Ping Identity

THE ARCHITECT'S GUIDE TO CLOUD CUSTOMER IAM

How to Safely & Swiftly Migrate Customer Identity Data to the Cloud

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

Cloud-first has become an everyday term and a pervasive rally cry. What started out as a U.S. government mandate nearly a decade ago has become the goal of commercial enterprises worldwide.

It makes sense that organizations large and small are favoring online services over onsite hardware and software. When you can leverage SaaS solutions that have zero infrastructure for you to manage, you're able to realize the pinnacle of cost savings and efficiency. And what enterprise isn't looking to save money and be more efficient?

Cloud-first initiatives have become so common that you'd be hard-pressed to find an enterprise that hasn't made cloud-first a strategic priority. And the search for SaaS offerings has extended beyond the IT department to every corner of the enterprise, including customer identity and access management (CIAM).

But moving your customer identities to the cloud—just like any large data migration—can be tricky. Because customer data also affects your ability to generate revenue and includes personally identifiable information (PII), it requires additional considerations.

First, you have to completely trust the security of the outsourced service that you select to store your valuable customer data. Additionally, you have to accept that there is no migration "easy button."

Your transition to the cloud can start now, but it will likely be a multi-year process to complete. Or, like many large enterprises, you may only transition some applications while continuing support indefinitely for other on-premises apps and data stores.

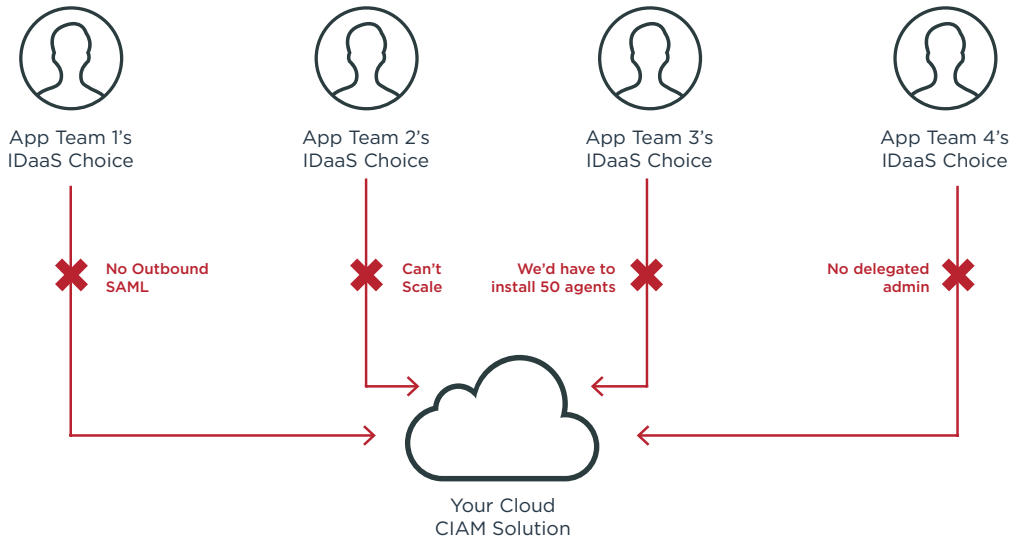
These types of hybrid deployments are increasingly common. You may elect to maintain on-premises infrastructure because you've customized your data stores and associated apps so much that they're difficult to decouple. Or you may not have adequate resources to devote to the migration. Furthermore, those on-premises applications may still be exposed to your customer base, and you may not be able to sacrifice them in the name of a SaaS solution.

Whatever your specific situation, you need to be aware of the obstacles you could encounter when implementing a CIAM solution. But the good news is that there's a path to SaaS for most large enterprises. You just have to be aware of the potential pitfalls you could encounter along the way. Read on to learn more about the unique requirements of CIAM and how to evaluate a SaaS solution so you don't end up making unacceptable compromises.

ENABLING YOUR APPLICATION TEAMS

Right now, as you read these words, it's very likely that several of your app teams are already considering SaaS-based solutions for their customer identities. You have an opportunity, if you act quickly, to influence those decisions and ensure that any solution being considered also addresses your requirements. If your app teams are left to their own devices, they may choose a solution that introduces security holes, disjointed customer experiences and integration roadblocks down the road.

As you get the lay of the CIAM landscape, you need to first know that many SaaS-delivered identity solutions are designed for small and mid-sized businesses (SMBs). These products are easy to use because they have extensive docs, APIs and a ton of sample code—all of which are important to the development teams implementing the identity solution.



The problem, though, is that SMBs don't have as many apps or as much existing infrastructure to support as large enterprises. As a result, they don't require the same caliber of integration capabilities, standards support or security features that you do.

Because your app teams (like SMBs) move fast, they may not consider the ripple effect their decisions can have. App teams often take a shadow IT approach to CIAM, implementing a solution for customer identity without consulting IT or realizing the need to address enterprise-level requirements around security, scalability, performance, integrations and the like.

This mistake is often innocent, and it may even work out okay in the short term. But as you probably know all too well, it can leave a large burden on enterprise architects and IT teams when it comes time to connect other apps to the cloud identity solution they've chosen. Beyond the headaches this creates, it can also affect customer experiences and the security of customer data.

So your objective becomes identifying what's needed in a SaaS-delivered customer IAM solution to satisfy both their needs and yours. In doing so, you can confidently guide your app dev teams to a sound decision. But how do you know what your needs are? You could ask other architects in large enterprises in similar situations. And we already did.

ASK THESE 3 QUESTIONS

Here are the critical questions to ask when evaluating a cloud CIAM solution, based on the lessons learned by architects who are a few steps ahead of you on their journeys.

QUESTION 1

Will it allow you to retain your on-prem identity models?

If you're a large enterprise interested in moving your customer identity data to the cloud, there's a good chance you'll end up replacing—or at the very least extending—existing customer IAM solutions that you have on-premises. A replacement is often warranted if your current solution:

- Can't support protocols like SAML, OpenID Connect and OAuth
- Has a rigid data schema
- Includes a customer data store that can't scale
- Lacks core identity provider capabilities

But for all the capabilities you seek, there may be several others that you already have and want to keep. For example, you may have invested a lot of time and energy defining different types of users or building multiple environments associated with different applications or regions, as well as implementing delegated administration across those environments.

If you've gone to great lengths to modify your current solution to meet your needs, you may understandably be unwilling to scrap these features as you move to the cloud. But modeling that type of architecture would be impossible with many SaaS-based CIAM solutions. Many are geared toward SMBs with a handful of apps, who don't share your challenges.

To be sure any solution under consideration is capable of modeling the architecture you've spent so much time building, you can advise your application teams to look for the following requirements:

Tenant-in-tenant Architecture

Can you host multiple environments under a single account?

Core Identity Provider Support

Does the solution support authentication and registration, user provisioning, MFA and other core capabilities you'd expect from an identity provider?

Delegated Administration across Environments

Can you vary administrative privileges across environments (i.e., can you give the same user more privileges in one environment and less in another without requiring them to have multiple logins or share accounts)?

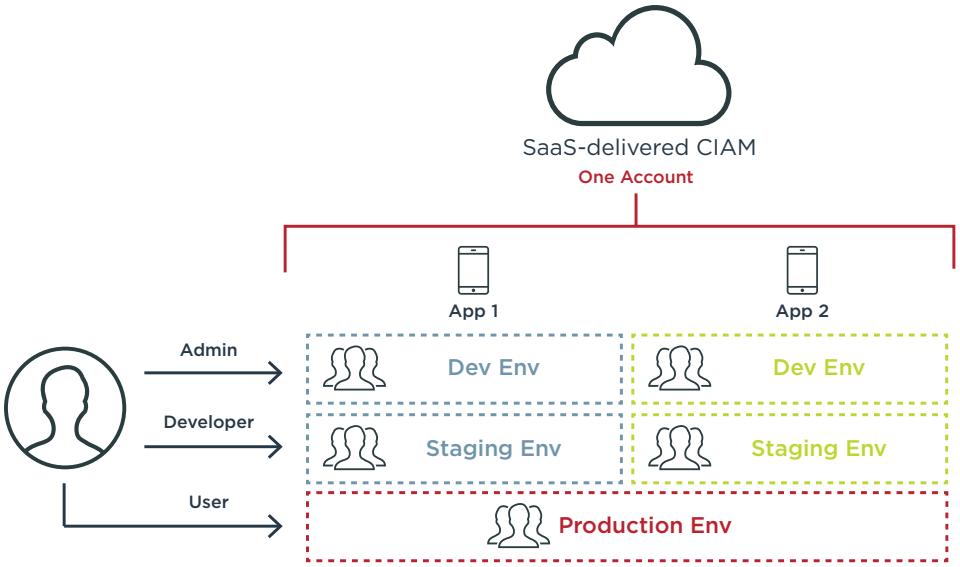
Multiple Schemas

Can you define different schemas for different user types? Can you add custom attributes—including JSON—to those schemas?

Standards Support

Does the solution support OAuth, OpenID Connect and SAML in the manner required to support your use cases?

These are capabilities that your development teams probably won't consider on their own. But if you educate them about their importance now, you'll gain the ability to model a solid identity architecture in the cloud, and you can use their app to jumpstart your migration as well.



A SaaS-delivered CIAM solution should be able to support multiple environments within a single account without requiring separate logins or API keys to manage. It should also allow delegated administration across those environments.

QUESTION 2

Does it support on-prem apps and infrastructure?

As much as we all wish it were easier, cloud migration isn't as simple as flipping a switch. While an SMB may have the luxury of forklifting all of their customer data to a SaaS solution, large enterprises typically don't. More often, there is a period of coexistence between cloud and on-premises applications—sometimes with no foreseeable end.

Your application teams may not realize what's involved in migration at the enterprise level. While they may see little issue in starting fresh with their customer identities in a new SaaS solution, you know to think beyond the scope of a single app. As a large enterprise, you probably have other customer identities you need to think about.

If you don't take a global approach, you may find it impossible to move identities to or synchronize them with the new cloud CIAM solution. For example, what if you want to use the new CIAM solution as an identity provider (IdP) and let customers use it to log in to other apps for a more consistent experience? Even if you can make these situations work, it may prove very difficult due to the separate agents and SDKs required for all of your on-prem apps, each with separate single sign-on (SSO) solutions.

Failing to address these considerations up front can result in workarounds—and lots of heartburn—later on. To guide your application teams to a solid solution the first time around, look for these specific features:

Support for Multiple Applications

If a SaaS-delivered CIAM solution requires extensive custom coding for development teams, doesn't have centralized authentication policies or doesn't allow you to store multiple schemas, it can spell trouble as you start attaching more and more applications to it.

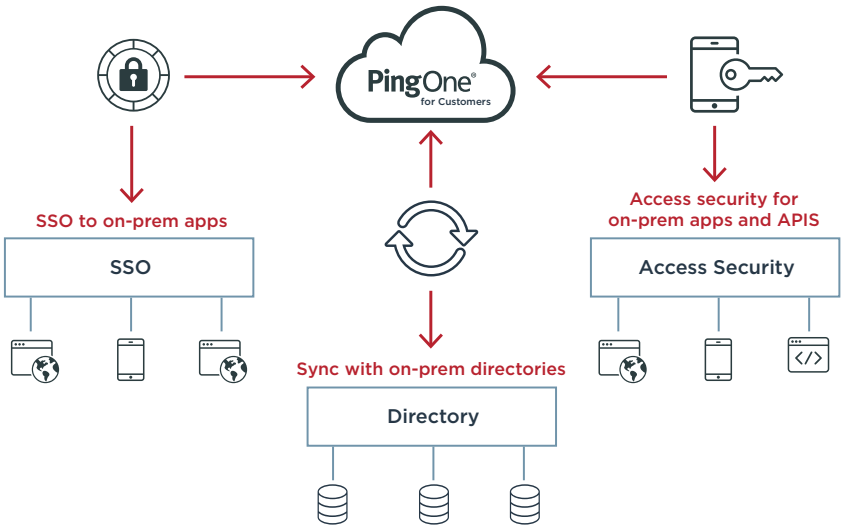
User Synchronization

You may have on-premises directories with connected apps that need to continue storing up-to-date customer data during your migration to the cloud. To support this, you need a solution that can bi-directionally synchronize users with an on-premises unified profile.

SSO Integrations

If you have an on-premises SSO solution, you may need that solution to be able to trigger authentication with the SaaS identity provider. Standards support is a part of that, but integrations that make it easy to trigger SaaS authentications from existing policies can save you a lot of time.

Suggesting that your app team prioritize a SaaS platform that allows you to integrate with the on-premises SSO solution—at the very least with standards support, if not with specific integrations—can help avoid a lot of problems down the road. Ensuring a CIAM solution can support coexistence during your transition to the cloud can also make your journey much smoother.



A SaaS-delivered customer identity solution should be able to coexist alongside your on-premises identity infrastructure.

QUESTION 3

Does it provide strong security capabilities?

Application teams don't typically have deep security expertise, so they may overlook basic security capabilities in their preferred SaaS solutions. This could result in gaps and loopholes that threaten the security of your customer data and could even put you at risk of a breach.

Taking the lead on security will ensure you end up with a SaaS-based CIAM solution that checks your security boxes. And it should be an easy sell to app teams since they typically want to offload as much of that responsibility as possible.

But be wary of potential pitfalls. You'll be hard-pressed to find an identity solution provider that downplays their security features. So you need to dig deeper to uncover a solution's specific capabilities. To ensure your enterprise security requirements are met, verify that the solution provides:

Password Hashing

Does it support the strongest algorithms (bcrypt, scrypt, and salted SHA-1, SHA-256, SHA-384, SHA-512)?

Multi-factor authentication (MFA)

Does the solution have customer MFA that doesn't require third-party apps or devices? Can it send customized messages to let customers know exactly what they're approving?

Configurable Authentication Policies

Does it support configurable authentication policies without requiring custom coding from developers (that aren't security experts)? Can those policies be different from app to app?

User and Admin Activity Audits

Does it have the ability to audit user and admin activity? Can you access that activity via APIs for use in third-party tools?

Delegated Administration

Is there delegated administration within a single environment? Can you limit administrative privileges based on which environment, app or user population?

Aside from MFA, your application team may not consider these important safety features. But failing to address them could result in security holes that put customer data at risk—and that will require plugging later on.

> **A mature approach to security and a well-defined internal security concept are key factors when evaluating CIAM products.**
>
> - KuppingerCole, Leadership Compass: CIAM Platforms

MIGRATE CUSTOMER IDENTITIES SWIFTLY AND SECURELY

Given the plethora of cloud CIAM solutions on the market, choosing the right one is critical. As an architect, you can guide your application teams to select a solution that not only meets their needs for ease of use and rapid deployment, but also meets your requirements for flexibility and data security.

To ensure a CIAM solution achieves the latter, you need to specify your requirements first. You can learn from those who've journeyed ahead by making sure that any cloud solution under consideration is able to:

- Model your existing architecture
- Coexist with on-premises applications
- Provide strong data security capabilities

Cloud-first initiatives are a top priority for enterprises across the globe—and in departments throughout your organization. You can help your application teams make the best decision for themselves and everyone involved by taking the lead—or at least providing sound guidance—on the must-haves of an enterprise-grade cloud CIAM solution.

To learn more about securing customer-facing applications, visit developer.pingidentity.com.

(You can share this link with your app dev teams, too!)

Ping Identity.