IT's Key Role In Your Customer Identity Initiative

✓ CHECKLIST

TABLE OF CONTENTS

INTRODUCTION

Customer identity and access management (CIAM) often bridges the gap between IT, marketing, application development and lines of business. It builds a foundation of identity and gives your enterprise the ability to identify customers and know their preferences no matter which channel or device they're using to interact with your brand. It also enables you to protect your customers' privacy and ensure that their data is safe from breaches.

A number of different solutions, not limited to customer IAM, claim to be scalable and secure, protect customer privacy and create unified profiles that facilitate omnichannel engagement. But without understanding the mechanics of how this is achieved, those claims could be marketing fluff as easily as they could be legitimate solutions. Or, a solution may be suitable for an isolated app launch or two, but as use cases expand and more sophisticated integrations are required, they fall short. Enterprises need to evaluate what's under the hood to ensure that they are able to achieve intended outcome after spending time and money implementing the solutions that make these claims.

You'll never run into a sales rep of any customer IAM solution who says their solution isn't secure, isn't scalable, can't comply with privacy regulations or can't create a unified profile in your environment. However, many CIAM products are evaluated by lines of business, marketing or individual app dev teams that don't have the necessary technical expertise to truly understand the larger ramifications of the solution they're choosing. In these situations, you risk implementing a quick fix that could potentially cause major roadblocks for future initiatives.

You can make a number of specific inquiries to filter through the marketing fluff and determine whether a solution has the scale, security, privacy protection and ability to create a unified profile that you need. To really dive into these details and confirm whether a solution will work in your specific environment and use cases, it's critical that IT be involved.

> "During the planning stage, or even as late as the implementation stage, some organizations find that their current on-premise IT infrastructure is in some ways insufficient for handling the projected needs of the CIAM solution...IT teams should welcome the opportunity to work with Sales and Marketing to transform IT into a revenue producing service."
>
> - John Tolbert, KuppingerCole Analyst

[1] *John Tolbert, "Ping Identity solutions for Customer Identity and Access Management," KuppingerCole, March 2017, accessible at https://www.pingidentity.com/en/resources/client-library/analyst-reports/2017/3208-kuppingercole-solutions-for-customer-iam.html*

AVOIDING CIAM ROADBLOCKS THROUGH IT INVOLVEMENT

Sometimes it can be hard to imagine how a few simple assumptions could turn into a roadblock, so here's an example. Let's say you talk with a customer IAM vendor who says they can create a unified profile that's scalable enough to handle the number of customers you have. After implementing, you discover that some production applications have identity data hosted on premises that can't be moved to the cloud for the foreseeable future (which could happen for a number of different reasons). As a result, you end up with some identities stored in a unified profile, and others in a separate repository.

For your customers, that means two applications may have different sets of information about them. So they could opt out in one and continue receiving communications from the other. Or they could update their preferences in one application, and the other wouldn't be able to leverage those preferences to consistently personalize across channels.

Furthermore, you may find that the unified profile can handle your volume of customers under normal usage circumstances, but in peak usage scenarios–think Black Friday for retailers or tax day for tax preparation software companies–it may crash. Peak usage scenarios are the most likely and the most costly times for systems to fail. It's critical that solutions are able to handle them.

These are just a couple small examples. Other scenarios exist that are difficult for those outside of IT to foresee in the realms of privacy, security, scalability or the creation of unified profiles.

HOW CAN IT HELP EVALUATE A SOLUTION?

IT will know to ask many questions due to their familiarity with the technical requirements of various systems across your enterprise. Often, whether a customer IAM solution will work comes down to a specific standard or use case that isn't supported. These details may sound insignificant in the context of a specific application launch, but IT will be able to instantly identify them and shed light on how certain details may affect future initiatives. Even if the current initiative the solution is tied to is small and relatively isolated, it's still important to consider future integration plans or digital business initiatives that may benefit from leveraging the customer IAM platform.

The line between a partial solution and a thorough one can be a little fuzzy in a few areas. If you're an application developer, marketing or line of business professional, we'll examine several of these areas and give some guidance into questions IT can ask to help you evaluate a solution. If you're an IT or security professional, share this with your application development, marketing and LOB counterparts to convey the importance of your involvement in these evaluations.

SCALABILITY

What does scalability mean? Does it mean 100,000? 10,000,000? More? It's important to define the answer to that question with any customer IAM solution and ensure that the solution can not only handle the scale for the initiative you're initially leveraging it for, but for scale that may be required for future initiatives and growth. IT can help evaluate this by asking questions like:

✓ **Can the vendor handle peak usage and unexpected demand spikes?**
Some scenarios that cause peak usage, like Black Friday and Cyber Monday, can be planned for. Others, like the Fed raising interest rates or a marketing campaign going viral, cannot. If your customers are unable to authenticate during these demand spikes, it can be very costly for your organization. IT can take a close look at a vendor's ability to handle peak load, and ensure that your CIAM solution won't go down at a critical time.

✓ **Can the vendor prevent Denial of Service (DoS) attacks or peak usage in a single app from bringing down other apps?**
If not, anything from a DoS attack or error in an application to actual peak usage in a single application could put all your other applications at risk. This is particularly important if the app that brings your system down is not critical. In these cases, it is much better to detect the load and shut down that app, without risking the availability of all your other production applications. IT can evaluate details like this to ensure that your customers will always be able to log in and access their data in your mission-critical applications.

✓ **Are there reference customers who have achieved the scale we'll need?**
This seems like a simple question, but it's imperative to get examples and referenceable customers who have achieved the scale you'll need. If you don't, you run the risk of apps going down. There is a big difference between a vendor being able to theoretically handle 100,000,000 users and associated peak load, and a vendor having actually done it a number of times. Scale is more than just a number of customers. IT can look into these reference customers and ensure that the scalability they've achieved matches your needs.

SECURITY

Security is a critical area to get right. If you put your trust in the wrong type of solution to secure your customer data, it can cause brand damage that catches the attention of your C-suite. If that happens, you definitely don't want to be asked why the system responsible for the breach wasn't thoroughly evaluated. All vendors are not created equal in the realm of security. However, every single vendor will tell you that they can adequately secure your customer data. IT and security teams can help ensure you've vetted customer IAM systems before trusting them with your customer data, but only if they're involved in the procurement process. Here are a few of the areas they can help evaluate:

Will we have control of securing customer data?

Often, CIAM vendors will require you to offload your customer identities into their cloud environments. In the process, your security teams must relinquish all control of the protocols that secure that data. It's imperative that you are confident the security practices the vendor has in place are up to your security team's standards for storing and securing your customer data. IT can help you ensure that this is the case, before you relinquish control of your customer data.

Does the vendor have a secure MFA solution that customers will actually use?

Many organizations leverage SMS or email for multi-factor authentication (MFA). Unfortunately, as pointed out by the National Institute for Standards and Technology (NIST)[2] and many others, these mediums aren't secure methods of performing MFA. SMS relies on phone numbers that can be moved from phone to phone, and as a result, aren't difficult for hackers to intercept. Email often relies on the same set of credentials that hackers may already have. MFA is supposed to be a second line of defense if those credentials get stolen, but that doesn't work if the credentials can also access the email address the MFA request is sent to.

Additionally, both of these mediums cause users to have to go into other apps, open up new browser tabs and/or copy and paste one-time passwords from clunky mobile UIs. These mediums are neither secure, nor convenient. Customers need an MFA solution that is both, and together with IT, you can evaluate that balance in a CIAM vendor's MFA offering.

Can the vendor prevent against insider attacks?

Many features at the data layer, such as sending alerts when new admin accounts are created or have passwords changed, can let you know about a potential insider attack before it happens. There is a long list of similar features—tamper evident logs, limitations on access to records for administrators and others—that aren't often thought about in the context of a single app launch, but are critical to protecting customers. IT can help you ensure that these features exist to protect against insider attacks on your customer data.

[1] *Dustin Maxey, "Should You Use SMS as a Security Factor for Customers?" Ping Identity, September 25, 2017, https://www.pingidentity.com/en/company/blog/2017/09/25/should_you_use_sms_as_a_security_factor_for_customers.html*

PRIVACY

With the publicity surrounding Facebook CEO Mark Zuckerberg's appearance before Congress, and Amazon and Apple refusing to infringe on customer privacy, even to help with criminal investigations, your customers are very familiar with privacy and expect you to take an active role protecting their data. Additionally, regulations like the General Data Protection Regulation (GDPR) are levying significant fines on companies that aren't good stewards of their customers' data. Customer IAM platforms generally provide some level of privacy protection for customers, but there are significant differences in providing a foundation of privacy and data access governance, and surface-level terms of service capabilities that don't actually enforce consent. IT can help you evaluate these differences by asking questions like the following:

✓ **Can the solution enforce data sharing on specific attributes?**
There is a difference between a solution enforcing the collection of consent, and enforcing data sharing based on user consent. Enforcing the collection of consent simply means that you're ensuring your customers have agreed to your latest terms of service. In that scenario, it's possible for you to misrepresent how you'll be using your data, and it isn't very digestible to customers. Alternatively, if you collect specific consents about which attributes can be shared and with whom, then you can actually restrict attributes from applications that customers haven't agreed to share. IT can help you evaluate which solutions provide surface-level privacy solutions, and which ones can enforce consent and provide a foundation of privacy at the data layer.

✓ **Can the solution adhere to data residency requirements?**
Many privacy regulations, such as GDPR, require you to store data for some customers in certain regions of the world. Software-as-a-Service (SaaS) or Identity-as-a-Service (IDaaS) vendors often have a finite number of places to store data. They may not have an option to store identity data in a region that complies with data residency restrictions you have to meet. They may also not have the means to selectively store some users in one location and others in another. If you're deploying on premises or in the cloud, there can be additional challenges. Some data may need to remain on premises, and storing certain attributes in those repositories may violate data residency requirements. A number of different scenarios may also require you to replicate or synchronize data across regions. Fully synchronizing that data may not comply with data residency requirements. Your IT team can help you identify whether a vendor has the capability to partially synchronize data, or otherwise ensure that data can be stored in a way that complies with data residency restrictions.

CREATING A UNIFIED PROFILE

Many vendors of all types, not limited to customer IAM vendors, will tell you they can give you a unified view of your customers. This could mean anything from storing all of your user data in the same place, to aggregating some info about the customer in a separate business application. Truly developing a unified profile needs to be done at the data layer. All applications need a developer-friendly way to access the exact same customer data. You also have to consider how to get all of your data into a unified profile. It's often not simple for all applications, and a batch import isn't always possible. IT can help you examine some of these areas and determine how feasible a vendor's vision of a unified profile is in your actual environment.

✓ **How will we migrate data to the unified profile?**
Having a unified profile that's scalable, developer friendly and secure is only half the battle. The other half is actually getting the data there. It simply isn't always possible to do a bulk import of all of your user data. Sometimes getting data into unified profiles may work well for some applications, but not others. This may leave you with a partially unified view of your customers that still causes them to have frustrating and disjointed experiences. IT can help ensure that a CIAM solution provides capabilities that facilitate the migration of customer data from all of your digital properties into a unified profile with zero downtime for the production applications.

✓ **How will we include applications that can't initially be migrated?**
While it may be your goal to eventually migrate all applications to a unified profile by pointing them at its REST APIs to get the user data they require, some apps may need to remain attached to their existing repositories for a while. It's important to confirm that these apps can still be included in the unified profile even before they're migrated. IT can help ensure that capabilities like real-time data synchronization can keep legacy repositories in sync with the unified profile so all apps can share the same view of the customer, even if they aren't ready to be migrated.

✓ **Can the unified profile handle schemaless and/or unstructured data?**
All unified profile schemas are not created equal. It could potentially be problematic if an application wants to add semi-structured data, like a JSON browser fingerprint, to the customer profile for a new feature. If a unified profile has a rigid schema, it may require a risky schema migration that could affect all of your applications. Or, if it can't store both structured and unstructured data, it may not be able to store some attributes, such as JSON objects, at all.

CONCLUSION

Privacy. Security. Scalability. Unified profiles. These terms may get tossed around as mere buzzwords, but in practice they can make or break the success of your customer IAM solution. That's why it's critical that you carefully evaluate what's under the hood to determine whether a vendor's offerings in these areas will actually meet your needs—and why involving IT early in the procurement process will help you make these determinations.

To learn about how Ping can help meet your needs in delivering secure and seamless customer identity and access management, visit https://www.pingidentity.com/en/platform/solutions/customer.html.