okta

Key Business Advantages of Alleviating the Identity Burden

Your teams are tasked with enabling world-class digital experiences that disrupt your industry or differentiate your business from its competition. However, this charter is becoming increasingly difficult as customer experience (CX) environments get more and more complex. Companies launch apps, acquire brands, expand to additional countries, and support more diverse devices and user types every day, although few are equipped to secure this complexity without introducing friction for their customers.

Although 86% of organizations expect the user experience (UX) to be their main competitive differentiator by 2021, only 40% currently have a customer identity initiative in place.[1] The virtual "front door" to your business, identity is the lynchpin for modern customer experiences like account registration, online shopping, and customer support. Yet, in the rush to get new apps out the door, many technology teams underestimate the demands of homegrown or code-heavy customer identity and access management (CIAM) solutions.

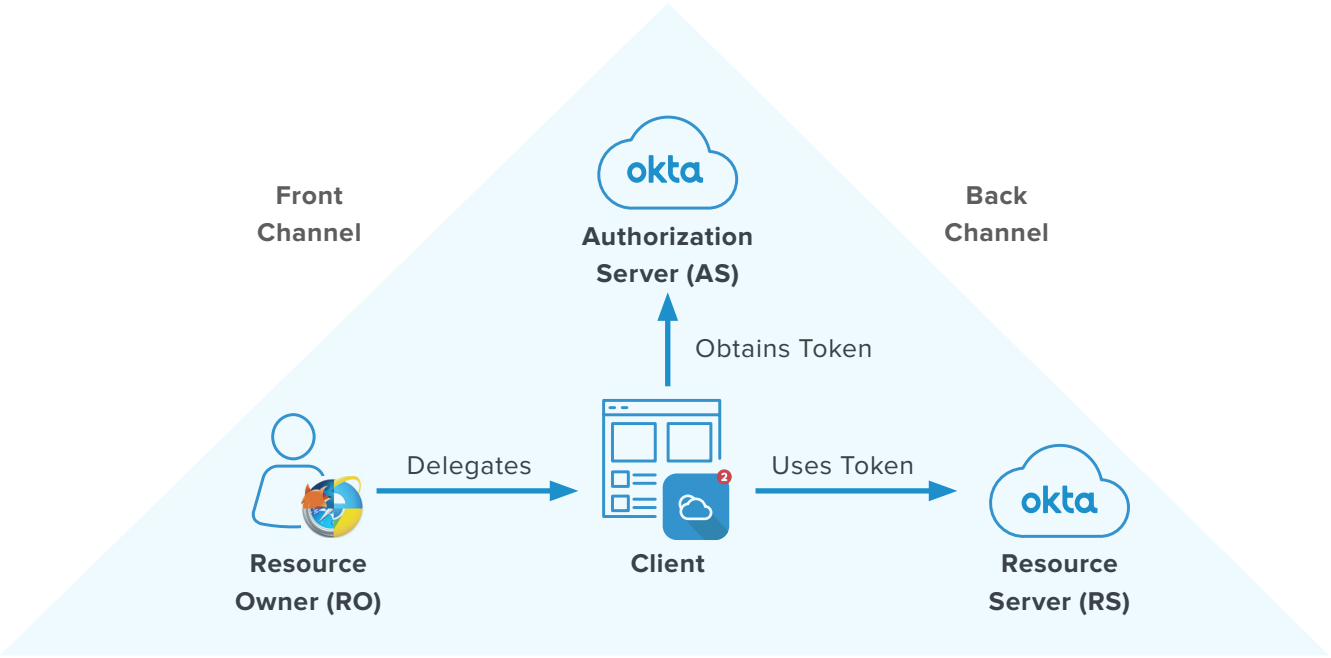
This is problematic because the threat landscape is constantly evolving, which leads to unpredictable vulnerabilities in your apps if you don't keep up with security innovations. And the more digital services you offer to customers, the more necessary it becomes to provide a seamless experience with one set of credentials. Unfortunately, pro-code and all-code approaches divert your valuable development resources away from revenue-driving projects and instead keep them immersed in the identity business.

Top 3 requirements for business-enabling CIAM

Third-party platforms can relieve some of these pressures, but it's important to realize that not all approaches to CIAM are created equal. The right solution turns identity into a business enabler, while the wrong choice introduces reliability, scalability, or security risks that can become a brand liability. With that in mind, there are three major questions every technology executive should ask themselves in order to evaluate whether their development team's approach to CIAM is sufficiently future-proof.

Does our identity solution create a frictionless CX?

Modern, best-in-class customer identity should enhance your digital offerings with a simple, clean CX that amplifies your brand. A bad login flow alienates customers quickly, so you need the flexibility to zero in on the perfect login policies and enrich them over time. This not only protects your brand, but has a real financial impact as well. In fact, companies with a well-designed user experience can double their visit-to-lead conversion rates.[2]



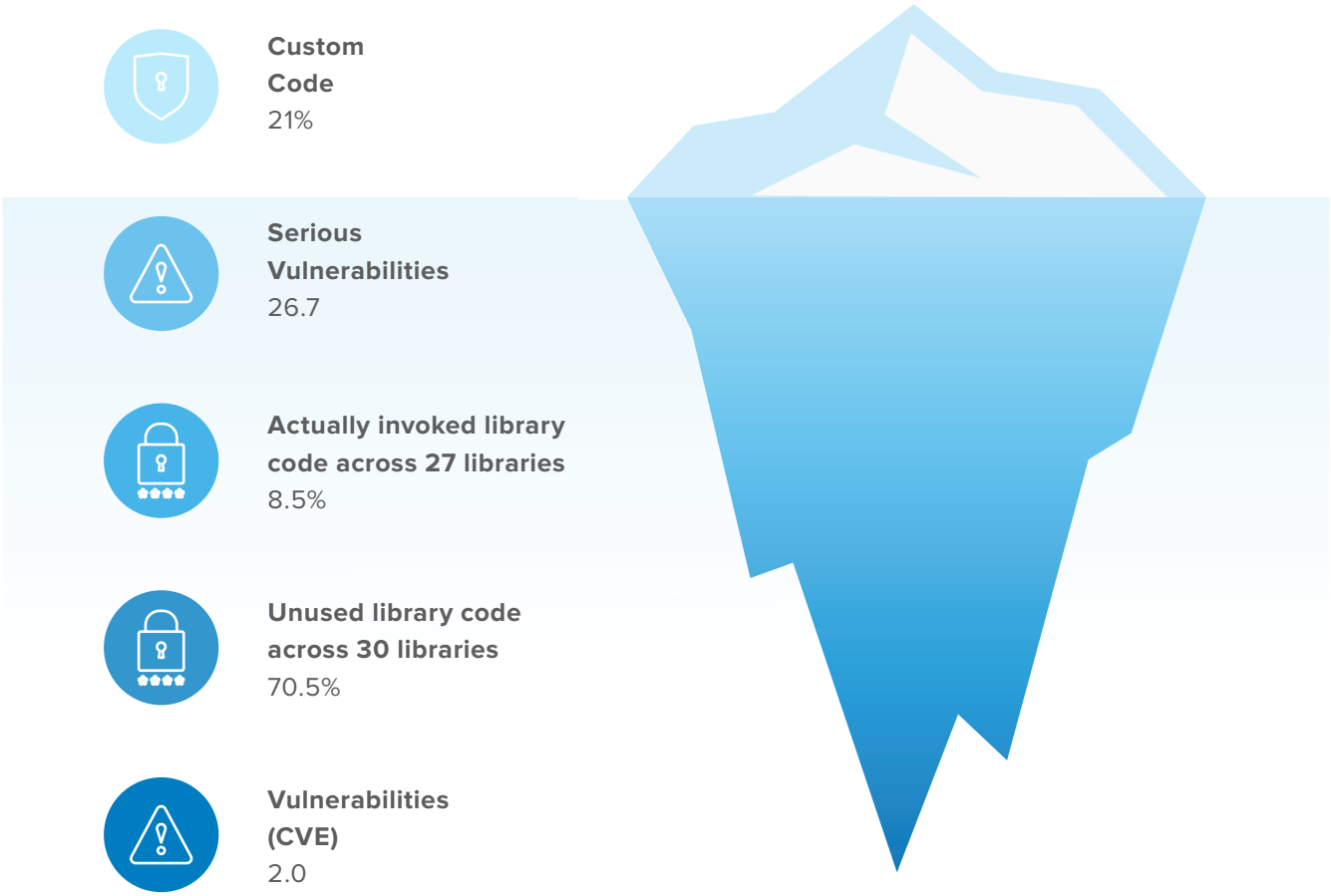
Trust is the key to customer loyalty. From your customer's perspective, there isn't much difference between going offline and going out of business. Not only does downtime discourage customers and cost sales, it keeps your team from working on the unique and important areas where your company excels. Remember that developers are a crucial lever for your CX, as their code makes or breaks the user experience. When you give your team plug-and-play, configurable identity, you'll free their time to do their best work.

Does the CIAM platform help or hinder developers?

Developers are happiest when they can devote more time to core product differentiation, rather than foundational capabilities. Login pages simply don't earn raises, but they are critical to securing your applications. Unfortunately, building and maintaining CIAM is not as straightforward as most think, even if you have all-star developers or seemingly simple requirements. Up to 80% of IT project failures can be attributed directly to uncontrolled scope creep,[3] which is part of the reason the cost of maintaining a homegrown identity solution is estimated to be twice that of going with an existing vendor.[4]

The right CIAM solution should be secure by default, minimize long-term maintenance needs, and support your team's continuous integration and deployment (CI/CD) processes to increase development automation and efficiency. Leverage a platform that provides robust documentation, SDKs, and self-service for your developers. You don't want them spending their time rewriting source code and redeploying customizations for every different app, or having to spin cycles each time your vendor deprecates or changes certain platform capabilities.

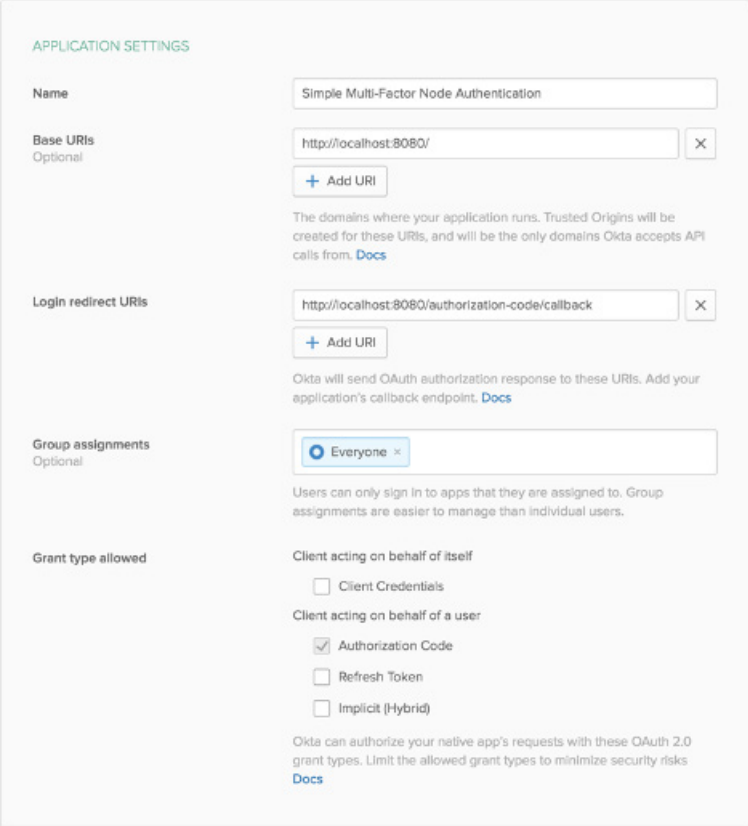
Average Application Iceberg



Does our CIAM accelerate time-to-resolution for security incidents (or, better yet, prevent them)?

Security experts know that identity is the new perimeter, and this is especially true for your customer apps. If your products are part of any app ecosystems, like the Apple App Store, you know how quickly security requirements evolve across platforms or operating systems. However, if access management is too deeply embedded in your apps, your security teams has to rely on busy developers to navigate the spaghetti code surrounding any CIAM changes, policies, or administration tasks they need completed. More code is more risk, so code-heavy approaches drag out the time it takes to identify and remediate security issues when they occur.

It's critical that your CIAM platform gives the security team more control by centralizing access management company-wide across multiple apps. You shouldn't have to be a JavaScript expert just to manage security policies. For example, Okta's configurable policy engine makes things like MFA factors easy to swap out.



Be sure you can rely on your vendor to build airtight security into their platform, without compromises. Otherwise, you'll be at risk of security vulnerabilities that could lead to a data breach, each of which costs nearly $4 million on average—or $42 million if it's a "mega-breach" of one million records.[5] Any breach undermines your customers' trust and erodes your brand's value in the market. In fact, 70% of customers say they'd abandon business dealings with a brand following a data breach,[6] and the hard truth is that companies without a mature approach to identity management see twice as many breaches and over $5 million greater cost per breach.[7]

Okta: Your trusted partner for Customer Identity

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

Clearly, there’s a benefit to avoiding CIAM tools that increase developers’ burden, hinder security, and introduce CX friction through poor reliability. By choosing a secure service like Okta, you have the opportunity to turn your identity strategy into an essential business enabler that ensures:

- More secure users, products, and services
- Greater developer agility and flexibility
- Reduced costs and operational overhead
- Happier customers, partners, and employees
- Increased automation and business efficiency

Ultimately, pre-built, robust CIAM like Okta can unlock even more innovation for your organization by improving security while attracting loyal customers and allowing your developers to focus on core aspects of the business that fuel success. For more information, visit https://www.okta.com/customer-identity/.

---

[1] Gartner, “Technology Insight for Customer Identity and Access Management,” May 2020
[2] Forrester, “The Six Steps for Justifying Better UX,” 2016
[3] Meta Group, 2010
[4] Forrester, “Making The Business Case For Identity And Access Management,” October 2019
[5] Ponemon Institute, “Cost of a Data Breach Report,” 2019
[6] Gemalto, “The State of IoT Security: Security Takes a Back Seat” 2017
[7] Forrester, “Stop The Breach: Reduce The Likelihood Of An Attack Through An IAM Maturity Model,” Feb 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