Whitepaper

# Build vs. buy

Customer Identity and Access Management.

# Contents

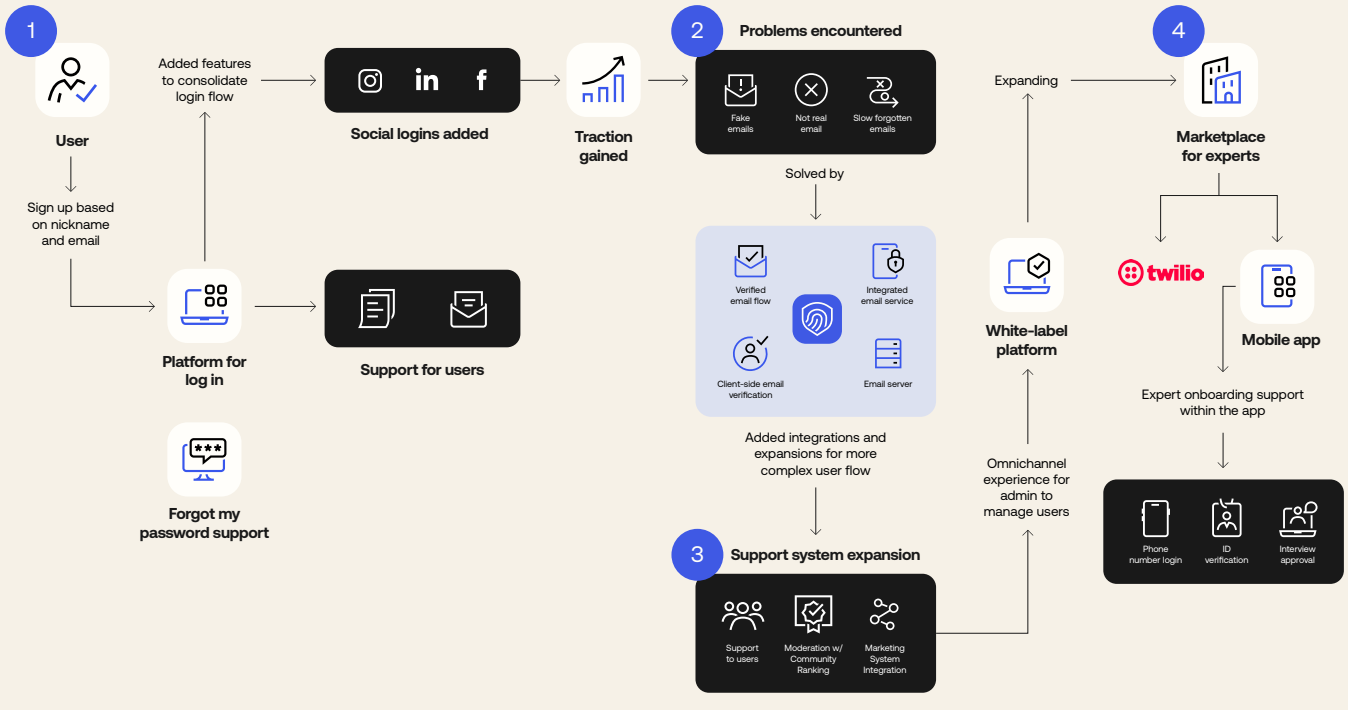
# Getting Customer Identity right is hard

Every team building a web or mobile app faces the same dilemma with every new piece of functionality: build in-house or use out-of-the-box services to make the job easier and faster.

Our developers can handle Customer Identity. It's a login box. How hard could it be?

But Customer Identity and Access Management (CIAM) is so much more than just the login box. As businesses grow and continue to add features, it's possible the complexity of maintaining a robust DIY CIAM system can become a larger drain on resources than anticipated. Developer hours are a precious commodity, and time spent maintaining DIY Identity, security, and privacy compliance is time taken away from core business innovation.

**Building it yourself is even harder...**



So how do you drive innovation and maximize developer time without compromising security, launch dates, or budget?

A pre-built CIAM system is one such solution. A digital Identity layer comprised of APIs, SDKs, and out-of-the-box customizable components can serve as building blocks to increase speed-to-market, lower development costs, and focus in-house developers on the core features of the application. Customer-facing applications require a common set of fundamental features related to authentication, authorization, and user management. Applications need to support common workflows such as account creation, user login, password reset, account recovery, and multi-factor authentication (MFA) enrollment. Additionally, applications need to accommodate different levels of access depending upon the user.

This whitepaper discusses the key considerations when making a build vs. buy decision and the advantages of a pre-built solution.

> "[Okta] is one of the things that I can put in my toolkit to say: Hey we're gonna move faster because we have this Identity component nailed."
>
> **Scott Howitt**
> CISO, MGM Resorts International

## Lower the total cost of ownership (TCO) of application development

Identity management is one of the highest-risk areas for cost overruns, because feature and system complexity are so often underestimated and in a state of constant evolution. A home-grown approach introduces greater uncertainty into the equation and costs increase significantly when internal teams get sidetracked on building deep user features or discover that their requirements have transformed due to a changing landscape. Teams may still deliver on time, but only with the help of costly contract resources. When you offload Identity to a trusted provider, you help ensure the development team delivers the full scope of your project on budget.

**Example TCO reduction of application development**[1]

| 3 | x | 6 | x | $200k | x | 90% | = | $270k |
|---|---|---|---|---|---|---|---|---|
| Developers | | Month identity timeline | | Fully loaded salary | | Improvement | | **Reduction to TCO** |

> "Things in the Identity space change almost by the hour, and we need a technology partner that can keep up with that pace of change on a daily basis."
>
> **Eash Sundaram**
> EVP Innovation, Chief Digital & Technology Officer, JetBlue Airways

[1] Common Google-esque calculation of the value of an engineer for companies where the technology is the primary generator of revenue. Here, we are calculating the average annual revenue contribution of an engineer multiplied by the number of engineers that are removed from the engineering pool to deliver an Identity layer.

**Focus resources on core application functionality**
Your success depends upon how well you execute the core product features that make your application useful to end users. A modern Identity layer frees your team to remain laser-focused on functionality that drives revenue and customer engagement; and allows your developers to more quickly move onto the second, third, or fourth app that your customers are demanding.

**Reduce the risk of a security and compliance breach**
When was the last time your team updated their password hashing algorithm? User data and PII are the most common targets of attacks, yet the average lifespan of an effective encryption algorithm is 18 months. Protecting users often falls by the wayside in favor of requirements that drive growth or revenue. Plus, a secure Identity service requires your team to have specialized knowledge—and time—to address vulnerabilities at every layer of infrastructure, from the operating system, database, and transport layer, to the application stack and code vulnerabilities. Because development teams rarely have this level of security expertise on staff, they may not know their user security has failed until sensitive data is already vulnerable. And they often aren't aware of security developments, like when an algorithm is compromised, or an attack vector is discovered.

A well-chosen Identity management service safeguards your user data from attackers because the team that built it is comprised of experts focused on advanced security to cover Identity and access attack vectors. Security measures include powerful encryption, API security, advanced firewall protection, and robust data management and system access procedures. These same security measures and infrastructure enable your teams to be compliant with geographic and vertical-specific regulations such as HIPAA, FedRamp and GDPR.

> “National Bank of Canada services millions of clients in hundreds of branches across Canada. As an organization, we have clear objectives, one of which is to simplify the customer experience. Okta's smart authentication and contextual capabilities enable us to give our clients a seamless, secure online experience.”
>
> **Rish Tandon**
> CTO, Heal

**Keep developers motivated**

Although Identity is important to the success of a customer-facing application, not all developers enjoy building Identity and security infrastructure. Although it’s a high-risk area and often fraught with complexity, user management is sometimes perceived as mundane, and many developers would rather work on features tied to core product differentiation and cutting-edge systems. The high overhead associated with implementing user security can be especially demotivating—there is a great deal of risk, and much conflicting guidance. On the other hand, many developers perceive working with modern REST-JSON API services as interesting and accessible.

**Deliver high scalability and reliability**

When user management fails, users are locked out. If the login experience fails due to a lapse in availability, end users won't know or care why—but their perception of your organization and your brand will suffer. The level of consumer load is unpredictable, and marketing departments do not always know or share when a promotion will drive an influx of users. If you decide to manage this yourself, you have to be confident in your team's ability to offer multiple lines of availability, and scale easily as the user base grows. You must be prepared to provide double or triple redundancy in your datacenter or in collaboration with an infrastructure-as-a-service provider. You will need to provide for seamless upgrades and maintenance to ensure uninterrupted service. Companies who take on these nontrivial responsibilities often find the maintenance overhead unmanageable. An outside user management service provider can completely remove the operational headaches.

> "Facilitating integration across the ecosystem, making sure Identity persists across systems, and having Identity be the central way we're relating to the customer, with a high degree of reliability and availability—that was really important to us."
>
> **James Fairweather**
> Senior Vice President of E-Commerce and Technology, Pitney

# Benefits of purchasing Customer Identity and Access Management

There are compelling reasons to purchase Identity management rather than build it:

**Increase revenue through faster time to market for apps**
Customer needs can change on a whim and organizations today need to be agile enough to capitalize on market opportunities or risk revenue. The right Customer Identity solution can deliver an Identity layer for secure customer experiences so your development teams don't have to reinvent the wheel when it comes to authentication, authorization, and user management, and can instead focus on building the features that differentiate your app and get them into the hands of consumers. And speaking of revenue—it's as much about preserving it as it is generating it—so scalability is also a factor here. Resource-intensive actions like authentication, password encryption, and search need to keep pace with user demand during peak periods.

**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. Time that was dedicated to testing and security for authentication can be returned to core app work. Integrating and mapping Identity providers is time-consuming and can be painful. With the right third-party solution, these integrations are already built and provided. An out-of-the-box CIAM solution 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**
When was the last time your team updated their password hashing algorithm? User data and PII are the most common targets of attacks. The average lifespan of an effective encryption algorithm is 18 months, but protecting users often falls by the wayside in favor of requirements that drive growth or revenue. A CIAM solution takes on the responsibilities of keeping user data stored and transported securely, and adheres to regional compliance policies and certifications. In addition, a CIAM 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.

## Case studies from different industries

**Schneider Electric - driving growth with unified Identity management**
With over 170,000 employees across more than 100 countries, 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 CIAM 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. Third-party Identity management could break down barriers within the corporation and solve challenging Identity integration problems. The Okta Customer Identity Cloud (formerly known as 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 Okta CIC was selected and implemented, many benefits were realized. Using its 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. Okta CIC also provided fast, thorough reactions to vulnerabilities.

"Before any news sites reported on last year's Heartbleed zero day vulnerability, Auth0 [now Okta Customer Identity Cloud], 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.

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."

**Stephen Berard**
Senior Global Software Architect, Schneider Electric

**Bluetooth - unifying Identity across on-premise and cloud apps**
Bluetooth, a global leader in wireless technology, had a growing ecosystem that presented various challenges. The business, which started as a single application, swiftly grew to multiple different apps. Apps developed in-house as well as third-party SaaS apps (Sharepoint, ServiceNow, SiteCore) all required different authentication credentials. Bluetooth's existing homegrown solution was forms-based and used username and password credentials. This platform was not suited for federated Identity. The company needed a modern Identity solution with single sign-on to support all of their homegrown and third-party SaaS apps. The solution had to be implemented while keeping the existing platform operating with a future path for full migration. User roles and access were also vital to ensure proper levels of access to confidential documents.

Third-party Identity fit the bill. It was easy to implement and allowed the team to add SSO and modern authentication. The legacy system was kept intact while a migration plan was implemented and carried out. It took only days to implement versus the months needed to implement an in-house platform. Top-notch documentation with detailed code samples covered introductory and advanced topics, allowing Bluetooth SIG engineers to quickly understand and implement their modern Identity solution. Bluetooth worked with developer success engineers to develop a proof of concept to jointly showcase the platform's capabilities. Support response times were short with rapid turnaround.

# Conclusion

**Innovation without compromise**
Managing modern Identity is challenging. 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 understanding how other companies have successfully evaluated and implemented their own solutions, you can reap the benefits of an Identity management solution – without compromising on security, user experience, or increasing developer hours.

Your organization can transform your CIAM 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 Okta Customer Identity Cloud, you can implement CIAM in days instead of months, future-proofing your organization by utilizing the easiest, most comprehensive and extensible CIAM solution available.

# How we can help

Okta 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 Okta Customer Identity Cloud as their Identity management solution.

Among the features and benefits:

- The ability to configure and implement enterprise federation and single sign-on requiring only basic configuration and no coding.
- Enterprise connections include Active Directory, LDAP, ADFS, SAML, Google Apps, and more.
- Social connections with all major providers including LinkedIn, Facebook, Twitter, Google, and many more.
- Traditional username and password authentication, via either the Auth0 DB or any Custom DB, with enhanced security features such as multifactor authentication, breached password detection, brute force attack protection, and anomaly detection.
- Users can be migrated from existing systems painlessly with no forced password resets.
- 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.
- Delegated administration allows companies to administer granular access, visibility, and user management to customers.
- With Okta Customer Identity Cloud 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 Okta Customer Identity Cloud, previously known as Auth0, please visit our customers' page, our pricing page or contact sales.