Whitepaper

CIAM helps find the balance between security and customer experience

Security is a moving target, a strong CIAM solution can help you find the right balance for your needs and your customers.

Did you lock the front door?

A lot goes on there — you're juggling coffee, kids, bags, and the cat who's trying to follow you through. It's easy enough to get lost in the shuffle and miss the basics, like locking the door. We get it, life moves fast.

Life moves fast at work, too. You're mid-sprint, the latest customer focus group results are in, your project manager is trying to book a meeting during your lunch break, and you're about to miss a standup. Now add in the ever-increasing speed of digital adaptation across sectors and the lingering effects of the COVID-19 pandemic and things just hit warp speed.

In fact, Twilio reports that the potent combination of pre-existing efforts and the acceleration brought on by the pandemic has led to many organizations seeing their transformation sped up by an average of 6 years with some industries reporting closer to 10. A full 97% of enterprise decision-makers in that poll believe the pandemic is responsible for this increased velocity. In order to manage this high-speed omnichannel adoption for your customers, you need to realize that a single, unified user management system is called for in your next release.

Customer Identity and Access Management (CIAM) is the solution that enables you to onboard, organize, and manage user accounts and data from one centralized location.

The login page is the front door for your customers. It's the first thing they see, so the login flow needs great UX. At the same time, it's the first place many hackers target when looking for a vulnerability to exploit in their attempts to steal your data, so it's got to be secure as well — it's up to you to determine how well secured. Do you leave it cracked to welcome any and all guests? Or do you add a deadbolt and chain so everyone has to knock, then wait for someone to let them in? Too little security and anyone can gain entry, too much and nobody will want to. It's a balancing act between security and customer experience.

Customer Identity and Access Management (CIAM) is the solution that enables you to onboard, organize, and manage user accounts and data from one centralized location. A strong CIAM tool will also allow you to set appropriate security measures to keep your customer's data safe and sound while ensuring users have a low-friction experience.

Simply put, friction leads to lost conversions — whether it's a new user who gives up after being asked to complete their third CAPTCHA or a loyal customer of many years who gets fed up with a clunky password reset flow. Examples of friction in the login process like these can cause users to abandon the process and your company. Then they'll take their friends with them causing untold damage to your brand in the long run.

As your digital front door, CIAM occupies a unique position at the crossroads of security, privacy, and convenience. Finding the right blend of these three fundamentals for your product and your customers brings us to a possible complication, as committing development resources to create your own solution will pull your developers and resources away from the core product. Your development team is the best at what they do. And they're using their extensive talents to build you the best core product possible. Why not treat your customers' logon experience and data security with the same care by turning to the experts in Identity management?

Bringing in a dedicated SaaS solution for Identity management not only allows your developers to focus their talents on that core product, but it also ensures every possible effort is being made to secure your customers' information, which goes a long way toward engendering trust in your brand. And according to Edelman's 2020 Trust Barometer Report, trust and brand reputation rank a joint second only to price when it comes to how people make their buying decisions.

CIAM lets you fine-tune security, privacy, and convenience

With the increased speed of digital adaptation across sectors has come a concurrent jump in cyberattacks designed to hit at the public-facing perimeter. Protecting brand integrity and reputation has thus been thrust to the forefront for many executives. That means locking down your customer-facing perimeter needs to be a business priority. Data breaches can do major damage not only to your brand reputation, but also to your bottom line with potential ramifications dragging out for years after the actual incident. Doing everything in your power to head off the potential for attack now just makes good business sense.

Most companies live and die by conversions, right? And since friction leads to lost conversions, it stands that doing what you can to lessen the friction at the login page can go a long way toward improving your conversion rate. Through CIAM you have the ability to control the flow of your customer login experience and the data necessary to continue evolving that experience as needs change. By setting the figurative sliders for security, privacy, and customer experience to just the right mix for your and your customers' business you get the level of security you need with the low-friction experience they demand.

CIAM brings more than just low-friction logon, however. A strong CIAM solution mixes that user experience with protection from cyberattacks, privacy for user data, and intuitive user account management controls.

CIAM helps protect against common attack vectors by strengthening perimeter defenses

Theoretical use case scenario: your organization is expanding its web presence. You recently acquired an eCommerce startup and completed work on developing a members-only portal for exclusive one-day deals to complement your existing web apps and stores. Your team is tasked with bringing all of that under one unified interface via a new web app. This is the ideal time to integrate an extensible, scalable CIAM solution so you can allow customers access to everything with one set of credentials, lessening your exposed attack surface.

Additionally, CIAM solutions that include features such as bot detection and remediation support, multi-factor authentication (MFA) integration, and log streaming help harden your defenses further. In today's world of distributed architecture, Identity is the perimeter. Extensibility, scalability, and partner

integrations are key when assessing whether a CIAM solution will allow your business to grow while keeping your perimeter and data secure.

By enforcing minimum password requirements (including re-use policies), streamlining the password reset flow, and including MFA, CIAM can tighten down your Identity perimeter.

A common theme connecting many attack vectors is the fact that people reuse passwords. In fact, a recent survey by LogMeIn, makers of the password manager LastPass, shows that while 91% of the public knows that reusing passwords constitutes a security risk, 66% admit to doing it anyway. CIAM can help you follow established best practices in this area. By enforcing minimum password requirements (including re-use policies), streamlining the password reset flow, and including MFA, CIAM can tighten down your Identity perimeter.

Consolidated user data is easier to protect

Single Source of Truth, or SSoT, is a data management framework that states the ideal situation for a business is to have one centralized location where all relevant data is stored, rather than having it in multiple siloed locations. CIAM takes that concept and extends it to your user data by bringing all account information together in one place. No matter how many platforms your apps end up residing on, your CIAM will be there to manage user accounts and direct all incoming data to the same Identity SSoT.

This makes it much easier to lock down that data, as there is only one location to protect. Centralized user account management is also important for compliance with major data privacy regulations. Under both GDPR and CCPA, for example, companies must provide upon request copies of a user's data as well as information on how that data is being used. And since this extends to partner systems and data, CIAM provides the easy access you need to ensure compliance, keeping your customers happy in the process.

Your Identity SSoT also enhances user experience. Single sign-on that pulls records from your SSoT means they only have to remember one set of credentials. That increased satisfaction makes it less likely that they'll abandon your app, it also means one less orphaned account is vulnerable to attack down the road. Keeping all stakeholders satisfied is never an easy task, using a modular CIAM SaaS tool can bring you one step closer to that ideal.

Streamlined processes keep users happy

When a customer creates an account or logs into an existing one, they're putting their trust in you. They're also trusting that your user story included a customer journey that won't lead to them becoming exasperated, leaving the process incomplete. When they see that the process you've built consists of a mere handful of intuitive steps and just like that, they're verified and their new account is ready to go — well you've just shown them that their trust was well placed.

A CIAM solution should do all of this, streamline the account creation process so new users feel welcome while also demonstrating that your data handling procedures are secure. According to PwC, an amazing 32% of customers will abandon a company after a single bad experience. You read that right. Fully one-third of those surveyed will completely cut relations with a company after only one unfriendly experience. Imagine what those people will tell their friends if that bad experience was literally their first encounter with your company. As you'll see in the next section, CIAM can do the same for all of your user account processes and flows.

A simplified user lifecycle is easier to secure

There are other reasons a user might be creating a new account. For example, maybe they've forgotten their password and find the "reset password" flow clunky. Of course, this results in a duplicate account that you've now got to manage, simply because you have no idea it's a duplicate. All along the user lifecycle there are security benefits to a fully-integrated CIAM solution.

Account creation

In order to eliminate account abandonment, it's key for the account creation process to be as frictionless as possible while still allowing for the verification of a user's Identity. CIAM solutions that offer single sign-on do exactly that. Allowing a user to log into your property with an existing social network account enables you to take advantage of the fact that their Identity has already been verified, and it enables the user to create their new account in a matter of seconds. This intuitive process also means a lower likelihood of a user reusing a password, rendering their account more difficult to hack and their data better protected.

Account maintenance

When it comes to the general upkeep of user accounts, automation is your friend. CIAM should offer an automated password reset flow in order to keep that all too common process low-friction. MFA options that can alleviate concern around the true Identity of the person logging in are the next step in a full-suite account management platform, while federated ID means that if a user accidentally creates a duplicate account it will be found and combined with their other account in your Identity SSoT. The additional security provided by that MFA and the elimination of duplicate or orphaned accounts keeps the chances of a successful breach down.

Account end-of-life

What happens when a user forgets about their account? Or moves on to another product, abandoning their account completely? In many cases, we fear the answer is nothing. With nothing being done about account hygiene, over time your Identity SSoT will become cluttered with abandoned, unused, and redundant accounts. This is not only a maintenance issue, but a security one as well since those credentials may be involved in a data breach somewhere and used in an attack on your systems. Automated account features like emails sent to accounts that have been dormant for a predetermined length of time, automatic account deactivation, and eventual deletion block this common attack vector.

Breached account credentials open a variety of attack vectors

Once user credentials are stolen in a data breach, they can be used again and again to gain entry to numerous other sites due to poor password hygiene. Cybercriminals have no problem obtaining usernames and passwords, even if they aren't technical enough to breach a database themselves.

These so-called "script kiddies" can purchase a "combo list" of credentials on the dark web, then use pre-existing scripts or full-blown applications also available on the dark web to instigate an intrusion by way of credential stuffing or another brute force-style attack. You need to be aware of these attack vectors and how they're being used if you want to integrate your CIAM in the best way possible for your use case.

Credential stuffing

One of the most prevalent vectors today is the brute force attack known as credential stuffing. This is when an attacker takes a list of usernames and passwords and runs them through a different site's login flow. The prevalence of reused passwords is what makes this attack vector so attractive to bad actors, there's a high likelihood the credentials they're trying will work at least often enough to be worth the effort. These attacks primarily rely on people being lazy and reusing basic, easy-to-crack passwords (the most common password in use today is "123456", with "password" not far behind).

Business email compromise (BEC)

Breached password data can also form the foundation for other attacks. For example, a hacker can purchase a combo list pertaining to a particular organization they want to target. By pulling out the network credentials for certain high-ranking executives and using spoofing, they can now send targeted phishing emails (this is known as spear phishing) that appear to come from this executive. These attacks are growing in frequency with the help of bots but are primarily a social engineering-based vector, relying on the human security (or lack thereof) factor for success.

Bot attacks

Some hackers just want to wreak havoc on the systems belonging to their target company. They don't want to steal anything, they simply want to make a point by bringing operations to a halt in order to watch the mayhem as the targeted organization attempts to stop the intrusion and recover from the downtime. Distributed denial of service (DDoS) attacks are the most common example, where the hacker uses bots to flood a site with traffic, rendering it inaccessible to legitimate visitors for a period of time. These attacks end up costing the affected business in reputation as well as the financial costs incurred during the ensuing downtime.

The other common bot-based attack is when they're used to swarm the login flow of an eCommerce site in order to buy up supplies of sought after items. Bot swarms like this were seen recently when Nvidia launched a new graphics card that had been eagerly anticipated by gamers around the world. Similarly when Microsoft launched the X-Box X and Sony their eagerly anticipated PlayStation 5, sites like Walmart and Amazon saw their processing capabilities taxed by hundreds of thousands of bot-created accounts being used to capture all available stock in order to drive up prices on the aftermarket. Not only do these swarm scenarios lead to low availability of prime merchandise, they also cause legitimate users to be unable to use the site until the attack is remediated, costing both money and a reputation hit for the organization.

How Okta does secure CIAM

> "When thinking about security you should always be thinking about risk. There isn't a one size fits all security solution and you want to make the right security decisions based on the risk specific to your business and to your customers and your users. You can dial up or dial down your security controls accordingly. And this will really help you to not over-engineer the security in your product which could negatively impact its convenience."
>
> **Duncan Godfrey**
> Vice President, Security Engineering, Okta

Duncan is elaborating on the fact that security is a moving target. To successfully address the security threats we've discussed here, along with those as yet to be unleashed by hackers, will take a combined effort that includes a robust CIAM solution developed to be scalable and extensible so you can find the right blend of security, privacy, and customer experience.

Because of its unique position at your organization's digital front door, CIAM sits at the frontline of your perimeter defenses as well. This is where bad actors are focusing their efforts as well as the first place your customers see when they come to interact or make a purchase. It's also where you govern, analyze, and securely store data on those customers.

Modularity is already fast becoming the norm in app assembly, with payment, messaging, and authentication systems leading the way in SaaS tools being integrated. Auth0's research found that 83% of modern apps being developed require authentication, yet only 58% of those surveyed report using a third-party SaaS tool. While your development team works on delivering the best core product possible, there are many reasons to let our team deliver the best, most secure CIAM solution possible.

> Ensuring that the security team has up-to-the-minute information can aid in identifying attacks in the early stages, shortening response time, and potentially heading off major fallout in the aftermath of a breach.

Open standards

As with any other cybersecurity tool, a CIAM solution can adhere to open standards or it can be a so-called “black box” solution. The latter means that you’re locked into that vendor since only they have access to the backend of their system. This is called “vendor lock,” and avoiding it allows you to remain agile in your security implementations and sets you up for easy extensibility (see below).

Open standards like OAuth2, OpenIDConnect, and SAML are also at the heart of how we make customer experience the center of attention while maintaining our developer focus. When a visitor can create a new account in a matter of moments using credentials they already have, their user experience improves dramatically. This allows them to use fewer, stronger passwords and everyone can rest easy knowing that their data is stored securely with their Identity provider rather than being spread across multiple systems.

Extensibility

The key to providing a solution that can flex and adapt along with your customers’ business needs is being able to add or customize features quickly and seamlessly. One of the ways Okta tackles this while allowing your users to find the balance they need is with Rules. For example, Rules enables the creation of a trigger for “impossible travel” scenarios. When a user in Chicago appears to be attempting a login from Brazil, the user attempting access from Brazil can be faced with an MFA prompt, while the user in Chicago who already verified their Identity will not. Rules can also be used to notify other systems of login events for event monitoring or customer service purposes.

For your developers, Okta’s partner ecosystem is the key to our extensibility. If you require a feature not yet included in our core offering, there is a high likelihood that you’ll find that’s because we have an integration with an industry leader available in our Marketplace. When you need to manage consent in order to remain compliant with new regulations, for example, there’s an integration for that.

Log streaming

One feature of a strong security posture is the ability to use the data being generated by your cybersecurity tools. For organizations that have a data infrastructure in place, Log Streaming sends real-time data from CIAM directly in existing Security information and event management (SIEM) or security orchestration, automation, and response (SOAR) solutions. This is also a key aspect in being compliant with the reporting and erasure requirements of the above-mentioned data security regulations.

Okta's Marketplace includes integrations with Splunk, Sumo Logic, Datadog, and others. Or your team can build a custom integration using our extensive APIs and our SDK library. Ensuring that the security team has up-to-the-minute information can aid in identifying attacks in the early stages, shortening response time, and potentially heading off major fallout in the aftermath of a breach.

Brute force protection

In their simplest form, brute force attacks are when an attacker tries several common passwords in an attempt to access a single user account. This seemingly unsophisticated attack can be successful, if inefficient, leading to its continued popularity. Should Okta detect more than 10 login attempts for a given account coming from the same IP address, brute force protection will block that IP for the affected user account (any other accounts at the same location will still have access) as well as send the user an alert email. The affected user will be able to unblock the IP from that email or it will be automatically unblocked when they change their password.

Bot detection

When it comes to stopping more complex credential stuffing attacks, Bot Detection is often the missing link. Using data from our 4.5 billion monthly logins combined with risk signal analysis, Okta Bot Detection can identify when login attempts are likely to be from a botnet or script and introduce a CAPTCHA step to the flow. Auth0 research has found that this can reduce the effectiveness of a credential stuffing attack by as much as 85%. For legitimate users logging in from known good IP addresses, for example, this added security step is not necessary — keeping the flow low-friction

for genuine customers. Mitigating risk while reducing friction for genuine users sticks with the concept of helping you find the right balance between security and customer experience for you and your customers.

Adaptive MFA

The National Institute of Standards and Technology (NIST) considers MFA a best practice and recommends its use at all times. And according to the industry group, The Open Web Application Security Project (OWASP), MFA is "by far the best defense against the majority of password-related attacks." Okta Adaptive MFA takes it to the next level of user experience and data security. By using contextual cues, like location, unique device identifier, time since last login, etc. adaptive MFA performs a risk analysis on each user logon event and presents a request for additional factors only when deemed necessary as in our impossible travel example above.

Passwordless authentication

Considering how problematic passwords can be, maybe it's time to allow your customers to remove them from the login flow altogether. With Okta Passwordless, you can do just that, substituting a one-time code sent to the user via email or SMS. By eliminating passwords, exposure to credential stuffing attacks and other forms of account compromise is mitigated. And with a public API that includes rate limiters, user data is protected from automated or bot attacks as well.

CIAM provides security while managing login friction

You and your team have enough going on to keep busy through your next sprint. Following the trend of modularization and integrating third-party SaaS solutions when possible means you can implement CIAM quickly and securely. Key to providing that security while maintaining customer satisfaction is understanding that with every increase in legitimate users comes a concurrent increase in bad actors trying to get at your data. A CIAM solution that understands this dynamic can scale protection along with user numbers.

Companies are paying increasing attention to how they craft their digital identities, and managing customer experience from the login page is key to creating trusting relationships.

See the potential benefits to your business of using Okta Customer Identity with our ROI calculator.