EBOOK

Choosing the right CIAM architecture

Navigating single-instance and multi-tenant SaaS solutions

strivacity

When it's time to buy a home, one of your first decisions is house vs condo or townhome. There's a lot to consider – party walls, proximity to neighbors, HOA restrictions, and other things make a huge difference in whether a place fits your lifestyle.

The same principle applies when considering a cloud solution for customer identity and access management (CIAM). Cloud architecture plays a pivotal role in shaping the efficiency, security, and scalability of the customer experience and your business outcomes.

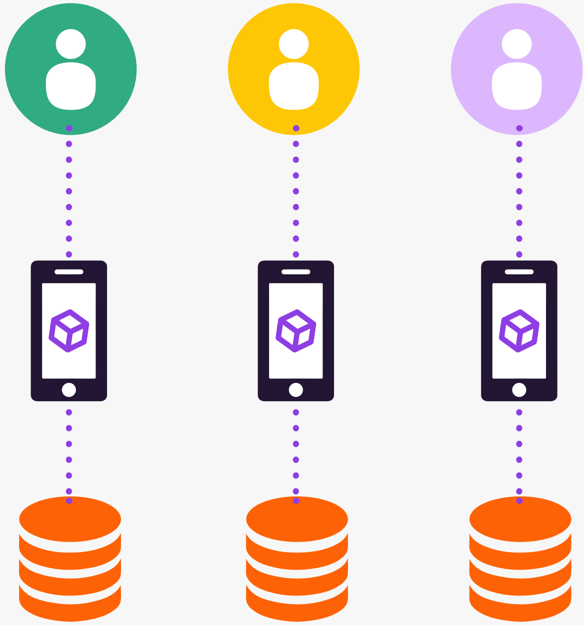
Because of this, the debate between single-instance SaaS and multi-tenant SaaS deployment architectures has now become an executive-level discussion.

Established players in the recently narrowed market, such as Okta and Ping Identity, have traditionally favored the multi-tenant approach – largely because they were designed for employee use cases and deployed on-premises.

But today, modern CIAM providers are offering a better choice for many brands: A single-instance SaaS approach that isolates customer data from threats and prioritizes the unique needs of customer identities. For a quick overview of how workforce IAM and customer IAM requirements are different **check out this blog post.**

Before we dive into the advantages, let's look at the differences between the two architectures.

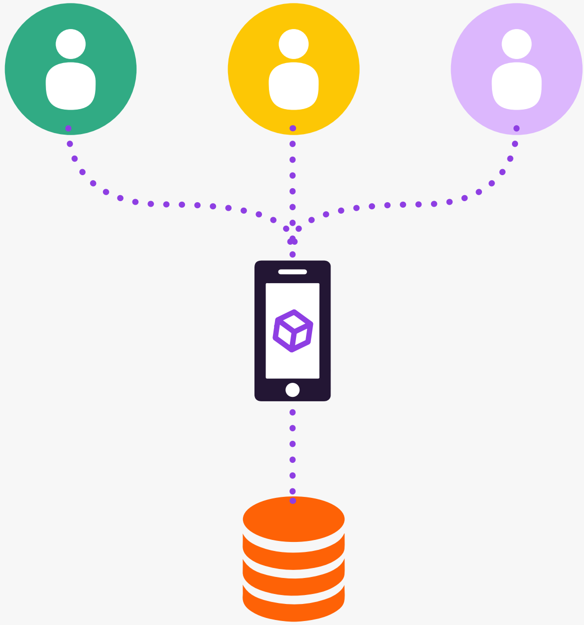
Single-instance



Customers are isolated from other tenants and customer data is not shared in any way.

Vs.

Multi-tenant



Customers share resources and data is stored in the same database.

What is multi-tenant SaaS?

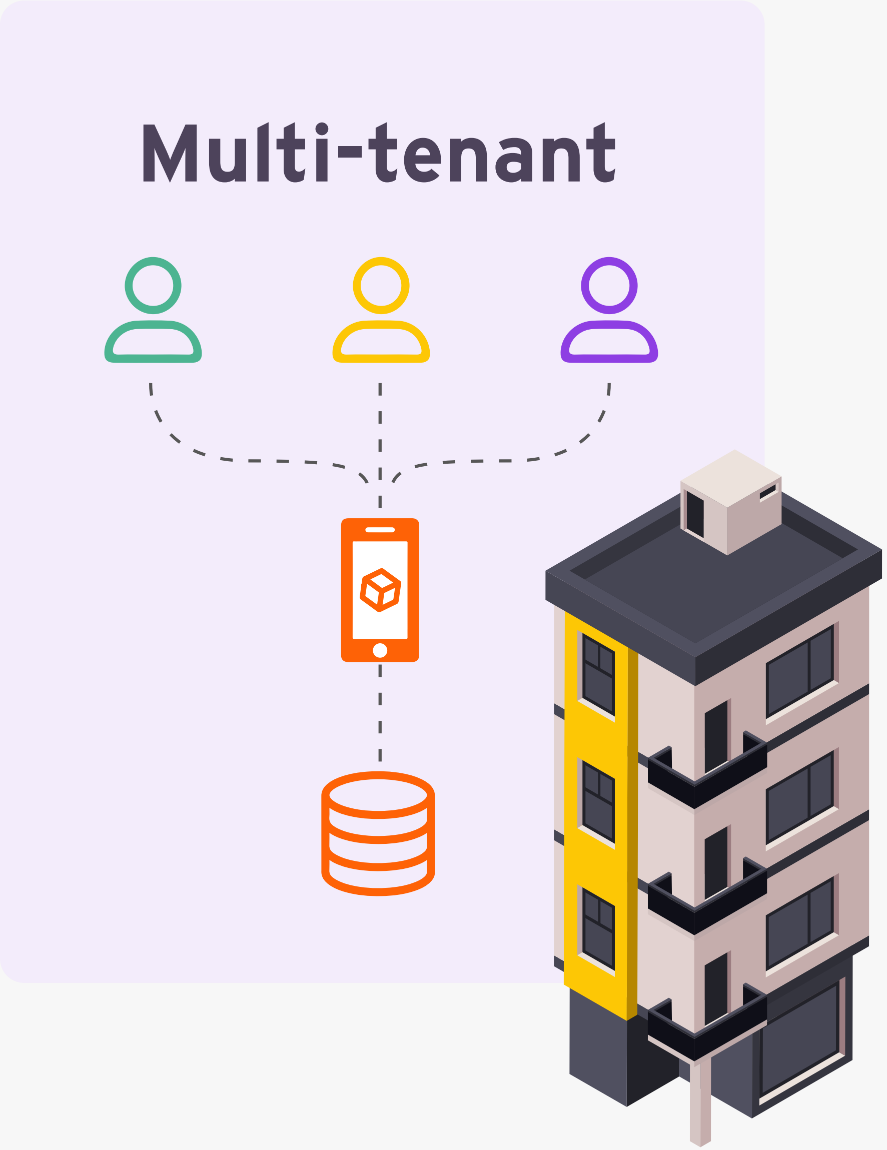
Multi-tenant architecture is like living in an apartment building, where each unit represents a brand that uses the solution.

Just like tenants share a common entrance and commingle in the elevator, stairwell, fitness center, and parking lot for their building, brands on a multi-tenant CIAM product share the same infrastructure and resources provided by the vendor.

This comes with some important trade-offs and risks – chiefly security and performance.

For example, if your neighbor's apartment catches on fire, at the very least you might be inconvenienced by the alarm. And when the gym is at capacity, your workout might be delayed.

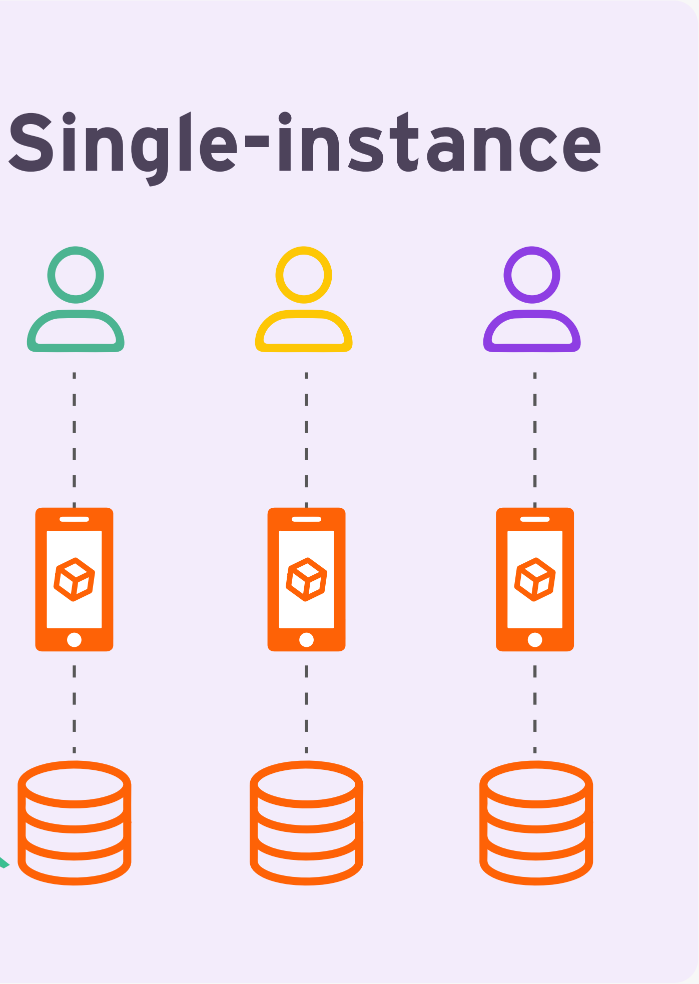
Similarly, if one brand on a multi-tenant CIAM solution experiences a data breach, all the others are at risk. And they all compete for bandwidth, which can slow site performance during peak seasons or events. As more brands are added on a multi-tenant solution, the greater the risk.



What is single-instance SaaS?

A SaaS based single-instance architecture is like a single-family house: You have exclusive use of the yard, the driveway, and everything else. If someone breaks into your neighbor’s house, there’s no way they can get to your stuff.

On a SaaS based single-instance deployment, each brand has its own fully isolated and dedicated instance, with exclusive access to underlying resources at all times. Any data breaches are isolated – with zero impact on other brands who use that solution.



Prioritize your customer identity requirements

When it comes to managing customer identity, there's a lot at stake. CIAM requirements vary by industry, market, business model, and other factors. There is no one-size-fits-all solution.

To help determine the architecture for your brand, first define your core requirements.

Understanding your brand's unique needs and objectives is essential before making decisions about underlying architecture. Consider factors such as scalability, customization options, security, privacy regulations, and resource allocation. Multi-tenant architecture offers cost-efficiency and streamlined management for brands serving multiple users with similar needs. On the other hand, single-instance architecture provides greater security, customization and control, catering to brands with distinct requirements or stringent data privacy regulations. By carefully evaluating your core requirements, you can choose the architecture that best aligns with your brand's goals and ensures optimal performance and scalability in the long run.

	You need...	
If your top requirement is...	Multi-tenant	Single-instance
Security	□	☑
Performance & scale	□	☑
Control & flexibility	□	☑
Privacy & compliance	□	☑
"Standard" CIAM features	☑	□
Tailored B2B2C use cases	□	☑
Ease of migration and vendor independence	□	☑
Deployment time	☑	□
Branding capabilities	□	☑
Shared resources (cost efficiency)	☑	□

5

reasons to consider a single-instance SaaS deployment for CIAM

Multi-tenant architectures have their merits and can be cost effective. But customer identity management comes with unique requirements. Sensitive data, high traffic, branded sign-in experiences – these and other needs make single-instance isolation a better option.

And if cost is a driving factor (when isn't it?), you might be surprised to learn some single-instance CIAM solutions cost less AND offer greater security and flexibility than multi-tenant workforce-centric CIAM providers.

Here's why a single-instance architecture stands out:

Greater security

We covered this above, but it's worth repeating. A single-instance architecture provides dedicated environments for each brand, minimizing unauthorized access and the risk of attackers compromising data. To establish and maintain the trust of customers, brands must make safeguarding customer data a top priority.

Performance and scale

Performance is critical for CIAM solutions since any outage can impact revenue. In a multi-tenant environment, resource contention can result in performance lags, especially during peak usage periods. Isolated tenancy minimizes the risk of performance fluctuations since resource allocation is specific to each tenant. And while multi-tenant architectures are known for scale, single-instance environments that employ microservices autoscale capacity even more reliably.

Brand customization and flexibility

For brands with unique sign-in flows or complex business models, multi-tenant architectures can limit your ability to customize, offering only standard features. Conversely, a single-instance architecture gives each brand greater control over configurations and branding policies.

Regulatory compliance and data residency

For brands in regulated industries, compliance and data residency standards often demand a single-instance CIAM solution. Unlike multi-tenant alternatives where data is commingled, a single-instance architecture ensures data isolation, aiding in meeting specific compliance requirements. This approach allows control over the physical location of customer data. For example, it enables serving multiple business units within the same global organization while keeping user data segregated to each unit. Data isolation also enhances control over audits and compliance reporting – crucial for regulated industries.

More migration options

Unlike multi-tenant environments, single-instance architectures offer a high degree of customization and independence for each brand. This makes it easier to migrate customer identities in ways that are less disruptive to your customers. For example, single-instance architectures allow for a phased approach where one customer can be migrated at a time. Phased migration minimizes the risk of errors and enables you to roll back changes without affecting other tenants.

Taken together, the advantages of a single-instance SaaS architecture present a compelling case for any brand looking to modernize its CIAM – with a clear business case for your CISO, CTO, and compliance and marketing teams.

We know, because our clients tell us all the time.

If you're ready to see how Strivacity's approach to CIAM architecture (and so much more) can make a difference for your business, we'd be happy to give you the house tour. Come on by and ring the bell anytime.

Choosing the right CIAM architecture:

Navigating single-instance and multi-tenant SaaS solutions

ABOUT US

Strivacity lets brands add secure log-in and identity management capabilities to their customer-facing applications without tying up a crew of developers or consultants. We offer a unified customer identity and access management (CIAM) solution that uses clicks (not custom coding) so organizations can get going fast and don't have to choose between creating great customer experiences, securing their customers' data and staying compliant with fast-changing privacy regulations like GDPR and CCPA. To learn more about Strivacity, visit www.strivacity.com.

205 Van Buren Street
Suite 120
Herndon, VA 20170

844 782 5486 strivacity.com