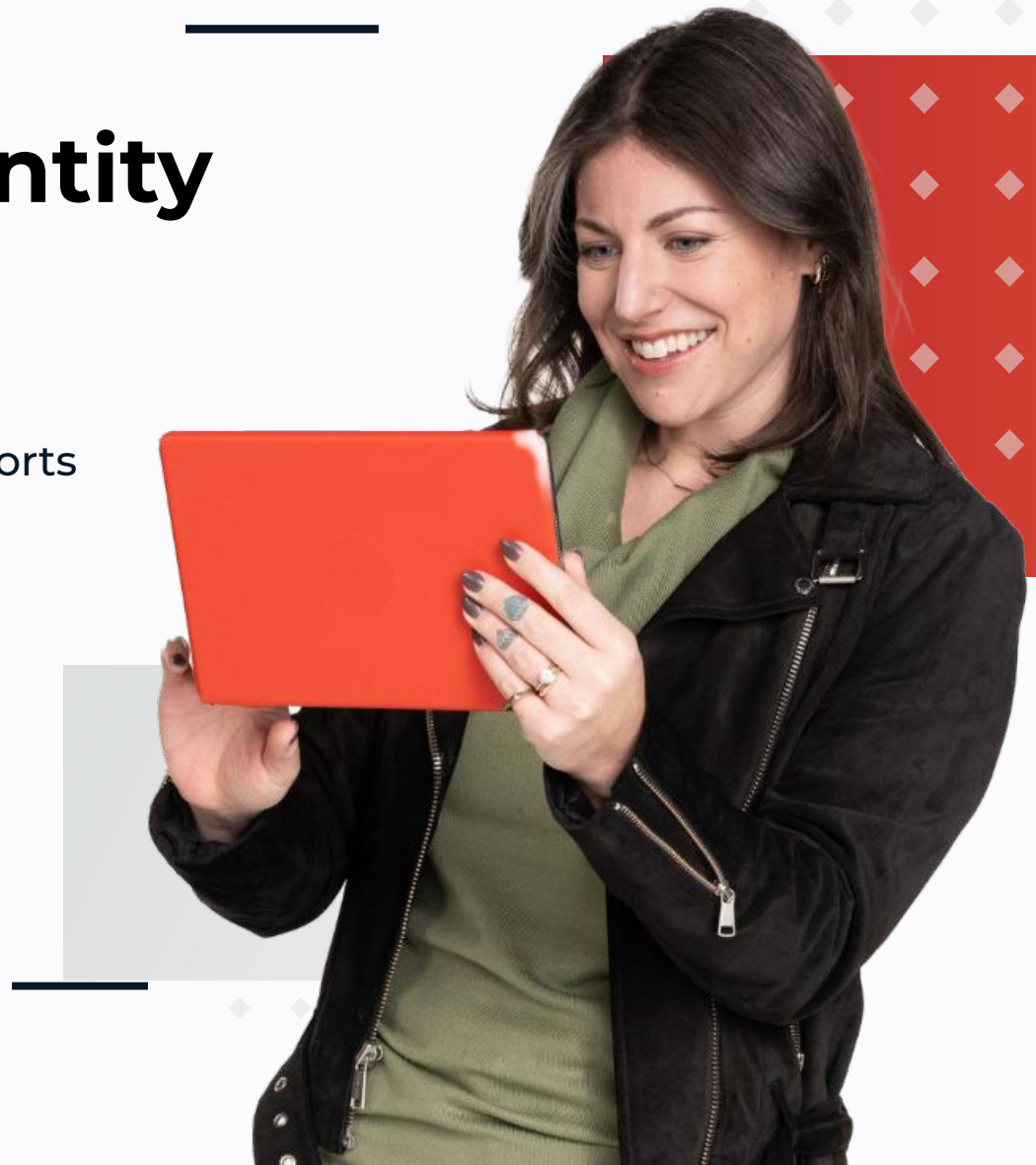




The Customer Identity Buyer's Guide

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



GUIDE

Table of Contents

03 Introduction

03 The Critical Role of Modern CIAM

04 Embarking on Your CIAM Journey

05 Getting Started with the Basics

07 Evaluation Deep Dive: The Comprehensive Criteria

07 Acquisition and Verification

09 Revenue and Loyalty

12 Fraud Prevention and Security

15 Regulatory Compliance

19 Implementation and Operational
Considerations

23 Evaluating Vendors & Solutions



Introduction

In today's digital landscape, identity is the cornerstone of customer engagement and you are increasingly reliant on digital channels to interact with your customers. This shift towards digital transformation brings both opportunities and challenges. Your organization must not only meet the growing expectations for seamless and personalized online experiences but also safeguard against escalating threats to security and privacy.

As digital trends continue to redefine business and societal interactions, the importance of robust customer identity and access management (CIAM) cannot be overstated. CIAM serves as the gateway to secure, convenient, and personalized customer experiences, enabling your organization to thrive in a hyper-competitive environment. It's not just about managing identities; it's about delivering trust, enhancing customer loyalty, and driving business growth in a secure manner.

This guide is designed to help your organization navigate the complexities of selecting and implementing a CIAM solution. By understanding the critical elements of CIAM, your team can make informed decisions that align with their strategic objectives and digital transformation goals.

DID YOU KNOW?

54% of consumers have stopped using an account or online service due to login frustrations.

– 2024 Ping Identity Consumer Survey

The Critical Role of Modern CIAM

As your teams strive to deliver exceptional digital experiences, they are often hindered by legacy identity solutions and homegrown systems that have become too costly and can no longer keep up. These outdated systems are ill-equipped to meet the demands of today's digital consumers who expect convenience, security, and personalization at every touchpoint.

Both homegrown and traditional IAM systems were designed for internal employee management, not for the complexities of customer interactions. They often fail to provide the scalability, flexibility, and security needed to manage customer identities effectively. Moreover, disparate and legacy systems can create significant security vulnerabilities, increase operational costs, and lead to fragmented customer experiences.

In contrast, modern CIAM solutions are purpose-built to address these challenges. They enable your organization to unify identity management across all digital channels, providing a single view of the customer. By integrating advanced security measures such as risk-based authentication and fraud prevention, CIAM solutions ensure that businesses can protect their customers without compromising user experience.

The way forward is clear: to stay competitive and secure, organizations must adopt a CIAM approach that is flexible, scalable, and capable of delivering personalized experiences. CIAM not only helps in safeguarding against threats but also plays a crucial role in building and maintaining customer trust and loyalty.



Embarking on Your CIAM Journey

Starting your CIAM journey requires a strategic approach. It begins with understanding your organization's specific needs and challenges. Are you looking to improve customer acquisition and retention? Do you need to enhance security to prevent fraud? Is your focus on providing a seamless, passwordless experience across all digital channels? Maybe it's all of the above!

Once your objectives are clear, the next step is to choose the right CIAM approach. This involves evaluating your current identity infrastructure and determining how a CIAM solution can be integrated or replace existing systems. It's crucial to consider both functional and non-functional factors such as security features and the ability to deliver personalized experiences, along with scalability and deployment options.

A successful CIAM strategy is primarily about aligning your identity management practices with your broader business goals—and then finding the technology that can deliver. Whether you are enhancing customer loyalty to drive retention and revenue growth, or ensuring compliance with regulatory requirements, your CIAM solution should be a key enabler of these objectives.

By taking a structured approach to CIAM, your organization can ensure that it is well-positioned to meet the evolving demands of their customers while maintaining a strong security posture.

“By 2026, 25% of IAM leaders will be responsible for both cybersecurity and business results, operating from the C-suite as CIDsOs.

– Gartner, Predicts 2024: The Changing Role of the Identity and Access Management Leader, Michael Kelley, Rebecca Archambault, Nathan Harris, Henrique Teixeira, Oscar Isaka, 1 December, 2023

Getting Started with the Basics

The first step in the process is to start with some high-level questions to streamline the list of vendors to which you'll apply the more elaborate evaluation criteria in the next section. Evaluate these higher-level questions to get started.

Question	Why it matters
How long has the vendor been in business?	Experience in the market can indicate stability and a track record of success.
Is the vendor a recognized leader within the industry?	Third-party recognition of leadership often reflects innovation, reliability, and a strong customer base.
Has the vendor demonstrated expertise in solving complex identity problems without large, post-sale surprise costs?	While most vendors can solve basic use cases, their costs compound exponentially for customizations that are required by most large projects
Can the vendor provide customer success stories and testimonials that relate to the problems you're trying to solve?	Real-world success stories provide insights into how the solution has performed for other organizations.
Has the vendor applied sufficient rigor in securing customer deployments?	A strong security posture is a critical requirement for ensuring customer data and mission-critical infrastructure are insulated from attack.
Has the vendor delivered performance and resiliency at a sufficient scale?	Delivering at scale is critical to being competitive and being able to expand within both internal and third-party ecosystems.
Does the solution allow you to easily design A/B tests to optimize the customer journey?	A/B testing is critical for improving conversion rates and retention by optimizing user experiences.
Does the vendor have a track record of innovation to meet evolving industry and customer demands?	Continuous improvement ensures that the solution stays ahead of industry trends and evolving requirements.
Does the vendor offer robust training, support and an active user community?	Strong support and training resources are essential for successful implementation and ongoing use of the solution.
Does the vendor have a strong implementation partner network?	Skilled IAM practitioners can be hard to find. Having skilled partners ready and able to make your implementation successful is critical.



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, evaluation criteria, and details about why each is important.

The criteria are organized such that they continue the alignment between common business initiatives and customer identity capabilities, while adding other important criteria considerations, such as compliance, implementation, and operations. 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.

Own Your Customer Identity Strategy

Discover the questions you **MUST** ask when evaluating CIAM vendors.

[Get the RFP Workbook](#)



We're not just looking at identity as a one-off, but rather the identity lifecycle. We need things like policies and consent services, but those should be both seamless and easily explainable to the customer in order to deliver a great experience—that is very important to us. So, it's about the features as well as the usage, and that's why we have chosen Ping Identity.

– Deniz Güven,
CEO, Mox Bank



Evaluation Deep Dive: The Comprehensive Criteria

Let's dive into the specific capabilities you should evaluate when choosing a CIAM provider. We've divided this section into subsections based on the category groupings as follows:

1. Acquisition and Verification
2. Loyalty and Revenue
3. Fraud Prevention and Security
4. Privacy and Regulatory Compliance
5. Implementation and Operational Considerations

Acquisition and Verification

The criteria in this section focus on your converting new customers and the key factors that can make all the difference between an unknown prospect creating a new account with you, or abandoning the process in frustration and moving on to one of your competitors.

CIAM Capability	Evaluation Criteria	Why It Matters
Social Registration	Does the provider offer social registration? Which social networking services are included in their offering?	Social registration allows users to register and authenticate quickly and easily using their existing information from a social networking service, such as Google or Facebook. This capability can increase customer conversions as users can enter little--or even no--information in order to complete a registration, as the data is leveraged from the customer's social account. Additional data can be collected later (see progressive profiling below).
Orchestration	Does the solution allow registration, authentication and authorization journeys to be easily created, viewed, and changed with no-code/low-code drag-and-drop user interfaces?	To provide secure, effortless user journeys, a CIAM solution should provide organizations with no-code/low-code identity orchestration capabilities. With a drag-and-drop workflow interface, the capability allows administrators to easily assemble and adjust workflow for steps such as registration, authentication, authorization, and more. This capability means users will receive highly tailored and personalized user experiences across channels and brands. This capability accelerates digital agility and reduces costs.
Orchestration	How does the vendor pre-identify a user's digital signal such as location, IP address, device type, operating system, browser type, and more before a username is even collected?	No-code/low-code identity orchestration also gives administrators the ability to build authentication workflows that easily configure, measure, and adjust user login journeys using a wide array of contextual signals. Administrators can also quickly consume out-of-the-box authenticators, utilize existing authenticators, and integrate with cyber security solutions. This capability strengthens security.



CIAM Capability	Evaluation Criteria	Why It Matters
Progressive profiling	Does the vendor support progressive profiling?	Rather than asking your users to fill out extensive registration forms, you can implement progressive profiling, a technique to collect user information as users interact with your system, on your website or application. For example, you might collect just the user's name, email, and password on the initial signup. At a later point in time, you might ask for the name of their company and their title. This capability reduces prospect abandonment.
Identity verification	Does the vendor provide native or third-party identity verification to enable KYC/identity proofing and customer checks post-login?	Deepfakes and AI-generated impersonation is becoming more sophisticated and difficult to detect and prevent. At the same time, onerous identity verification can cause unnecessary friction and increase the risk of abandonment. Identity verification helps organizations combat risks while reducing unnecessary friction at onboarding, call center, and hybrid channel touchpoints. This capability strengthens security and enhances customer experience.
Risk-based authentication	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. This capability strengthens security and enhances customer experience.
Multi-factor authentication	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. This capability strengthens security posture and enhances customer experience.
Single sign-on (SSO)	Does the vendor provide federated 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. This capability strengthens security and enhances customer experience.



CIAM Capability	Evaluation Criteria	Why It Matters
Passwordless Authentication	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. This capability strengthens security and enhances customer experience.
Account Recovery	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. This capability strengthens security posture and enhances customer experience.



We needed a solution that allowed for secure and quick onboarding of new customers and businesses with an exceptional digital experience throughout the customer lifecycle. Ping Identity could provide the highest level of security as well as the flexibility we required to deliver the services our customers need.

– Joko Kurniawan, SVP of IT Digital Service Enablement,
BTPN Bank



Revenue and Loyalty

The following criteria relate to things a CIAM solution can provide that help reduce customer churn and increase customer loyalty by providing easy sign on methods, personalized experiences and intuitive self-service options.

CIAM Capability	Evaluation Criteria	Why It Matters
Orchestration	Does the solution allow access journeys to be easily created, viewed, and changed with no-code/low-code drag-and-drop user interfaces?	To provide secure, effortless user journeys, a CIAM solution should provide organizations with no-code/low-code identity orchestration capabilities. With a drag-and-drop workflow interface, the capability allows administrators to easily assemble and adjust workflow for steps for all access journeys. This capability means users will receive highly tailored and personalized user experiences across channels and brands. This capability accelerates digital agility and reduces costs.
Access journey analytics	Does the vendor enable login evaluations that provide abandonment insights?	To continuously improve and secure the customer journey, data-driven insights are essential. As part of identity orchestration, user login analytics provide metrics and timers to analyze end-user interactions and their devices across all channels and business lines. These platforms should empower administrators to optimize the customer journey by using contextual and behavioral analytics to examine factors like devices and browsers used, login locations, and the duration of login processes across the user base. This capability strengthens customer experience and drives revenue.
Identity lifecycle management	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. This capability strengthens customer experience and drives revenue.
Identity relationship management	How does the CIAM solution support unique IAM configurations for different hierarchies or lines of business (LOBs)?	Most enterprise organizations create a hierarchy of departments or lines of business (LOB) to fit their needs around how they structure their business. These hierarchies inform how they then delegate administration as well as access rights to users within those organizations. The hierarchical, multi-brand, and complex organization design feature gives enterprises the flexibility to set up unique identity and access management configurations, like password policies and access permissions, for different audiences. This capability strengthens security, and customer experience, and reduces costs.



CIAM Capability	Evaluation Criteria	Why It Matters
Identity relationship management	Does the vendor provide identity relationship modeling at a granular level for identity management between those relationships?	To create secure, personalized, omnichannel experiences, CIAM providers must allow organizations to aggregate relational data between people and their IoT things to create a highly comprehensive, single view of the customer. This is achieved by establishing a common customer data model, connecting a broad range of data sources, implementing simple synchronization and reconciliation logic, and allowing access to customer data in an appropriate format. This capability strengthens customer experience and drives revenue.
Single view of identity	Does the vendor enable integration with third-party systems to consolidate identity data silos to create a single view of the customer organization-wide?	A single view of a customer (an identity) organization-wide improves security, customer service, marketing initiatives, and more. For CIAM platforms to support a unified view of identities, they must have the ability to integrate with other systems and consolidate multiple customer data silos to create a single view of an identity organization-wide. This capability strengthens customer experience and drives revenue.
MFA / software development kit (SDK)	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. This capability strengthens customer experience and drives revenue.
Personalization	Does the CIAM platform include flexible hosted UI options?	Every user is unique and should be treated as such. Organizations with multiple brands or channels, like branches, must recognize each user and provide a personalized experience, guiding them to the appropriately branded access point. In multi-party ecosystems, organizations need to manage different business units or user groups separately within their identity hierarchy, sometimes extending certain privileges to partners to better manage their end customers (B2B2C). A robust CIAM solution should offer multi-brand UI theming, allowing organizations to create tailored user journeys that align with the appropriate brand or channel. It should also support hierarchical user tiers and delegated administration for more effective management. This capability strengthens customer experience and drives revenue.

Discover the ROI of IAM

Explore the impact of identity in real dollars.

[Crunch the Numbers](#) or [Book a Meeting](#)

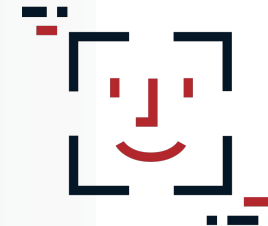


CIAM Capability	Evaluation Criteria	Why It Matters
Impersonation	Does the vendor support OAuth 2.0 token exchange including a CIBA (client-initiated backchannel authentication) grant?	Organizational representatives, like call center staff, may occasionally need to "impersonate" a user to take defined action on their behalf. A secure impersonation feature allows users to grant temporary control of their account to another party for a specified period. Extending consumer digital services to third parties requires support for OAuth 2.0 token exchange. This capability strengthens security and customer experience.
Self-service	Does the vendor provide an account recovery and easy-to-use password policies?	Most customers will forget their passwords at some point. Providing a secure and simple account recovery process by using password reset best practices and centralized password policies improves customer experience and reduces call center costs. This capability strengthens security and customer experience.
Privacy	Does the vendor enable users to have visibility into, and control of, their consent and privacy settings?	By giving customers the ability to control who and when their data is shared with third parties, organizations can achieve regulatory compliance with privacy regulations (such as the GDPR) while building long-lasting customer trust and loyalty needed to maximize lifetime value. This capability strengthens security, customer experience, and compliance.



From the customer perspective, it's a better user experience. They can access any service they want using the same credentials through the same portal. They can get to the services they want faster, and make new service requests or changes themselves without needing us to do it manually.

– Rolf Hausammann, Head of IAM, Swisscom



Fraud Prevention and Security

Fraudulent activities often begin with attacks on customer identity and the supporting identity systems. Things like account takeover (ATO), new account fraud (NAF), synthetic identities, deepfakes, and the malicious bots that often help perpetrate fraud, can typically be detected and prevented by identity systems—provided they have modern security features. The following criteria can help evaluate fraud prevention and security solutions by looking at risk detection, decisioning, and mitigation capabilities, as well as the customer experience impacts of these solutions.

CIAM Capability	Evaluation Criteria	Why It Matters
Fraud Detection	Does the vendor provide online fraud detection?	As businesses have moved online, fraud has as well. Ask your vendor if they can detect identity fraud threats in real time, identifying attempts at account takeover, session hijacking, new account fraud, synthetic identity fraud, automated attacks, and more. Ensure your vendor has the capability to detect the types of threats that are most impactful to your business.
Fraud Detection - ATO	Does the solution detect account takeover?	Account takeover (ATO) occurs when a bad actor gains unauthorized access to a user's digital identity account, and is often the source of data breaches, theft, and other fraudulent activities that lead to lost revenue, damaged brand reputation, and significant mitigation costs.
Fraud Detection - NAF	Does the solution detect new account fraud?	New account fraud (NAF) occurs when a bad actor creates a new account with malicious intent. These new accounts may be used to abuse promotional or loyalty bonuses, test stolen payment information, make fraudulent applications for credit, and other fraudulent activities that lead to lost revenue, damaged brand reputation, and significant mitigation costs.
Fraud Detection - Malicious Bots	Does the solution detect malicious bots and other automated attacks?	47% of internet traffic today is bots, and they can be used to perpetrate fraud at scale. To stop things like password spraying, brute force attacks, sniping, fraudulent new account creation at scale, card testing, and more, you need a solution that can accurately distinguish between human and non-human users.
Fraud Prevention - Synthetic Identity & Deepfakes	Does the solution protect against synthetic and stolen identity fraud and deepfakes?	Organizations are increasingly dealing with cases of synthetic and stolen identities being used to commit fraud, made worse by advancements in AI and deepfake technology. Your organization needs an AI-enabled solution that can accurately identify users and stop these identity crimes in an era where human eyes and ears can no longer accurately distinguish what is real in the digital sphere.



CIAM Capability	Evaluation Criteria	Why It Matters
Fraud Prevention - Composite Risk Scoring	Does the solution pull together fraud and risk signals from multiple sources and tools, and provide composite risk scoring?	The average organization has 5-8 sources of risk signals and data that can be used to evaluate the riskiness of a user or session, but these tools rarely talk to each other. You need a solution that can bring all of these sources of context into a single real-time decision, delivering a composite risk score based on your organization's unique requirements, so that you can respond appropriately to the level and type of threat.
Fraud Prevention - Authentication	Does the vendor support risk-based authentication policies?	No matter how convenient you make MFA, it still adds friction. Intelligent policies that take real-time risk into account allow you to adjust authentication requirements up or down depending on risk, introducing friction only when the request warrants it and letting safe users stay logged in longer.
Fraud Prevention - User Journey	Does the solution monitor and protect the entire user journey, invoking additional security measures at any point in the user session when risk is high?	Most identity solutions only protect at the initial authentication. However, this approach means that the context collected throughout the rest of the user journey is not taken into account when evaluating risk. Organizations need fraud prevention solutions that measure risk continuously, so that it is possible to stop cyber criminals as they attempt to perform other activities beyond authentication. Doing so ensures you have multiple opportunities to identify and stop bad users, and have the maximum amount of context to make accurate decisions.
Fraud Mitigation	Does the vendor support a variety of fraud mitigation methods to be deployed based on the level and type of risk?	Many fraud vendors stop at detection. You need a solution that can evaluate the threat signals coming in from fraud detection tools, make a decision in real time, and initiate fraud mitigation. It is important to have various mitigation methods, based on the level and type of threat. From various forms of MFA, to identity verification against a government-issued document, to various workflows that send users down different paths depending on the risk level and type, you need the flexibility to mitigate in a variety of ways.

Level Up Your Customer Identity Game

Unlock Ping's answer to key evaluation questions.

[Get the RFP Workbook](#) or **[Book a Meeting](#)**



CIAM Capability	Evaluation Criteria	Why It Matters
Authorization	Does the vendor support fine-grained dynamic authorization?	Fine-grained authorization enables the principle of 'least privileged access'. This means only granting access that is essential to perform an intended purpose. For example, customers are only permitted to access the exact information and resources necessary for a particular and legitimate purpose. Additionally, fine-grained policy controls allow you to build a decisioning framework that enables a real-time response to perceived threats.
Data Protection	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.
API Protection	Can the vendor provide access control to applications and APIs?	Behind every app are APIs that can be exploited to cause a breach. You need a CIAM solution that can ensure your APIs remain protected from bad actors.



Security is now part of the business. This is the new reality. Our customer ID management is in the middle of everything the business does and it's very important for the business's success. We're not just there to support the business, we are part of the business.

– Eliran Hayun, Principal Cybersecurity Architect, Healthcare Services Corporation (HCSC)



Regulatory Compliance

CIAM systems and the identity data that they process are directly impacted by privacy regulations and other compliance factors, such as data residency and data sovereignty requirements. These are important considerations for any CIAM solution—especially for global enterprises.

CIAM Capability	Evaluation Criteria	Why It Matters
Open standards	Does the vendor support both basic and advanced open standards, including OAuth2, OpenID Connect, SAML, OAuth2, UMA 2.0, Device Flow and OAuth 2.0 Proof-of-Possession, FIDO2, WebAuthN, and Client-Initiated Backchannel Authentication (CIBA)?	Open standards are established technical norms that developers use to ensure consistent capabilities and functionality across systems. Identity security is fundamentally built on standards like OAuth2, OpenID Connect, and SAML. However, leading digital identity providers are going beyond these core standards to support emerging trends by integrating advanced protocols. For example, UMA 2.0 enables users to securely share access to personal data with third parties. Other advanced standards include OAuth 2.0 Proof-of-Possession, which ensures that the bearer of a token is its legitimate owner, and OAuth2 Device Flow, designed for client devices with limited user interfaces. This capability strengthens security and compliance.
Data sovereignty	How does the vendor solution deliver granular data sovereignty?	Security concerns, like data sharing and data sovereignty, have led many large organizations to hesitate in adopting fully cloud-based CIAM platforms. Traditional SaaS vendors often use multi-tenant architectures that combine multiple customers (tenants) into a single instance, increasing the risk that one organization's actions could affect others. To address these concerns, the ideal CIAM SaaS platform should offer full tenant isolation, ensuring that data and workloads are completely separate. This isolation not only reduces risks but also simplifies scaling and storing sensitive identity data in the cloud. This capability strengthens security and compliance.
Scale and performance	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 risks going down, leaving customers unable to sign in or access their data. Vendors should be capable of supporting hundreds of millions of stored identities and billions of attributes, even during peak usage with hundreds of thousands of concurrent users. To ensure they can meet customer needs, they should also provide references that confirm high availability and low latency during peak demand periods. This capability strengthens performance and security.



CIAM Capability	Evaluation Criteria	Why It Matters
Scale and performance	Can the vendor scale their identity registration, authentication, and authorization services by several orders of magnitude to handle both anticipated peaks, like those during high-profile events, and unexpected surges?	Scale, performance, and availability are critical in an CIAM platform because if the identity platform goes down, so will the business. CIAM providers should support both 'service availability' and 'session availability'. Service availability ensures users can access a site when a server goes down. Session availability preserves and keeps a session running if a server goes down. CIAM providers should also support a variety of scale scenarios. This includes a shifting number (often in the millions) of users, devices, and things that need to be stored in a database, as well as changing frequencies and lengths of simultaneous and concurrent sessions. This capability strengthens customer experience, performance, and security.
Data residency	Does the vendor offer flexible data residency?	Data residency and data sovereignty are crucial concepts that govern where user data is stored and the legal authority that applies to it, regardless of location. Data residency typically requires that a user's data be collected, stored, and processed within their country's borders. To comply with regulations like GDPR, CIAM providers should offer flexible data residency options, enabling privacy-bound data storage and fractional replication of personal data across data centers in multiple jurisdictions. This ensures that user data can be processed in a way that is sensitive to the legal and regulatory requirements of specific regions. This capability strengthens security, performance, and compliance.
Privacy	Can the vendor collect and store auditable consent records?	When collecting customer consent, you must collect the data in an auditable way. Your CIAM vendor should be able to store the time the data was collected, evidence of collection (such as an IP address), and other information needed for privacy audits. This capability strengthens compliance.

Own Your Customer Identity Strategy

Discover seamless customer journey orchestration.

[Request a Demo](#)



CIAM Capability	Evaluation Criteria	Why It Matters
Privacy	Does the vendor support privacy and consent framework based on the UMA 2.0 standard?	Privacy regulations like GDPR require that users have control over their personal data, including privacy, security, and usage preferences. To ensure global and regional compliance, CIAM platforms must incorporate Privacy by Design principles and consent mechanisms based on the UMA 2.0 standard. They should also integrate with other tools that help meet regulatory requirements. These mechanisms should offer users fine-grained control to manage and audit data related to themselves, their devices, and their 'things.' Equally important is that the user interface for these privacy and control features is intuitive and user-friendly. This capability strengthens compliance and enables customer trust.
Privacy	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 application. This capability strengthens compliance and enables customer trust.
Federation standards	Does the vendor offer federated single sign-on based on open standards such as OAuth, WS-Federation, WS-Trust, OIDC and SAML?	Federated single sign-on (SSO) allows users, like partners, to securely access multiple organizations' web properties and applications using a single account. This trusted system is based on federated relationships between organizations and enables SSO by passing authentication tokens between their identity providers. Federated SSO relies on open standards like OAuth, WS-Federation, WS-Trust, OpenID Connect, and SAML to facilitate secure authentication across different organizations. This capability strengthens compliance.
IAM auditing	Does the vendor enable auditing for system security, troubleshooting, usage analytics, and regulatory compliance?	System auditing and analytics capabilities are mission-critical functions. CIAM platforms must be able to conduct audits for system security, troubleshooting, usage analytics, and regulatory compliance. Audit logs ought to gather operational information about events occurring within a deployment to track processes and security data, including authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. This capability strengthens compliance.



CIAM Capability	Evaluation Criteria	Why It Matters
KYC, AML, and open banking	Does the vendor support the identity, authentication, consent, and fine-grained authorization requirements mandated by PSD2 regulations, Open Banking specifications, and KYC/AML requirements?	PSD2 (and soon-to-be PSR1/PSD3), privacy, and open banking requirements continue to evolve rapidly across most parts of the world. To enable organizations to meet regulatory requirements and maximize ROI on open banking and open finance investments requires modern customer identity and access management (CIAM) solutions that include comprehensive fine-grained authorization capabilities. This capability strengthens compliance, accelerates revenue, and reduces costs.
FAPI conformance	Does the vendor conform with the Open ID Foundation Financial Grade API (FAPI) 2.0 certification?	Financial services organizations looking to advance their open banking offerings need to ensure the external APIs that allow applications to access customers' financial accounts, data stored therein, and privacy settings are secured and compliant with industry standards. FAPI 2.0 specifications provide the basis for doing so. This capability strengthens compliance, accelerates revenue, and reduces costs.
Strong customer authentication	How does the vendor support authentication, authorization, open banking strong customer authentication (SCA), and fine-grained authorization (transaction flows)?	Open banking providers need to provide customers with a wide range of SCA options to introduce the appropriate amount of friction/security needed to protect customer data. Higher assurance of verification can also be required to complete high-value transactions. This capability strengthens security, customer experience, and compliance.

“As we move into new regions like the U.S., we don't have the time or budget to rewrite every app to meet each country's privacy requirements. We also want to be able to quickly add new features like social login and configure them on the fly. Most identity solutions require extensive programming to make these changes. But Ping Identity allows us to make changes in a low code manner. It's easy-to-use drag-and-drop interface allows us to create customizable and secure user journeys, allowing us to quickly enter new markets just as we recently did in the U.S.

– Ashwini Kumar, Senior Engineering Manager, Mobile Premier League



Implementation and Operational Considerations

Implementation and operational considerations can make or break a CIAM program. Choice of deployment options, like multi-tenant cloud, private cloud, software deployment, or a hybrid combination are just the tip of the iceberg. When evaluating a CIAM solution, it's critical to evaluate things like: how you can migrate from old solutions without disrupting customers; how easy will it be for your organization's IT administrators and developers to administer and integrate applications. Even though some of the evaluation criteria in this section addresses non-functional requirements; consider them just as carefully as any other group in this document.

CIAM Capability	Evaluation Criteria	Why It Matters
API-first model	Does the provider use an API-first development model to create one common REST API framework across the entire platform?	The API First Model is a developer-centric method of creating a solution. Within this model, a provider first creates the API and then builds the platform around it. This results in less complexity for external developers and organizations. For ease of use, scalability, and flexibility, digital identity providers should apply this API first development model to create one common REST API framework across the entire platform to provide a single, common method to invoke any identity service. The result should be a simple and secure way to extend identity to all realms, including social, mobile, cloud, and IoT. This capability drives revenue.
Non-standard app support	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 digital properties in your portfolio. This capability accelerates agility and reduces costs.
Partner ecosystem	Does the provider have a strong ecosystem of respected consultancy, technology, and integration partners?	The strongest CIAM solutions are those that work well with a wide variety of other technologies, software, and industry leaders to solve the unique goals of each organization. As such, CIAM providers must have a strong ecosystem of respected consultancy, technology, and integration partners. This ecosystem should include pre-built, tested, and always updated integrations ready to be easily utilized. This capability accelerates agility, reduces costs, and drives revenue.
Administrator experience	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. CIAM vendors should make this easier by providing tools and resources to ensure your success, including extensive API documentation, sample apps, and out-of-the-box integration kits to get you up and running quickly. This capability accelerates agility, reduces costs, and drives revenue.



CIAM Capability	Evaluation Criteria	Why It Matters
Administrator experience	Does the vendor enable applications to access to 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. This capability accelerates agility.
Deployment flexibility	Does the vendor support multiple deployment options?	You should be able to choose where to deploy customer identity to meet your specific business needs. A CIAM vendor should be able to provide you with deployment options, including the simplicity of a multi-tenant SaaS solution, the configurability of a single-tenant managed solution, or the customizability of an on-premises solution. This capability accelerates agility, reduces costs, and drives revenue.
Deployment flexibility	Does the vendor offer both multi-tenant and single-tenant Identity-as-a-Service (IDaaS) deployment options?	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. This capability accelerates agility, reduces costs, and strengthens security.
Deployment flexibility	Does the vendor support containerization and orchestration for DevOps?	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 self-managed). If either of these apply, be sure your vendor can support your preference. This capability accelerates agility, reduces costs, and strengthens security.

CIAM Capability	Evaluation Criteria	Why It Matters
Deployment flexibility	How does the vendor support modern deployment DevOps approaches with containerization and orchestration technologies such as Docker and Kubernetes?	DevOps enables software development and deployment to run in a continuous cycle, allowing organizations to roll out new capabilities faster by reducing time to production. CIAM providers should provide a DevOps-friendly architecture with the ability to leverage DevOps tools, such as automating and orchestrating push-button deployment and continuous delivery. They should also use containerized images for rapid automation, with Docker support, as well as have an intelligent architecture that separates configuration from binaries to easily leverage version control for DevOps artifacts. This capability accelerates agility, reduces costs, and strengthens security.
Deployment flexibility	Can the solution be deployed within any cloud environment, including multi-cloud, bring-your-own-cloud, or hybrid cloud?	CIAM platforms should include flexible consumption options that include multi-cloud and hybrid-cloud deployments. Multi-cloud environments have become popular due to their increased flexibility, availability, and scalability. These environments allow organizations to eliminate vendor lock-in and speed time-to-market while reducing complexity and saving time and money. Hybrid environments include both on-premise and cloud environments. Cloud environments support needs at scale, while on-premises environments are advised to store sensitive data for better security. This capability accelerates agility, reduces costs, and strengthens security.
Migration	Does the vendor support co-existing with legacy systems to enable you to do a phased migration to a modern CIAM solution?	For most organizations, 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. This capability accelerates agility, reduces costs, and strengthens security.



With Ping Identity, Availity supports 12 billion transactions per year, over 800,000 daily logins, and connects two million providers to healthcare plans through the U.S.”

– Jason Carmichael, Manager, Enterprise Architecture, Availity



Explore Insights From Industry Experts:

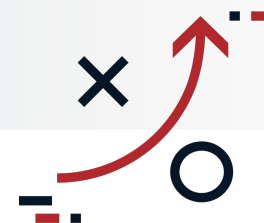
- [Gartner® Magic Quadrant™:](#)
Access Management, 2025
- [Gartner Critical Capabilities:](#)
Access Management, 2025
- [KuppingerCole Leadership Compass:](#)
CIAM, 2024
- [KuppingerCole Leadership Compass:](#)
Identity Fabrics, 2025
- [Forrester Wave:](#)
CIAM, 2024

Disclaimer: Gartner, Predicts 2024: The Changing Role of the Identity and Access Management Leader, 1 December 2023, Michael Kelley, Rebecca Archambault, Nathan Harris, Henrique Teixeira, Oscar Isaka GARTNER is a registered trademark and service mark, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.



Providing a secure, scalable portal with unified identity and access management is a key part of our business strategy and has helped Utah maintain its top ranking for business friendliness. It's probably the most critical piece of our enterprise architecture.

– Dave Fletcher, Chief
Technology Officer,
State of Utah



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 can use a Google Sheet or Excel spreadsheet. 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 exceed requirement

Where to Go From Here

Choosing a customer identity solution is an important decision. The first step is identifying your organization's critical objectives and measures of success. 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.

Modernize Your Customer Identity Strategy

Discover the questions you **MUST** ask when evaluating CIAM vendors.

[Get the RFP Workbook](#) or **[Book a Meeting](#)**

