Brought to you by:

auth0

# Customer Identity & Access Management (CIAM)

for dummies®
A Wiley Brand

Why CIAM matters now (more than ever)

How a modern CIAM solution can help you

What to look for in a CIAM solution

Lawrence C. Miller
Jeremie Certes

Auth0 Special Edition

# About Auth0

Auth0, recently acquired by Okta, provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and application teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

# Customer Identity & Access Management (CIAM)

Auth0 Special Edition

**by Lawrence C. Miller and Jeremie Certes**

for dummies®
A Wiley Brand

# Customer Identity & Access Management (CIAM) For Dummies®, Auth0 Special Edition

Published by: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate Chichester, West Sussex, www.wiley.com



ISBN 978-1-119-86655-8 (pbk); ISBN 978-1-119-86656-5 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

## Publisher's Acknowledgments

**Contributing Writer:** Jack Hyman

**Project Manager:** Martin V. Minner

**Acquisitions Editor:** Ashley Coffey

**Senior Managing Editor:** Rev Mengle

**Business Development Representative:** Molly Daugherty

**Production Editor:** Mohammed Zafar Ali

# Table of Contents

# Introduction

You've no doubt used customer identity and access management (CIAM) in your personal life as a customer of other businesses — whether you realized it or not. Perhaps you've logged into a website to purchase concert tickets. Or maybe you've used your social media account to log into a new e-commerce site. You may have used your mobile phone to do some online banking and received a one-time passcode via text message to login to your account. These are some everyday examples of how customers are already using CIAM with their favorite applications, websites, and portals.

In this book, you'll discover how modern CIAM can help your organization deliver secure, seamless digital experiences for your customers and partners.

## About This Book

*Customer Identity & Access Management (CIAM) For Dummies,* Autho Special Edition, consists of eight chapters that explore:

- The basics of CIAM (Chapter 1)
- Why CIAM is more important than ever (Chapter 2)
- Why you shouldn't try to build CIAM yourself (Chapter 3)
- What a modern CIAM solution is and how it can help your organization (Chapter 4)
- What to look for in a modern CIAM solution for your organization (Chapter 5)
- Thriving thanks to a CIAM solution tailored to your business needs (Chapter 6)
- The future of CIAM (Chapter 7)
- Ten important things to consider in a CIAM solution to help your organization thrive (Chapter 8)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though we don't recommend upside down or backward).

## Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but we assume a few things nonetheless!

Mainly, we assume that you work in a role that is responsible for building, scaling, modernizing, integrating, architecting and/or securing a customer/partner application, website, or portal. You may be an application developer or architect, a product manager, an engineering manager, a digital manager, a chief technology officer (CTO), a chief information officer (CIO), a chief product officer (CPO), a chief information security officer (CISO), a chief marketing officer (CMO), or someone who specializes in or is familiar with identity and access management.

## Icons Used in This Book

Throughout this book, we occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin.

TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon.

TIP

Tips are appreciated, but never expected — and we sure hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice.

## Beyond the Book

There's only so much we can cover in this short book, so if you want to learn more, check out `https://auth0.com/ciam`.

IN THIS CHAPTER

- Defining customer identity and access management
- Recognizing how a bad CIAM experience affects customers
- Improving the CIAM user experience in mobile apps, websites, and portals
- Understanding key CIAM capabilities

# Chapter 1
# What Is CIAM?

Usernames and passwords have become a part of everyday life. Consumers manage different accounts for online shopping, bank accounts, and mobile apps. This is customer identity and access management (CIAM), and you no doubt recognize some of the differences between good CIAM and bad CIAM in many of your digital experiences. For example, your mobile banking app may give you a strong sense of security and ease of use by simply authenticating you with a fingerprint or face scan. On the other hand, you've likely abandoned more than one online shopping cart when a retailer wants you to complete a lengthy registration process. Registration can take more time than finding the products you were looking for!

In this chapter, we cover the basics of CIAM including what it is, how a bad CIAM experience negatively affects customers, why you need CIAM for your customers and applications, and the core capabilities that every CIAM solution must have.

## What Is CIAM?

You may not be familiar with the CIAM acronym, but CIAM is part of your life every day, whenever you access an app on your mobile phone, sign up for a new online service, or sign in to your

favorite website. CIAM provides a digital identity layer that can be embedded into your customer-facing apps, websites, and portals. CIAM helps you identify who your customers are and what they have access to when they use their favorite devices to access your customer-facing services, including your apps, portals, and websites, from anywhere in the world. CIAM includes not only the sign-in/login experience, but also the registration and sign-up process throughout the entire customer journey.

A bad CIAM experience can drive your customers to a competitor that offers a more frictionless and intuitive customer experience. So, what exactly defines a bad CIAM experience?

## What Is Bad CIAM?

Critical to the experiences you provide to your customers is the ability to secure their access and data. But having secure access is worthless if the experience is so difficult and frustrating that your customers decide it's too much work to engage with you. You've no doubt had a bad CIAM experience yourself in some of your personal and business transactions. Some examples of typical customer pain points when it comes to CIAM include having to:

- Create an account and password just to browse a website
- Create more accounts and passwords for different apps, websites, and portals of the same company
- Log in with different accounts and passwords to access different services of the same company
- Provide your life story (well, it may seem like it) in a lengthy registration process just to create your account
- Navigate different login experiences and functionalities across devices
- Call customer service to reset a forgotten or incorrect password
- Enter an SMS passcode, in addition to your password, every time you log in — even if you are always logging in from the same location and device

By comparison, a good CIAM experience might provide:

- Easy registration and account creation that requires the minimum amount of information necessary to get started
- Face recognition on your smart device (look Mom, no password!)
- A text message or email verification for a sensitive financial transaction to make you feel more secure
- Access to all the services of a business from the same account

Bad CIAM introduces needless friction throughout the customer journey such as lengthy and intrusive registration processes and manual password resets that require call center interaction. Bad CIAM requires your developers to build custom integrations and connections for new apps, thereby slowing your speed-to-market. Bad CIAM requires customers to create separate user accounts for different apps, websites, and portals across a company's digital estate — and requires your administrators to manage these accounts in separate directories. Finally, bad CIAM does not provide the reliability and scale that agile businesses require in the digital economy.


TIP

Don't let your CIAM touch points become pain points for your customers. Make CIAM the start of a delightful customer experience that continues throughout the customer journey.

## Customer, Business Model, and Application Types

You need a modern CIAM solution to ensure a seamless, omnichannel customer experience across all your products and services, 24x7x365, wherever your customers are interacting with you. CIAM is the first step in the customer journey for many apps, websites, and portals, so it is critical to the overall customer experience.

Your business may sell directly to individual consumers, to other businesses, or to both. A CIAM solution needs to support these different types of customers and a variety of business models including business-to-consumer (B2C), business-to-business (B2B), and business-to-business-to-consumer (B2B2C).

Your different customers may also have a preferred channel for doing business with your company. For example, individual consumers may prefer using your mobile app while business partners may prefer engaging your business from their work computers. CIAM must support your different customer types on their preferred channels and devices.

Additionally, to support B2B and B2B2C business models, you may need to provide secure connections and integrations to your partners' apps and portals. You may also need to federate identities for your partners using enterprise directory services such as Active Directory and Lightweight Directory Access Protocol (LDAP).

Finally, your customers can access your services across all your mobile apps, websites, and portals. The customer experience needs to be consistent across all application types with like functionality delivered in a frictionless manner.

## Key Capabilities

The three main capabilities of an effective CIAM solution are authentication, authorization, and user management. In CIAM, your users are your customers and partners.

Proper *authentication* ensures that the people logging into their accounts are who they say they are, preventing bad actors from accessing sensitive user data (such as payment details, addresses, and Social Security numbers) or making fraudulent transactions (such as transferring money from a bank account).

Effective *authorization* helps businesses confirm that a user has the right level of access to an application and/or resources.

Clear *user management* allows administrators to update user access permissions and implement security policies, better enabling seamless and secure experiences.

IN THIS CHAPTER

- Delivering a superior customer experience
- Establishing trust as a cornerstone of customer relationships
- Enabling and driving digital transformation

# Chapter 2
# Discovering Why CIAM Matters Now (More Than Ever)

Customers today expect and demand a modern, seamless, personalized, customer experience at every touchpoint. Organizations that fail to deliver such an experience will be unable to attract and retain new and existing customers.

Trust is also non-negotiable. Organizations that fail to protect the security and privacy of their customers' personal information will lose customers — including customers who aren't directly affected by a data breach but have lost confidence in the organization because of a breach.

Finally, digital transformation is no longer an initiative — it has become a mandate. Every company, regardless of industry, must become a technology company to survive and thrive in the modern digital economy.

This chapter shows how customer experience, security and privacy, and digital transformation are not only driving but also accelerating the need for a modern CIAM solution in your organization — now more than ever.

# Addressing the Demand for Modern Customer Experience

The modern customer experience is seamless, personalized, and omnichannel. It provides your customers with frictionless 24x7x365 access to products, services, information, and other resources at their fingertips on their preferred device — whether it's a smart device, computer, tablet, or smartphone.

Not so long ago, people shopped almost entirely at bricks-and-mortar stores and watched movies in theaters or when they aired on television at a specific day and time. As people started interacting with businesses from their computers at home, it became increasingly important to deliver a friendly user experience on websites. Today, people use their smartphones to order groceries to be delivered to their doorsteps while they are at work, and can watch their favorite shows anytime, anywhere, on any device. Companies like Amazon and Netflix are setting the standard for seamless customer experiences across all channels, and consumers expect the same from every company they do business with — including yours. Thus, it is now more critical than ever for organizations to offer such modern access experiences to their customers.

WARNING

An Entrepreneur.com article ("Vroom! Why Website Speed Matters," May 19, 2017) reported that, according to analytics by Kissmetrics, "47 percent of consumers expect a page to load in two seconds or less" and "40 percent of consumers will abandon a website that takes more than three seconds to load." So, what makes you think your customers will tolerate a slow, clunky login experience that takes forever?

Organizations need a modern CIAM solution that helps deliver a superior customer experience to:

- **Unify digital experiences across devices:** Customers don't enjoy registering or logging in multiple times for different services from the same company. Instead, they want a consistent and fully functional experience whether they are visiting your website on their computers or mobile devices or using the different mobile apps in your digital estate. That experience includes a seamless, secure, and branded login on any device, anywhere in the world, 24x7x365.

- **Personalize customer journeys:** Collecting first person, authoritative preference information — including consent — across channels helps you build a 360-degree view of your customers. You can then consolidate customer identities and profiles in one place and tailor the customer journey based on individual preferences. The more consumers feel you understand them, the more likely they are to do business with you and share their positive experiences with others.
- **Enable new and modern experiences:** Technology evolves at a breakneck speed and helps shape customer expectations and trends. Ten years ago, smartphone customers were calling people and checking their personal emails. Today, your customers can order a critical part on your company's app installed on their smartphone while commuting to work on a bus or train — and they expect it to be delivered overnight. A modern CIAM solution can help you deliver a seamless experience for your customers with innovations like passwordless authentication (such as facial recognition and fingerprint identification) across devices.

REMEMBER

Both workforce identity and customer identity solutions are crucial technologies in an organization's tech stack. However, although your employees likely won't leave your company because of a poor login experience; your customers won't think twice about going to your competitors if you fail to deliver a superior end-to-end customer experience that includes a seamless, personalized, omnichannel login experience.

## Cultivating Customer Trust

Building and preserving customer trust is crucial to every organization's success, but the personal data and account information with which organizations are entrusted is under constant threat. Far too often, it is compromised. Protecting customer accounts and information is imperative. If your customers don't trust you, they will quickly become your competitors' customers.

WARNING

When customers have a bad experience doing business with your organization or lose trust in your organization, they don't keep it to themselves. You can thank social media for that!

Modern cyber threats and attacks are more sophisticated, destructive, frequent, and massive in scale than ever before. The recent global pandemic offers no reprieve from the bane of cybercriminals as nearly 16 billion records were compromised in the first half of 2020 — a 273 percent increase compared to the first half of 2019, according to *Security Boulevard* (`https://securityboulevard.com`).

For consumers, the financial and personal devastation of a data breach is undeniable. It can take years for an individual to recover from financial and/or identity theft — and many may never recover.

For organizations, the financial damage can easily exceed tens or hundreds of millions of dollars. In 2018, Marriott International reported that attackers had stolen data on more than 380 million guests. The breach cost Marriott more than $44 million in the first quarter alone after the breach was disclosed, and the company has since been fined $25 million by the U.K. Information Commissioner's Office (ICO). But the revenue cost due to brand reputation damage and loss of customer trust is inestimable. Many organizations never recover from — and will not survive — the loss of customer trust when personal data and accounts are compromised.

Organizations need a modern CIAM solution that helps build and preserve customer trust to:

- **Secure customer accounts:** Cyberattacks are becoming ever more sophisticated and destructive. Passwords aren't enough to secure your customer's accounts — and no one likes dealing with passwords anyway. Secure the customer identity lifecycle for all your apps by protecting customers at registration, authentication, and during in-app activity with innovations like multi-factor authentication (MFA) and passwordless authentication.
- **Manage privacy and consent:** Customers demand security and privacy for their personal information. The fundamental right to privacy has now been codified in many new laws including the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), among others. Your CIAM solution must enable a seamless and intuitive customer experience that empowers your customers to manage what personal information they are willing to allow your

organization to use, share, and store. If your identity platform can't support the latest regulations, you're putting your organization in legal jeopardy.

- **Comply with regulatory mandates:** GDPR and CCPA are just two examples of the dozens of stringent security and privacy regulations that have been enacted by governments around the world in the past five years. This trend will inevitably continue for the foreseeable future. For example, CCPA hadn't even been enacted for a full year before the California Privacy Rights Act (CPRA) was passed in November 2020. Organizations that fail to comply with applicable regulations risk financial loss due to audit failure and/or being forced to cease operations.

## Digital Transformation

Today, every company must become a technology company to survive and thrive. Every industry is being affected by digital transformation and this trend is accelerating now more than ever. For example, video rental stores (and even movie theaters) have disappeared in the wake of streaming media services and taxi companies are struggling to compete against ridesharing services. However, many organizations face significant technical debt as they attempt to migrate away from burdensome legacy systems. Digital transformation requires companies to modernize their technical infrastructure and can enable a transition into the application programming interface (API) economy.

REMEMBER

Technical debt is the implied cost of rework caused by a previous decision to implement an easier solution, rather than the right solution.

Organizations need a modern CIAM solution that helps drive and accelerate digital transformation including:

- **Moving to the cloud:** For most companies, the cloud is an integral part of their digital transformation strategies. Legacy infrastructure hinders an organization's flexibility and ability to provide a modern customer experience. However, it can take many years for a company to move to the cloud. A single identity layer for modern web and mobile apps, as

well as legacy on-premises apps, simplifies the management of these hybrid cloud environments composed of public cloud, private cloud, and on-premises resources. Benefits of the cloud include:

- *Improving application development and deployment agility while reducing costs*: Organizations can deploy cloud services and resources quickly and scale on-demand, allowing legacy identity infrastructure to be retired and eliminating the need for costly ongoing maintenance.
- *Leveraging a microservices architecture and APIs*: Nowadays, software developers build apps leveraging microservices and APIs. Such architecture requires a holistic and centralized identity approach to ensure secure access for your customers and partners. A modern CIAM solution built in the cloud will let your developers seamlessly embed authentication, authorization, and user management capabilities into the apps they are building so that they can focus on your core business.

  *Microservices* are small, containerized services that are independently deployable and loosely coupled to deliver the individual components of an application. An *application programming interface* (API) allows different applications to talk to each other through a software connection.


TECHNICAL STUFF

- **Joining the API economy:** APIs are not only a development technique anymore; they have now become a business model driver as an organization can generate new revenue streams by monetizing access to its proprietary APIs. Some common examples include overlaying a map in a ridesharing app or enabling secure checkout via a social media account for a food delivery app. A modern CIAM solution can control and secure access to APIs so that organizations can grow and scale their API-driven businesses.

IN THIS CHAPTER

- Building seamless and secure customer experiences
- Keeping your limited developer resources focused on your core business
- Ensuring reliability at scale, integrating with your tech stack, and reducing time-to-market
- Considering the full cost of a build-versus-buy decision

# Chapter 3
# Building CIAM Is Hard

Chapter 2 shows why a modern CIAM solution is critical to your organization: delivering a superior customer experience, ensuring customer trust, and accelerating digital transformation. At this point, the do-it-yourselfer in you may be thinking, "I can build this on my own." But remember, friends don't let friends build their own CIAM solution. In this chapter, we explain why.

## A Delicate Balancing Act: Customer Experience Versus Security and Compliance

Building a CIAM solution requires you to carefully balance two key requirements that are at times diametrically opposed: delivering a superior customer experience while also ensuring security and compliance.

Think about some of the things that characterize a superior customer experience for you — after all, you are the customer in many of your own daily personal interactions. What makes you a

happy online customer? Perhaps your customer experience utopia includes:

- **A frictionless registration process:** The onboarding process should be simple and fast the first time you visit a website or use an app. For example, you might be asked to provide a little bit of relevant information during your initial visit and subsequent visits, rather than for your life story the moment you "walk in through the virtual door." This is known as *progressive profiling.*
- **An intuitive and seamless login process:** The login process should offer different authentication methods that are customized to your individual preferences. People generally don't like dealing with passwords, so anything that does not require them to create and remember another password, such as using an existing social media account or facial recognition on a smartphone, is ideal.
- **Single sign-on across different apps from the same company:** A customer portal should seamlessly integrate all your apps into a single login experience.
- **A branded customer experience:** You should immediately be able to identify the brands that you recognize and trust, even for different apps or services provided by the same company (such as Amazon Prime Video and Whole Foods, both accessed via the same Amazon website).
- **Omni-channel in any language:** A consistent login experience from any device, at any time, anywhere in the world — in your preferred language.
- **Personalized recommendations:** You should get relevant recommendations for products and services based on your profile information and purchase history.

Alas, building superior customer experience into your own CIAM solution begins with defining your customers' requirements — and there are a lot of them. To flip an old proverb, one man's treasure is another man's trash. What thrills some of your customers may confound others.

Addressing security and compliance challenges while delivering a frictionless customer experience is a challenge in and of itself.

## B2B NEEDS CIAM TOO

Although this chapter focuses on the business-to-consumer (B2C) customer experience, business-to-business (B2B) apps also need to deliver a seamless and intuitive customer experience. In many B2B relationships, one business is the supplier while the other is the customer. Thus, many CIAM requirements for B2B are the same as for B2C. But you can add a few additional B2B requirements such as the ability to log into a partner website or app using your corporate credentials rather than having to create another account.

In case you're seriously considering CIAM yourself, be aware of the following risks:

- **You need to build it first — and that's easier said than done.** You need to build the security methods that your customers want and need. These methods might include multi-factor authentication (MFA), adaptive MFA (AMFA) that only prompts for additional factors according to a risk score, passwordless authentication, one-time passwords, and others.
- **Staying ahead of cybercriminals is a never-ending struggle.** Even dedicated security teams are constantly trying to keep up in the race to protect against new vulnerabilities and exploits. Sophisticated cyber threats and attacks are increasingly taking advantage of compromised online account credentials. If you build it (that is, CIAM), hackers will come. Don't let your homegrown CIAM solution replace users as the proverbial "weakest link" in your organization's security.
- **Your customers' demands will keep changing.** Today, they don't want passwords. Tomorrow, they may decide passcodes sent to their smartphones via text message are too much trouble. Keeping up with your customers' changing demands is hard. If CIAM is not your core business, it is just one more thing you have to constantly adapt to keep your customers happy.
- **The compliance landscape is undergoing a seismic shift.** More accurately, it's constantly changing and growing increasingly complex. Security and privacy regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA), are just a few of the confusing and often conflicting requirements that are

continuously being enacted, updated, superseded, and revised. A non-compliant DIY CIAM solution could subject your organization to severe fines and other sanctions.

Finally, if you decide to build your own CIAM solution, you'll need to consider additional tradeoffs including:

- **Security innovation never sleeps; neither will you.** Any innovative features that you plan to build — such as adaptive multi-factor authentication (AMFA), passwordless authentication, biometric identification, and one-time passwords — must be future-proof to stay on the bleeding edge of innovation. However these features must also be frictionless for your customers. This is the first tradeoff because requiring any additional authentication factor introduces friction.
- **Internal people within an organization will have diverging opinions and priorities.** Marketing will want a seamless and superior user experience. Sales will want it "yesterday." Security will want extremely secure access above all else. Product and Engineering will want to focus on the core product rather than building authentication. Finance will want the option that has the biggest return on investment (ROI) — and a minimal investment. And your CEO will want it all!

REMEMBER

On the one hand, organizations need to offer a superior customer experience that includes a frictionless and intuitive registration and login process for quick and easy access to your applications. On the other hand, customers demand that companies keep their personal information secure and private. If your customers don't trust your organization, they will take their business elsewhere. Before you decide to build CIAM yourself, consider all the challenges of striking the right balance between a seamless customer experience on the one hand, and robust security and compliance on the other. Then talk to your developers (see the next section).

## Attracting and Retaining Skilled Developers

Okay, you have skilled developers. In fact, you'd probably say you have some of the best developers in the world. That's why you pay them so much, right? But do you have enough skilled developers?

Facing a worldwide shortage of skilled developers, most companies struggle to attract and retain top talent.

Now, what other IT professionals are in short supply globally? That's right, security engineers. If you have a developer who can build secure CIAM capabilities that deliver a superior customer experience, robust security and privacy, and ongoing regulatory compliance, then you have a rare unicorn indeed. But unless your core business is identity and access management (IAM), why do you have Princess Twilight Sparkle, Rainbow Dash, and Spike (for the uninitiated, those are *My Little Pony* unicorns) building a CIAM solution? Shouldn't your precious developers be 100 percent focused on your core business and the apps and websites that generate your revenue?

REMEMBER

Building CIAM yourself requires a lot of custom code. According to the *Open Web Application Security Project (OWASP) Top Ten* (`https://owasp.org`), 93 percent of all application vulnerabilities are discovered in custom code. Those vulnerabilities expose your organization and your customers to major security flaws and create significant technical debt and opportunity cost. In addition, according to Stripe.com (`https://stripe.com/files/reports/the-developer-coefficient.pdf`), developers spend 42 percent of their time debugging and maintaining bad legacy code rather than building new apps. Attracting and retaining top talent is much harder if your developers are constantly stuck on "bug duty."

## Looking at Additional Considerations

In addition to balancing a seamless customer experience with robust security and compliance, and diverting expensive developer resources from focusing on your core business, you should consider several other challenges before deciding to build your own CIAM solution:

- **Ensuring reliability at scale:** Customers demand seamless and secure access to your mobile apps, customer websites, and partner portals on their preferred devices from anywhere, 24/7/365 — including Black Friday, tax season, ticket pre-sales for a popular concert, major sports event, or blockbuster movie, and any other peak demand periods. Downtime causes lost revenue and damages your brand. Designing, building, and maintaining the required infrastructure to support a reliable service at scale is complex and expensive. Do you really want to

manage your own infrastructure and deal with outages, maintenance downtime, and upgrades?

- **Integrating with your tech stack:** Your CIAM solution must securely connect to the other tools and applications in your tech stack — such as security, privacy, marketing, and service management software — to extend its capabilities and maximize your ROI.
- **Reducing time-to-market:** Organizations need to bring new, seamless, and secure customer experiences to market quickly in order to meet ever more demanding customer expectations and to address increasingly sophisticated and complex security and compliance risks. As you have by now discovered, building custom CIAM capabilities to meet such requirements is difficult and costly at any point in time, but what if your customers don't want to use text messaging for MFA anymore or you need to meet regulatory requirements in a new country your business is expanding to? Building a CIAM solution is not a one-time effort. It is a perpetual cycle that demands continuous innovation and product development to adapt to rapidly changing customer demands and security threats.

## A Classic Build-Versus-Buy Business Decision

It is extremely difficult to build a CIAM solution tailored to your customers' specific needs; it is also very costly to maintain it going forward. It takes a clear understanding of your customers' requirements for a seamless yet secure customer experience; a team of very scarce, well-skilled, highly-paid developers to build and maintain secure code; a very complex, expensive infrastructure to ensure 24x7x365 access at scale; and to build integrations with your entire tech stack while reducing time-to-market for new functionality in your core business apps.

Before you decide to build a CIAM solution, be sure to consider the total cost including technical debt, risk of security breach, and opportunity costs.

REMEMBER

Building your own CIAM solution is hard — and unnecessary. Do not make compromises though! In Chapter 4 you discover how a modern CIAM solution can help your organization, and in Chapter 5 you learn what to look for in a modern CIAM solution.

IN THIS CHAPTER

- Defining a modern CIAM solution
- Extending CIAM capabilities with a platform approach
- Providing secure, reliable, and scalable services with modern CIAM
- Exploring key use cases and customer success stories

# Chapter 4
# Understanding How a Modern CIAM Solution Can Help You

As explained in Chapter 3, building a customer identity and access management (CIAM) solution yourself is extremely hard and costly. It just doesn't make sense for organizations to divert scarce app development resources away from their core business to go the do-it-yourself route with CIAM. In this chapter, we explain why you should choose to partner with an expert offering a modern CIAM solution that can help you address your pain points and thrive by delivering a seamless and secure experience to your customers.

## What Is a Modern CIAM Solution?

A modern CIAM solution provides a digital identity layer that can be quickly and seamlessly embedded into your customer-facing apps, websites, and portals. It helps businesses address customer demands by delivering frictionless user experiences, fast speed-to-market, centralized management of all identities and access policies, and Internet-scale security.

## Frictionless user experiences

To deliver frictionless experiences, you need to know and understand your customers. A modern CIAM solution allows you to build a 360-degree view of your customers across all your apps and products, regardless of which device they are using, whenever and wherever they interact with your brand. Then you can use this information to offer tailored experiences while reducing access friction by:

- Providing a unified and consistent experience across all your different apps and websites, instead of asking your users to log in to every one of them
- Requiring fewer (or no) passwords across all your channels and customers' devices
- Minimizing the amount of information you ask your prospects for during the registration process
- Allowing your business partners to login with their corporate credentials, instead of asking them to create another username and password
- Using personalized and branded customizations to help build your customers' trust and confidence

TECHNICAL STUFF

Progressive profiling allows you to collect user information incrementally throughout the customer journey, rather than requiring your customers to complete a lengthy registration process to get started on your app. Social login lets your users share (with their permission) some basic information from their social media accounts instead of providing it manually, so that they can access your services faster.

## Speed-to-market

A modern CIAM solution helps you reduce your time-to-market with a broad range of tools to embed identity and access management quickly and effectively into your customer-facing apps, websites, and portals. These tools range from out-of-the-box solutions that are easy to configure and fast to deploy for organizations with simple identity needs and who favor low-code deployments, to an extensive range of application programming interfaces (APIs) and software development kits (SDKs) for

companies with more complex needs requiring extensive customization. Thanks to these tools, your development teams can quickly embed CIAM into your customer experiences instead of having to build it from scratch, thereby accelerating your speed-to-market.

## Centralized management

As the number of your customer experiences across all your channels increases, centralizing identity and access management becomes more crucial. A single source of truth across all identities for all users, groups, and devices can scale with your business by reducing administrative overhead with a single-pane-of-glass interface that enables you to manage all the different access policies, group memberships, and security policies. It will ensure consistency, reduce configuration errors, prevent security gaps, and maintain compliance.

WARNING

Managing identity and access management on an app-by-app basis is inefficient and risky. It requires a lot of duplication of effort and leaves you vulnerable to security gaps because you can't be certain that access and security policies are being applied consistently across your entire digital estate.

## Internet-scale security

A modern CIAM solution is built on a secure cloud-based platform that is managed by the service provider. You don't need to worry about securing and updating the underlying platform or infrastructure components — that's all the service provider's responsibility.

A modern CIAM solution offers advanced security capabilities, like adaptive multi-factor authentication, across a broad set of factors addressing threat intelligence and contextual response capabilities. Extensive analytics reporting and dashboards provide real-time visibility into potential threats and attacks, enabling teams to respond, investigate, and remediate issues swiftly.

REMEMBER

A modern CIAM solution enables you to leverage the latest security innovations, like risk-based policies and passwordless authentication, without having to build them yourself. Your development teams can focus on your core business, instead of dealing with the latest security threats.

## Taking a Platform Approach

A modern CIAM solution takes a platform approach to identity and access management to broadly support any identity use case, for any user, and for any technology.

A platform approach allows your organization to find IAM synergies across all your different users including employees, partners, and customers regardless of their locations, apps, or devices. For example, a business-to-business (B2B) reseller partner and an internal sales rep will most likely need access to similar sales-related tools and apps, product catalogs, and so on. If an organization builds a CIAM solution itself, it might end up being built by different product teams — one team focused on the internal use case, the other on the partner use case. Each team will create a different user experience and set different security and access policies, thereby wasting valuable time and other resources. The result is an inconsistent user experience, all while potentially introducing new security risks. A modern CIAM solution built on a unique platform provides a consistent IAM approach for any end-user and optimizes synergies.

An independent and neutral platform approach also extends CIAM capabilities by integrating your digital properties with any technology. You can connect your on-prem and cloud apps seamlessly to offer your customers a unified access to your legacy and modern products, while leveraging data points from your favorite tools with pre-built integrations into best-of-breed technology. For example, you can feed user contact details gathered during the registration process into a marketing tool that automates customer outreach.

## Built on Secure, Reliable, and Scalable Infrastructure

For organizations that try to build their own CIAM solution, it is a constant and expensive challenge to design, build, and maintain the infrastructure that provides the security, reliability, and scalability required for a successful business.

If it is not secure, customers will leave because they cannot trust your band. If it is not reliable, users will not even be able to access

your services because your site is down. If it is not scalable, many customers will get tired of waiting to log in during a traffic spike and will take their business elsewhere.

A modern CIAM solution is built on a secure, reliable, and scalable cloud-native infrastructure and delivered as a service.

This way, you don't have to worry about hiring and paying internal infrastructure experts, budgeting for your cloud infrastructure consumption costs, or scaling your infrastructure to address peak demand. You also don't have to deal with system or software patches and upgrades that require maintenance windows and interrupt service to your customers.

To ensure reliability, a modern CIAM solution must have extreme redundancy at every layer of the infrastructure stack in case a server or network link, for example, goes down. This redundant infrastructure must have automated workflows that can redirect traffic across several geographies as needed to provide maximum uptime without requiring human action.

To ensure scalability, you need on-demand capacity that can automatically scale up or down, as needed, so that you don't waste money on unused capacity or lose money (that is, revenue) due to insufficient capacity.

To ensure security, you need to stay current on the latest threats and vulnerabilities across your entire infrastructure stack.


TIP

An external modern CIAM partner can manage all these requirements for your organization so that you can focus on your core business.

# Exploring Use Cases

A modern CIAM solution helps organizations address a broad range of use cases to meet different business needs. In the following sections, we explore some of the most common use cases and learn about some real-world success stories from Okta customers.

## Protecting against account takeover

Account takeover is an increasingly common identity attack method in which a bad actor gains unauthorized access to a user's

account for financial gain or data theft. These attacks can be either human-driven or automated using bots. To prevent account takeovers, you need an identity platform that combines security with a seamless user experience.

## Building highly scalable applications

Organizations build apps and websites to attract as many customers as possible, which means your CIAM solution must be reliable and scalable, especially when there is a surge in customer traffic or demand — whether it's tickets for a concert or sporting event, or a flash sale during the holidays.

## Unifying customer identities across applications

Your customers don't particularly enjoy registering for new accounts and managing multiple credentials across different apps and websites — especially if they belong to the same company or brand. Unifying customer identities across all your digital properties is crucial to creating a frictionless customer experience.

## MAJOR LEAGUE BASEBALL

No longer restricted to ballparks and television, Major League Baseball (MLB) fans are consuming and engaging with baseball through a variety of technologies, including mobile devices, live-streaming, and ballpark apps. MLB decided to modernize its digital properties to provide a frictionless omnichannel experience that could scale to meet the demands of millions of fans.

MLB only had nine months to build its new consumer-facing platform before Opening Day of the 2019 season and decided to partner with Okta after having successfully implemented Okta workforce identity solutions across its ball clubs. It worked closely with Okta to migrate millions of users from an internal database. To make sure they were ready for traffic spikes, they ran performance tests for up to 138,000 authenticated requests per minute.

The new platform launched smoothly on Opening Day 2019 and tens of millions of fans now enjoy MLB apps on their favorite devices, anytime and anywhere.

## ALBERTSONS

Albertsons Companies serves more than 30 million customers each week across more than 20 brands (banners). Shifting customer demands presented new challenges for the well-established retailer, which needed to create a seamless, consistent experience while maintaining the look and feel of the individual banners.

Albertsons wanted to be able to eliminate duplicate customer accounts. For example, if a customer had previously registered with both Vons and ACME, Albertsons needed to merge those accounts and their associated data with zero customer impact. They needed a solution that would make it easy to unify all the data related to a single consumer across all its banners and apps.

Okta helps Albertsons deliver a personalized, frictionless experience for millions of customers across all their banners, supports growth as more brands are added through acquisitions, and has streamlined the user migration process.

## Integrating enterprise identities

A modern CIAM solution eliminates the need for B2B customers to create separate identities and credentials when connecting to partner apps, websites, and portals. Instead, modern CIAM integrates enterprise identities so that B2B customers can reuse their existing corporate identities and credentials across their partners' digital estates.

## Securing access to APIs

For companies joining the API economy (discussed in Chapter 2), protecting access to their APIs is critical to ensuring bad actors can't exploit vulnerabilities or gain unauthorized access to connected applications.

## HPE GREENLAKE

In 2019, Hewlett Packard Enterprises (HPE) introduced HPE GreenLake. This new offering enables customers to build a seamless experience between their public and private clouds as well as manage and optimize their hybrid IT infrastructure. HPE needed to securely federate all its user identities and authenticate various user types including administrators, support teams, customers, and partners — all within a single user interface.

Okta's B2B Integration enables HPE to give its enterprise customers the ability to federate their own identity systems and isolate their own customers into their unique user store. When customers log in to GreenLake, they're routed through a specific Okta integration to their identity provider.

Okta was deployed in only two months and has enabled HPE GreenLake to deliver a user-friendly, front-end customer experience, branded as HPE with Okta providing identity services in the background.

## PITNEY BOWES

From its humble beginnings as a shipping and mailing innovator more than 100 years ago, Pitney Bowes has become one of the largest software companies in the world today as it moves to the digital economy. In 2016, Pitney Bowes launched its Commerce Cloud offering to digitally capture all the data that it produces around location and commerce; to make these data accessible via APIs to its employees, partners, and customers; and to monetize access to these APIs. Therefore it was critical to secure access to these APIs in order to build a robust API business and partner with third-party vendors with confidence.

Okta's integration with Commerce Cloud gave customers improved access to Pitney Bowes digital assets without interrupting their current access. Pitney Bowes can now expose their digital capabilities via secure APIs so that developers and partners can build on them.

IN THIS CHAPTER

- Identifying key CIAM product capabilities
- Supporting any identity use case with an independent and neutral platform
- Ensuring a reliable and secure service at scale
- Partnering with an industry leader

# Chapter 5
# Knowing What to Look for in a Modern CIAM Solution

With an understanding of how a modern CIAM solution can help your business deliver a secure and frictionless customer experience (see Chapter 4), you can start evaluating your options. In this chapter, you learn which capabilities and features you need to look for in a modern CIAM solution.

## Product

A modern CIAM solution should provide out-of-the-box capabilities that are easy to configure and fast to deploy, as well as developer-friendly tools such as application programming interfaces (APIs), software development kits (SDKs), and hooks to further customize and expand the CIAM solution.

Some key out-of-the-box product capabilities to look for include:

- **Authentication, authorization, and user management** — the table stakes for any CIAM solution (see Chapter 1). Beyond the basic capabilities, you should expect the following advanced features:
  - *Authentication:* Social login and generic OpenID Connect (OIDC) support, single sign-on to third-party applications, passwordless authentication, risk-based authentication, a pre-built sign-in widget, and customized branding at the application level.
  - *Authorization:* API access management built on top of OAuth 2.0, integration with API gateways, and role-based access control to applications.
  - *User Management:* A highly scalable cloud-based user store to manage all your users, groups, and devices; user profiles mapping; and support for your preferred user migration approach (bulk import, just-in-time, existing directory).
- **Predefined and customizable user flows** that can quickly deliver best-in-class user and customer support function such as self-service registration, password reset, and account/username recovery.
- An intuitive **centralized administration** interface and customizable management dashboards that provide security and admin teams with the ability to manage security policies centrally and consistently.
- **Multi-factor authentication (MFA) and adaptive MFA** with support for different factors and methods, from basic email and text messages to more advanced ones like biometrics (for example, TouchID and FaceID). Adaptive MFA adds an intelligent layer of risk-based authentication leveraging context information, like location and device, to enforce MFA only when it is necessary.
- **Automated provisioning with lifecycle management** including automated workflows tied to where your customers are in their lifecycle, so you can provision and deprovision users to downstream apps and systems across your technology stack (for example, automatically granting CRM access to B2B partner sales as soon as the partnership starts).

- **Business-to-business (B2B) integration** to connect partner apps and portals, and federate identities across enterprise directories such as Active Directory and Lightweight Directory Access Protocol (LDAP) to make it easier for corporate users to log in (without having to create new credentials) and for organizations using CIAM to always be up to date on their corporate users.
- **Integration with legacy on-premises apps** to offer your customers unified access to all your products and accelerate your digital transformation.

For organizations that want or need to go beyond these out-of-the-box capabilities, look for a solution that offers an extensive set of APIs, SDKs, and hooks for the languages your development teams use. These developer-friendly tools will help you:

- **Quickly and efficiently embed CIAM into your apps** without having to custom build everything from scratch.
- **Customize and brand CIAM to your exact needs** so that you offer tailored customer experiences and gain a competitive advantage.
- **Leverage best-of-breed solutions from your tech stack** to extend your CIAM capabilities and delight your customers even more (see the next section for details).

## Platform

As you know from the previous chapter, you should look for a CIAM solution built on an open, independent, and neutral platform so that you can securely build upon it to solve any identity use case, for any end-user interacting with your business, while leveraging any technology you want.

You should choose a CIAM solution supporting a broad range of end-users, including consumers, partners, and even your employees. A platform approach will provide a future-proof foundation as your needs will likely evolve over time. For example, your organization may currently be looking for a CIAM solution offering out-of-the-box B2B integration for a partner portal. A year from now, your organization might expand to consumers and need

customizable, passwordless authentication for a new business-to-consumer (B2C) mobile app. But this doesn't mean that you will require two distinct CIAM solutions. Both use cases can be addressed by a single, platform-based CIAM solution that enables cost savings and operational efficiencies through easier administration and simplified workflows. Additionally, your organization might want to streamline its identity and access management capabilities for its employees too. All these user types can be seamlessly managed through the same CIAM platform.

A platform approach also enables you to leverage best-of-breed solutions across your different use cases and tech stack needs, on premises or in the cloud, so that you can use the best tool in the market rather than settling for mediocre solutions in a bundled package. As such, you should look for a CIAM solution supplying a large catalog of pre-built integrations with core applications and services in your tech stack such as:

- API gateways
- Bot detection
- Customer data integrators
- Identity proofing
- Infrastructure as a Service
- Privileged access management
- Security analytics

You should also look for a solution providing no-code connectors so that your teams can build automated workflows to your key technologies without having to write custom code.

Finally, your CIAM solution also needs to provide easy integration via APIs, SDKs, and hooks. Inline hooks allow developers to modify inflight CIAM processes with custom logic and data from an external source. Event hooks send CIAM events to a downstream system via an HTTP Post as they occur, just like a webhook. Figure 5-1 shows an example of an inline hook and an event hook.

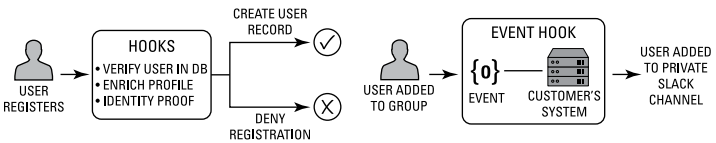


**FIGURE 5-1:** An example of an inline hook (left) and an event hook (right).

# Infrastructure

A key advantage of a modern CIAM solution is that it is delivered as a service, thereby freeing you from having to purchase and maintain the infrastructure necessary to provide the scalability, reliability, and security that businesses require in today's fast-moving and rapidly changing digital economy. Specifically, look for a modern CIAM solution that provides:

- **Scalability:** Your solution needs to support the level of scale your business demands now and in the future. You don't want the system to go down or become a bottleneck for traffic when your apps go viral and customer demand surges, and you don't want to have to replace your CIAM vendor because they can't keep up with the growth of your business. Look for a CIAM solution that can scale to support hundreds of thousands of authentications per minute and a vendor with a proven track record of ongoing investment and innovation in their solution.
- **Reliability:** Look for a CIAM partner that guarantees — and delivers — the highest uptime. Downtime results in lost revenue, brand damage, and potential loss of customers to your competitors due to a bad customer experience and poor reviews. There is no point in having the best products if your customers can't access them.
- **Security:** Look for a CIAM partner with an end-to-end security strategy with controls such as:
  - *Infrastructure and physical security:* This means built-in security and availability at every layer from physical security to computer, network, and storage.
  - *Secure personnel:* Look for a security-focused culture that starts with executive leadership and extends throughout the company.
  - *Secure development lifecycle:* Strict security checkpoints should govern every step of the development lifecycle from design through to coding, testing, and deployment.
  - *Secure customer data:* Protect customer data at rest and in transit with state-of-the-art encryption technology that meets the highest industry standards such as the National Institute of Standards and Technology (NIST) 800-53 and International Organization for Standardization (ISO) 27001.

- *Security and penetration tests:* Your partner should hunt for bugs in its software with internal tests, third-party security audits, a public bug bounty, customer bug reporting, and customer-conducted penetration tests.

REMEMBER

Your CIAM solution directly affects your customer experience and your business. Your customers won't hold your CIAM provider responsibility for scalability, reliability, and security issues — they'll hold you responsible and take their business to your competitors if you fail to meet their needs. You need to work with a trusted partner that has a proven track record of delivering a modern CIAM solution that is highly scalable, reliable, and secure.

## Industry Leadership

Finally, when evaluating your options for a modern CIAM solution, do your due diligence. CIAM is a continuous journey and you need a CIAM partner that is committed to your success for the long haul — not just a "one-and-done" vendor that sells you their product and moves on. Customer expectations will continue to evolve, as will security threats, regulatory requirements, and technology innovations. Consider a partner that demonstrates industry leadership, for example, through the following:

- **Independent third-party validations** including analyst reports and certifications such as:
  - *Service Organization Control (SOC) 2 Type I and Type II*
  - *Cloud Security Alliance (CSA) Security, Trust, & Assurance Registry (STAR) Level 2 Attestation*
  - *International Organization for Standardization (ISO) 27001:2013 and ISO 27018:2014*
- **Compliance with regulatory requirements** such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act
- **Demonstrated expertise via customer references and success stories** that are relevant to your industry, size, and geography and that you can contact directly for references
- **A future-proof solution** as evidenced by a track record of innovation, product roadmaps, thought leadership, and participation in developer communities and standards groups

IN THIS CHAPTER

- Mapping the path to CIAM maturity
- Starting with the basics
- Automating to grow and scale
- Optimizing your customer experiences without compromising on security
- Setting the new standard as an industry leader

# Chapter 6
# Unlocking CIAM Potential Based on Your Business Needs

Chapter 5 explains what to look for in a modern CIAM solution, but where should you start? Your organization is unique, and you want to make sure you choose the solution that is the right fit for your specific needs. This chapter shows you where and how to start your path to customer identity and access management maturity.

## The Path to CIAM Maturity

No matter how far along your company is on its identity journey, there's a common set of challenges companies face at every step. As a result, the path to CIAM maturity can be broken down into four key stages: Basic, Automated, Intelligent, and Continuous (see Figure 6-1).

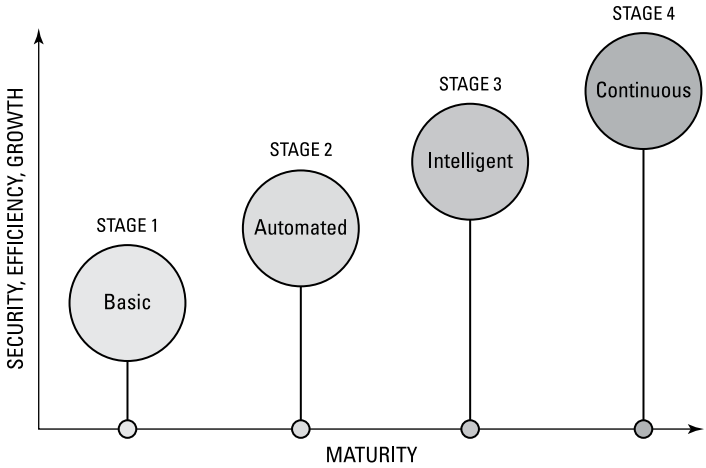


**FIGURE 6-1:** Where is your organization on the CIAM maturity curve?

Wherever you are on your journey, you can take several clear steps on the road to continuous customer identity and access management. The next sections take a closer look at each stage and what it means for your company.

## Basic: Build Versus Buy

The first stage is the Basic stage. From a business standpoint, you are just getting started and you are trying to prove your product/market fit. For example, your organization may have a great idea for a new customer app and want to get it off the ground as quickly as possible. Your app is early in its product development lifecycle and you need to demonstrate its viability in the market. Your team's core focus is to design, build, and validate the app's business case, but it is a small team. Thus, you are faced with tradeoffs.

On the one hand, you need to:

- Quickly ship an early minimum viable product to which basic identity is a prerequisite
- Get your product in front of potential customers
- Prove that you are solving the right problem for your customers

On the other hand, you are facing several challenges:

- You need to ship your product and iterate as you learn more.
- Basic security issues could derail the whole project.
- You have limited engineering resources and lack insight into where identity fits into your design.

This is the first stage of the CIAM path to maturity: the Basic stage where you need to decide whether to spend your limited time and precious resources building your own CIAM solution, or partner with a third-party provider.

As Chapter 3 explains, building and managing tools internally takes valuable time from your developers and engineers, who would otherwise be focused on your core business products. Therefore, you should take advantage of an external solution to quickly set up the core CIAM capabilities (authentication, authorization, and user management) that you need. It will lay the right foundation to start delivering secure access experiences to your customers while maximizing developer efficiency.

REMEMBER

According to a Harris Poll conducted by Stripe.com, developers spend 17.3 hours a week, on average, debugging and maintaining legacy and bad code. A modern CIAM solution can speed up development and reduce the pain of maintenance later, allowing you to focus on your core business.

Achieving basic CIAM maturity means you've integrated crucial identity security features into your app — and you've successfully brought it to market. Next, it's time to think about expanding your product offering to serve a growing customer base.

## Automated: Centralize and Scale

Congratulations! Your application was a hit and you're now looking to build additional products for your customers. You're hiring, and you even have a CTO or a VP of Product or Engineering leading your project. However, this new growth stage comes with a new set of challenges. For example, your growing paying customer base demands more advanced or enterprise-grade features,

which you might not have the time or experience to build. So, you need to prioritize your own initiatives to scale effectively and keep growing.

From a CIAM standpoint, you might consider building identity capabilities in-house because it is so critical to your customers, but you really should focus on other critical goals, like building and successfully launching new products to continue growing your customer base.

You are now at the Automated stage where the right external CIAM solution will help you:

- Offload the risk and management of external customer identities. Your end-users should be able to sign in with existing identity providers and you should be able to delegate authentication to existing Active Directory or Lightweight Directory Access Protocol (LDAP) directories. This will allow your business to centralize user management and scale effortlessly.
- Leverage modern authentication standards such as OpenID Connect, OAuth, and Security Assertion Markup Language (SAML) to automatically adopt the latest security and identity practices without constantly playing catch-up.
- Meet various compliance requirements like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).
- Automate processes like provisioning and deprovisioning with customer lifecycle management.
- Strengthen security as you scale and become a larger target by automatically flagging insecure or compromised passwords.
- Offering your customers modern ways to reset their passwords or authenticate themselves (text messages, voice, email, or one-time passwords) and managing these security policies in a centralized admin console.

Moving beyond the Automated stage of CIAM maturity means you've expanded your product reach and increased the sophistication of your user management, compliance, and security capabilities. As you continue to scale, you need to invest in stronger security protections and new customer experience features.

# Intelligent: Optimize Without Compromise

At this stage, organizations are well positioned to lead their market. To keep growing, they need to optimize their product offering, but they cannot compromise on all the identity requirements of a complex set of internal stakeholders (for example, product, engineering, and marketing) who are all trying to deliver a seamless and secure user experience at scale.

A modern CIAM solution will help you balance these tradeoffs and improve your infrastructure to leverage application programming interfaces (APIs) and microservices by:

- Offering a sophisticated onboarding experience with a higher level of assurance through identity proofing and account verification capabilities
- Ensuring a frictionless user experience without compromising on security with solutions like adaptive multi-factor authentication MFA (an adaptive intelligence layer that uses contextual information and behavioral inputs to assign risk and additional authentication if needed), passwordless authentication (for example, email magic links and WebAuthn), and progressive profiling that captures user profile attributes over time
- Meeting the latest privacy and security compliance requirements by consolidating user lifecycle and data management in a central connective system
- Optimizing it all by extending the CIAM capabilities to your full tech stack with pre-built integrations or custom workflows, and leveraging best-of-breed technology (for example, bot mitigation, customer relationship management, and marketing analytics tools)

At this point, your application provides customers with strong, perhaps even passwordless, protection. Your use and storage of customer data enables personalized improvements and is fully compliant with data privacy regulations. With industry-leading integrations, your identity security is stringent and you can proactively detect and mitigate risks. Customers use your services with trust and ease, and you're well-positioned to explore other advanced functionalities.

# Continuous: Lead and Set the New Standard

This is the last stage of the CIAM maturity curve, reached by industry leaders who have digitally transformed themselves. They have a dedicated in-house CIAM team supporting an omnichannel strategy that optimizes for both security and user experience. What sets these leaders apart from their competitors is that they understand and view identity as a continuous journey that requires a long-term strategy.

Indeed, to remain at the top you need to continuously set the standard for excellence. At this stage, CIAM means more than just making sure customers can log in seamlessly and securely. It should help you:

- Track your customers across channels (web and mobile, as well as bricks-and-mortar stores) to build a 360-degree view of your customers so that you can delight them with personalized experiences across every channel.
- Implement fine-grained authorization and risk-based authorization to maximize access control over any data exposure, meet very strict industry standards like Financial-grade API (FAPI) and minimize customer friction. Risk signals can be set for categories like network, location, device, and transaction type. A risk score can be computed dynamically or triggered by specific conditions (such as timings and user events).
- Automate security orchestration and response with flexible workflows, and reduce the time and effort spent managing identity and security policies with artificial intelligence (AI) and machine learning (ML) capabilities.

REMEMBER

Whether you're a first-time product developer or an established market leader, embedding CIAM into your product roadmap is crucial. Knowing your stage on the CIAM maturity curve means that your organization can monitor successes and identify focus areas to give you a competitive advantage.

IN THIS CHAPTER

- Offering more engaging experiences to delight your customers
- Driving better security outcomes to build trust with your brand
- Ensuring regulatory compliance and safeguarding user privacy
- Supporting increasingly complex architectures and use cases

# Chapter 7
# Envisioning the Future of CIAM

In this chapter, we look ahead and explore four key trends that are shaping the future of CIAM and explain how they will help your business thrive.

## Increase Customer Engagement

Customer-facing organizations must constantly innovate and enhance how users interact with their brand to increase customer engagement and maximize customer lifetime value. It makes sense, then, that one of the biggest trends shaping the future of CIAM is improved customer engagement and faster time to value. Ultimately, if you're building a new product, you want users to engage with that product — and delivering a superior experience is vital to fostering those relationships.

TIP

To help increase customer engagement, a modern CIAM solution built with an eye to the future will:

- **Enable you to require the right level of input at the right time to the right person during their customer journey.**

Rather than trying to extract loads of information about potential new customers through a lengthy registration process, leverage innovations like progressive profiling to minimize customer friction and improve conversion rate.

- **Give your customers the right content in the language and format that speaks best to them.** Build confidence by speaking to your customers in their native tongues, and manage translation and customization separately.
- **Allow your organization to brand every identity touch point to build trust and connect with your customers.** Embed your brand assets into every step of the customer identity journey. For example, let your customers use your own, branded multi-factor authentication (MFA) app leveraging a device software development kit (SDK) or application programming interfaces (APIs).

REMEMBER

Creating a valuable and enjoyable experience is one of the quickest ways to drive customer engagement — and highly engaged customers are more likely to purchase more of your products, more frequently.

## Drive Better Security Outcomes

A modern CIAM solution needs to achieve the right balance between security and customer experience to help build trusted relationships between your customers and your brand. As cybersecurity threats continue to evolve and become more sophisticated and dangerous, it may be tempting to tilt this delicate balance toward maximizing security and sacrificing usability.

Instead, businesses can drive better security outcomes — for themselves and their customers — by empowering users to keep their data secure at a level they are comfortable with, and by adding security controls that do not require direct customer input. The end goal should not just be more security, but *better* security.

Rather than implementing the most stringent and disruptive security options available in a modern CIAM solution, businesses should focus on applying the right security at the right time, providing flexible policies, and keeping things as simple as possible.

To drive better security outcomes for the future and build trust with your brand, consider the following tips:

- **Apply the *right* level of security at the right time in the customer journey.** Even businesses that have thousands of customer-facing apps can keep things simple by requiring only the minimum input needed (that is, introduce friction) at the appropriate point in the customer journey (for example, during registration). For example, only prompt your customers with MFA when it's necessary, such as when they are logging in from a suspicious location or unknown device.
- **Set different security policies for *each* application to optimize the balance between customer friction and the security risk.** For example, apps that allow customers to register and make a purchase should require a greater level of security than apps that only allow customers to check the status of an order, even if it is the same user and the same brand.
- **Enable end users to *opt-in* for MFA.** Rather than requiring your customers to register for MFA, give them the option. Although MFA is becoming more commonplace, plenty of people are still annoyed by it. Instead, you could track other risk factors without their input (for example, device, location, or network).
- **Empower your customers to recover their accounts via *any* factor.** Offering flexible self-service options (for example, email, text message, one-time password, and so on) for your customers to recover their accounts or reset their passwords without having to contact a call center is always a win.
- **Extend CIAM at every touchpoint to integrate third-party services.** Leverage specialized technologies to add functionality and improve the customer experience at every touchpoint along the customer journey.

## Safeguard Privacy

Privacy regulations, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), are already reshaping how business is conducted today, and more regulations are on the way globally as customers demand more control over their personal information. To continue building customer trust, businesses must adapt, but privacy is complex

and more than just "consent." From a CIAM standpoint, future capabilities will need to address three primary use cases:

- **Preference management:** Processing and storage of customer data
- **Privacy management:** Sharing of customer information
- **Compliance management:** Mapping and potential deletion of personal data

Such capabilities can be offered out-of-the-box by a CIAM solution or through integrations with third-party vendors that specialize in privacy and consent management use cases.

Success in safeguarding user privacy will result in increased customer trust, end-to-end compliance, and a thriving business.


TIP

To navigate the complex regulatory landscape today and in the future, leverage a modern CIAM solution to orchestrate preference, privacy, and compliance management of your customers' personal data.

## Manage Complexity

Organizations today must deal with complexity everywhere: from building, testing, and launching modern cloud-native apps for demanding consumers, to federating external and fragmented identity stores across partner portals, while maintaining legacy products until a multi-year digital transformation corporate initiative is finalized. This complexity means CIAM is no longer a simple solution enabling your customers to log in to a single app or website.

CIAM must enable and facilitate business flexibility and growth despite this complexity. Specifically, it will need to:

- Support a multi-org architecture at scale with numerous testing, staging, and production environments
- Handle a mix of modern cloud apps and legacy on-premises products while ensuring data segregation
- Offer extended API coverage and intuitive cross-organization administration
- Help organize fragmented identity systems

IN THIS CHAPTER

- Going through an actionable checklist to implement CIAM
- Starting by identifying your technical and business requirements
- Selecting the right CIAM solution for your organization
- Taking CIAM to the next level of innovation
- Creating seamless customer experiences that deliver competitive advantage

# Chapter 8
# Ten Considerations for CIAM

Here are ten key considerations to help you successfully plan and implement the right CIAM solution for your organization:

- **Understand the pain points for your customers and your internal teams.** Are your customers frustrated by a lengthy registration process? Did you experience a security breach? Are your digital transformation initiatives being slowed down?
- **Define your customer experience aspirations.** What do you want your customers to experience when they interact with your brand? Do you want to provide access to all your apps with a unique and branded login experience? Across which channels do you want to provide this experience?
- **Determine your security specifications.** How do you ensure a secure access experience now? What do you want to offer in the future? Are there applicable security and privacy regulations that you need to comply with?

- **Set your business objectives.** From a business standpoint, what do you need to achieve? Perhaps, international expansion or a new product launch? In what timeframe?
- **Assemble all your CIAM needs.** Prioritize your must-haves and nice-to-haves among all your user experience, security, and business requirements. Align internally and decide how you will balance the potential tradeoffs.
- **Estimate the opportunity cost to build versus buy.** Building and maintaining your own CIAM solution is hard and costly so you should focus on your core business. Read Chapter 3 to understand what building your own solution fully entails.
- **Outsource to a CIAM expert (so it can be done right).** Now that you know what you are looking for and understand your opportunity cost, identify the right CIAM expert for your organization. Look for a trusted partner with a proven track record that will address your present and future needs.
- **Deploy and enable seamless customer experiences.** Once you've chosen a modern CIAM solution, you can start deploying it broadly and rapidly across all your customer-facing apps, websites, and portals to deliver seamless and secure customer experiences.
- **Unlock innovation through the CIAM maturity curve.** A modern CIAM solution opens the door to a world of opportunities for your business. Read Chapter 6 to learn about the possibilities along the CIAM maturity curve.
- **Focus on your competitive advantage.** A modern CIAM solution can be a competitive differentiator for your business, helping you create a reputation for trust, innovation, and superior customer experiences.

## Build secure, seamless customer experiences

If you've logged into a website to purchase concert tickets or used your social media account to log into a new e-commerce site, you've already interacted with customer identity and access management (CIAM). CIAM provides a digital identity layer that can be embedded into customer-facing apps, websites, and portals. In this book, you'll discover how CIAM can help you provide secure, seamless experiences for your customers and partners.

## Inside...

- The basics of CIAM
- Why CIAM is more important than ever
- Why you shouldn't build CIAM yourself
- What a modern CIAM solution is
- What to look for in a CIAM solution
- Thriving with a CIAM solution tailored to your business needs
- The future of CIAM


**Lawrence C. Miller** has worked in information technology for more than 25 years and has written more than 200 For Dummies books. **Jeremie Certes** is a Senior Product Marketing Manager at Okta.

**Go to Dummies.com™**
**for videos, step-by-step photos, how-to articles, or to shop!**

**ISBN: 978-1-119-86655-8**
**Not For Resale**


for dummies®
A Wiley Brand

# WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.