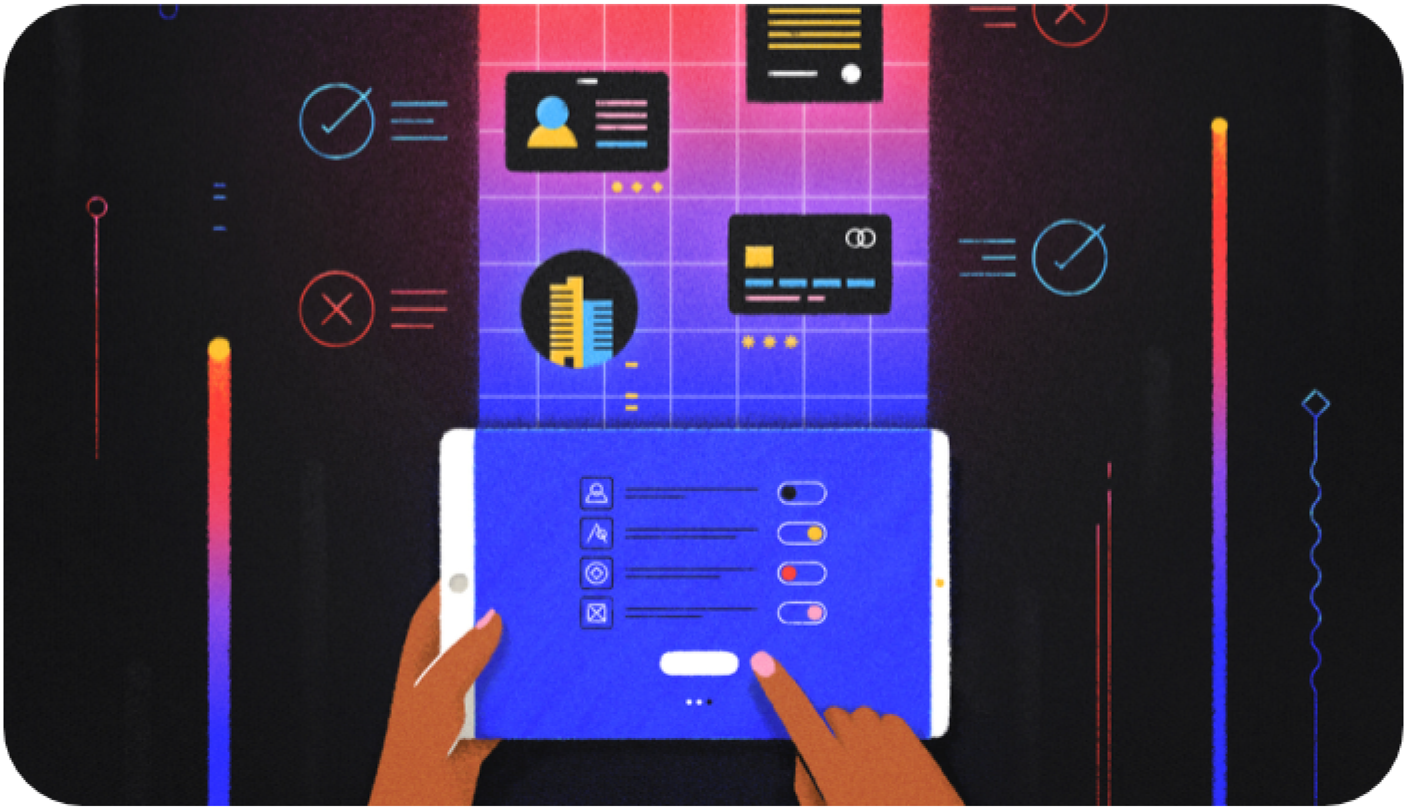
Auth0

Build vs. Buy for Retail

The Retailer's Guide to CIAM + IAM

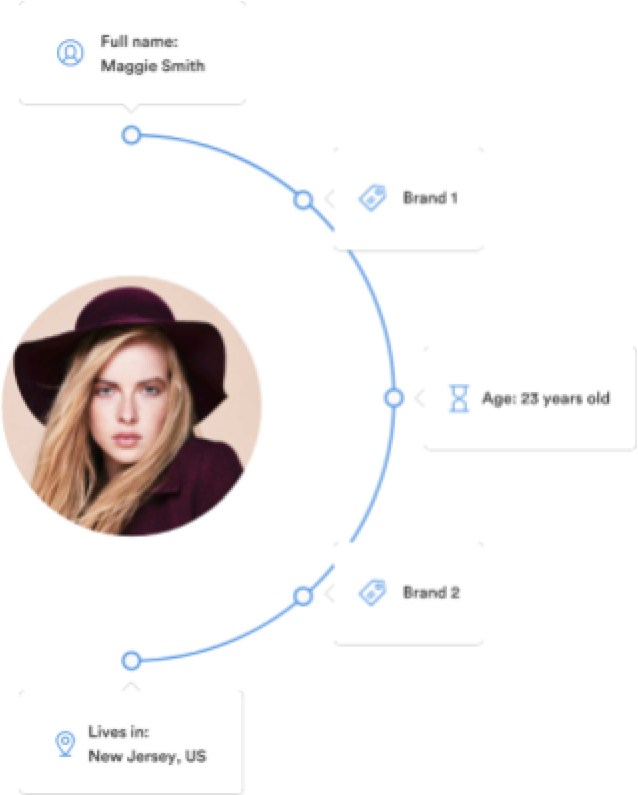


Contents

What Is CIAM + Identity Management (IAM)?

Customer Identity and Access Management (CIAM) is how companies give their end users access to their digital properties as well as how they govern, collect, analyze, and securely store data for those users.

CIAM sits at the intersection of security, customer experience, and analytics. In retail, this means providing an easy, frictionless way for users to create an account, log in, and make purchases. Protecting sensitive data from malicious intrusion and taking steps to prevent data breaches is also central to a sound security policy and compliance with data privacy laws. And compiling user data into a single source of truth is essential for understanding your customers.



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

The right CIAM + IAM solution provides benefits for retail organizations including distinct and specialized features to serve business partners, customers, and employees.

- **Customers:** Providing social authentication to consumers through Facebook, Google, or other social media identity providers.
- **Business partners:** Providing federated identity management to retail business partners, to access systems for supply chain logistics, customer resource management, inventory management, and more.
- **Employees:** Providing Single Sign-On to its employees.

We'll cover identity solution (CIAM + IAM) benefits with regard to all three retail business cases in this paper. An identity solution 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 into 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.

CIAM & 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. So what holds us back from building security systems that are simple, straightforward, and easy to use?

> **Multi-Factor Authentication utilizes separate stages of authentication to provide two (or more) steps to log in. Passwordless can use SMS, magic links, or even biometrics like fingerprints 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.

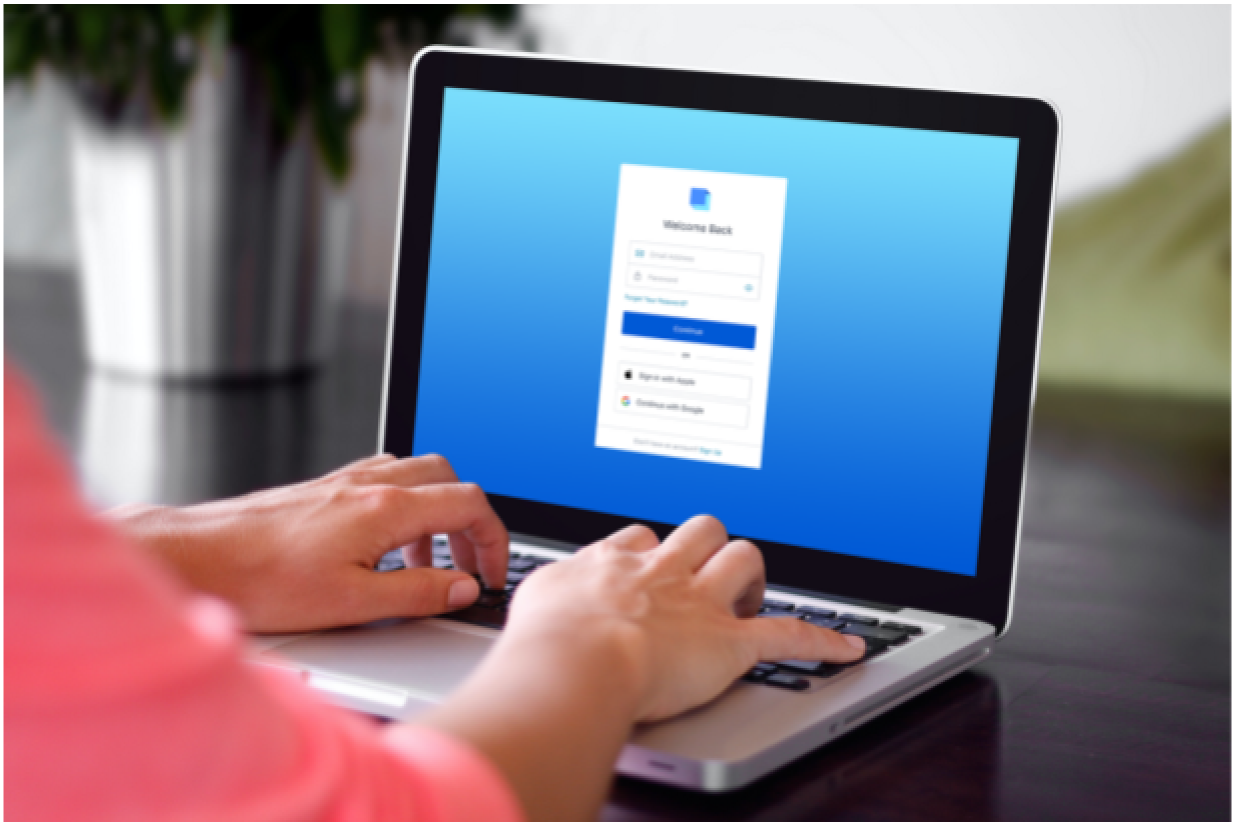
Another trend driving identity solution adoption is the need for users to access apps from anywhere on any device. With the expansion of personal computing, companies need the ability to provide secure access to their users regardless of where they are or what device they may be using. Identity management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

For retail companies, social authentication is another trend driving the adoption of CIAM solutions. Potential customers use a variety of social media on a daily basis. CIAM 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 Solution

Retail Use Cases for All Users

- You need a standards-based solution, such as OpenID Connect, SAML, WS-Federation, and/or OAuth.
- You have users who 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.



Retail Use Cases For Customers

- Your main source of user data comes from directly asking users on account registration forms. Being able to easily extract third-party data about your customers would help you better understand their needs and drive more sales and personalized marketing.
- You don't offer an easy one-click signup option through social identity providers.
- You've faced performance concerns as you've increased your customer base.
- Your support teams spend time on password reset requests.
- You have multiple retail brands that all use separate login portals.

Retail Use Cases For Business Partners

- Your business partners need to use enterprise credentials to log into your organization's applications. 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 partners' help desks.

Retail Use Cases For Employees

- 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.

The Retailer’s Business Case for Purchasing an Identity Solution

> There are many compelling reasons to purchase an identity solution for all use cases, including business partners, customers, and employees. A few examples are as follows:

Retail Use Cases for All Users

Reduction in engineering costs: Implementing a third-party identity 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 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 identity solution, these integrations are already built and provided. The platform should also offer SDKs for popular development stacks, further reducing additional coding needed to integrate the authentication system. A company’s engineering team can then focus on configuration rather than coding and customizing.

Increased security: Storing data with a third-party identity solution strengthens security. identity 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 Identity 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).

Retail Use Cases for Customers

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

Retail Use Cases for Business Partners

Increased partner adoption: An identity 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 partner 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 your business partner users to remember additional usernames or passwords. This improves ease of access and security.

Reduction in partner onboarding time: Federated identity allows partner companies to use their own credentials with a product or service while ensuring security requirements are fulfilled. This promotes faster onboarding cycles. There is no need to introduce partner users to a new, unfamiliar login or make them remember another password. They can use their enterprise credentials to have Single Sign-On for the appropriate applications and at the right level of access.

Retail Use Cases for Employees

Third-party SSO: An identity solution provides Single Sign-On, which allows retail employees to sign into multiple third parties with one login. Regardless of cloud or on-premises apps, SSO allows employees 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 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 Identity Solution

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

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

Ease of integration: One of the many advantages of using an identity solution is cutting 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 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 solution 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 identity 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 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 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 identity solution's customer support team should have experts ready to assist with any challenge 24 hours a day. The team should also include senior engineers with extensive practical experience in implementing identity solutions.

Case Studies for Retail Companies

WineDirect Supports 1,800 Wineries, Processes 5M Orders Yearly

WineDirect is the international leader in the direct-to-consumer (DTC) wine industry. WineDirect processes millions of orders each year across the U.S., Canada, and Australia. Headquartered deep in the heart of California wine country with its technology operations based out of Vancouver, BC, WineDirect provides commerce, marketing, and logistics solutions to help wineries grow their businesses. In an era of rapidly increasing consumer expectations, our unique end-to-end platform enables wineries to provide next-level service and create customer relationships that last.

With 1,800 wineries counted among WineDirect's members, Single Sign On (SSO) quickly became a priority. The company needed a solution that would allow customers at different levels of technology to easily integrate with the WineDirect platform. They also needed a scalable solution that would allow them to transition to a microservice-based approach as the business continued to grow.

Before turning to Auth0, WineDirect experimented with the idea of developing SSO technology in-house — but they quickly ran into questions they couldn't answer.

"We were running into issues in production with managing JWT tokens and managing new services overtime...figuring out how to manage expiry. Other questions we had were, 'Do we store it in the cookies in the browser? Do we store it on the server? Do we session cache it?' All these questions that Auth0 just comes in and answers for you," said Klaassen. "It'd probably take at least two full-time developers to initially build that and continue to maintain it, depending on how quickly we scale."

Klaassen explains that hiring a senior and a junior developer to oversee the technology would be cost prohibitive in the long term. Instead, Auth0 was able to quickly and seamlessly step in and provide a comprehensive SSO solution.

"Everyone thinks they need to reinvent the wheel with authentication until they realize that companies out there or experts in the field are providing the tools to be able to do it really quickly. Within a week we had a working prototype within Auth0."
- Lucas Klaassen, Full Stack Web Developer

Thanks to the SSO authentication services provided by Auth0, WineDirect has been able to identify the customers using each of its services and allocate resources across multiple applications — all under one login umbrella. Read the full case study.

How THE ICONIC Manages Massive User Growth

THE ICONIC, Australia and New Zealand's leading online fashion and sports retailer, started in 2011 with a tiny team but a big idea: to bring a tech-driven, customer-first business model to online fashion retail. Soon after, THE ICONIC became a brand with a reputation matching its name. Today, the company boasts over 13 million visits per month, and is the most downloaded fashion app in Australia and New Zealand.

THE ICONIC credits its success to its DIY ethos and its relentless focus on customer experience. But that success posed a challenge to THE ICONIC when its user base rapidly expanded, and its in-house identity management system needed support to keep up with the growing demand. THE ICONIC needed an authentication solution that protected customer data, integrated with their legacy applications, and didn't sacrifice UX. And they needed it quickly.

In the early days, building identity in-house didn’t seem like a big deal. “It was a simple application,” Piers Warmers, Principal Software Engineer, recalls. But rapid growth meant THE ICONIC had an even larger security responsibility, in the form of millions of customer names, addresses, and credit card data. “At one stage, we were yelling and screaming and cheering that we placed 1,000 orders, and suddenly you blink, and you're sitting on millions of credentials and thinking, wow, this is a very different landscape,” Warmers says.

With a constantly evolving landscape of digital threats, security is of central importance to THE ICONIC. They gravitated toward Auth0 for features that would enhance security without compromising the customer experience. “For us, it was really about protecting our customers,” Warmers says.

To keep data secure, THE ICONIC is making use of Auth0’s credential stuffing features like IP address monitoring, which protects against brute force attacks. They’re also excited about conditional multi-factor authentication (MFA) to protect against malicious behavior without sacrificing CX. As Warmers explains, “for us, it's also about being able to provide a very rich customer experience.”

By delegating identity to Auth0, Warmers and his team estimate they saved over 5,000 hours of developer time on implementation, plus an ongoing 70 hours per month on maintenance.

Today, the company’s leadership recognizes that partnering for identity doesn’t mean they’re compromising their DIY spirit; in fact, it allows the company to focus on continuing that DIY approach. As Warmers says, “The lesson that we've learned is that Auth0 is there to provide identity services and give us more time building the products we want to be building.” Read the full case study.

Conclusion

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

In summary, your organization can transform your CIAM and 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 identity in days, not months, supporting your organization by utilizing the easiest, most comprehensive and extensible identity solution available.

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 solution.

Auth0's enterprise identity platform provides customers with 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.
- With Auth0, it takes less than 30 minutes for a developer to set up robust and customizable identity management for any technology stack.

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. You can also learn more about our retail specific solutions at auth0.com/retail.

The blog at auth0.com/blog is a source of all the latest news and tutorials on emerging and popular technologies and security topics.

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 billions of 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.