

EBOOK

The 15 essential CIAM capabilities



CIAM that delights

Just like 10x vs 2x goals, rethinking CIAM is all about mindset.

It starts by setting aside limiting ideas about what's possible, which tend to be over-informed by what your current solution can do or how workforce IAM solutions handle sign in journeys.

It goes beyond asking what your customers expect, what your CISO will approve, what your IT team can support, and what your marketing team will accept. Those are important questions, for sure, but they don't go far enough.

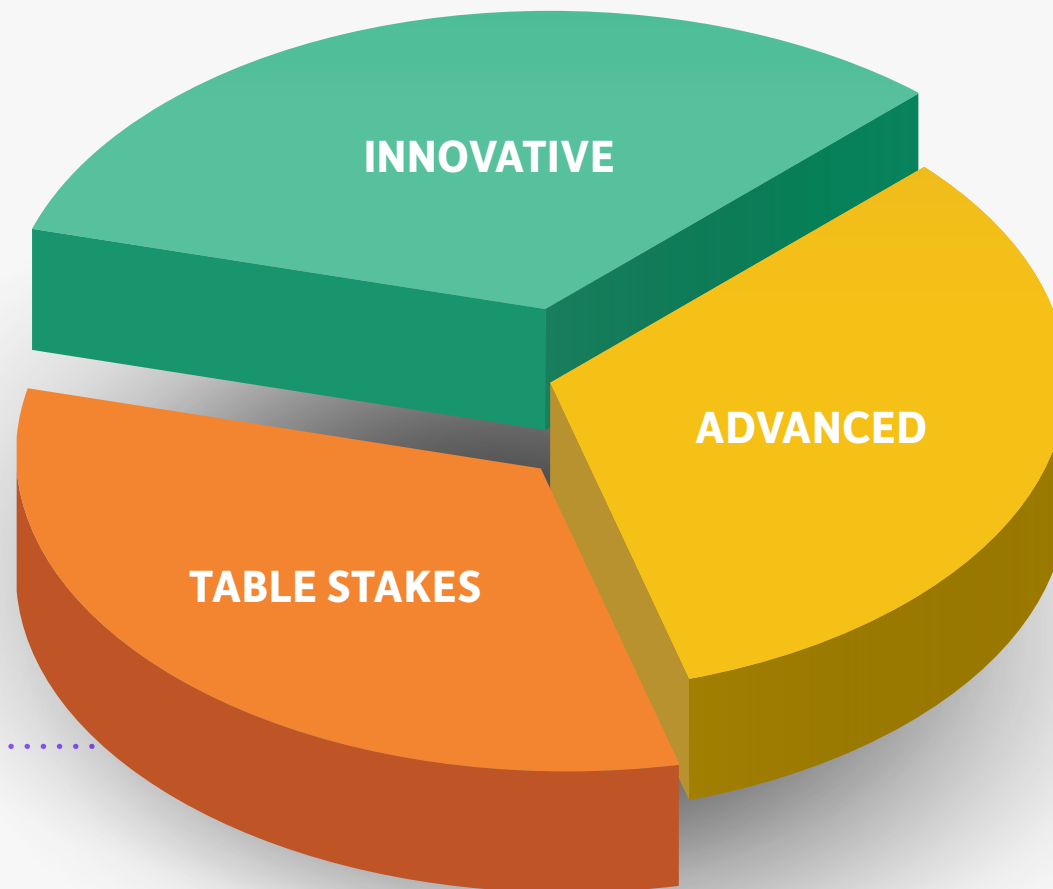
Instead, the driving question is: what would delight my customers, my CISO, and my marketing and IT teams?

To help you imagine what that looks like, we've compiled this list of 15 capabilities that make CIAM truly delightful: frictionless for customers, uncompromisingly secure, data-rich and capable of syncing with your customer intelligence systems, and easy to configure and customize.

15

Key CIAM capabilities you should evaluate

Of course, everyone is at a different spot in their CIAM journey. We've arranged capabilities into three groups. If you're just getting started you'll want to begin with the "table stakes" capabilities. Or, if you've got a running start and are looking to improve, take a look at the advanced and innovative features.



CIAM Table Stakes

These are capabilities that most CIAM solutions have but are often way harder to deploy than they should be..

Market availability: **Common**
(but often patched together)

SSO & MFA options



Rolling out authentication shouldn't be a complex or isolated task. CIAM solutions should enable you to customize and configure authentication options across multiple sites and brands with a straightforward configuration-based approach, no heavy engineering project required. Bonus points if the provider has an easy way to build and apply MFA policies in conjunction with adaptive MFA. This flexibility enables you to tailor authentication choices to meet the specific needs of your customers while also securing your business.

Account opening and progressive profiling



Converting customers and getting to know them over time should be easy for both you and your customer. A great CIAM solution streamlines this process by offering a selection of pre-built account opening and profiling templates, so you can launch quickly without building them from scratch. Using templates simplifies the onboarding process and helps eliminate form fatigue, so you collect only the data you need to provide personalized experiences.

Passwordless and social sign in options



Customers increasingly expect low-friction ways to sign in. Choose a provider that supports passkeys (the passwordless approach customers already rely on for signing in via Face ID, fingerprints, or PINs) and hardware security keys for situations requiring heightened assurance. Customers should be able to choose the method that works best for them. On the social side, look for a solution with seamless integrations with popular providers such as Google and Facebook. Social sign in simplifies the sign in process and captures data to better serve your customers.

Self-service profile management



Make it easy for customers to recover lost passwords and manage their own experience. In doing so, you can free up helpdesk support and obtain accurate customer data for upsell/cross-sell campaigns. Look for a CIAM provider that excels in automating self-service account opening, account recovery, and account management. Opt for a solution with an intuitive interface and easy customization to align with your brand, so teams can configure or code as needed.

Consent management



You should be able to build, deploy, revoke, and redeploy consents for any customer journey with simple policy settings and configuration. Your customers deserve the ability to self-manage their consents, with clear tracking mechanisms in place. Be cautious of providers urging you to build or integrate with a separate third-party product. Consider a CIAM solution that integrates consent management within its core product.

Advanced CIAM

These are capabilities that support more complex business needs, but which providers often bolt on, either by acquisition or via partners, because their CIAM solution doesn't offer them.

Market availability: **Medium** (but often added on)

B2B management (delegated administration and organizational management)



B2B customer experiences pose unique challenges, because each business partner wants autonomy over how they manage access, with their own distinct sign in flows. A strong CIAM provider handles both sides of this. First, delegated administration should be standard, so you can offload day-to-day access management to each B2B partner without building and supporting that yourself. Second, the best providers let you create separate organizations for each partner, linking each one to applications that serve both B2B and B2C customers, each with tailored policies such as MFA and self-service. Each partner can also bring its own identity provider (IdP), so their users keep signing in with the credentials they already use, including partners still on a legacy or on-premises IdP, with no need to migrate first. Configuration should be as straightforward as changing a policy. Providers that force custom coding for B2B use cases drive up implementation and services costs; the best solutions let you configure these flows directly and extend them with APIs and SDKs as needed, keeping those costs down.

Risk and fraud



Avoid the hassle of yet another add-on solution to detect and prevent risk and fraud. A modern CIAM solution should let you configure risk and fraud rules out of the box and evaluate every account opening and sign in against real signals in real time. Look for adaptive, risk-based access that evaluates signals like device recognition, IP reputation, geolocation, bot detection, and behavioral anomalies, then steps up, steps down, or blocks based on what it sees. The strongest solutions also flag risky signals like SIM-swap activity and suspicious phone or email provider reputation, block passwords exposed in known breaches, and throttle brute-force and credential-stuffing attempts. Give bonus points to a CIAM solution that can consume fraud intelligence from multiple sources so your decisions get sharper over time.

Identity verification and identity proofing



Fraud prevention keeps bad actors out. Identity verification does the opposite job: it confirms a legitimate customer is who they claim to be, both when they open an account and each time you're required to re-confirm it over the course of the relationship. Whether it's matching phone and address records against a claimed identity, or higher-friction checks like physical document verification (think drivers' licenses and passports), these capabilities should be available out of the box and easy to deploy. The payoff is less time integrating separate products and faster, more secure conversion.

Data residency



Keeping your customers' identity data in specific physical locations is a strict requirement, rather than a preference. Regulations like GDPR and a growing patchwork of regional data-protection laws mean you may need to guarantee that customer data stays within a specific country or region. Look for a CIAM solution that offers data residency by design, so you can meet these obligations without re-architecting, standing up separate deployments, or paying a premium for a private deployment. A single-instance architecture makes data residency more straightforward because your data isn't pooled with other organizations' data in a shared environment.

Multi-brand support and UX customization



User experience is critical to any online sign in, and a poor UX can reduce conversion rates and slow adoption. Two related capabilities make the difference. First, larger organizations need multiple branding policies across various applications from a single product. In complex B2B deployment models this is even more critical, since different partners require their own branded experiences to build trust in account opening and authentication; the right cloud architecture lets you configure numerous brands from a single product instance rather than deploying separate instances for each. Second, many CIAM providers separate UX development from their product, forcing engineers to use APIs to connect to the CIAM solution. A native branding editor makes it easier and faster to create and maintain your ideal customer experience. It can also speed up iteration through the editor, while APIs and SDKs let developers extend or automate the experience when they want to.

Innovative CIAM

You might be surprised to see what else CIAM can do. Here are a few capabilities that very few providers offer, even though they can really accelerate your business.

Market availability: **Rare**

Identity for AI agents



AI agents increasingly act on a person's behalf, such as booking, buying, or updating an account, without a human clicking every step. These agents raise a new identity problem: brands need to know an agent is who it claims to be, confirm it has permission to act and on whose behalf, and keep a record of what it did. The most innovative CIAM providers verify an agent is from an accountable organization before granting it access. Customers also get a way to see, scope, and revoke an agent's access themselves, with no separate system bolted on. You may not need this on day one, but the providers building it now are the ones who will be ready when agents show up in your customers' journeys.

Policy configuration and extensibility



You should be able to configure the majority of CIAM capabilities yourself, without professional services or custom coding. Services costs have historically run several times higher than the cost of the CIAM product itself, so configuration you can do on your own directly protects your budget. Innovative solutions let you use drop-down menus and policy settings to control everything from MFA options to B2B organization configuration to self-service policies and consent management. Configuration should extend to runtime, too. Strong solutions let you orchestrate real-time steps inside a customer journey, calling out to other systems and keeping data in sync as the journey happens, through configuration rather than hand-built integrations. Configuration keeps the majority of changes fast and self-service, while APIs and SDKs are there to extend the product when you need to customize further.

Customer insights and analytics



Most CIAM solutions tell you whether a login succeeded. Far fewer will tell you what it meant for the business. The same system running every account opening and sign in is the ideal place to show where customers convert, where they abandon, and where friction is quietly costing you revenue. Look for insights built in: dashboards that let you drill from any data point straight into the underlying event, even replaying a customer's journey step by step to see exactly where it broke, plus native A/B testing to prove a change against live traffic before you roll it out. The payoff is shared truth: digital, marketing, product, and security teams can all use this information to fix issues with friction, address fraud, and improve the funnel.

AI-assisted configuration



Even when a CIAM product is built for configuration over custom code, someone still has to know which policies to set and how to tune them. An AI assistant lowers that bar. Instead of hunting through documentation, admins can describe what they want in plain language and get guided help building and adjusting policies, journeys, and integrations. The payoff is faster time to value, less reliance on specialized expertise, and fewer misconfigurations that create security or experience gaps. Few providers offer this today, which is exactly why it belongs on your evaluation list: as identity grows more complex across customers, partners, and AI agents, an assistant that helps you keep up is a real accelerator.

Lifecycle management and provisioning



A customer's identity doesn't end at sign in. As relationships begin, change, and end, access and data have to be updated and removed across every connected system. Updating access by hand is slow and leaves stale accounts behind. Most CIAM solutions stop at authentication and hand this off to a separate identity governance product built for employees, not customers. Look instead for a CIAM solution that manages the full identity lifecycle natively, automatically provisioning access when needed, and orchestrating cleanup across systems when it's not. When a customer relationship ends, their access and data are removed everywhere they exist, not just from the login screen. The payoff: one product instead of two, fewer integrations, and automated cleanup that makes compliance obligations like GDPR's right to erasure practical without engineering heroics.

A foundation, not just a feature set

It's tempting to evaluate CIAM as a checklist of features. But the capabilities that matter most in three years may not be the ones you're comparing today. Customer identity already stretched to cover partners. Now it's stretching to cover AI agents. The pattern won't stop there.

So don't just ask whether a provider checks every box. Ask whether the same foundation can absorb what comes next without forcing you to start over. A product that treats customers, partners, and agents as one problem, on one architecture, is one you grow into, not out of.

Use this list to compare capabilities. Then ask which providers are building the foundation you won't have to replace.



The definitive list of essential CIAM capabilities

Stay ahead in 2026

ABOUT US

Strivacity is The AI Identity Company that helps brands deliver trusted digital experiences by managing agentic, customer, and partner identities in a single product. It brings identity orchestration, account opening, sign in, consent management, and fraud prevention together to reduce friction, improve conversion, and give business and security teams clear visibility into where identity drives or blocks growth. Built on a single-instance SaaS architecture with data residency by design, Strivacity helps organizations modernize customer identity while preparing for the agentic AI era.

©2026 Strivacity. All rights reserved.

205 Van Buren Street
Suite 120
Herndon, VA 20170

844 782 5486 strivacity.com