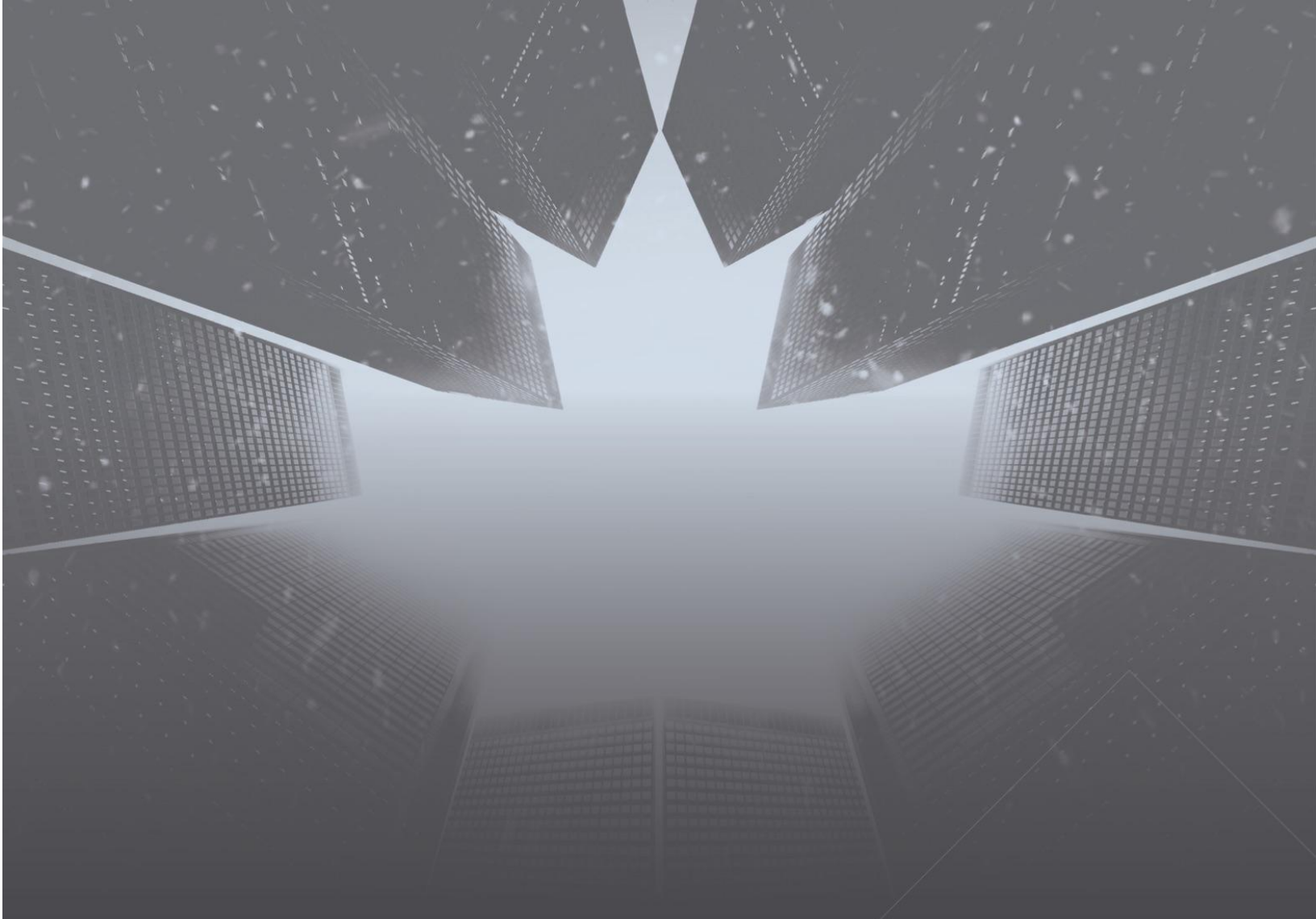


Build vs Buy

Guide to Identity Management

auth0

Contents

What is Identity Management?

Identity and Access Management (IAM), or simply identity management, refers to a service or platform that identifies individuals, and controls their access to system resources through user rights and restrictions. Identity management is important for security and increases the productivity of users by implementing a central directory — meaning users don't need to remember and keep track of several different usernames and passwords.

IAM also helps protect companies and their users from data breaches. In 2019, 28 million Canadians were affected by a data breach. The most common cause of them was unauthorized access.[1] At $4.5 million, Canada has the third highest average cost of a data breach.[2]

Identity management can offer protection against these types of threats with security features like multi-factor authentication, breached password protection, anomaly detection, and more. Identity management solutions provide benefits for all types of businesses. IAM can also provide distinct and specialized features to serve B2B, B2C, and B2E use cases.

- **B2B**: A business provides federated identity management to another business, such as Trello allowing another business to log into Trello with their enterprise credentials.

- **B2C**: A business provides social authentication to consumers through Facebook, Google, or other social media identity providers.

- **B2E**: A business provides single sign-on to its own employees.

We'll cover IAM benefits with regard to all three business types in this paper. Identity management encompasses many different authentication solutions, including but not limited to:

- **Federated Identity**: Federated Identity Management is a method of transferring authentication data without violating the same origin policy, generally by using an external authorization server.

- **Single Sign On (SSO)**: SSO is a type of Federated Identity Management. SSO occurs when a user logs into one client and is then signed in to other clients automatically, regardless of differences in platform, technology, or domain. A token or cookie is generated to authenticate the user across domains.

- **Enterprise Federation**: Enterprise Federation is Federated Identity Management with enterprise connections such as Active Directory, LDAP, ADFS, SAML, Google Apps, etc.

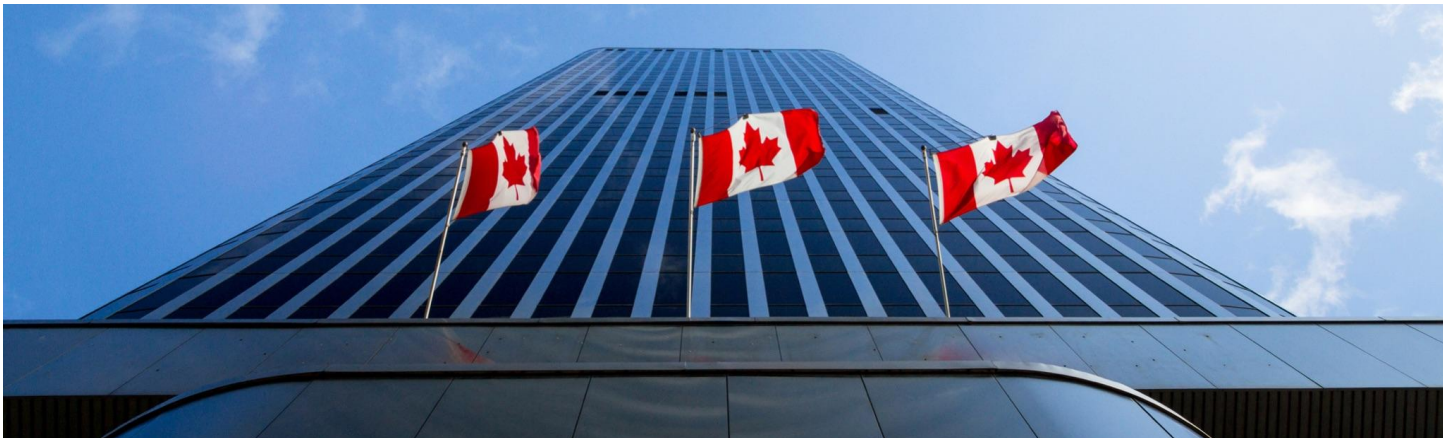
Identity management continues to evolve. The digital landscape grows and changes very rapidly. Personal smartphones and tablets are everywhere and businesses have gone digital. To be successful, companies need to protect and secure identity across a wide variety of devices and platforms. Within the last few years, identity management concepts like Multi-factor Authentication (MFA), Passwordless, and Single Sign On (SSO) have come to the forefront when addressing identity management for modern, distributed systems.

Multi-factor Authentication uses separate stages of authentication to provide two (or more) steps to log in. Passwordless can use SMS, magic links, or even biometrics like fingerprint authentication to authenticate users.

One trend driving identity management adoption is cloud-based applications. Cloud apps and services, like Google Apps and Amazon Web Services (AWS), utilize a network of remote servers to store, manage, and process data. IAM is a vital component of apps that use cloud-hosted services. Identity management provides methods to monitor and provide secure user access to the necessary resources.

Another trend driving IAM adoption is the need for users to be able to access apps from anywhere on any device. With the shift to remote work, companies need the ability to provide secure access to their users regardless of where they are or what device they may be using. Identity management centralizes authentication so user identity can be confirmed under all different login circumstances.

For B2C companies, social authentication is another trend driving the adoption of IAM solutions. Potential customers use a variety of social media on a daily basis. IAM solutions provide social authentication with a variety of social identity providers, allowing customers to authenticate with logins they already use regularly without needing to create and remember new credentials.



Signs You Need to Move from DIY to an Identity Management Solution

All Use Cases

- You need a standards-based solution, such as OpenID Connect, SAML, WS-Federation, and/or OAuth.
- You have users that authenticate with various identity providers but lack a way to link their accounts.
- You have applications on different domains and require users to log in separately for each.
- Your best developers spend their time building and maintaining identity management and authentication instead of building core business applications.
- Your company has experienced any type of data breach or you are concerned with a data breach.
- You're being asked for industry certifications that you haven't considered/addressed.

B2B

- Your customers are asking to use their enterprise credentials to log in to your product. You need to support Enterprise Federation with many types of identity providers, such as Active Directory, in addition to a username/password option.
- You can't delegate user management to your customer's help desk.

B2C

- Your main source of user data comes from directly asking users on forms or surveys. Being able to easily extract third party data about your users would help you better understand your customers and drive more revenue through upsells and targeted marketing.
- If you sell to consumers, you don't offer an easy one-click signup option through social identity providers.
- You've faced performance concerns as you increased your user base.

B2E

- You need to manage different authorization and access levels for your employees.
- You need to be able to provision and deprovision users easily when employees join or leave your company.

Business Case for Purchasing an Identity Management Solution

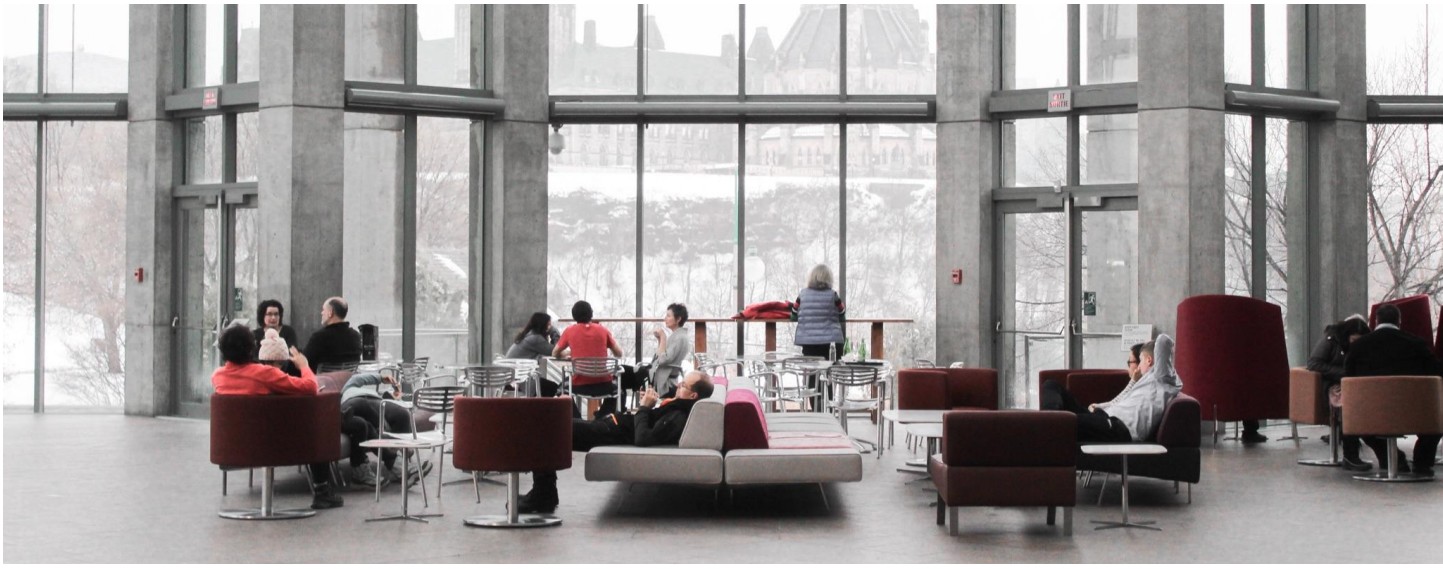
There are many compelling reasons to purchase identity management for all use cases, including B2B, B2C and B2E. A few examples are as follows:

All Use Cases

Reduction in engineering costs: Implementing a third party identity management solution is straightforward and enabling powerful features can be as easy as flipping a switch. Hundreds—if not thousands—of valuable development hours can go back to writing business logic instead of being spent building authentication. Lots of time dedicated to testing and security for authentication can also be returned to core app work. Integrating and mapping identity providers is time-consuming and can be painful. With an IAM solution, these integrations are already built and provided. An IAM should also offer SDKs for popular development stacks, further reducing additional coding needed to integrate the authentication system. A company's engineering team can focus on configuration rather than coding and customizing.

Increased security: Storing data with a third-party identity management solution strengthens security. IAM solutions adhere to security compliance policies and certifications. A solution takes on the responsibilities of keeping user data stored and transported securely. In addition, an IAM solution provides federated identity so that users don't engage in bad practices like reusing the same password to avoid having to remember multiple login credentials.

Improved compliance: Under the Personal Information Protection and Electronic Documents Act (PIPEDA), it's essential to limit access to stored personal information. An identity management solution provides better control of access permissions and, therefore, improved compliance with the legislation.



B2B

Increased enterprise adoption: An identity management solution offers robust Enterprise Federation, enabling enterprise connections such as Microsoft Active Directory, LDAP, ADFS, SAML, Google Apps, and more. Enterprise federation increases adoption by companies already using those technologies by allowing users to log in with their existing enterprise credentials. With single sign-on, there's no need for users to remember additional usernames or passwords. This improves ease of access and reduces churn.

Increased enterprise revenue: An identity management solution ensures that an app can support any type of Enterprise Federation customers may request. It also ensures that security requirements are met, thus reducing costs. Potential enterprise customers with existing credentials can authenticate with the same login. This helps generate revenue from enterprise customers as well as reduces friction for users.

Reduction in sales cycle/onboarding: Federated Identity allows companies to use their own credentials with a product or service while ensuring security requirements are fulfilled. This promotes faster sales cycles and customer onboarding. There is no need to introduce customers to a new, unfamiliar login or make them remember another password. They can use their enterprise credentials to have single sign-on across all properties.

B2C

Increased consumer adoption: By providing a unified, user-friendly login box for customers, identity management provides a consistent, frictionless signup and login experience across all applications regardless of browser or device. An identity management solution can gather more data about users. In turn, companies can utilize data to effectively drive adoption and upsell opportunities. A solution that provides an intuitive login box for optimized signup and login rates can also reduce the need for design and marketing resources. A third-party solution is built to scale to as many authentication requests as needed to maintain high performance and availability.

B2E

Third party SSO: An IAM solution provides SSO, which allows users to sign into multiple third parties with one login. Regardless of cloud or on-premises apps, SSO allows users to log in once and access any app without being prompted a second time for credentials. SSO can be utilized to authenticate apps such as ERP, Salesforce, Workday, Office 365, and more.

Management of authorization levels: An identity management solution provides the means to easily control different access levels for users. Privileges can be assigned and changed as employees join a company or are promoted. Users can also be deprovisioned, revoking all access and permissions.

Top Considerations for Evaluating an IAM Solution

There are several factors you should consider carefully when selecting an identity management solution for your business.

Deployment options: Look for the option to host anywhere. Your identity management solution should have the option to be deployed to the solution's cloud, your cloud, or your own data centre.

Ease of integration: One of the many advantages to using an IAM solution is to cut down on development time. 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: A good identity management solution should support virtually all popular sources of identity. For employees, this includes Microsoft Active Directory, ADFS, Office 365, Google Apps and SAML solutions. For consumers, this includes support for any custom database, social identity providers (like Google, Twitter, Facebook etc.) and passwordless solutions such as SMS, email, and Touch ID.

Extensibility: Your business does not remain static, therefore your identity management shouldn't either. Your IAM should allow you to easily customize the authentication and authorization pipeline. Ideally you should be able to customize the product to your needs right in the dashboard without needing to contact support or purchase a custom package. Your IAM solution should also allow you to extend its functionality, such as importing/exporting user data, easy integrations with additional apps, authorization, or executing custom scripts to extend the functionality of the base product.

Best-in-class security features: Your IAM selection should be peer reviewed by international security experts and comply with standards such as SAML, OAuth, WS-Federation, and certifications like OpenID Connect, SOC2, HIPAA, etc. Check for important features to protect against attack threats and compromised data, such as breached password detection and brute force protection.

Ease of migration: Moving to and from your identity management solution should be supported and unrestricted. Make sure there is no vendor lock-in that may inhibit migrating users out of the system in the future. The solution should also connect to any user store that you already use and shouldn't require users to manually reset their passwords when migrating to the new solution.

Fast support from security experts / customer service: Your IAM's customer support team should have a team of experts ready to assist with any challenge 24 hours per day. The team should also include senior engineers with extensive practical experience implementing IAM solutions.

Case Studies from Different Industries

Building trust with millions of home security customers

ecobee has been providing smart home solutions to Canadians since 2007. When it recently expanded into the home security space, ecobee needed a rock-solid identity and access management system. Customers were now entrusting the company with a new set of data — video from their homes.

The company chose Auth0 because it offers “the whole package,” said Jordan Christensen, VP of Technology. It was essential to implement multi-factor authentication (MFA). “We’ve really relied on the rules and custom database capabilities to do things like enforce a requirement for MFA for anyone who has a camera in their home.”

Having Auth0 handle authentication has saved ecobee time and resources, and Christensen estimates it would have taken three or four engineers 18 months to build a comparable solution. But the savings go beyond up-front costs.

“It’s the security posturing we would have to have and the expertise we would need to run a system like that in-house,” Christensen explains. Ultimately, we’re not only buying the Auth0 service, we’re buying the expertise. And that’s been a huge win for us too.”

Driving Growth with Unified Identity Management

With over 170,000 employees across more than 100 countries including Canada, Schneider Electric, a global leader in energy management and automation, needed an identity management strategy that could scale with the company's next phase of growth while maximizing efficient use of resources. Schneider Electric's primary need when choosing IAM was a single sign-on system to create a unified authentication process. This way, they could use the same identities and credentials for all of the company's diverse systems and applications.

A cost-benefit analysis quickly proved that Schneider Electric would be better off leveraging its employee resources to deliver on core business goals and objectives. Using Auth0 for identity management could break down barriers within the corporation and solve challenging identity integration problems. Auth0 also provided a robust and flexible solution that was developer-focused and easy to integrate. The platform was web and mobile friendly, supported open standards, and offered robust features and future-proofing with broad identity provider support and easy migration.

Once Auth0 was selected and implemented, many benefits were realized. Using Auth0's identity management solution eliminated extra development work. This freed up more resources for IT innovation.

Time to market was faster and the system benefited from increased security and best practices. Auth0 also provided fast, thorough reactions to vulnerabilities.

> "Before any news sites reported on last year's Heartbleed zero day vulnerability, Auth0 emailed us to alert us to the situation. There was already a patch to eliminate the Heartbleed threat from Auth0's systems, followed by a confirmation email that Auth0 had already installed this patch on the Schneider Electric instance of Auth0's service," said Berard. "Auth0 helps our platform team look really good. In this scenario, not only had the security issue been patched, our IT team was able to save valuable time by leveraging the detailed steps on how the issues were mitigated to report directly to our internal team. What's more, Auth0 cycled the certificates, something else that would have been very labor intensive for the team to do on its own."

"With the Auth0 platform, we can plan and integrate identity architecture early to save critical time and ensure a secure system is in place when a project gets off the ground."

Conclusion

Managing modern identity is a challenging task. Keeping up with evolving standards, best practices, and constantly patching security bugs takes time and money away from the core business. By considering features that grow with your organization's needs and how other companies have successfully evaluated and implemented their own solutions, you can reap the benefits of an identity management solution.

In summary, your organization can transform your IAM from a critical point of risk and a potential blocker for business, into a system that not only enables your organization's ability to drive revenue but actually enhances it. With Auth0, you can implement IAM in days, not months, future proofing your organization by utilizing the easiest, most comprehensive and extensible IAM solution availab

Resources

For more examples of how other companies evaluated Auth0, please visit auth0.com/customers or contact sales@auth0.com

You can try Auth0 for free; setup only takes minutes. You can also view the Auth0 pricing page here: auth0.com/pricing

You can review Auth0 Case Studies or learn more about Auth0's enterprise solution. Auth0 also provides robust documentation for APIs, SDKs, quickstarts, and much more. The blog at auth0.com/blog is a source of all the latest news and tutorials on emerging and popular technologies and security topics.

Footnotes:

[1] https://www.cira.ca/cybersecurity-report-2020

[2] https://www.insurancebusinessmag.com/ca/news/cyber/report-canada-has-the-third-highest-average-cost-for-data-breaches-229320.aspx

We Can Help

Auth0 can help you manage identity for your users. As security experts, we have built an identity-as-a-service (IDaaS) platform designed with state of the art security in mind. Over 80,000 developers in 167 countries trust Auth0 as their identity management solution.

Auth0's Enterprise identity management platform provides customers many features and benefits, including:

- The ability to configure and implement enterprise federation and single sign-on requiring only basic configuration and no coding.
- Auth0's supported enterprise connections include Active Directory, LDAP, ADFS, SAML, Google Apps, and more.
- Auth0 supports social connections with all major providers including LinkedIn, Facebook, Twitter, Google, and many more.
- Auth0 provides traditional username and password authentication, via either the Auth0 DB or any Custom DB, with enhanced security features such as multi-factor authentication, breached password detection, brute force attack protection, and anomaly detection.
- Users can be migrated from existing systems painlessly with no forced password resets.
- Auth0 provides methods to audit and view identity-based analytics to ensure organizational compliance and upsell opportunities.
- Companies can easily manage user access with fine-grained permissions and powerful, custom rules.
- Auth0's delegated administration allows companies to administer granular access, visibility, and user management to customers.

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 **https://auth0.com** or follow **@auth0** on Twitter.