Ping Identity®

CUSTOMER IAM

ULTIMATE GUIDE

Ultimate Guide to Customer IAM

TABLE OF CONTENTS

INTRODUCTION

As today's hyper-connected customers transact business online using mobile apps, self-service web portals, kiosks and connected devices, they expect a secure and seamless experience with your brand. Customer identity is central to providing a consistent, unified experience across these engagement channels, and it can give you an edge on your competition.

At the same time, protecting customer identity and profile data is crucial. Managing customer identities requires a careful balance between convenience and security. But how do you strike that balance?

When it comes to identity and access management (IAM), there's a fundamental difference between your customers and your employees: your customers have a choice. They can go to a competitor and won't hesitate to do so if their customer experience expectations aren't met.

They'll also do business elsewhere if they question the security of their interactions or fear their personal data may be compromised. In our always-on world of news and information, a breach involving customer identities has the potential to be extremely damaging.

Customer identity and access management (CIAM) addresses these specific concerns. A CIAM solution can provide secure, seamless customer experiences and the ability to support digital services across multiple engagement channels at extreme scale and performance. It can also help customer conversion through consistent registration and authentication options. These critical benefits are not addressed by traditional IAM solutions.

Understanding the opportunities that CIAM brings, how it's different than enterprise IAM and how to choose and implement a CIAM solution may seem like a daunting task. This guide will put you on the right path to selecting the best CIAM solution for your enterprise.

CHAPTER 01

MARKET OPPORTUNITY

Closing the Customer Experience Gap Creates Opportunity

There's been a major shift in how enterprises look at and secure their customer identities. Always-connected consumers are blurring the lines of customer interactions. They're adopting new ways to engage with and experience brands. They're spreading their customer journey across multiple channels.

Customer access isn't just about web apps anymore. It's grown to include mobile, IoT and other channels. And applications no longer live exclusively inside the firewall.

Today's enterprise needs to deliver a seamless and secure customer experience across every touchpoint to address evolving customer behaviors. As a result, new business requirements have been created, which require partnering with cross-functional IAM teams to deliver the right solution.

> "Customers demand that their digital interactions with your brand be seamless and span devices; that they be able to engage with your brand whenever and wherever they'd like; and that every encounter meet their needs in the moment.[1]"
>
> - Forrester

Most enterprises have large numbers of customers who come in from many different access points, using a broad range of devices. As the number of customers, applications, websites and services continues to grow, the data collected on each customer is also increasing exponentially. This data is often spread across various disparate identity stores, creating inconsistent user experiences and hindering your ability to have a single unified view of your customers.

Companies that leverage customer insights have the competitive advantage. The right CIAM solution can enable your rise to the top. It should set the foundation for a secure and seamless customer experience. It must also adhere to privacy regulations, increase business agility and be scalable to support tens (or even hundreds) of millions of customer identities.

For companies who fail to address these changing requirements, the customer experience gap will widen and shortcomings in performance, security or privacy could spell disaster for brand reputation and customer loyalty. On the other hand, organizations that build their future on a solid CIAM platform can capitalize on the market opportunity and outpace their competition.

[1]*Deanna Laufer, Allegra Burnette, Tony Costa, Andrew Hogan, and Kelly Price, with David Truog, Gabriella Zoia, and Rachel Birrell, Improve Digital Customer Experiences, Forrester, Jan 10, 2017.*

CHAPTER 02

CIAM VS. ENTERPRISE IAM

Differentiation IAM for Enterprise and for Customers

Enterprises shouldn't be fooled into believing an IAM solution that's purpose-built for employees is a good fit for their customer interactions. Why? Because customer needs are very different than those of employees.

Your employees are expected—if not explicitly required—to comply with and conform to your systems and technologies. There isn't a great need to fine-tune digital experiences in the workplace, unless they begin to detract from employee efficiency.

Customers, on the other hand, have a choice. They either choose you or they choose your competitor. Their decision is based on a number of factors, ranging from experience to security. From both your company's and your customers' perspectives, there are several key differences that set CIAM apart from employee IAM.

The unique requirements of customer identity—scale, performance, privacy, usability and multi-channel support—have made CIAM its own market segment with competitive offerings. These requirements are widely agreed to be distinct from traditional employee IAM solutions. As a whole, the industry recognizes that treating customer identities as an extension of existing enterprise IAM solutions isn't the right approach.

Key Differences:	EMPLOYEE IAM	CONSUMER IAM
BUSINESS DRIVERS:	Reduce Risk & Improve Efficiencies	Attract & Retain Users
SCALE:	Thousands of Users	Many Millions of Users
IDENTITY EVOLUTION:	Employees Known When Hired	Consumers Identified Over Time
PRIVACY PROTECTIONS:	Employee-Centric	User-Centric
SERVICE LEVELS:	High	Extremely High
USER INVOLVEMENT:	Employer Sets Policies & Procedures	User Sets Preference and Profile

> "Consumer use cases are different from employee use cases. CIAM implementations require specialized functions to support the consumer user experience and to leverage standard IAM capabilities in different ways.[2]"
>
> - Gartner

[2]*Mary Ruddy and Lori Robinson, Consumer Identity and Access Management is a Digital Identity Imperative, Gartner, Dec 30, 2015.*

CIAM VS. ENTERPRISE IAM

Given the growing number of CIAM solutions available, choosing wisely is important. Done poorly, CIAM can be a burden and significantly detract from the customer experience and business agility. And if it's not secure enough, you run the risk of being the next brand making headlines for a major breach. Striking the right balance between experience and security is key.

At the most basic level, a CIAM solution needs to solve for the complete spectrum of activities related to delivering a secure, seamless customer experience:

- **Self-service Registration**
  Convenient self-service registration, account management and account recovery features
- **Single Sign-on (SSO)**
  Customer authentication to internal and partner applications, using a common set of credentials or social login
- **Multi-factor Authentication (MFA)**
  Secure, fully customizable MFA that balances security and convenience for customers
- **Unified Profile Across Channels**
  Creating a unified view of the customer from disparate identity repositories that is accessible to all applications
- **Scale and Performance**
  Low-latency, high-performance access to identity and profile data from many millions of customers
- **Privacy Management**
  Enforcing customer consent and governing access to identity data on an attribute-by-attribute level to ensure privacy regulatory compliance
- **End-to-end Security**
  Securing customer identity and profile data from authentication to the data layer

You may have noticed there there is some overlap between employee and customer IAM. For example, SSO, profile unification and security are requirements when managing both employee and customer identities. However, customer IAM requires different capabilities and poses unique risks. We detail specific CIAM solution requirements later in Chapter 7.

CHAPTER 03

MARKET DRIVERS

Driving Business Initiatives with CIAM

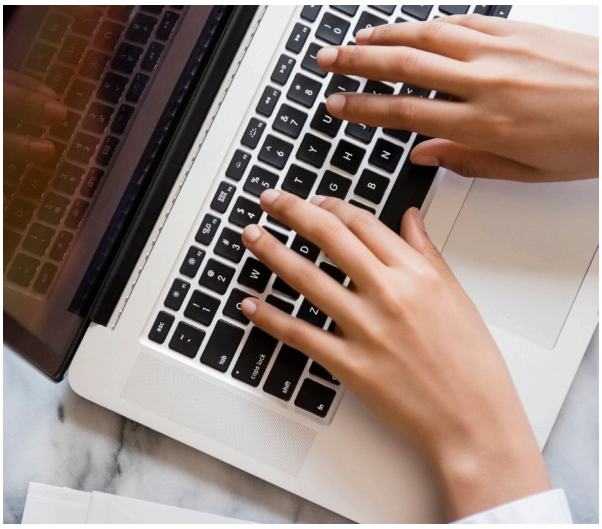
One of the primary values in a well-designed CIAM solution is its ability to span across channels and business units to create an accessible and unified customer profile. It also enables app dev teams to leverage centralized security, privacy controls and other CIAM capabilities. This streamlines and speeds time to market for future digital business initiatives, and reduces the need to rethink these capabilities for each new app you launch.

So where can CIAM help you deliver immediate value that can benefit the entire organization? To help answer that, consider these six business initiatives that typically drive the need for CIAM:

> "Firms that invest in improving digital customer experiences aligned with both customers' reality and their own core business initiatives will reap rewards.[3]"
>
> - Forrester

Digital Business Transformation

Customer experience has been called "the heart and soul of digital transformation."[4] CIAM is a key enabler for digital business strategies and supports positive customer interactions and personalization across all channels and apps.



Security Risk Reduction

The alarming rise in new attack vectors, coupled with the scale and frequency of data breaches—not to mention the costly damage they can cause brands—puts securing customer data at the top of the IT team's priority list. Customer identities must be secured from authentication all the way to the data layer. CIAM solutions provide features such as MFA, end-to-end data encryption and more in their security arsenal.

Internet of Things (IoT) Adoption

CIAM's capabilities, including scale, security, performance and profile unification, are fundamental to supporting IoT initiatives. As companies seek to offer innovative IoT products and services, CIAM is key to securing interactions between devices and humans.

[3]*Deanna Laufer, Allegra Burnette, Tony Costa, Andrew Hogan, and Kelly Price, with David Truog, Gabriella Zoia, and Rachel Birrell, Improve Digital Customer Experiences, Forrester, Jan 10, 2017.*

[4]*Vala Afshar, The State of Digital Transformation, Huffington Post, Sept 9, 2016.*

Privacy Regulatory Compliance

Data privacy is a growing concern for customers, who are sharing more information with more organizations and their partners. As a result, the regulatory environment is getting increasingly complex and can vary widely by geography and industry. Organizations must adhere to dynamic sets of rules that vary from customer to customer. CIAM solutions offer centralized policies and fine-grain data access governance that can be used to enforce customer consent on an attribute-by-attribute level and adhere to regulations in a dynamic privacy landscape.

Mobile Application Development and Delivery

Mobile applications can be an exciting new medium for customers. Providing a mobile customer experience that is consistent with web apps and other channels requires a modern CIAM solution. Though mobile is only a single piece of the multi-channel puzzle, mobile initiatives can be a catalyst to incorporate scale, performance, security, single sign-on (SSO) and other CIAM capabilities into an enterprise.

Partnership, Merger and Acquisition Activity

The integration of multiple web properties under a single brand—often driven by new business partnerships, mergers and acquisitions—can create disparate data silos. This results in disjointed customer experiences and requires varying levels of data unification. CIAM solutions provide single sign-on and data synchronization capabilities that can help create a single unified customer view across organizations, web properties and applications.

CHAPTER 04

BUSINESS BENEFITS

Reaping the Many Benefits of CIAM

Business and marketing leaders who want to improve customer experience increasingly rely on CIAM to enable the types of experiences that customers expect. CIAM also gives enterprises a competitive advantage by enabling them to quickly and securely execute new digital business strategies.

As you move toward selecting and maturing your CIAM solution, you can realize business benefits across six key areas:

1. Higher conversion rates
2. More customer engagement
3. Greater customer loyalty and retention
4. Improved business agility and simplified CIAM administration
5. Stronger security posture and mitigated risk
6. Increased revenue

> "Well-executed digital experiences can reduce costs, expand your customer base and boost loyalty with current customers to the tune of billions of dollars.[5]"
>
> - Forrester

Higher Conversion Rates

CIAM supports your ability to acquire more customers faster, increase conversions and craft loyalty-building introductions to your brand. With CIAM solutions, you can:

- Deliver simple and secure authentication experiences via SSO to any application across any digital property, including third-party applications.
- Reduce customer friction and improve conversions by leveraging social login, allowing customers to reuse accounts from social identity providers like Google and Facebook.
- Speed time to market by leveraging out-of-the-box registration and authentication capabilities, such as email verification, password policies, account recovery, reCAPTCHA and more.

More Customer Engagement

After a customer is registered, a CIAM solution should deliver a unified customer profile that enables personalization and a consistent experience across all channels and devices. Consider how these aspects of CIAM will improve your customer engagement:

- Offer self-service convenience that allows customers to manage their account, preferences and data-sharing consent from any channel.
- Capture and manage explicit customer preferences, and leverage them for real-time, consistent personalization across all channels.
- Provide lightning-fast response times and no outages, even during peak usage scenarios.
- Scale to support deployments containing hundreds of millions of identities and billions of attributes.

[5]Deanna Laufer, Allegra Burnette, Tony Costa, Andrew Hogan, and Kelly Price, with David Truog, Gabriella Zoia, and Rachel Birrell, Improve Digital Customer Experiences, Forrester, Jan 10, 2017

Greater Customer Loyalty and Retention

CIAM helps you retain customers by securing sensitive data and adhering to customers' data-sharing consent and privacy directives. A CIAM solution supports increased trust and loyalty by enabling you to:

- Protect customer data and ensure privacy by enforcing attribute-by-attribute-level consent and giving customers control over who has access to their data.
- Leverage centralized preferences to consistently enforce customer opt-in/opt-out choices, communication preferences and more across channels.

Improved Business Agility and Simplified CIAM Administration

CIAM can increase your agility and speed your time to market with modern developer-friendly REST APIs or LDAP (Lightweight Directory Access Protocol). This reduces your hardware footprint and total cost of ownership through data storage efficiency, simplified management and system-wide visibility. You're able to:

- Speed your time to market for new apps with features like centralized security, SSO and privacy policies. App dev teams can focus on building apps, not managing and securing identities.
- Bi-directionally sync and/or migrate data across heterogeneous data sources to create a unified customer profile accessible to all apps and channels.
- Deploy your applications flexibly and anywhere your customers need, whether on-premises, in the cloud or in virtual environments.

Stronger Security Posture and Mitigated Risk

CIAM solutions secure authentication, application access and sensitive customer data to protect your brand and minimize risks. CIAM solutions promote a strong security posture, so you can:

- Provide support for customizable MFA with secure second factors—such as the ability to send push notifications for authorization—and support for out-of-band transaction approvals and web and mobile authentications.
- Encrypt customer data at all stages, provide active alerts, restrict admin access, secure data access logs and enforce security best practices.
- Ensure authorized access to only the web, mobile and API resources your customers need.
- Reduce attack vectors by restricting sensitive customer data attributes from being accessed by potentially vulnerable applications and devices that don't need them to function.

Increased Revenue

We've discussed how CIAM solutions enable you to use SSO for convenient authentications. We've also seen how you can benefit from unified profiles with rich customer data that can be used to personalize experiences across channels and give customers insight and control over their privacy and consent preferences. Several of these capabilities contribute directly to increased revenue by allowing you to:

- Deliver a unified and consistent customer experience, strengthening brand loyalty.
- Craft personalized, cross-channel experiences that increase customer engagement.
- Demonstrate the highest regard for personalization and privacy, building brand trust.

Partnering with IT

The advantages of CIAM are undeniable. However, as a business leader, you must look beyond the surface-level benefits. All vendors will use words like "scale" and "security" to describe their product offering, but not all CIAM solutions are created equal. Some have less under the hood than others. Make sure you involve your IT team early so they can carefully evaluate a solution's scalability, performance, security and overall technical capabilities before entrusting a vendor with your customer identities.

CHAPTER 05

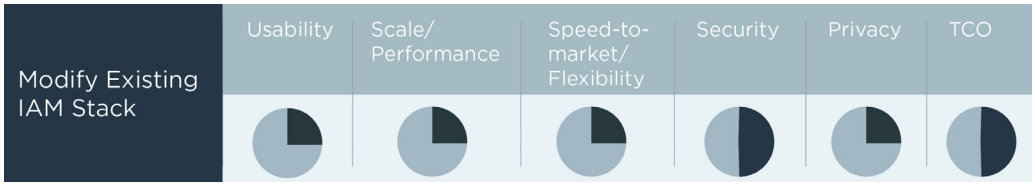
EVALUATING OPTIONS

Choosing the Best CIAM Approach

Before you select a CIAM solution, you have to identify the right approach for your organization. Your choices generally include modifying existing infrastructure, building a CIAM solution in-house or adopting a purpose-built solution. Let's review the basic definition of these three common approaches and the key considerations of each, plus take a snapshot look at the thoroughness of each approach.

Modifying An Existing Infrastructure

Approach: Repurpose a traditional enterprise IAM stack (Active Directory, Oracle, Novell, CA).



You may be tempted to squeeze more value out of your enterprise IAM stack. While there are elements of traditional stacks that match the capabilities required for CIAM solutions, they are few. It makes sense when you think about it. Most IAM solutions were built decades ago for web applications. Back then, all apps were on-premises, and users (employees) and endpoints (enterprise-owned devices) were controlled. These legacy systems were built to favor employee efficiency over user experience.

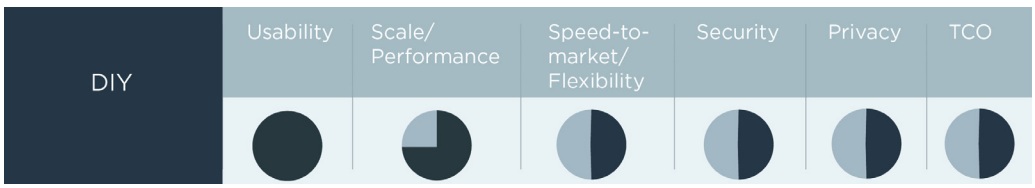
In the customer-facing enterprise, delivering a seamless experience is a top priority. Furthermore, the scalability and security required to enable customer access anytime and on any device far exceed the capabilities for which traditional IAM was intended.

Key Considerations:

- Lack of horizontal scalability and elasticity hamstrings your ability to accommodate typical spikes in customer engagement.
- Lack of easy integration for strong authentication and no strong password encryption (PBKDF2/scrypt/bcrypt) open security risks.
- Not being architected with customers in mind leaves no ability for self-service registration and account management.

Building A Solution In-house (DIY)

Approach: Build your own identity platform on top of NoSQL (Cassandra, MongoDB).



Before building or extending an existing CIAM solution, consider the full weight of a DIY approach. Architecting and maintaining a homegrown solution requires adequate staffing for ongoing maintenance, development of standards and best practices for all of the capabilities you'll need to build, defense of your security to S&R teams, and an often lengthy implementation.

As you assess the full scope of what's required, your resulting to-do list will almost always illuminate the many advantages of adopting a purpose-built CIAM solution instead.

Key Considerations:

- Lack of support for standards requires developing your own identity-centric APIs, resulting in project-specific solutions that aren't easily extensible across the organization.
- Managing passwords yourself increases overhead and risk.
- It's nearly impossible to synchronize changes out of these environments, dramatically increasing cost of maintenance.

Adopting A Purpose-built Solution

Approach: Choose a solution that is purpose-built for CIAM.

Purpose-built CIAM solutions cater to the specific challenges customer-facing enterprises have in today's digital world. They have capabilities ranging from SSO and data access governance to data synchronization and encryption. In hybrid environments, they ease the process of cleaning up an existing, disparate identity infrastructure to create a scalable, unified profile.

Solutions built specifically for CIAM incorporate best practices to facilitate successful implementation. Those include scalability, privacy, registration and end-to-end security. These challenges are insurmountable when trying to repurpose an existing employee-centric IAM stack, and they're often more intricate and time-consuming than expected with a DIY approach.

Key Considerations:

- Synchronization capabilities ensure a smooth migration and unification of customer identity and profile data, even in hybrid environments.
- Being purpose-built to address the scalability and elasticity requirements of peak and/or unpredictable usage makes meeting even stringent SLAs easy.
- Out-of-the-box best practices for registration, SSO and other CIAM features make deployments and maintenance easier than with other approaches.

CHAPTER 06

BUILDING YOUR BUSINESS CASE

Gaining Cross-functional Support for a CIAM Solution

More often than not, leading enterprises find that a purpose-built CIAM solution works best for their needs today and in the future. But gaining the necessary buy-in for CIAM is much different than it is for enterprise IAM.

CIAM's distinct technical requirements for usability, scalability, security and consistency push the decision process beyond IT to include CMOs, CDOs, CIOs and CTOs. That's a lot of Cs and Os that aren't always part of identity technology decisions.

While the ultimate decision maker may vary, enterprise teams must collaborate to identify the right solution for their organization. This starts with recognizing and understanding the objectives and requirements across functions. Aligning these will close the gap between what your organization delivers and what customers expect.

Building a business case for a CIAM solution may seem daunting, but it's easier than you think. Because of its ability to drive critical business initiatives, a CIAM solution can make a huge impact on your organization's top line. Here are some of the typical objectives driving CIAM projects from a business and IT perspective, and some shared goals as well.

Business Drivers of CIAM

The three common business objectives driving customer IAM are:

- Grow market share by launching customer-facing apps that enhance customer experience.
- Increase average revenue per customer by delivering seamless and personalized multi-channel experiences.
- Build customer trust and loyalty by capturing and enforcing customer privacy settings and preferences.

> "Firms need deep customer insight to successfully deliver new products and services that can increase and sustain brand loyalty. While marketing teams have traditionally managed customer data, today's complex IT environments and multiple interaction points require a cross-functional approach for managing and securing customer data.[6]"
>
> - Forrester

[6]*Andras Cser and Merritt Maxim, Identity And Access Management Metrics For Business Value Performance Management: The Identity And Access Management Playbook, Forrester, May 27, 2016.*

IT Drivers of CIAM

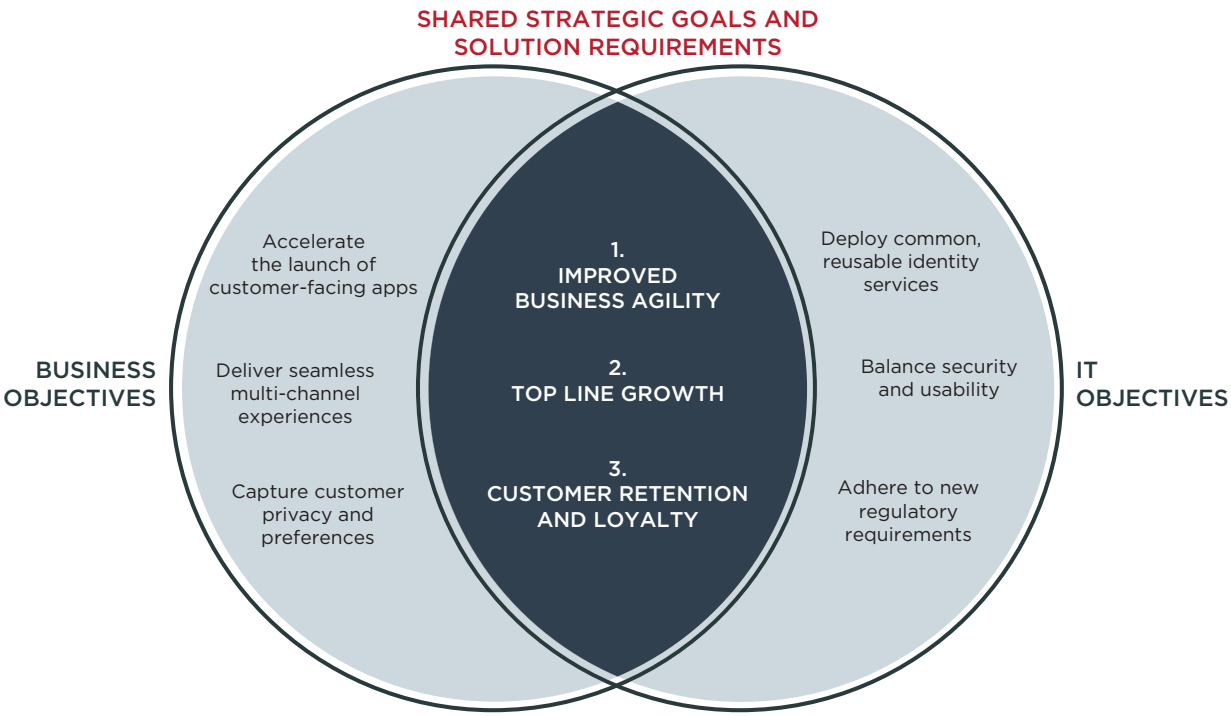
IT's goals are typically focused on bottom-line business efficiency and security:

- Deploy common, reusable identity services built on best practices. Build customer trust and loyalty by capturing and enforcing customer privacy settings and preferences.
- Reduce complexity, while balancing security and usability.
- Adhere to regulatory requirements around data access and security.

Shared Goals & Requirements

Business/marketing and IT may have distinct objectives, but they aren't that disparate. In the delta between them, three shared goals emerge that serve the entire enterprise:

- Improve business agility.
- Drive top-line growth.
- Increase customer retention and loyalty.



CHAPTER 07

SELECTING A CIAM SOLUTION

Choosing the Right Vendor and Solution

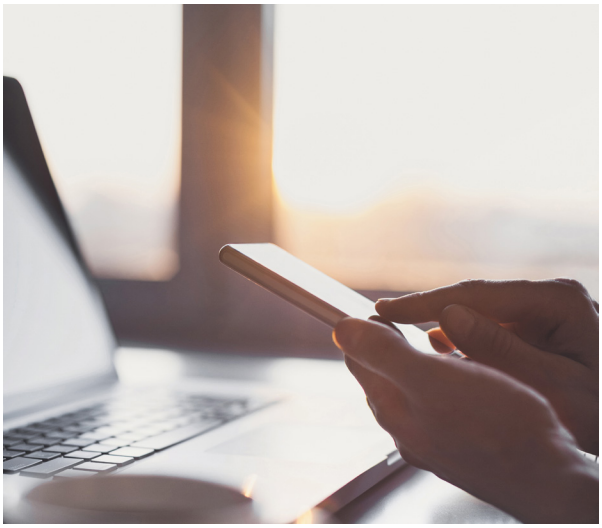
CIAM has been recognized as a distinct category of identity and access management since 2015. Not surprisingly, the list of vendors in the space is growing. But not all solutions are created equal. There are several considerations when evaluating CIAM solutions for your organization. Generally, you want a solution that:

- Offers scalability and elasticity to accommodate growth, even to hundreds of millions of customers.
- Provides flexible deployment options (including cloud, on-premises or as a PaaS).
- Requires minimal operational staff by giving responsibility to the vendor for maintenance, certificate management, etc.
- Centralizes security and administration, so app development teams aren't burdened with security, scale or other CIAM concerns.
- Eases migration of data from your existing, disparate identity silos into a unified profile (using advanced migration and data synchronization capabilities).

When evaluating vendors, there are the obvious considerations of experience, financial viability and customer references. But selecting a CIAM vendor also requires a deep dive into the solution's purpose, its capabilities and future direction. There are several questions you should ask before choosing a CIAM solution:

How complete is the solution?

Many CIAM solutions offer surface-level features catered towards marketing and business teams. These teams may not be equipped to fully evaluate the technological capabilities and fit of a solution. It's imperative that you involve IT teams early to assess a solution's scalability, security and ability to work with your existing applications and infrastructure.



Does the vendor have flexible deployment options?

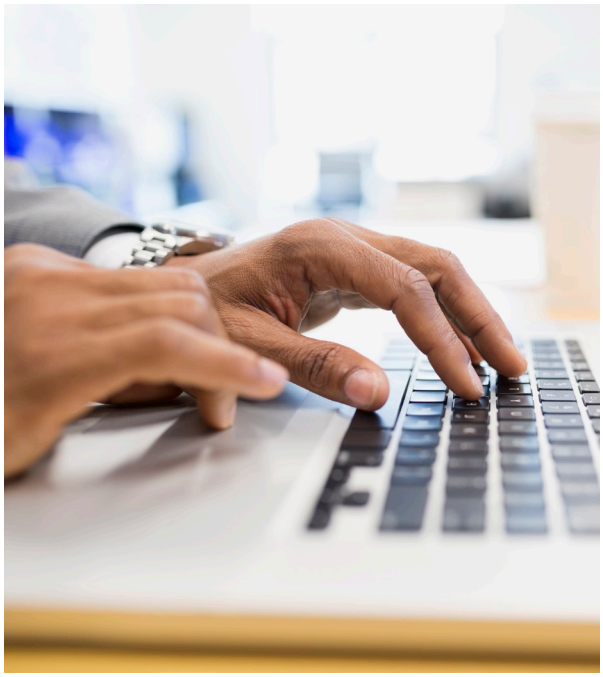
Many enterprises, particularly larger ones, simply aren't ready for full cloud migrations of all of their customer identity data. Based on your situation, you'll want to know how well a solution meets your deployment needs for cloud, on-premises or a hybrid environment.

Does the vendor have a customer MFA solution?

Customer credentials can be exposed in a number of ways that are outside of your organization's control. MFA solutions are becoming a requirement to increase your defense against compromised customer credentials. But finding a workable solution is key. Customers don't want to download a third-party MFA app, and certain second factors, such as SMS, are less secure than push-notifications. You'll want to prioritize vendors who offer customer MFA solutions that balance security and convenience.

Can the vendor help create a unified customer profile?

Organizations often have customer identity data stored in disparate user stores. CIAM solutions should facilitate creation of a unified customer profile by migrating or synchronizing customer identity and profile data from any source. The unified profile must be secure, scalable, able to store unstructured data and accessible to all applications through REST APIs. A solution should not require the organization to clean up their own data before doing a batch migration into a CIAM vendor's directory.



How will the vendor secure my customer identities?

Securing your customer identities is a crucial part of CIAM. There is a long list of security best practices and capabilities that CIAM vendors should have. These include secure data encryption in every state, passive and active alerts, and customer MFA, among others. All vendors will position their solution as secure, but it's imperative that your security or IT team evaluate the specific security capabilities of a CIAM solution to make an informed decision.

Can the vendor scale to meet your growing customer needs?

As your customer base grows, CIAM scale becomes vital. The solution should be able to manage tens or even hundreds of millions of customer identities and billions of attributes. Also look at the vendor's ability to handle peak usage scenarios at large scale. Make sure that any vendor you engage has referenceable customers that match the level of scale you'll need in the next few years.

Will the vendor implement the solution?

Will you need to hire a team of experts to implement and maintain the solution? If the vendor doesn't have the resources you need for implementation, do they have a strong partner ecosystem to help you? Ask these questions to ensure you choose trusted IT pros to work with your team.

CHAPTER 08

BENEFITTING FROM BEST PRACTICES

Three Keys to Driving Success

All of the major analysts agree that CIAM is a key ingredient for a superior digital customer experience. But without best practices in the driver's seat, a CIAM solution can quickly lose its effectiveness—and its benefit to the organization.

Here are the top three best practices for a successful CIAM implementation:

1. Balance Usability With Security

How do you protect customer data without completely killing the customer experience? As Forrester found, "Customers have a low tolerance of poor UX."[7] But they have an even lower tolerance of data breaches, so striking the right balance between the two is critical. This requires close collaboration between business/marketing and IT/security teams, which might be a first in your organization. "Line-of-business and marketing teams can no longer manage customer identities in isolation from their [security] counterparts," says the same Forrester report.

2. Plan for Scale

Even if you're just beginning your CIAM journey, plan for the road ahead. Don't just focus on the total number of users, but on both expected and unexpected spikes in usage as well. Ensure that whatever solution you're looking at is priced for consumer use and works at consumer speed. Response times of greater than one second don't cut it with consumer apps.

3. Plan for Multi-Channel/Omnichannel Consistency

Whether you call it multi-channel or omnichannel, your customers are already engaging with you in many ways, whether via the web, mobile, IoT, call center or in-store. While you're still in the planning stage, anticipate how your CIAM solution will facilitate the journey across channels to deliver the consistent, seamless multi-channel experience customers demand. "As you assess how a CIAM solution can help solve some business challenges, don't overlook the importance of providing a common customer experience across all channels, as that's ultimately what customers will expect and demand from their most favored brands," Forrester urges.[8]

[7] *Merritt Maxim and Andras Cser, Market Overview: Customer Identity and Access Management (CIAM) Solutions, Forrester, Aug 4, 2015.*

[8] *Ibid*

CHAPTER 09

ENSURING SUCCESS

Measuring CIAM Success as a Whole

Because CIAM spans both security and business agendas and value, you need to define a set of criteria that measures its impact across the organization. Successful teams will track and communicate the positive impact their CIAM solution has had on customer acquisition rates, conversion rates, retention rates, password reset cost reduction, identity administration and more.

Forrester Research has developed a balanced and comprehensive CIAM scorecard[9] that highlights the importance of CIAM to marketing and business stakeholders. It can help security teams more easily get the funding they need for revamping and improving their CIAM solutions for customer-facing web properties and mobile apps.

To measure CIAM success, Forrester highlights these key areas to consider:

Work for the top line by creating customer-facing IAM metrics.

If a customer-facing app isn't performing, CIAM metrics like slow logins and high abandonment rates can highlight the importance of smooth CIAM to marketing and business stakeholders, and help security and risk functions get funds for improving CIAM.

Improve the company's security posture.

To reduce the risk of security breach, business leaders and CIOs can use CIAM metrics, like uncorrelated accounts, weak or expired passwords, or time to deprovision user access, to expose weaknesses that cybercriminals can exploit.

Highlight and quantify surprising operational inefficiencies.

Identify process bottlenecks and eliminate them. CIAM metrics often lead to the identification of significant operational inefficiencies, like improper resource allocation and unusually long wait times for access permission.

Demonstrate the benefits of CIAM automation—including reduction of compliance costs.

Track how CIAM reduces the number of password resets and authentication times to help pass compliance audits and to prove the ROI of your CIAM project.

Increase employee, partner and customer service and satisfaction, while improving business agility.

Use metrics to show how automatic CIAM features like self-service enrollment, password resets and profile updates can reduce the time it takes to complete access requests, saving the organization money and improving satisfaction and productivity.

Ensure smooth, on-time completion of CIAM projects.

Define and track common quantifiable goals, like reduced password resets and identity compliance findings, that are priorities everyone can identify with.

[9]*Andras Cser and Merritt Maxim, Identity And Access Management Metrics For Business Value Performance Management: The Identity And Access Management Playbook, Forrester, May 27, 2016.*

CHAPTER 10

CONCLUSION

Today's hyper-connected customers expect access anytime, from anywhere and on any device. The changing face of customer interactions is driving the need for CIAM solutions that specifically address the needs of managing customer identities and that are separate and distinct from traditional IAM solutions.

Not all CIAM solutions are created equal, so you must carefully evaluate the options before making a decision. At its core, a CIAM solution must be scalable, high-performance, secure and able to deliver a consistent experience across all channels.

A best-in-breed CIAM solution goes beyond basic requirements by offering frictionless access and self-service profile management, enforcing customer data-sharing consent, and helping to create a unified customer profile from disparate identity silos. The right CIAM solution can build brand loyalty, strengthen competitive advantage and drive top-line revenue growth for your business.

To clarify your specific requirements and make the right decision for your enterprise, read the Customer IAM Buyer's Guide.

#3146 | 01.22.2020 | v001