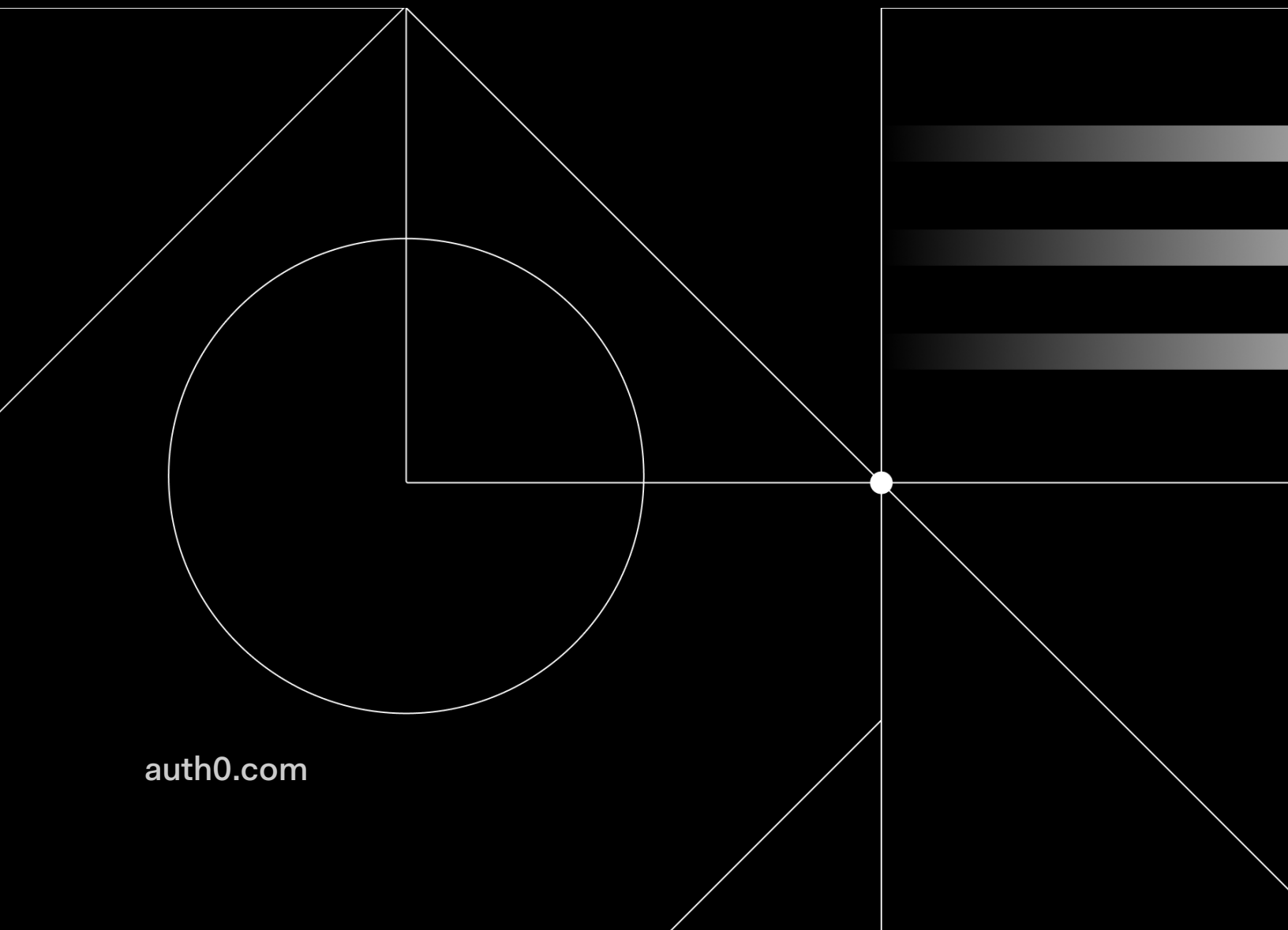
Auth0

CIAM Buyer's Guide

How to pick the right solution for now, next year, and five years from now



auth0.com

Contents

Your CIAM potential

Online should be a place where you can learn more about your customers over their lifetimes, understand how best to communicate about new products and changes in service, and get their advice on how you can not only improve what you make and how you make it, but also attract new customers.

Building that trust digitally can be a challenge for companies. And its absence 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." One bad experience can have a big impact, the survey found: "One in three consumers (32%) say they will walk away from a brand they love after just one bad experience. This figure is even higher in Latin America, at 49%."

Your customers' login experience directly impacts 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, Customer-Obsessed IAM Operating Model, April 2020

Sign-up is often the very first interaction that a consumer has with your brand online, and login can form a strong association given how frequently it occurs. This is the point where consumers entrust you with critical information. Your customers expect a frictionless and secure user experience. Delivering that experience via the Customer Identity Access Management (CIAM) solution that best allows you to capture, convert, and retain customers will not only allow you to meet the expectation that you will keep your customers safe, but will also fuel your business's growth.

In *Create Trust and Safety on the Internet* (June 2020), a report on the intersection of security and CX, Gartner predicts, "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."

Moreover, 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."

This is to say that the digital choices you make today will have a direct impact on your ability to give your customers a delightful experience 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 strings attached in the form of friction or too much required 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.
- **Gain a 360° view of your customer.** Sound support for new CRM or customer analytics initiatives increases your ability to create a complete user profile. Those insights can help you promote your services more effectively and build more personalized experiences your customers will love.
- **Reduce risk exposure due to compliance/data privacy inconsistencies.** Standardizing how sensitive data is handled can streamline compliance for key regulations and data privacy laws, ultimately reducing risk.

How to pick the right CIAM for your business

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

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

- **Be extensible for integration** with other enterprise, analytics, and CRM systems.
- **Be customizable** for optimizing experience per use case.
- **Work across all app platforms** to handle all user access types.
- **Generate rich data** and audit trails.
- **Continuously monitor** security, threat, and access information.
- **Gather insights** for improving customer experience.

Additionally, here are three questions to think about as you're assessing your unique business needs:

1. How do you build trust digitally?
2. What is your brand's "first impression"?
3. Have you created a digital brand customers want to visit frequently?

Your brand's online experience begins with how you power your primary point of customer contact — the login box. The right solution can build that trust digitally using CIAM.

As your customer proceeds on their journey, you can learn more about them through additional low-friction conversions and progressive profiling. You can then leverage this data to create and customize additional digital experiences and future conversion opportunities.

Customer experience

When a potential customer engages with your online brand, you have a very narrow opportunity to convert them. Most users need to have a perception of value from your brand before they engage, and friction during registration/login or the perception that a customer cannot trust your brand all work directly against a potential conversion.

Moreover, when you invite a customer to convert, you're inviting them to trust you. The fact that even major brands aren't always as careful with data as they could be is one of the reasons we're seeing a global rise in data privacy laws like GDPR, CCPA, and 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.

Instead of being an adjunct to bringing a product to market, your company's digital customer experience 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 customer experience that is flexible and scalable enough to evolve with your company?

Larger companies monitor each aspect of their account creation and sign-in flows because of the impact of those flows on revenue. If your account creation flow is difficult, each point of friction could result in drop-off for your customers.

Do you have the tools to convert your customers?

Unlike workforce identity solutions where you have a captive audience willing to slog through tedious sign-ins on a daily basis so long as they get their paychecks, consumers have choices.

The PwC survey that found customers would abandon brands they loved after one negative experience also found that 70% of those surveyed said that "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." These areas can help you get it right:

- **The frictionless foundation:** Getting your digital customer experience right begins with a frictionless, customizable flow that allows you to create that sense of "speed, convenience, and helpful service." This flow may include smart applications of chat bots, product discovery journeys, and recommendations sensitively designed to be perceived as helpful rather than creepy or intrusive.

- **Social login is a must-have.** For consumers looking to satisfy an impulse buy or who have merely grown cautious (or tired) at the thought of another username/password combination, social login offers speed and ease as well as an increased sense of security, because users are choosing the amount of information they share. Providing social login can have a big impact on registrations. A multinational food consumable goods manufacturer told Forrester that its consumer social registration and login made up 30-40% of its registrations.

- **Can you measure your impact?** Some CIAM solutions will present you with out-of-the-box metrics that measure only the basics. Stronger CIAM options let you consume your data your way via integrated ecosystems. Regardless of how you prefer to consume your customer data, in order to understand your funnel, you should have access to all the richness of information pushed to analytics tools.

Customer-centric approach of respect

The EU's General Data Protection Regulation (GDPR) shifted data privacy into the spotlight. Other regulations like the California Consumer Protection Act (CCPA), Japan's Act on Protection of Personal Information (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 have a direct impact on the fine levied as well as your potential to lose (or save) your reputation in the eyes of your customers.

A recent PwC survey found that trust levels directly impact the sharing of personal information: "88% of U.S. consumers say that how much they trust a company determines how much they're willing to share personal information."

While Californian consumers 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 trying to align different states in the U.S. Both Apple's Tim Cook and Microsoft's Satya Nadella have called for global privacy regulations.

Respecting that customers may only want to give you the minimal amount of information you need to complete the transaction gives you the opportunity to build a respect-based, mutually beneficial relationship over time. The customer realizes that by sharing more information, they receive greater benefits — and you've 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, with 24.82% of U.S. customers saying that 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, with 36% of customers saying they needed to purchase five or more times to consider themselves loyal.

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

Customer obsession can pay off, says Forrester in a recent report. Connecting your CIAM to your marketing campaigns can maximize your loyalty programs. They cite a food service firm using CIAM as a "central clearinghouse of all marketing campaigns," using registration from buy-one-get-one-free coupons to gather billing information and creating a password that automatically enrolled the customer in the company's loyalty program. Placing online orders required that the customer be enrolled as well as logged in to the mobile app.

Our own customer research has found that mergers and acquisitions can drive loyalty program changes. New brand experiences can be key moments that put all your hard loyalty efforts at risk. Acquiring companies often find themselves needing to unify multiple legacy databases under high pressure to prove return on investment, since 70-90% of mergers and acquisitions end up failing, reports KPMG.

Customers often view loyalty rewards as actual cash in their pockets. Creating a customized, frictionless user experience with strong brand messaging via CIAM can help protect against customer loss during M&A transitions.

Personal preference and security

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

- Increasing customization and expressing personal preference
- The degree of desired friction or privacy

Although you have to pay to have it coded, the lack of physical expression (outside of the size and shape of your phone), means that it's relatively inexpensive to deliver experiences that delight. While this may have begun simply with letting people pick a favorite photo as their screen saver, it's quickly spread into UX positions and options, with the increasingly prevalent expectation that everything will run smoothly. As mentioned earlier, customers will leave a trusted brand after just one bad experience.

But because humans become attached to the things they rely on, the ability to personalize an experience can make it harder to turn away. Increasingly, CIAM solutions are allowing 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 customer in this particular situation can make the difference.

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 cannot remember their passwords can use other options to reset it without relying on a customer support agent.

The ability to reset without having to wait on a call for a human can make the difference between an extremely frustrated customer who might abandon your service and a customer who feels that they can securely access critical information without having to dig through their memory for an infrequently used password. And, of course, self-service greatly reduces your help desk costs. Industry experts say that each avoided help desk call saves $70, although we've seen a stronger ROI from customers in industries like banking and insurance.

Why you don't need to sacrifice TTM to create a delightful UX

Balancing customization and security with privacy requirements can sound like added 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.

Moving existing or acquired users to your new or updated product could 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 allows you to tailor your migration to your specific need:

- **Retiring legacy systems.** Maybe you have an on-premise 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. Depending on your solution, this

can remain unseen by your users; with some solutions, bulk migration may force unnecessary password resets.

- **Avoiding 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.
- **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.

The need to migrate your users on your timeframe is critical whether or not your CIAM solution is platform-neutral. Unlike workforce identity, CIAM needs to work cleanly across platforms: iOS, Android, and web experience.

Scalability

> "In today's online-first, intensely competitive environment, creating a monolithic inflexible CIAM system will quickly put on you on the path towards extinction."
>
> - Forrester's Customer-Obsessed IAM Operating Model, April 2020

Most people are willing to put up with at least a few inconveniences to collect a paycheck. Maybe they have to log into two or three or even four systems. Maybe the Single Sign-On (SSO) process is ridiculously lengthy. For workforce identity, the captive audience of workers has a static set of needs based on preassigned roles and controlling what workers can and can't access in order to prevent breaches or unseemly knowledge is prioritized over access.

Consumer identity presents a completely different set of challenges.

While customer experience is paramount, the ability to scale to millions — even billions — of users, often in response to short-term events like Black Friday or the World Cup, is critical.

If your CIAM solution won't scale, it won't work, because your target audience is not captive. They have lots of choices. If ordering a tasty sandwich from your company doesn't work, they will just satisfy their hunger with a click elsewhere.

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

Making sure you can get to the future from here

As mentioned earlier, you might be exploring a CIAM solution to solve an immediate problem, but you really want to plan for where you want to be in five years. If you don't, you might not be able to reach that future without a whole lot of pain.

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

- **Where does your business want to be in five years? 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 just to ensure that your users can continue to log into your product easily. Your ongoing maintenance budget should include regular updates for cryptography and a cyberattack protection strategy.

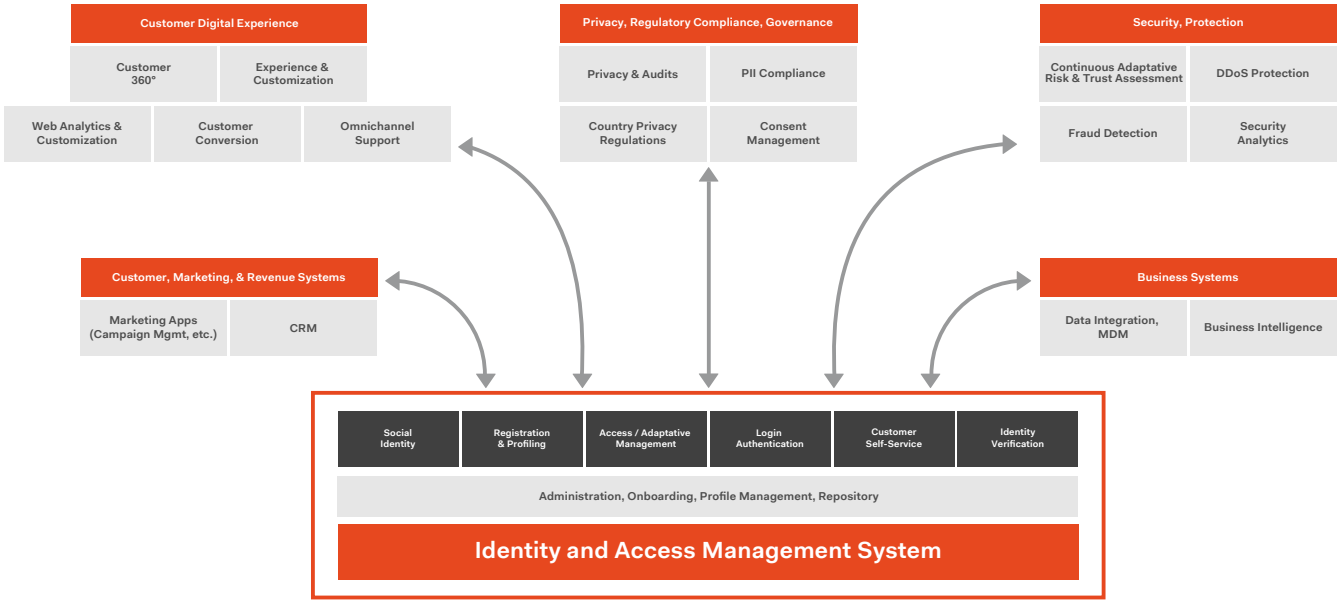
CIAM is definitely more than a login box

The solution you choose to power your login box will include a lot of moving pieces that need to evolve over time to keep up with your customers' changing needs (and demands) as well as 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. Also 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*, May 2020

Because of the need for scalability, CIAM is important to any company hoping to reach consumers. But for enterprises, it's a foundational element for 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:

- **Customer Digital Experience:** Customer 360°, Experience & Customization, Web Analytics & Customization, Customer Conversion, Omnichannel Support
- **Customer, Marketing, & Revenue Systems:** Marketing apps, CRM
- **Privacy, Regulatory, Compliance, Governance:** Privacy & Audits, PII Compliance, Privacy Regulations, Consent Management
- **Security/Protection:** Continuous Adaptive Risk & Trust Assessment, DDoS Protection, Fraud Detection, Security Analytics
- **Business Systems:** Data Integration, MDM, Business Intelligence

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

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

- **Customer convenience:** The need to provide the lowest-friction experience possible, in which customer needs are anticipated.
- **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 GDPR, CCPA, and/or 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 should provide facilities to leverage — and customize — how these four forces 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, for example, 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 Act on the Protection of Personal Information (APPI). This means how you've previously handled personal information may not be up-to-date, and this can be expensive, since fines have increased 100x over previous amounts.

The truth is that how well your CIAM functions as a central clearinghouse that feeds the rest of your organization can make the difference between the success and failure of your current and future initiatives.

Using the right mix of OOTB and extensibility to increase speed

Resolving all of the needs and demands across departments for something that is central to your ability to do business (if your customers can't log in, they can't buy or access your product) can be daunting.

It might conjure up memories of multi-year digital transformation projects that stalled after failing to deliver an ROI. But a weeks- or days-long turnaround is possible with the right CIAM solution.

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 and identify what you can roll out quickly (as short as five days for some businesses) and what might require more planning to execute.

An extensibility checklist

Many CIAM solutions claim extensibility but 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/compliance, and a consistent security/compliance profile.
- **Optimizable** to allow for balancing priorities including security/user experience and conversion/privacy. Permit customizations to balance (or optimize) for each of these four business priorities.
- **Open** to third-party ecosystem providers, communities, and external data sources/systems. No single platform can address all use cases, so opt for a vendor who provides a number of integration and extension points for 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. Yet 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 Customer-Obsessed IAM Operating Model, April 2020

The traditional thinking is that you always have to make a decision between security and convenience when it comes to interacting with your customers and how much effort you put into securing them and their data. The thinking is generally that greater friction equals greater security. That is the case, but with modern Multi-Factor Authentication (MFA) or continuous authentication scenarios, you can still moderate risk without sending your customers clicking elsewhere.

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 U.S. Breach-related costs include actual fines and reputation erosion that can lead to customers shifting to competing brands.

Many businesses make the mistaken assumption that CIAM security is only about fraud detection — making sure the right people have access to the right data at the right time. They get stuck in a security framework that pushes customer interactions as the potential for loss.

One of the largest pain points when it comes to CIAM is having to deal with decentralized data, for the simple reason that it's very difficult to secure what you don't know about. Decentralized data makes it even harder to comply with privacy regulations that require you to provide personal information data 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. The balance between security and convenience becomes less about friction vs. frictionless environments and more about what encourages trust in your customer at various stages in 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 are aware of the impact of the risk. Cyberattacks 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 and impatience with sign-in flows that take too long.

Attackers count on people being overwhelmed by volume and reusing passwords, which is how your ecommerce site can find itself the target of high-volume credential stuffing attacks. These can prove costly not just in the potential for breaches, fines, and reputational impact, but also in raising the cost of your services.

We find that seamless, low-friction MFA can not only avoid potential breaches, but when delivered at the right stage in the customer journey, can also be viewed as a 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 to determine whether or not a bot or human is attempting to access an account, can also be viewed as positively protective.

If you do suffer a catastrophic event, 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 by being based on open standards so that your security engineers (if you have them) can clearly understand how the data is flowing through your system, as opposed to solutions where data flows through the black box of proprietary code.

Various privacy regulations like GDPR, CCPA, and APPI require that you understand how your third-party providers are using or handling the flow of data throughout your system. Open standards will also make it easier for you to understand what you must do to comply.

Additionally, your CIAM solution should offer critical certifications like PCI, ISO20071, SOC 2 Type 2, HIPAA (for the U.S.), and Gold CSA Star, which signify that you are going through regular security checks via a third party rather than just claiming a strong security posture.

Increase protection and customer satisfaction

Centralizing identity will protect you in the specific instance of having a customer log into one app right now, but it will also set you up to create a unified (and more secure) brand experience. Instead of pushing your developers to work through potentially tedious security implementations again and again, you will have solved the CIAM challenge effectively and can apply it across multiple products, with final implementation taking minutes or days instead of months — or even longer.

Forrester points out, “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 is part of 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. Or that this customer has two other username/passwords at the coffee chain you're about to purchase, 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.

You also don't know that otterdog459/dolphinswimmer has racked up a ton of loyalty points, and that your merger has them pretty stressed that those points are going to evaporate after the merger — or what used to be worth six caramel macchiatos will be reduced to four cups of brewed coffee.

Not having a single source of truth makes it harder for you to understand your customer — and can cause them enough anxiety to move to a more convenient and comfortable experience with your competitor.

Why identity is the natural single source of truth

For some industries, like banking, knowing that you're doing business with the right person is a business requirement. Regardless of your needs, the more usable data you have, the better you can understand your customer and create experiences that delight.

The important part of that equation is "usable." You may have amassed a fair amount of data on your customers, but creating a 360° view of your customer is challenging, because some of that data is stuck in a CRM that is overdue for an upgrade and other data was gathered by an app written by a freelance coder who did not comment on the code.

Or maybe you run an umbrella insurance company with subsidiaries specializing in life insurance and property protection. You are able to draw a number of 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 five years from now. But the data from your life insurance and property protection brands is siloed, because each brand comes with its own login and sign-up flows, generating scads of siloed data.

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. That siloed information is making you miss opportunities.

If you undertake a massive effort to unify the data without solving the sign-up 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 sign-up clicks into moments of understanding, because you can generate a single source of truth in the form of a user profile.

Generating a user profile can help you resolve issues like duplication of customer data while 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 impact 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%, which is actually down from 3.42% in 2014. Today's customers have no patience for filling out frustrating registration forms. But that impatience can actually be to your benefit.

Implementing social login, allowing your customers to use their credentials from apps like Facebook or Google, can erase friction.

Open-source hardware and software ecosystem Arduino was able to reduce logins to "way less than a second" thanks to social login, greatly increasing opportunities for engagement with their 30 million users.

Likewise, Eric Jensen, Lead Mobile Engineer at nonprofit microlender Kiva, says, "By enabling native social authentication, our app's Facebook login times have been reduced by 50% compared to web authentication. And successful Facebook logins in our app have increased by 16%."

Your data, your way

One of the challenges with CIAM solutions is 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. Your privacy and compliance teams require a different set of insights, and your digital experience team has other priorities altogether.

No one CIAM is built to satisfy all of those needs. You could decide on tradeoffs, but because 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 information your way 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.

Bottom line: Regardless of how you prefer to consume your customer data, to understand your funnel, you should have access to all information pushed to tenant logs.

Operational costs

> "It's often, I think, underestimated how much does go into identity and some of those parts of the platform."
>
> - John McKim, VP of Product & Technology, A Cloud Guru

Pausing your business to deal with identity maintenance can cause friction that will send your customers to lower-friction competitors. The hard truth is that identity is not something you solve once. It evolves with your business.

Attack protection

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

Globally, data breaches are increasing in frequency. Forbes reported an astonishing 4.1 billion records exposed in the first six months of 2019, while 2020 is already setting data breach records.

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 updating to protect your customers, you may need to update to make 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. You might take on new partners and need to integrate their capabilities. Or you might expand into an entirely new region, which means required updates to your privacy and consent forms to comply with various countries' data privacy regulations.

Every day, technology is evolving, which means you're also 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. What you need in a CIAM now is not necessarily what you will need six months or a year or five years from now. You need a CIAM that can keep pace with you, helping drive innovation and growth instead of blocking it.

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 core focus to push the possibilities of innovation so you can 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 be costly in terms of operational costs as well as lost opportunities.

Especially if developers have to hard-code your changes instead of relying on last-mile customization, you're looking at a large time investment. Your developers may be extremely talented, but not at all 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

As a consumer-focused product, you're more likely to see that cost spread, because the wait will directly impact your customer experience by increasing friction which can lead 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. Multiplied by millions of customers, the cost quickly adds up.

Certification costs

Certifications like SOC 2, HIPAA, and ISO 27001 require an upfront investment to achieve the accreditation plus yearly costs to maintain it. But not having those certifications can be a growth blocker, especially when you're courting enterprise customers. "Most Fortune 500 companies won't sign deals if you don't have the applicable certifications," says Auth0 Senior Director of Governance, Risk, and

Compliance Adam Nunn. “Yearly tooling costs can vary from organization to organization, ranging from $25,000 to multi-millions, depending on the size of the org.”

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

Planning for CIAM success

> "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*, May 2020

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

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, there is a risk that you'll accidentally create siloed technology. It's worth taking another look through the list below and systematically thinking through your particular org 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 agreement between teams handling:

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

You're likely in for some intense discussions around the balance of security vs. convenience and privacy vs. revenue and retention. As Forrester points out, "CIAM is hard even if the tools are good." They recommend a monthly stakeholder meeting during and after implementation so that the critical juncture that is CIAM can keep pace not only with your evolving business needs, but also with the global pace of technology.

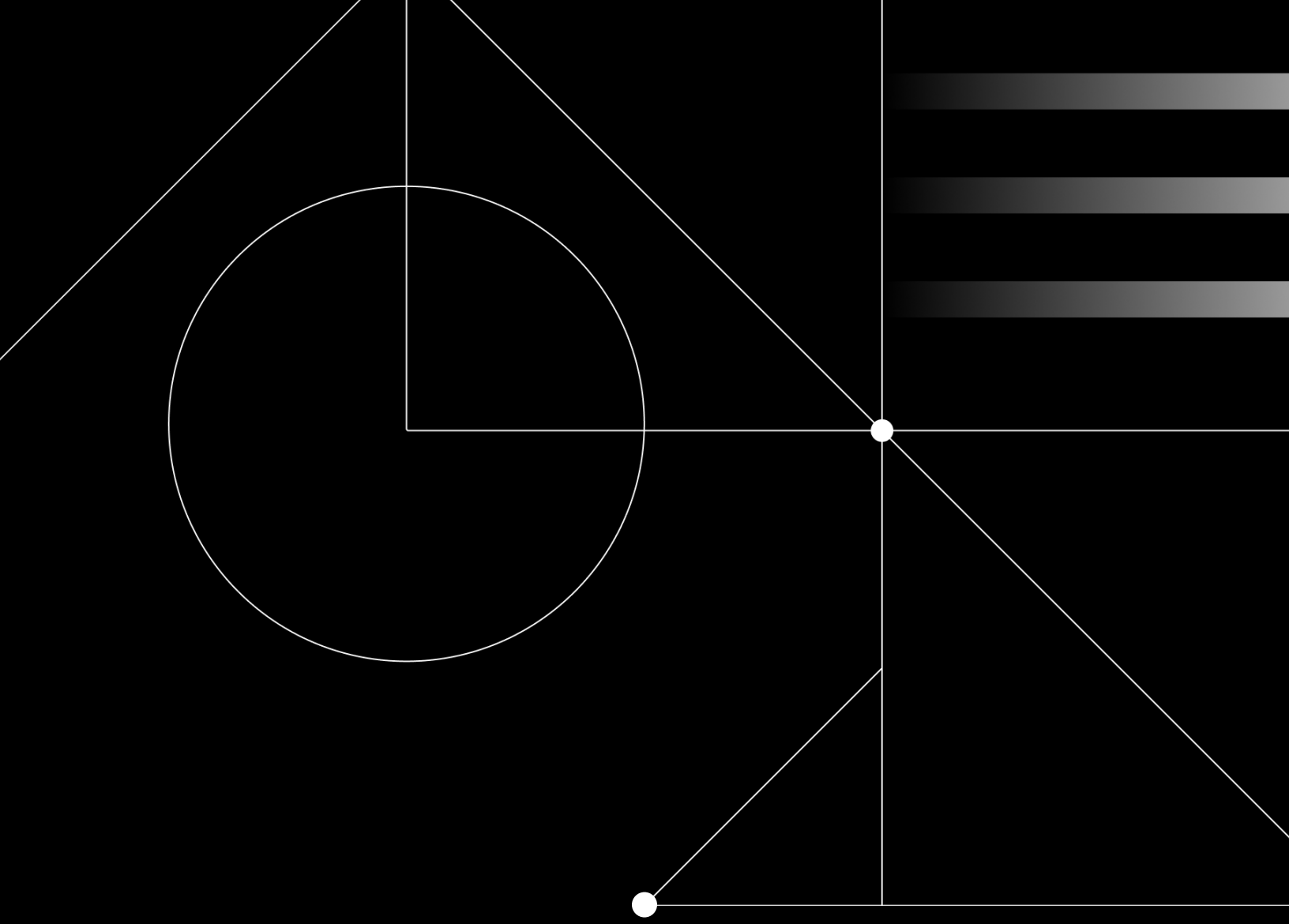
Identity impacts your entire customer journey. Resolving CIAM challenges with the help of a vendor focused not only on current but also future business possibilities means that you can use the CIAM

discussion as a framework to drive consensus and momentum for your evolving digital transformation strategy.

Here are few questions you should take 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/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 retention? Identity touches all functions.
- Does everyone understand the tradeoffs you're making for your unique situation?

For companies seeking a digital competitive advantage, Auth0 provides an extensible CIAM platform that improves user convenience, facilitates top-line customer conversion, and supports world-class security and extensibility. If you'd like to learn more about how Auth0 can help your company meet your unique goals, please reach out to an Auth0 Resource.



Auth0

About Auth0

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and application teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit www.auth0.com or follow @auth0 on Twitter.