Top Developer Benefits of Modern CIAM

Development and IT teams are under intense pressure to build digital experiences that disrupt their industry or differentiate their business. This is no easy feat, especially since expectations from both executives and end users are increasingly demanding. That's exacerbated by the fact that today's customer experience (CX) environments are extremely complex—they span more apps, brands, geographies, devices, users, and privacy regulations than ever before.

As the "front door" to most mobile apps and web-based services, identity is the lynchpin of a modern CX. Yet, in the rush to get new apps out the door, many development organizations underestimate the demands of homegrown or code-heavy customer identity and access management (CIAM) solutions. In particular, a constantly evolving threat landscape and corresponding security requirements add risks that place a huge maintenance burden on app developers.

The more digital services you build, the greater your opportunity if you can bring it all together in a seamless omni-channel CX. By doing so, you'll delight your customers with easy access to everything your brand offers using just one set of credentials. Unfortunately, pro-code and all-code approaches require extensive developer effort and add barriers to this type of strategy by introducing technical debt and locking you in to inflexible solutions.

3 ways a low-code identity platform adds value for developers

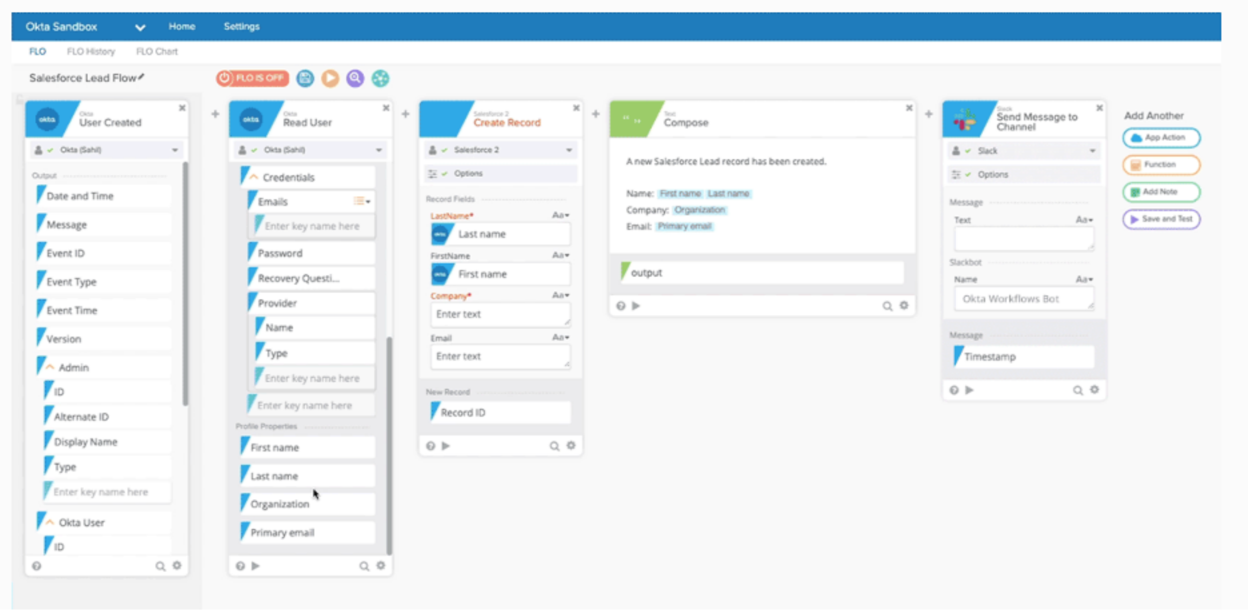
Third-party CIAM platforms free you up to spend less time coding login pages and more time developing differentiated app features you can be proud of. However, it's important to realize that all approaches to CIAM are not equal. If your team is thinking about adopting a dedicated identity service to better protect your customer apps, ask whether it will truly help you do more with less code, reduce maintenance complexity, and avoid hidden costs. Avoid tools that might lead to data breaches, lost business opportunities, or developer inefficiency from having to augment a basic identity toolkit.

Out-of-the-box building blocks let you do more with less code

Custom code slows product innovation and increases cost of ownership over the long term, so it's a best practice to write as few lines of code as possible when it comes to your identity stack. Of course, the reality is that most customer identity platforms require at least some customization to work for your applications. Be aware that the more code you add, the greater your risk of an unintended vulnerability, lower developer productivity, and slower time-to-market.

By leveraging a modern CIAM platform like Okta for authentication, authorization, and user management, you'll minimize the amount of code and time needed for tasks like:

- Password storage and security
- User directories
- Profiles and groups
- Administration interfaces
- Registration, sign-in, and account recovery workflows
- Provisioning
- MFA factor support
- Security monitoring
- Compliance reporting
- Supporting DevOps requirements for high availability
- Help desk support for account issues like onboarding and password resets



A new Salesforce Lead record has been created.

Name: First name Last name
Company: Organization
Email: Primary email

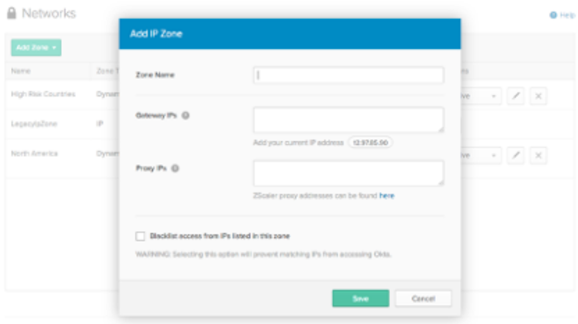
Certain CIAM toolkits alleviate this workload for small, single projects. But very little of the code you write for them is reusable when your needs or ecosystem grows. As you launch more apps or products, building security policies again and again becomes risky. This is because as your requirements change, improvements you make typically get applied to some, but not all, systems. Moreover, you must design, build, test, and release more code—reinventing the wheel by building additional login pages, password reset flows, and more for each app in your portfolio (and learning all the security practices and processes behind each). Of course, this takes developers away from focusing on value-add projects, hence the value of a low-code third-party identity platform increases as your number of CX projects grows.

Reduced maintenance complexity frees time for strategic projects

Even if you save some time in initial project stages with a development-heavy customer identity platform, you'll need to enhance, maintain, and secure your identity components in perpetuity. This frequently involves unplanned efforts around creating and managing:

- IP whitelists
- Per-app or per-group MFA policies
- New assurance factors
- Granular registration and login flows
- Dashboards for non-technical roles

For example, at some point you'll want to evolve your login flows so they increase protection at the right time, in order to minimize user friction. You'll also need mechanisms to share user data internally so you can support reporting, compliance, IT, help desk, and customer success requests. Each of these tasks entails identity-specific code that must be self-maintained with its own specific audits, troubleshooting, and redeployments—beyond your standard code management and deployment process for the overall app. By comparison, low-code platforms like Okta provide rules templates that are easily configurable, even by non-developers, so you won't have to waste time digging through spaghetti code



Add IP Zone

Zone Name

Gateway IPs

Add your current IP address 12.97.85.90

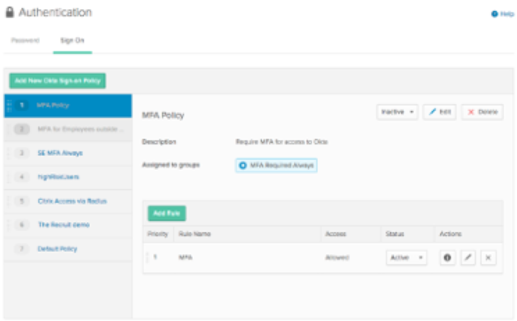
Proxy IPs

ZScaler proxy addresses can be found here

□ Blacklist access from IPs listed in this zone

WARNING: Selecting this option will prevent matching IPs from accessing Okta.

Admins can whitelist IPs via UI



MFA Policy

Description: Require MFA for access to Okta

Assigned to groups: MFA Required Always

Priority	Rule Name	Access	Status	Actions
1	MFA	Allowed	Active	

Policies can be managed centrally

In addition, unforeseen identity and security requirements might arise if your original developers move on to other projects. Software engineers experience one of the highest turnover rates of any sector at a whopping 21.7%, according to LinkedIn.[1] This means the rest of your team could be forced to delay other projects while figuring out how new logic impacts existing services built by former developers. Likely, you'll find yourself needing to rewrite source code and redeploy to make critical identity updates.

Teams are also caught off guard by the added vendor management burden associated with pro-code solutions, which need to work effectively alongside your DNS providers or dev tools such as Twillio, AppDynamics, Splunk, and SendGrid. Imagine if you could get out of the business of identity altogether, and spend that maintenance time on the core, business-driving functions of your app.

Enterprise-grade capabilities help avoid hidden costs

Average Application Iceberg

Custom Code
21%

Serious Vulnerabilities
26.7

Actually invoked library code across 27 libraries
8.5%

Unused library code across 30 libraries
70.5%

Vulnerabilities (CVE)
2.0

All of this cumulated developer inefficiency will be a massive drain on your team's limited resources. In fact, Stripe noted that global GDP loss due to poor use of engineering talent is $300 billion annually.[2] Keep in mind that even just one line of bad code also increases your risk, and the costs of a data breach are severe. In addition to the extensive technical cost of remediating a breach, 70% of customers abandon business dealings with a brand following a data breach, creating a major revenue impact.[3]

A proven solution that supports enterprise requirements for security, availability, and scalability will mitigate these kinds of problems and increase your ROI over the long run. Choose a platform that gives you the ability to adopt secure engineering practices—such as revoking access tokens as needed—and more easily attain compliance certifications.

And don't forget the opportunity cost of diverting your focus from improving other principal elements of your CX to focus on identity tasks. For example, if you're working on a project that's expected to bring in $50,000 in revenue per month, and it's delayed six months due to resource constraints, that's $300,000 of lost potential revenue to the business. Meanwhile, a competitor who launched earlier might already be in the market.

Unlock Innovation with Okta Customer Identity

Clearly, there are big benefits to be gained when you shift CIAM from being a development resource drain to a critical business enabler. By adding a secure identity service like Okta, you'll dramatically improve the speed with which you can deliver frictionless, rather than fragmented, experiences. Modern CIAM ensures more secure users, products, and services for happier customers, partners, and employees. At the same time, it gives your technology team greater agility and flexibility, so they can reduce costs and operational overhead by increasing automation and efficiency.

Okta alleviates these "Heavy Code" issues to unlock innovation

Frictionless experience

- Deliver a consistent experience across apps
- Simplify registration and authentication

Speed-to-market

- Meet project timeliness
- Maximize developer efficiency

Centralized management

- Centralize access management company-wide
- Give security team more control

Internet-scale security

- Prevent security breaches
- Meet compliance requirements

Okta's pre-built, admin-friendly UI and configurable policies allow you to centralize identity management and balance the requirements and skills of all your stakeholders. As a result, you'll greatly reduce your development burden as your apps' identity and security needs evolve, in turn unlocking even more innovation. For more information, visit developer.okta.com.

[1] LinkedIn, "These 3 Industries Have the Highest Talent Turnover Rates," March 2018
[2] Stripe, "The Developer Coefficient: A $300B Opportunity for Businesses," 2018
[3] Gemalto, "The State of IoT Security: Security Takes a Back Seat," 2017

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 8,400 organizations, including JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

Learn more at: www.okta.com