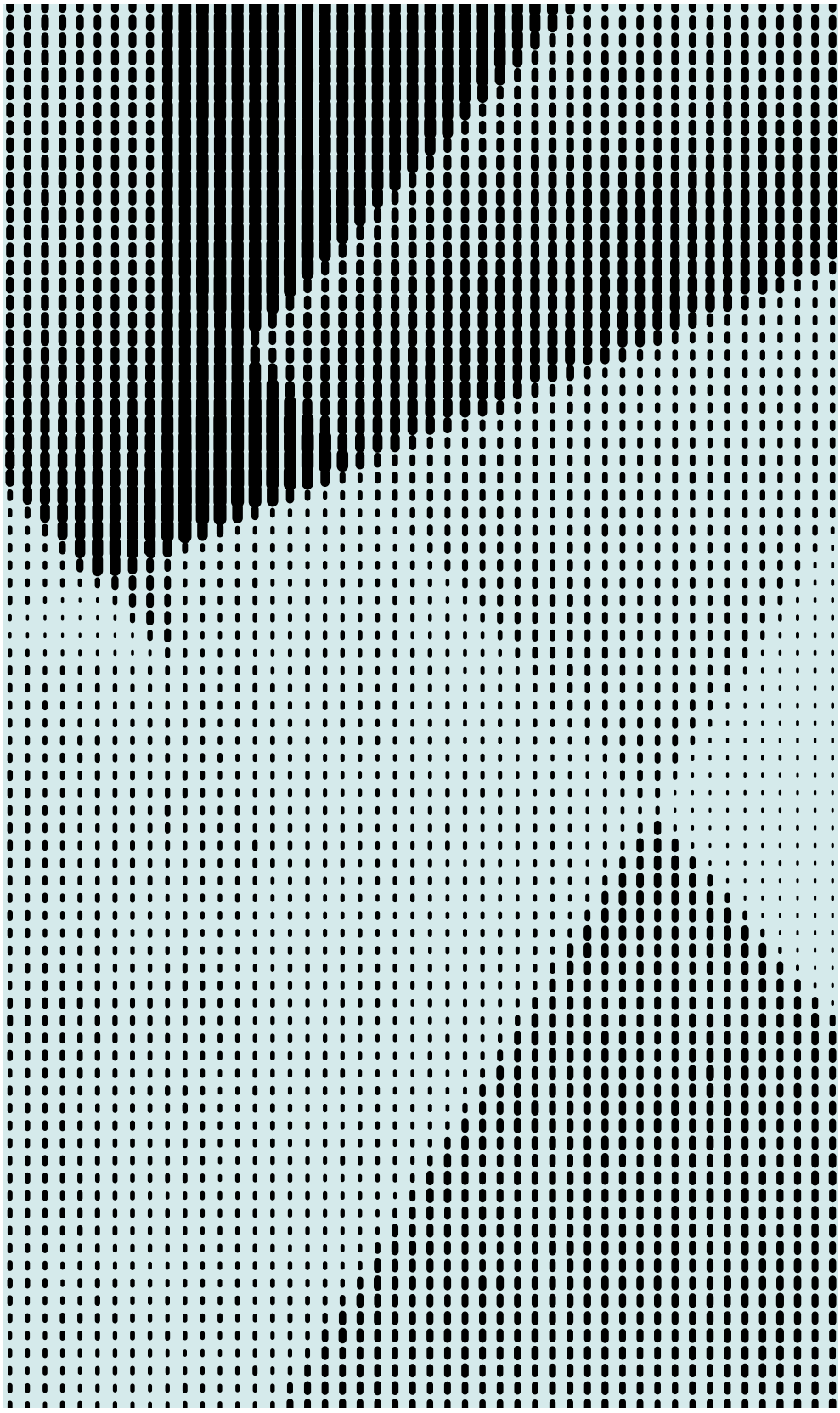
CIAM Buyer's Guide

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



okta

Contents

Your CIAM Potential

Having an online presence should be good for business. Online, you can learn more about your customers throughout their entire customer journeys, which helps you understand how best to communicate about new products and changes in service. Digital channels can facilitate direct customer input on how you can improve what you make and how you make it—and how you can attract new customers.

However, it can be challenging for companies to build user trust digitally, and a lack of trust can have major consequences. A recent PwC survey found that "most people only make the connection between technology and customer experience when tech fails, is slow or disrupts the process." And a single bad experience can have a big impact: "One in three consumers (32%) say they will walk away from a brand they love after just one bad experience."

Your customers' login experience directly affects revenue

> CIAM has a direct impact on the bottom line: if your online user management and security functions do not work, customers flee to your competitors.
>
> Forrester's Apply Customer-Focused Principles And Operating Levers To CIAM

Sign-up is often the very first interaction that a consumer has with your brand online, and login is a frequent touchpoint that can form a strong brand association. When they log in, consumers entrust you with critical information, so they expect a frictionless and secure user experience (UX). On top of that, to build brand loyalty, it's important to provide consistent experiences across all of your touchpoints. That's something you can deliver through customer identity and access management (CIAM). The right CIAM solution will allow you to capture, convert, and retain customers, both fueling the growth of your business and keeping your customers safe.

In Create Trust and Safety on the Internet, a report on the intersection of security and customer experience (CX), Gartner predicts that "by 2023, 30% of banks and digital commerce businesses will have dedicated trust and safety teams to protect the integrity of all online customer/brand interactions, up from less than 5% today."

In addition, Gartner says, "by 2022, digital businesses with a smooth customer journey during identity corroboration will earn 10% more revenue than comparable businesses with an unnecessarily frictional customer journey."

In short, the digital choices you make today will have a direct effect on the quality of experience you will be able to give your customers in the future. Here are some ways that implementing CIAM helps you deliver more value to your users:

- **Trial experiences.** Giving your customers an opportunity to experience the value of your brand before they commit should not come with friction or strings attached, including asking for too much personal information.
- **Loyalty program changes or additions.** Making sure your customers are informed about new affinity opportunities can impact retention rates, as can properly implementing single single-on (SSO) across multiple brands or properties during a merger or acquisition.
- **A 360° view of your customer.** Support for new customer relationship management (CRM) or customer analytics initiatives assists you in creating complete user profiles. Insights drawn from CRM data can help you promote your services more effectively and build more personalized experiences your customers will love.
- **Reduced risk exposure due to compliance or data privacy inconsistencies.** Standardizing how your organization handles sensitive data can streamline compliance for key regulations and data privacy laws, ultimately reducing risk.
- **Support for your business customers.** Enhance interactions with your partners, vendors, and contractors through seamless and secure digital experiences.

How to pick the right CIAM for your business

CIAM buyers should plan for an identity system based not on where their business is today, but where they want it to go. If you intend to launch new products and new partners, you're going to need to add key features you may not identify in your evaluation process.

In this CIAM Buyer's Guide, we'll look more closely at the areas of CX, scalability, extensibility, security, customer insight, and operational cost. But the bottom line is that any CIAM solution you choose must meet these criteria:

- **Be extensible for integration** with other enterprise, analytics, and CRM systems.
- **Be customizable** to optimize user experiences per specialized use cases.
- **Work across all app platforms** to handle all user access types.
- **Generate rich data and audit trails** to help comply with data privacy regulations.
- **Continuously monitor** security, threat, and access information.
- **Gather insights** for improving CX.

As you assess your unique business needs to identify the right solution, consider these four guiding questions:

1. How do you build consumer trust digitally?
2. What first impression does your brand leave on consumers?
3. Have you created a digital brand customers want to engage with?
4. How do you support business and vendor relationships and collaboration?

Your brand's online experience begins with how you power your primary point of customer contact—the login box. Once users sign in, you can follow them along their journey and gather data through low-friction conversions and progressive profiling. With data, you can create and customize personalized digital experiences and future conversion opportunities. The right CIAM solution sets the foundations of trust right from the beginning.

Customer Experience

When a potential customer engages with your online brand, you have a narrow window of opportunity to convert them. Most users need to perceive value in your brand before they engage—and to trust it. Friction during registration or login works directly against a potential conversion.

When you invite a customer to convert, you're inviting them to trust you. Yet even major brands aren't always as careful with data as they could be, which is one of the reasons we're seeing a global rise in data privacy laws like the General Data Protection Regulation (GDPR), California Consumer Protection Act (CCPA), and Act on Protection of Personal Information (APPI). There is now a focused interest in protecting the consumer.

If you're not creating an experience that delights your customer, they may no longer volunteer the data you need to understand them. In this era of increased data privacy, how you craft your customer experiences matters more than ever.

Your company's digital CX is now a critical factor in maintaining your competitive edge. And that means your CIAM solution can't be one-and-done. What does it mean to build a digital CX that is flexible and scalable enough to evolve with your company's and customers' expectations?

Businesses should monitor each aspect of their account creation and sign-in flow because it affects revenue. If your account creation flow is difficult, each point of friction could cause customers to drop off.

Do you have the tools to convert your customers?

In today's digital world, consumers have endless options for buying products and services. The same PwC survey that noted negative experiences drive customers to abandon brands also found that for 70% of those surveyed, "speed, convenience, helpful service, and friendly employees" matter most. "Those who get it right prioritize technologies that foster or provide these benefits over adopting technology for the sake of being cutting edge." Here's how to get it right:

- **Build a frictionless foundation.** Getting your digital CX right begins with a frictionless, customizable flow that allows you to create that sense of "speed, convenience, and helpful service." This flow may include applying chat bots, product discovery journeys, and recommendations that are designed with sensitivity to help, rather than intrude.
- **Know that social login is a must-have.** Consumers looking to satisfy an impulse buy—especially those who hesitate, out of caution or fatigue, to create another username and password combination—use social login. It offers speed, ease, and a sense of security because users choose the amount of information they share. Providing an option for social login can also have a big impact on registrations.

A multinational food consumable goods manufacturer told Forrester that 30-40% of its registrations come through consumer social registration and login.

- **Measure your impact.** Some CIAM solutions offer out-of-the-box metrics that only measure the basics. Stronger CIAM options let you consume data the way you want via integrated ecosystems. Regardless of how you prefer to receive it, you should have access to the full richness and depth of customer information. Equipped with data, you can push it to analytics tools and gain a better understanding of your funnel.

A customer-centric approach requires respect

The EU's GDPR shifted data privacy into the spotlight. Additional regulations like the CCPA, Japan's APPI, and other data privacy laws regulate how data is handled, but they also regulate how breaches are reported and fines are levied. If a breach happens, your response can directly affect the fine imposed as well as your potential to lose (or save) your reputation with customers.

A PwC survey found that people base their decisions to share personal information on trust, so much so that 88% of US consumers say that how much they trust a company determines how much they're willing to share personal information.

While Californian consumers only recently demonstrated an interest in greater data privacy protections by supporting the CCPA, EU residents came to the GDPR with high expectations based on decades of data privacy protections. Piecing together differing definitions of "personal information" across global enterprises can prove challenging for businesses, whether they're navigating differences between countries and regions or even different states in the US.

Respect that some consumers may not want to give you more information than the minimum you need to complete a transaction. Starting there gives you the opportunity to build a respect-based, mutually beneficial relationship over time. When your customers eventually realize that by sharing more information, they receive greater personalization and benefits, you'll have already proven they can trust you with their data.

Using CIAM to maximize your loyalty programs

In 2019, Yotpo reported that brand loyalty is increasing among consumers; 24.82% of US customers claimed they were more loyal to brands in 2019 than in the previous year. The more difficult news is that it takes repeated purchases to earn and re-earn that loyalty, as 36% of customers said they needed to purchase five or more times to consider themselves loyal.

Meanwhile, more than half of those surveyed by Wisecard indicated that rewards had a significant impact on their habitual or big purchases.

Customer obsession can pay off, says a recent Forrester report. Connecting your CIAM to your marketing campaigns can maximize your loyalty programs. The report cites a food service firm that uses CIAM as a "central clearinghouse of all marketing campaigns." Gathering billing information when customers register for buy-one-get-one-free coupons, the firm automates password creation and enrolment of these new users in a loyalty program. To place online orders, customers must be enrolled and logged in to the mobile app.

Our own customer research finds that mergers and acquisitions (M&As) can drive loyalty program changes. According to KPMG, 70-90% of M&As fail, and acquiring companies often need to unify multiple legacy databases under high pressure to prove return on investment (ROI). Yet key moments within new brand experiences may put all your hard loyalty efforts at risk.

Creating a customized, frictionless user experience with strong brand messaging can help protect against customer loss during M&A transitions. CIAM enables that.

Personal preference and security

From an authentication perspective, two main areas characterize the digital revolution:

- The desire to express personal preferences via customization
- The desire to preserve privacy via an appropriate degree of friction

The lack of consumer customization opportunities (outside of the size and color of their phones) means that it's relatively inexpensive to deliver digital experiences that delight. While this may have begun with letting people pick a favorite photo as their screen saver, it's quickly spread into UX positions and options, with the expectation that everything will run smoothly.

But the ability to personalize an experience can make it harder to turn away. Increasingly, CIAM solutions allow companies and even end users to specify personal preferences about a wider range of interaction details, such as how much authentication friction or privacy is desired.

Especially in institutions where friction is necessary to protect against identity fraud and theft, the ability to select the appropriate amount of friction for your customers in any given situation can make a big difference. For example, a financial institution may introduce more friction for large, high-risk transactions in order to ensure they're safe and secure.

Where self-service can help

When customers show you trust by providing information like their email address or phone number, you open the door to self-service. Users who can't remember login details can use other options to reset them without relying on a customer support agent.

The ability to reset without having to wait on a call for an associate can make the difference between a frustrated customer, who might abandon your service, and one who feels satisfied with their experience of secure access. And, of course, self-service greatly reduces your help desk costs. Industry experts say that each avoided help desk call saves $70, and we've seen an even stronger ROI from customers in industries like banking and insurance. Intuitive, self-service user flows for account recovery can help support and retain your customers.

You don't need to sacrifice time to market to create a delightful UX

Balancing customization with security and privacy requirements can sound like adding months to your go-to-market timeline, but it doesn't have to be that way.

Adding personalization options over time through features like progressive profiling allows your customers to provide information at their own pace—while your product is already on the market.

On top of that, moving existing or acquired users to your new or updated product may put them at risk for password resets that could, at best, strain your help desk or, at worst, drive customers to your competitors.

Your CIAM solution should offer a menu of combinable options that allow you to tailor your migration to your specific need:

- **Retire legacy systems.** Maybe you have an on-premises solution that is aging out, or you need to rapidly adjust a stack for security or compliance reasons. Bulk migration, where you migrate all your users at once, may be the best option. With the right solution, your users won't notice, although less robust options may force unnecessary password resets.
- **Avoid password resets at all costs.** Maybe you're building your system and you're fine with your users migrating as they sign in. Trickle migration allows you to seamlessly move users free from password reset friction. You can also consider a combination approach where you allow users to trickle for a specified period of time, then push a bulk migration.

- **Match your schedule.** Maybe you need to set a specific migration schedule based on your digital transformation workflow. A CIAM solution shouldn't force you into changes you're not ready to make.

Migrating your users on your timeframe is critical whether or not your CIAM solution is platform neutral. CIAM needs to work cleanly across platforms: iOS, Android, and web.

Scalability

> In today's online-first, intensely competitive environment, creating a monolithic inflexible CIAM system will quickly put you on the path towards extinction.
>
> Forrester's Apply Customer-Focused Principles And Operating Levers To CIAM

Customer identity presents a completely different set of challenges.

While CX is paramount to your brand, the ability to scale to millions—even billions—of users, is critical for the business, especially if you need to respond to short-term events like Black Friday or the World Cup.

If your CIAM solution won't scale, then it won't work, because your target audience has many choices and can easily look somewhere else.

This is a big enough reason for many companies to go with a reliable third-party CIAM provider.

Making sure you can get to the future from here

You might be exploring a CIAM solution to solve an immediate problem, but you really want to plan for where you hope to be in five years. If you don't, it may be a lot more painful to get there.

Whether or not your target CIAM vendor can handle your proposed scale is a simple question. Here are a few others to take back to your team:

- **Where does your business want to be in five years, and what does that mean for your scaling needs?** Thinking strategically about your company's future state allows you to avoid inadvertently building in incompatibility and tech debt.

- **How fast can you get your product to market?** Your CIAM is not scalable if your progress is measured in years.
- **What's your ongoing maintenance budget?** Ongoing maintenance will be required to ensure that your users can continue to log in to your product easily. Your ongoing maintenance budget should include regular updates for cryptography and a cyber attack protection strategy.

CIAM is more than a login box

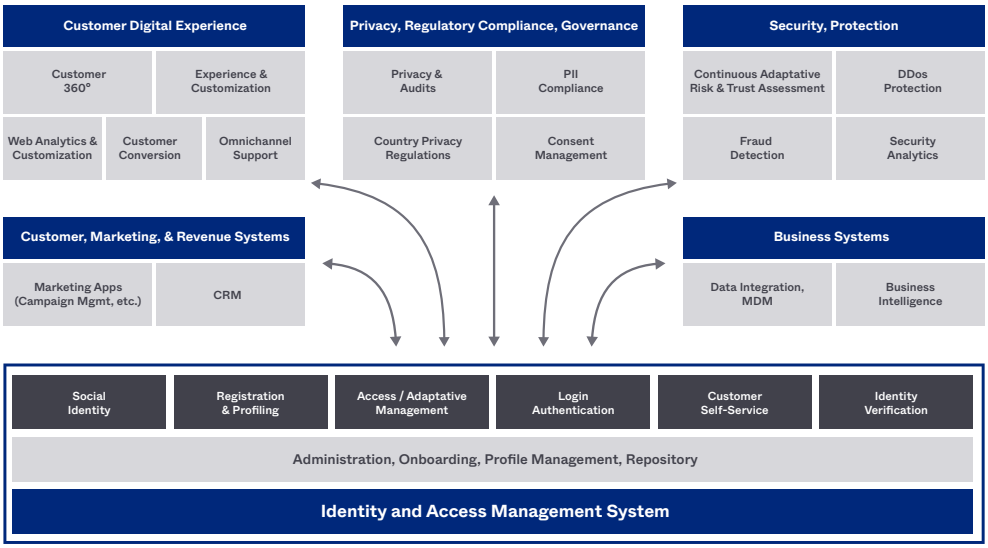
The solution you choose to power your login box will include several moving pieces. These need to evolve over time to keep up with your customers' changing needs (and demands), as well as with your own business strategy. Choosing a partner who continues to innovate will open up previously unconsidered business possibilities that bring their own branching potential for growth. Plan to find a partner with a track record of flexibility so that future goals are always within reach.

Extensibility

> CIAM technology popularity has surpassed homegrown solutions, but integration with adjacent technologies is still key to address digital experience and risk management needs.
>
> Gartner, Technology Insight for Customer Identity and Access Management

Every company that hopes to reach consumers needs the option to scale, and that makes CIAM essential. But for enterprises, it's also a foundational element of multiple internal organizations and functions.

For an enterprise, the success of the business requires instrumentation and input from multiple departments, many with outwardly competing functions.



Fortunately, all of these areas feed and take from your CIAM solution, which means you can use CIAM as a tool for building consensus across teams. Of course, that's provided you choose an identity provider who can handle your particular extensibility needs.

In addition to resolving how your company will balance the above responsibilities across departments, you will also need to resolve four competing business tensions:

- **Customer convenience:** the need to provide the lowest-friction experience possible, in which customer needs are consistently anticipated and met.
- **Security:** ensuring security for your customers' credentials and data, as well as ensuring security for your own data and service.
- **Consumer data privacy:** adhering to regulations such as the GDPR, CCPA, and other consumer-focused privacy and compliance needs.
- **Conversion, revenue, and retention:** driving revenue and customer lifetime value by encouraging repeat service use.

Every company will strike its own balance of these four forces, often prioritizing some over others. The CIAM system you choose should enable you to leverage them by customizing how they are applied and adjusted.

Accommodate legacy tools and customizations

Each of your departments relies on a set of tools that likely comes with its own set of legacy modifications. Even if you're switching to an entirely new CRM provider, you may want to extend a specific customization without having to wait an additional six months for actionable data.

Or maybe your business has recently expanded into the Japan market, only to encounter changes to their APPI. This means the way you've previously handled personal information may not be up-to-date, which can lead to a hefty expense.

Ultimately, you stake the success of your current and future initiatives on how well your CIAM functions as a central hub to feed the rest of your organization.

Using the right mix of out-of-the-box and extensibility to increase speed

When your customers must log in to access your product, CIAM is essential to doing business—and resolving the demand for functionality across departments can be daunting.

It might conjure up memories of stalled multi-year digital transformation attempts that fail to deliver ROI, but with the right CIAM solution, implementation could take only a matter of weeks—or even days.

The chart above hints at why identity can be so complex, but also why it can be used as a framework for clarifying your business strategy. The right mix of out-of-the-box functionality and extensibility allows you to systematically work through the needs of multiple departments, helping you identify what's possible to roll out quickly and what might require more planning to execute.

An extensibility checklist

Many CIAM solutions claim to provide extensibility, but they may not offer what you need for your specific situation. Here's a quick checklist to help you recognize extensibility:

- **Fast** out-of-the-box implementation for basic functionality: get pilots and simple applications up and running quickly with minimal setup or configuration
- **Developer-friendly** options for coding extensions (e.g., node.js): allow for future developer customizations to meet unforeseen use cases
- **Applies across identity use cases** for CIAM, B2B, and workforce identity: use a single platform across all identity use cases to maximize digital agility, privacy and compliance, and a consistent security profile
- **Optimizable** to allow for balancing priorities including security vs. user experience and conversion vs. privacy: permit customizations to balance and optimize each of these four business priorities
- **Open** to third-party ecosystem providers, communities, and external data sources and systems: no single platform can address all use cases, so opt for a vendor that provides a number of integrations and extension points with partners
- **Global** scale for all extensions, including options for data sovereignty and execution locations: applications must be globally available by definition, including execution performance of extensions; CIAM platforms must also allow for data at rest to comply with specific privacy regulations

Security

> The security customer experience for the customer's journey and the CIAM functions' availability pave the way for secure and low-friction customer acquisition and retention.
>
> Forrester's Apply Customer-Focused Principles And Operating Levers To CIAM

The traditional thinking is that you have to make a decision between security and convenience when you interact with your customers. Typically, greater friction equals greater security, but with modern multi-factor authentication (MFA) or continuous authentication scenarios, you can still moderate risk without inconveniencing your customers and driving them away.

A strong security stance builds customer trust

How you handle security can have a big impact on your bottom line. A 2020 IBM-Poneman study found that data breaches cost an average of $3.86 million per incident globally, with the number rising to $8.64 million on average in the US. Breach-related costs include actual fines and reputation erosion that encourage customers to shift to competing brands.

Many businesses assume that CIAM security is only about fraud detection—making sure the right people have access to the right data at the right time—but this is a mistaken view. Don't get stuck in a security framework that only views customer interactions as potential threats to their organization's security posture.

One of the largest pain points with CIAM is dealing with decentralized data. Why? For the simple reason that it's difficult to secure what you don't know about. Decentralized data makes it harder to comply with privacy regulations that require you to provide personal information when it's requested by the customer.

A strong security CIAM stance not only supports a centralized view of the customer, but also makes it easier to meet privacy requirements globally by ensuring security at scale and preventing security breaches. The balance between security and convenience becomes less about friction and more about what encourages trust in your customers at any stage of the customer journey.

Using your customer journey to reduce risk

Your customers know that they're trusting you with their data, and the increasing number of data privacy regulations shows that they're aware of the risk. Cyber attacks show up in their newsfeeds on a nearly daily basis, often attached to formerly trusted brand names. But the sheer hassle of recalling the 70–80 passwords most people are expected to remember leads to password reuse, especially when users get impatient with sign-in flows that take too long.

Attackers count on people being overwhelmed by passwords, which is how e-commerce sites can find themselves the targets of high-volume credential stuffing attacks. These can prove costly not only in their potential to cause breaches, fines, and reputational impact, but also because they may raise the cost of your services.

We find that seamless, low-friction MFA can effectively prevent potential breaches and account takeovers, but that's not all. When delivered at the right stage in the customer journey, MFA can signal that you care about your customers' personal information and are willing to take the steps necessary to protect it. Likewise, the well-placed delivery of a CAPTCHA, a picture-driven challenge that screens for bots, can also be viewed as positively protective.

If you do suffer a catastrophic breach, that's an opportunity to fortify your CIAM posture, says Forrester, noting that this is a prime time to push for CIAM centralization, SSO, and stronger authentication.

Your CIAM solution should enhance your security posture

With everyone on board, your CIAM solution should enhance your security posture. If it's based on open standards, your security engineers (if you have them) will be able to clearly understand how the data flows through your system. (In contrast, they won't have that visibility with a solution that flows data through the black box of proprietary code).

Privacy regulations such as the GDPR, CCPA, and APPI require that you understand the ways your third-party providers use or handle the flow of data throughout your system. Open standards also make it easier for you to understand how to comply.

Additionally, your CIAM solution should offer critical certifications like PCI, ISO20071, SOC 2 Type 2, HIPAA (for the US), and Gold CSA Star, which signify that you perform regular security checks via a third party. These prove your strong security posture isn't just a claim.

Increase protection and customer satisfaction

Centralizing identity will protect your customer logins right now, but it also sets you up to create a unified (and more secure) brand experience in the future. Instead of pushing your developers to work through potentially tedious security implementations again and again, you will have solved the CIAM challenge effectively, and you'll be equipped to apply it across multiple products, reducing the timeline of final implementation to minutes or days instead of months. Having a single pane of glass for governance, and to orchestrate your customer identity information, will allow your developers to handle identity quickly and focus on your core business.

Forrester points out that "using a commercial CIAM solution, one company was able to free up a developer previously working on in-house Facebook social registration and login to work on other, non-CIAM-related, functional aspects of the customer-facing portal—contributing directly to increased customer satisfaction."

Customer Insights

Delightful, personalized experiences can be the difference between keeping a customer and losing them to the convenience of a faster click.

Say you have a regular coffee shop customer who buys coffee in person, orders beans online, and participates in your loyalty card program. But because your system isn't connected by a strong CIAM, you don't know that otterdog459 in your loyalty program is dolphinswimmer when they shop your online store. You also don't know that this customer has two other usernames and passwords at the coffee chain you're about to acquire. That's because they forgot their password and it wouldn't reset properly, so they created a new one after spending ten minutes trying to get through to the help desk.

Similarly, you don't know that otterdog459/dolphinswimmer has racked up many loyalty points, and that your merger has them stressed that those points are going to disappear or lose value.

Not having a single source of truth makes it harder for you to understand your customer—and a fragmentary experience can cause them enough anxiety to try a competitor.

Why identity is the natural single source of truth

For some industries, such as banking, knowing that you're doing business with the right person is a requirement. Regardless of your exact needs, the more usable data you have, the better.

The important part of that equation is "usable." You may have amassed a fair amount of data on your customers, but it's still challenging to turn that into a 360° view. Some information may be stuck in a CRM that needs an upgrade or in an app written by a freelance developer who didn't leave comments on the code.

Or maybe you run an umbrella insurance company with subsidiaries specializing in life insurance and property protection, but the data is siloed because each brand comes with its own login and registration flows. You can draw inferences from basic demographics, but seeing what your customer clicks on before they sign could make a big difference in the products you offer them now and in five years.

An Accenture study found that 91% of consumers are more likely to shop with brands who recognize them, remember them, and provide relevant offers and recommendations. Therefore, that siloed information is making you miss opportunities.

If you undertake a massive effort to unify the data without solving the registration flow, your data will always be out of date because every time your customer clicks, they will increase the amount of siloed data you need to resolve.

The easy solution is to fix the point of communication—your login box.

Powering your login box with a strong CIAM solution allows you to turn login and registration clicks into moments of understanding. That's because you can generate a single source of truth in the form of a user profile.

Generating a user profile helps with issues like duplication of customer data while also providing a seamless, branded experience that can be tailored to welcome customers during a merger or acquisition.

Increase conversions by reducing friction

You need to understand your user activity and returning users to find patterns of opportunity that specifically affect your conversion and retention rates. Often, these opportunities come in the form of reducing friction.

In 2019, the average global website conversion rate was 2.58%, down from 3.42% in 2014. Today's customers have no patience for filling out frustrating registration forms. But implementing social login by allowing your customers to use their credentials from apps like Facebook or Google can erase friction and reduce frustration.

Cybrary, a cyber security career development company that offers expert-led courses and virtual labs introduced social logins to help logins happen faster. When the new system rolled out, 40% of their users adopted social login, which greatly reduced login friction.

Your data, your way

One of the challenges with CIAM solutions is that they're often built with a specific set of users in mind. The data that works best for your marketing and revenue teams, for example, isn't necessarily the same data that your security team needs to protect your customers. Similarly, your privacy and compliance teams require a different set of insights, and your digital experience team has other priorities altogether.

No one CIAM solution is built to satisfy all of those needs. You could decide to make tradeoffs, but since it's not clear what data your teams will need next year or in five years, you could be walling yourself off from future opportunities.

Look for an extensible CIAM solution with a strong ecosystem of integrations that allows you to consume your customer information in the way you want, without vendor lock-in. You don't want to find you've outgrown a system in two years and can't easily take your hard-earned data to a new vendor.

The bottom line is, regardless of how you prefer to consume your customer data, for the best understanding of your funnel, you should have access to all customer information pushed to tenant logs.

Operational Costs

> Our research into building that [customer identity] system ourselves showed a rapid decline into a complex space that was frankly not our domain.
>
> Shantanu Bose, VP of Engineering, Classy

Pausing your business to deal with identity maintenance can cause friction that will send your customers to lower-friction competitors. In truth, identity is not something you solve once—it evolves with your business.

Attack protection

As a consumer-based business, you are a high-priority target for attackers who recognize that you're charged with protecting critical pieces of identity: names, addresses, emails, and payment information. Even if you only collect a handful of details, attackers will target you because people reuse password information. A Google and Harris survey found that 66% of people reuse passwords for multiple accounts. Similarly, in a recent LastPass survey, 91% of respondents said they understand the risk, but reuse credentials anyway. Attackers know this, and they have the time and computing power to piece the data together.

Globally, data breaches are increasing in frequency. Fortune reported that the number of data breaches in 2021 has surpassed the total number in 2020 by 17%.

This means that you need to provide regular app security updates for your customers to protect them from ever-increasing attacks.

Updates will happen

In addition to upgrades that protect your customers, you may need to make an update to release a new feature available or add additional products or payment methods. You might acquire one brand (or five) and need to integrate them in a seamless and logical way that makes it easy for your customers to make tailored discoveries, or take on new partners and need to integrate their capabilities. Additionally, you could expand into an entirely new region, which would mean mandatory updates to your privacy and consent forms to comply with various countries' data privacy regulations.

The evolution of technology continues every day, which means you're always going to be getting updates from third parties that may not suit your timetable.

As Forrester pointed out in a recent Now Tech report on CIAM, "choosing a flexible, easy-to-change, and API-based CIAM system also reduces the time to adapt the CIAM to quickly changing business and security requirements."

Unintentionally limiting your business strategy

Your team may have come up with a fantastic set of innovations likely to drive a dramatic increase in revenue, but if you've created a CIAM system that devolves into legacy software, it becomes a blocker instead of an enabler. Having to tell the team that you're pausing their great ideas can mean you lose talent as well as time. You need a solution that can keep pace with you, helping drive innovation and growth instead of blocking it when your requirements change.

Manual processes can get expensive

Finding and hiring talent is an ongoing challenge for every tech company. Once you find that talent, you want to put it behind your company's core focus to push the possibilities of innovation and deliver more to your customers.

Asking your in-house developers to step away from their core focus to tweak yet another update or data privacy change can cost you in operational costs and lost opportunities.

And if developers have to hard-code every one of your changes, you're looking at a large time investment. Your developers may be extremely talented, but few are experienced in the complexities of identity. Asking them to come up to speed—and keep pace—as identity evolves is an unnecessary expense.

Cost spread to customer experience

If you create a consumer-focused product, you're more likely to see that cost spread because the wait time will directly impact your customer experience by increasing friction and leading to expensive password resets.

The often-quoted stat is that password resets run $70 per call. For some industries, that number can be significantly higher, and multiplied by millions of customers, the cost quickly adds up.

Certification costs

Certifications like SOC 2, HIPAA, and ISO 27001 require an up-front investment to achieve the accreditation, plus yearly costs to maintain it. But not having those certifications can block growth, especially when you're courting enterprise customers.

A strong CIAM solution will provide its own certifications that cover the CIAM you're purchasing as well as annual investments in third-party auditors, compliance staff salaries, internal compliance tools (excluding engineering tools or tools deployed for security purposes), and continually improving processes—eliminating both certification worries and costs for customers.

Planning for CIAM Success

You're building a CIAM solution not for who you are today, but for who you plan to be tomorrow. This guide has discussed the core CIAM capabilities, the importance of extensibility, and the functions critical for your success now, six months from now, in a year, and beyond.

But there is one more area that is key to your success—determining who drives this process within your business.

Because CIAM sits at the center of so many core functions, you must take care not to create siloed technology. Think systematically through your particular organizational structure to identify who needs to be on your decision-making team (or who might have been inadvertently missed).

For CIAM success, you'll need to broker an agreement between teams across the business:

- Product management
- Security
- Business systems
- Customer analytics and digital experience
- Privacy, regulatory, compliance, and governance
- Marketing and revenue systems/analytics
- IT/IT operations

Expect discussions around the balance of security against convenience, and privacy against revenue and customer retention. As Forrester points out, "CIAM is hard even if the tools are good." Establishing a monthly stakeholder meeting during and after implementation will help your CIAM solution keep pace with both your evolving business needs and the global pace of technology.

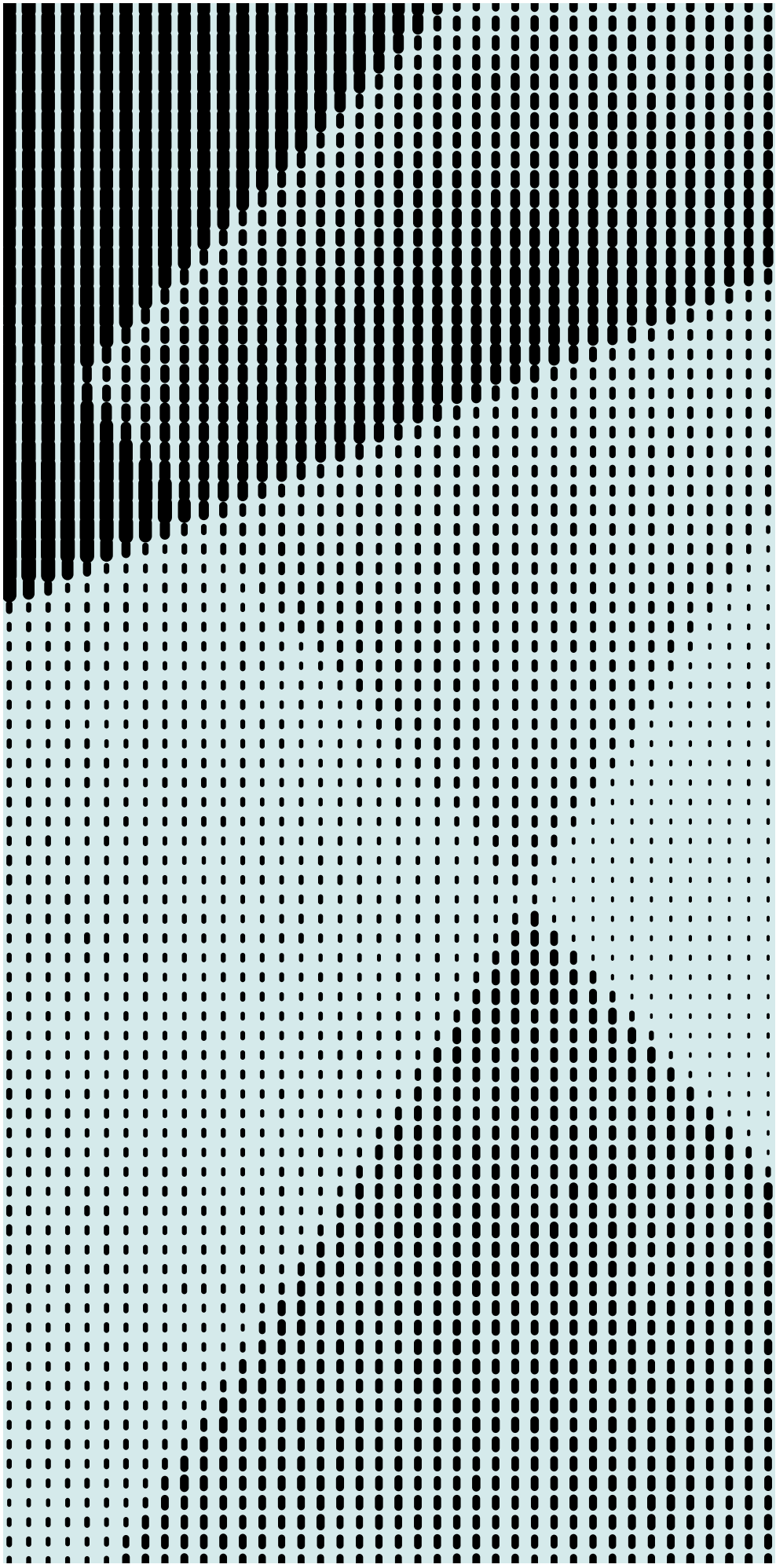
Identity impacts your entire customer journey. Resolve today's CIAM challenges with the help of a vendor who also focuses on the future. That way, you'll be able to use the CIAM discussion as a framework to drive consensus and momentum for your evolving digital transformation strategy. You can start the conversation by taking these questions back to your decision-making team:

- If some decision-makers are still leaning towards building in-house, have you budgeted for ongoing talent, maintenance, and evolving complexity?
- Have you identified core stakeholders from each of the areas listed above? Are any of them missing from the decision-making team?
- What's your growth trajectory? How rapidly do you need to be able to scale and take on new partners and products to remain flexible and innovative?
- How does your proposed solution help you balance the opposing needs of security and convenience? What about privacy and revenue or customer retention? Identity touches each aspect.
- Does everyone understand the tradeoffs you're making for your unique situation?

For companies seeking a digital competitive advantage, Okta provides an extensible CIAM platform that enables frictionless experiences, speed-to-market, centralized management, and internet-scale security. If you'd like to learn more about how Okta can help your company meet your unique goals, please reach out to an Okta sales representative.

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 14,000 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. To learn more, visit **okta.com**.



okta