

Information

Ping
Identity.

The Customer Identity Buyer's Guide

How to Choose a Customer Identity and
Access Management Solution that Supports
Your Most Critical Business Objectives



BUYER'S GUIDE

Information

Female
Age 45

INTRODUCTION

Delivering seamless and secure digital experiences for your customers is no longer a “nice to have” for your brand. The meteoric success of marketplaces like Amazon and AliExpress are testament that customers want ease and convenience when it comes to making purchases. Events like the global COVID-19 pandemic are further accelerating this trend and solidifying digital customer experience as the battleground on which market share is won and lost.

As more and more customers come through your digital front-door, your ability to provide a smooth user journey and delightful digital experiences is a requirement that can move the needle to meet business goals and ensure you remain competitive. From creating an account and signing on to getting support and managing preferences, your customers want to have a secure but frictionless experience. If you fall short on delivering it, they won't hesitate to go elsewhere.

“Increasing brand engagement can be achieved through community building (e.g., ASOS Marketplace), loyalty programs, and a **seamless mobile and desktop user experience.**”

Digital Market Outlook, Worldwide eCommerce, Statista

The way you design, manage and deploy customer identity can make or break your customers' experience. Customer identity and access management (CIAM) gives you the capabilities to deliver seamless experiences at every point in your customers' journey, making it fundamental if your organization's strategic objectives include continued growth in customer acquisition, loyalty and revenue.

This buyer's guide will help you align your business priorities to CIAM capabilities so you can more easily evaluate solutions that will deliver your desired results. Read on to gain a deeper understanding of customer identity and the role CIAM plays in enhancing your customers' experience, security and privacy.

“By 2022, CIAM will be a **key component** of a competitive UX strategy by 85% of organizations, up from 40% today.”

“Technology Insight for Customer Identity and Access Management,” Gartner, May 2020

WHY YOU NEED CUSTOMER IDENTITY

Customer identity can help you ensure that every stage of your customer's journey is seamless, secure and delivers the experience they expect. That alone makes it a must-have for enterprises who wish to remain competitive and truly put their customers first.

But while customer identity holds the potential to significantly improve your customers' experience—and your organization's bottom line—the devil is in the details. Without a well-conceived strategy, identity initiatives can introduce unnecessary friction. If your customers find things like registration, authentication and managing preferences to be cumbersome, your customer identity transformation could fail to deliver the results you need. And your customers could go elsewhere.

Before embarking on your CIAM journey, you need to uncover what your customers want. In understanding their needs, you can harness the power of customer identity wisely and to your greatest advantage. While gaining this understanding may seem like a tall order, it really comes down to two things:

Delighting Your Customers

- Recognize your customers across channels. Don't expect them to make changes to their accounts, preferences and other settings more than once.
- Make things like registration and sign-on as quick and seamless as possible. Don't make the simple things harder than they need to be.

Protecting and Respecting Your Customers

- Be a good steward and protector of your customers' data. Don't put them at risk of fraud or breaches.
- Give your customers transparent insight into and control over the personal data. Don't disrespect their privacy.

When done correctly, customer identity makes delighting, protecting and respecting your customers easy. And when you approach customer identity with this understanding, you're creating the foundation on which exceptional customer experience (CX) is built.

It's no secret that CX is the new competitive differentiator. It should also come as no surprise that you can map customer identity capabilities directly to your customer's experience, beginning at registration and continuing at every stage of their journey.

Robust and flexible customer identity capabilities are a must-have to deliver the convenient, seamless and secure experiences your customers want. Once you're able to do that, you can rise above your competition and help your organization achieve its most critical objectives, including:

- Acquiring more customers
- Retaining existing customers
- Growing revenue
- Increasing customer loyalty
- Earning customer trust



[Watch the video](#) to learn how you can deliver great experiences with customer identity.

GETTING STARTED ON YOUR CIAM JOURNEY

Selecting the right customer identity solution starts with an understanding of your organization's most critical objectives. Unlike workforce IAM, customer identity has top-line revenue implications, so it's directly tied to your overall strategic objectives and key performance indicators like:

- Customer acquisition
- Customer retention
- Revenue growth
- Customer loyalty
- Customer trust

When you have clarity about the objectives and metrics your organization values most, you can choose a solution that's capable of delivering the desired value and providing the capabilities needed to do so.

As shown in Figure 1, CIAM capabilities directly correlate to different stages of the customer journey. For example, registration, authentication, self-service and support directly impact customer acquisition and retention. Therefore, if these are key metrics for your organization, you'll want to be sure you prioritize these capabilities when evaluating customer identity solutions. Similarly, to support revenue growth, you should focus on capabilities like self-service, support and personalization.



Figure 1: Customer identity has an impact on every stage of your customer's journey and ties directly to many organizations' critical business objectives.



To learn more about how CIAM supports the customer journey, read the [Ultimate Guide to CIAM](#).

CHOOSING YOUR CUSTOMER IDENTITY APPROACH

As you begin to form a picture of what your CIAM solution must include, you can further finetune your focus by considering the scope of your customer identity needs. Depending on your objectives, requirements and current maturity, you'll want to identify whether your organization can get by with incremental enhancements or if you'd achieve better results from high-impact transformation.

Are Incremental Improvements Enough?

If your organization needs a quick win to get customer journey improvements started or to repair a particularly cumbersome area of your journey, then an incremental approach may be enough. When you focus on improving just one capability at a time, you can roll out improvements more quickly. You can home in on one area at a time and take a learn-as-you-go approach.

For example, as shown in Figure 2, you might determine that personalization is the number one place you need to improve to impact revenue. In this case, you would want to focus your efforts on creating a unified customer profile so you can deliver seamless multi-channel experiences.

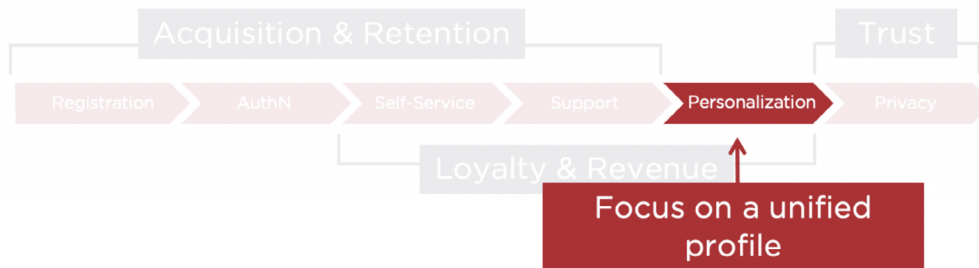


Figure 2: An incremental approach to CIAM involves rolling out a single product or capability to rapidly meet functional requirements.

While an incremental approach can produce quick wins, it can also slow you down later on. By limiting your ability to fully realize the impact customer identity can have on top-line revenue, customer acquisition and retention, and customer lifetime value, you're prioritizing short-term gains over long-term impact.

There are also risks in taking a point solution approach. You may end up with disparate systems that don't easily integrate when you inevitably need this ability down the road. To ensure you're set up for continued success when taking an incremental approach, be sure to evaluate a vendor's abilities beyond your immediate needs. You'll want to partner with a vendor with broad capabilities and a holistic approach to identity to ensure your quick gains don't become negated by future challenges.

Or Would High-impact Transformation Produce More Meaningful Results?

If you're able to forgo fast results for sustained success, you may be better suited to a high-impact transformation. This is still a focused approach, but instead of narrowing down on a single capability, you'll start by tackling a single stage of the customer journey.

High-impact transformations typically involve the implementation of a comprehensive CIAM solution that combines the necessary CIAM capabilities in a single package to produce improvements in one specific stage of the customer journey. The customer journey typically includes three stages. Depending on which stage best aligns to your business priorities, your CIAM initiatives will be focused as follows:

Acquisition & Retention

To acquire and retain more customers, focus on enabling capabilities like seamless registration, convenient single sign-on (SSO), self-service features and support options (Figure 3).

Loyalty & Revenue

To drive revenue growth and increased customer loyalty, focus on enabling user-friendly self-service and support options, and delivering personalized, multichannel experiences that keep customers interacting with your brand.

Trust

To build customer trust, focus on giving your customers full control over their data, while protecting them and your brand against threats like data breaches, identity theft and consumer fraud.

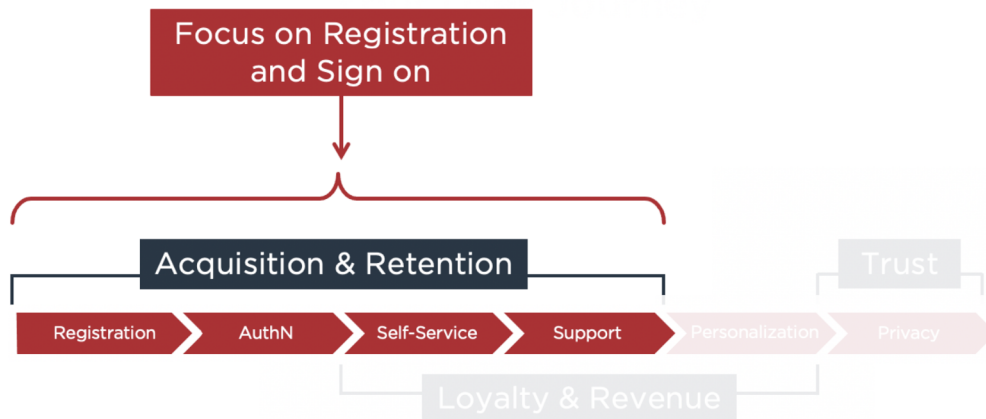


Figure 3: To acquire and retain more customers, focus on making improvements to your registration and sign-on processes.

In taking this approach, you're still focusing on a clear objective, just at a higher level that gives you the ability to deliver more meaningful improvements and tangible business impact. For these reasons, many find this approach to be the better fit for their objectives. With the right CIAM solution, you can even realize the benefits of a high-impact transformation initiative in a shorter timeframe than you may think.

“We are not believers in a single-application solution for identity and access management. Ping’s **flexible CIAM platform** allows our customers to have a secure, unified profile and set of credentials to access all of their various services.”

Stephanie Kesler, Enterprise Architect/Technologist, [GCI](#)



ESTABLISHING YOUR EVALUATION CRITERIA

Once you've clarified your business objectives and gained buy-in to move forward, you need to identify vendors to consider. When evaluating a vendor, consider the following:

- How long has the vendor been in business?
- Is the vendor a recognized leader within the industry?
- Does the vendor have demonstrated expertise in the form of customer success stories and testimonials?
- Does the vendor engage in continual R&D to improve and enhance products and meet evolving industry and customer demands?
- Does the vendor offer robust training, support and an active user community?

Of course, you also need to evaluate vendors' capabilities to meet your specific objectives and requirements. To help you do that, we've provided an overview of CIAM capabilities, as well as details about why each is important.

The criteria are organized such that they continue the alignment between common business initiatives and customer identity capabilities. In establishing your evaluation criteria through this lens, you'll be able to prioritize the capabilities that will make the greatest impact on your organization's specific objectives.

Aquisition & Retention



These criteria center on evaluating a vendor’s ability to make it easier for your customers to do things like register, reset passwords and resolve problems.

EVALUATION CRITERIA	WHY IT MATTERS
Does the vendor provide federated single sign-on (SSO) capabilities?	Your customers expect to have access to all of your applications without having to remember unique credentials for each one. Give them what they want by providing a consistent and convenient login experience with federated SSO.
Does the vendor provide social login?	Make it quick and easy for your customers to sign-up and sign-on by giving them the option to use their social media logins (such as Facebook and Google) during registration and authentication.
Does the vendor provide account recovery and easy-to-use password policies?	Most customers will forget their passwords at some point. Provide a secure and simple account recovery process by using password reset best practices and centralized password policies.
Does the vendor support multiple forms of multi-factor authentication (MFA)?	You need to give your customers convenient options that make it easy for them to use MFA so everyone can reap the security benefits. Vendors should support methods like SMS and email OTPs, soft tokens, FIDO and more.
Does the vendor support the FIDO standard?	FIDO allows customers to leverage credentials stored on a trusted device. It’s a very convenient and secure standard that’s growing in use and can ultimately replace passwords entirely.
Does the vendor embed MFA in your own mobile app?	Boost security for your customers by turning your mobile app into a second factor using secure push notifications. They’re more convenient and secure than many other forms of MFA.
Does the vendor support passwordless authentication?	As passwordless authentication gains traction, it could become expected for customer use cases as well. Ask if your vendor supports passwordless authentication to ensure you’re prepared.
Does the vendor support risk-based authentication policies?	No matter how convenient you make MFA, it still adds friction. Intelligent policies that allow you to step MFA requirements up or down depending on risk introduce friction only when the request warrants it.
Does the vendor provide APIs to give UX teams full control over sign-on and registration experiences?	Consistent brand representation is an important element of an exceptional customer experience and something your organization has worked hard to build. Ensure your vendor enables your UX teams to maintain control over registration and sign-on to deliver a consistent brand experience.

Loyalty & Revenue



These criteria center on evaluating a vendor’s ability to make it easier for your customers to do things like register, reset passwords and resolve problems.

EVALUATION CRITERIA	WHY IT MATTERS
Does the vendor provide preference management capabilities?	You need to give your customers the ability to explicitly define preferences. When these are stored in a unified customer profile, you can also deliver consistent and personalized experiences across channels.
Does the vendor’s directory store unstructured data?	The data you’ll want to collect about your customers may be diverse and include unstructured data like browser fingerprints. Applications should be able to store complex datasets and JSON blobs.
Does the vendor allow apps to easily add custom attributes?	Apps should be able to easily add custom attributes without requiring risky schema migrations that could affect other applications.
Does the vendor provide real-time, bidirectional synchronization capabilities?	Real-time bidirectional data synchronization lets you consolidate disparate identity silos to create a unified profile. It also reduces mitigation risks and prevents downtime.
Can apps access the customer profile with REST APIs?	Legacy protocols like LDAP are necessary for communicating with legacy directories to create a unified profile, but modern apps prefer APIs when accessing customer data. A unified profile should provide those APIs.
Does the vendor embed MFA in your own mobile app?	Boost security for your customers by turning your mobile app into a second factor using secure push notifications. They’re more convenient and secure than many other forms of MFA.
Does the vendor handle extreme scale and performance and have a track record of success to support it?	If your unified profile can’t scale, it may go down, leaving customers unable to sign-in or access their data. Vendors should be able to support millions of stored identities and billions of attributes, even in peak usage scenarios with hundreds of thousands of concurrent users, to adequately address customer use cases. They should also be able to provide customer references attesting to availability and low latency during peak demand.

Trust



These criteria are focused on evaluating how a vendor can help you protect your customers' privacy and ensure overall security, including preventing fraud, identity theft and data breaches.

EVALUATION CRITERIA	WHY IT MATTERS
Can the vendor provide access control to applications and APIs?	You need the ability to centrally manage access control to specific URLs and APIs. Vendors should provide centralized contextual access control policies to enable this.
Does the vendor support fine-grained dynamic authorization to meet privacy regulations?	Privacy regulations are diverse and can vary by organization, industry, geography and more. CIAM solutions should contain centrally managed privacy policies that let you enforce customer consent and govern data sharing on an attribute-by-attribute level to every app.
Does the vendor provide deep insights into API traffic to detect potential threats?	Behind every app are APIs that can be exploited to cause a breach. You need a CIAM solution that monitors all API traffic to detect potentially malicious behavior and prevent attacks.
Can the vendor store user data in multiple regions to comply with data-sovereignty requirements?	Many geographic regions have regulations that govern where customer data is allowed to be stored. Since this applies to where your customers are located (not where the business is located), you need an identity vendor capable of supporting data sovereignty requirements.
Can the vendor collect and store auditable consent records?	When collecting customer consent, you must collect the data in a way that's auditable. Your vendor should be able to store the time the data was collected, evidence of collection (such as an IP address) and other info needed for privacy audits.
Can the vendor enforce customer consent?	Many identity vendors stop at the way they collect consent. Unfortunately that leaves it up to disparate application teams to write code that ensures that consent is enforced. If your organization is large or growing, you want the ability to centrally enforce consent.
Does the vendor handle extreme scale and performance and have a track record of success to support it?	If your unified profile can't scale, it may go down, leaving customers unable to sign-in or access their data. Vendors should be able to support millions of stored identities and billions of attributes, even in peak usage scenarios with hundreds of thousands of concurrent users, to adequately address customer use cases. They should also be able to provide customer references attesting to availability and low latency during peak demand.

EVALUATION CRITERIA	WHY IT MATTERS
Does the vendor encrypt data at every state and implement other data layer security best practices?	To ensure that your customer data is protected at all times, it must be encrypted in every state—at rest, in memory and in motion.

How does the vendor protect from insider threats?	Malicious insiders pose a significant threat to organizations of all sizes and types. Ask your vendor what safeguards they have in place to thwart insider attacks, such as alerts for suspicious admin activity, tamper-evident logs and admin record limits.
--	--

Basic Requirements

In addition to evaluating a vendor’s ability to help you deliver on business objectives, you also need them to provide a core set of capabilities. Here are some foundational criteria you’ll want to include, regardless of your specific objectives.

EVALUATION CRITERIA	WHY IT MATTERS
Does the vendor support open standards?	It’s vital for a modern customer identity platform to support open standards like SAML, SCIM, OAuth and OpenID Connect to ensure the solution is extensible and versatile.

Can the vendor connect to custom applications that are not standard-based?	While your platform must support standards, many of your customer-facing applications may not. Your vendor should be able to connect to these applications and provide simple access to any and all digital properties in your portfolio.
---	---

Does the vendor support strong end-to-end security at every layer?	To ensure the security of sensitive data, your CIAM vendor should provide strong security during authentication, at the application and API layer and at the data layer.
---	--

Does the vendor provide best practices, sample apps, and out-of-the-box UIs?	You need to deliver secure and seamless experiences for your customers. Your vendor should make this easier by providing tools and resources to ensure your success, including extensive API documentation, sample apps and OOTB integration kits to get you up and running quickly.
---	--

Does the vendor support co-existing with legacy systems to enable you to do a phased migration to a modern CIAM solution?	For large enterprises, it usually isn’t feasible to take a rip-and-replace approach when moving from a legacy system to a modern CIAM solution. When your vendor can support a phased-migration approach by allowing the legacy and modern systems to co-exist, you’ll greatly minimize the potential for downtime and other risks.
--	---

EVALUATION CRITERIA	WHY IT MATTERS
---------------------	----------------

<p>Does the vendor support multiple deployment options to enable you to put identity where you require?</p>	<p>You should be able to choose where to deploy customer identity to meet your specific business needs. A vendor should be able to provide you with deployment options, including the simplicity of a multi-tenant IDaaS solution, the configurability of a single-tenant managed solution or the customizability of an on-premises solution.</p>
--	---

<p>Does the vendor offer both multi-tenant and single tenant Identity-as-a-Service (IDaaS) deployment options</p>	<p>Many organizations are prioritizing deployments in clouds that are managed for them. If yours is one of them, you need a vendor that offers IDaaS deployment options that suit your needs, whether that's multi-tenant or private-tenant IDaaS to give you the control you need over your environment.</p>
--	---

<p>Does the vendor have an extensive list of OOTB integrations?</p>	<p>Many vendors might list password-vaulting or "supporting SAML" as integrations but you'll want to investigate deeper to ensure your vendor has robust integrations to support your environments and use cases.</p>
--	---

<p>Is the vendor able to deploy in private clouds?</p>	<p>Some organizations want to maintain full control over their identity solution by managing identity in an environment they fully control (whether that's a private cloud or on premises). If either of these apply, be sure your vendor is able to support your preference.</p>
---	---

<p>Does the vendor support containerization and orchestration for DevOps?</p>	<p>For private cloud or on-premises deployments, the ability to support containerization with Docker and orchestration with tools like Kubernetes is critical to ensure efficient deployment and scalability of your customer identity solution.</p>
--	--

<p>Can the vendor deployment models work together?</p>	<p>In some cases, enterprises may need to deploy their identity solution across several types of environments. They may want to use a single or multi-tenant IDaaS for some apps, while other critical apps are in private cloud or on-prem environments. If you have these types of needs, make sure your vendor can maintain a unified identity solution during cross-environmental deployments.</p>
---	--

Evaluating Vendors & Solutions

After you've defined your evaluation criteria, you'll want to organize them in a way that makes it easy to evaluate how your shortlist of vendors stack up. You may want to use a Google Sheet or Excel spreadsheet for this. We suggest first creating rows for each of your evaluation criteria. Next, add columns for each vendor you want to evaluate. Then you can rate each vendor on how well they meet your criteria using a point-based rating system like this:

- 0 = Does not meet requirement
- 1 = Very limited support for requirement
- 2 = Partially meets requirement
- 3 = Meets or exceeds requirement

Using this system, you rate each vendor from 0-3 on each of the criteria. Then tally each vendor's totals to see who rises to the top.

CHOOSING THE RIGHT CUSTOMER IDENTITY SOLUTION FOR YOUR NEEDS

Choosing a customer identity solution is an important decision, and there is no one-size-fits-all solution. The first step is identifying your organization's critical objectives and measures of success. You'll want to weigh the pros and cons of taking an incremental approach vs. a high-impact transformational effort. Then you can apply your understanding of customer identity capabilities as detailed throughout this guide to ensure you prioritize vendor solutions that meet your specific requirements.

“Building a digital identity capability has formed a critical foundation on which we can provide the **seamless experiences** our customers demand, regardless of their channel of choice. Ping has supported BNZ in our identity journey as we transform for a digital world, putting **customers in control of their identity.**”

Stephen Bowe, General Manager of Digital & Applications, [Bank of New Zealand](#)

If you're like many tasked with identifying customer identity solutions, you'll also want to consult objective and unbiased analyst resources like Gartner's 2020 Magic Quadrant for Access Management to see what the industry experts recommend.



To learn more about critical CIAM capabilities and how Ping Identity stacks up, get your free copy of the [2020 Gartner Magic Quadrant for Access Management](#).

ABOUT PING IDENTITY: Ping Identity is pioneering Intelligent Identity. We help enterprises achieve Zero Trust identity-defined security and more personalized, streamlined user experiences. The Ping Intelligent Identity™ platform provides customers, employees, partners and, increasingly, IoT, with access to cloud, mobile, SaaS and on-premises applications and APIs, while also managing identity and profile data at scale. Over half of the Fortune 100 choose us for our identity expertise, open standards leadership, and partnership with companies including Microsoft and Amazon. We provide flexible options to extend hybrid IT environments and accelerate digital business initiatives with multi-factor authentication, single sign-on, access management, intelligent API security, directory and data governance capabilities. Visit www.pingidentity.com.