



Customer Identity and Access Management (CIAM)

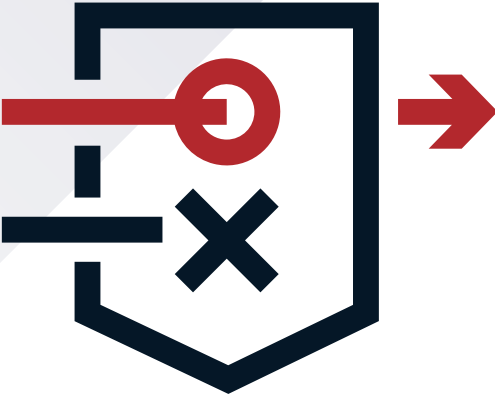


Table of Contents

CHAPTER 1

Extraordinary User Journeys in the Digital World 4

The Digital-First Customer 5

CHAPTER 2

Digital-First Customers Know What They Want From Your Business 6

1. Convenience: Make Every Digital Engagement Effortless 7

Omnichannel: Don't Make Me Repeat Myself

Frictionless: Don't Make Things Harder Than They Need To Be

Fast: Don't Make Me Wait

2. Security: Safe and Secure Digital Interactions 9

Breaches: Don't Expose My Personal Data

Fraud: Protect Me, But Don't Treat Me Like a Criminal

3. Privacy 11

Delivering on Convenience, Security and Privacy Expectations Without Compromise

CHAPTER 3

Design Extraordinary Digital Experiences That Have It All 12

The Challenges That Get In The Way 13

The Ever-Changing Threat Landscape

Legacy and Homegrown Solutions Hold You Back

Integrations and Optimizations Slow You Down

Don't Have a Single View of the Customer

Turn Digital Experience Visions into Engagement Driving Reality

What Is Identity Orchestration?

Identity Orchestration Is Your Secret Advantage

Give Your Teams an Agility Boost

Consistent Experiences Across Every Channel

Full Control Over Your Customer's Experience

Table of Contents

CHAPTER 4

The Influence of Customer Identity on Digital Experiences 17

Understanding the Basics of Customer Identity 18

The Identity Touchpoints in the Customer Journey 18

Browse the Website - Detect Online Fraud

Creating an Account - Verify Who Your Customers Are

Self-Service - Profile Management Made Simple

Signing-In - Seamless and Secure Customer Authentication

Passwordless Authentication: Maximizing Security, Minimizing Friction

Use Services - Authorization for What Customers Can Do

Support: Making It Easy for Customers to Get the Help They Need

Respect Customer Privacy Everywhere

CHAPTER 5

Taking the Right Customer Identity Approach for Your Business 25

Option A: Extending Your Enterprise Identity Solution 25

Bottom Line: Enterprise Identity Often Lacks Critical Capabilities for Customers

Option B: Building Your Own Customer Identity Solution 27

Bottom Line: DIY Solutions Can Create More Problems Than They Solve

Option C: A Purpose-built Customer Identity Platform 28

Bottom Line: A Purpose-built Customer Identity Platform Provides Everything You Need

CHAPTER 6

Making the Business Case for Customer Identity 30

Customize Your Business Case For Every Audience 30

Engagement: Drive Business with Delightful Experiences

Calculate the Value of Customer Identity

Security & Privacy: Boost Agility to Protect Customers

Use Customer Identity to Power Engaging Digital Journeys 33

CHAPTER 1

Extraordinary User Journeys in the Digital World

Our world has rapidly evolved into a digital reality over the last few years, and digital experiences have become the norm. Customers have formed some strong opinions on how easy it should be for them to consume these digital services, while ensuring they're still in control of their data. In response, organizations have had to throw the traditional brick-and-mortar engagement rulebook out the window in order to meet their customers where they are at—the digital front door. And, in order for businesses to keep up, they'll need to find a way to guarantee the type of user journeys that customers expect.

Delivering experiences that satisfy every customer's desire has kept businesses under constant pressure to innovate the entire digital user journey. Finding that elusive sweet spot between convenience and security is foundational to unlocking the returns associated with innovation.

That is where the opportunity lies for you to provide your customers with seamless and frictionless experiences, without having to sacrifice protection against fraud or breaches.

That “sweet spot's” name is customer identity.

If done right, customer identity is a way to transform the entire online experience so customers can seamlessly and securely interact with brands. This starts by providing a simple and safe way for them to create accounts, log in and update preferences that permeates across every digital channel.

Unfortunately, building digital experiences that are both convenient and secure isn't as easy as it sounds. Most organizations struggle getting that balance right. Due to complexity, legacy tools, and general lack of resources, weaving the necessary customer identity services together in order to create a cohesive journey can be rather challenging. And, it's these challenges that end up manifesting as friction for the customer; the very thing you're trying to avoid in the first place.

The good news? There are several approaches you can take to eliminate that friction and finally build those customer experiences using customer identity that keep your users happy, thus driving engagement for your business in the long term.

Read on to learn:

- Your customers' expectation of you
- The role customer identity plays in creating extraordinary experiences
- How you can use customer identity to deliver business impact



The Digital-First Customer

The rise of the digital-first customer isn't limited to a single industry. More customers are choosing to engage with brands online than ever before, in nearly every industry.

Banking Has Left the Branch



78% of adults in the US prefer to bank via a mobile app or website ([Source](#))



58% of consumers surveyed are open to the idea of opening a personal bank account online ([Source](#))

Retail Shopping Online All the Time



30% of global shoppers shop online once or more than once a week ([Source](#))



69% of customers have been inspired by social media to make a purchase ([Source](#))

Healthcare Doesn't Start at the Doctor's Office, But at the Patient Portal



44% of patients access test results using an online patient portal ([Source](#))



61% of patients will switch healthcare providers to one that has an online patient portal ([Source](#))



CHAPTER 2

Digital-First Customers Know What They Want From Your Business

A consequence of our economy going digital is that customers have more opportunities to engage with brands online. This also creates more opportunities for these customers to form impactful opinions of a brand, based on their overall experience of that digital interaction.

Not only do customers have more chances to define their preferences, but engaging with a wider variety of businesses digitally changes the game in how customers compare experiences between brands. Now, every digital interaction a customer has is viewed through the lens of their favorite online experience. This means that no matter the industry, customers will likely have high expectations of the brands they interact with, comparing their interaction to what they now believe a perfect digital experience should look like.

Customers have set the bar outrageously high for businesses to deliver seamless and secure digital experiences. For you to meet that standard, it all comes down to how your organization uses customer identity effectively to design user journeys. These journeys should not only improve the customer's digital experience, but if done right, help your business acquire and retain customers, boost revenues and earn loyalty.

And, though that bar is high, simply recognizing—and addressing—just three main expectations can help you create those digital experiences that customers associate with their favorite brands:



Convenience



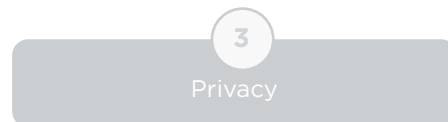
Security



Privacy

1. Convenience:

Make Every Digital Engagement Effortless



Registration and sign-in aren't the reason your customers are visiting your site or using your mobile app. However, if you make these critical interaction points time-consuming or complicated, it could be the reason they abandon your brand. The moment one of your customers touches any of your digital properties to open an account or log in, is an opportunity for you to make it easy and simple for them to access the services they need or to make a transaction.

Designing customer journeys that keep them coming back for more relies on eliminating any unnecessary friction in each interaction, in order to deliver streamlined and secure experiences across every digital property which are tailored to each customer's preferences.

Omnichannel: Don't Make Me Repeat Myself

One digital channel is no longer enough to drive engagement with customers. Now, every brand has an omnichannel strategy to extend its reach, with the goal of attracting and retaining more customers. The resulting digital journey is an intricate web of online, mobile and support applications, possibly managed by multiple teams within your organization.

But for the customer, they just see one thing: your brand.

When customers interact with your brand, they're often not paying attention to where one application stops and another one begins. What they're really focused on is how seamless their overall journey is, as well as whether or not the information they give you is accurately reflected along that journey.

This means if a customer changes their name on their checking account, they expect you to make the change on their associated savings and investment accounts as well. Similarly, if a customer updates their preferences to opt-out of emails on your mobile application, they expect that you'll understand they don't want emails from your website, either.

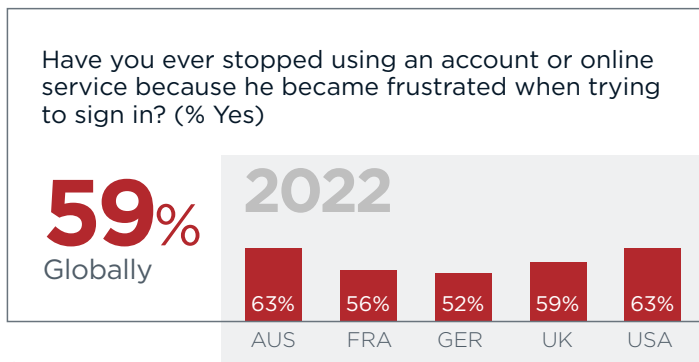
By unifying the customer experience across all of your mobile applications, websites, in-store kiosks and more, you can prove to your customers that you know who they are and deliver consistent, personalized experiences that keep them coming back for more.

[A Unified Approach to Delivering Exceptional Customer Experiences](#)



Frictionless: Don't Make Things Harder Than They Need to Be

When you're unable to deliver consistent experiences, you introduce friction. Friction makes it harder for customers to engage with your brand online. Customers have little patience for friction and are content to leave one brand for another that offers a digital experience that feels less clunky. Unfortunately, it's very common for unnecessary friction to get introduced when businesses are designing user journeys that strive to balance convenience and security in online experiences.



[Source](#)

A classic example is complicated password policies. In an attempt to maintain security, some organizations require users to create very long passwords that contain specific combinations of capital letters, numbers and symbols.

This is an area where a balance between convenience and security is critical. If policies are unnecessarily complex, it can be difficult to come up with a password initially, let alone enter it twice without making a mistake.

Remembering these intricate passwords is just as difficult, leaving many customers in the position of having to reset their forgotten passwords every time they log in. Expecting that your customers will continue this dance is unrealistic. More likely, they'll abandon your brand in favor of competitors that offer a smoother experience.

You can eliminate the likelihood of customers forgetting their passwords simply by not requiring them. Taking a passwordless approach to login makes the experience frictionless for your customers and if done correctly, it also enhances security by relying on more secure methods of authentication, like biometrics, rather than the easily hacked password.

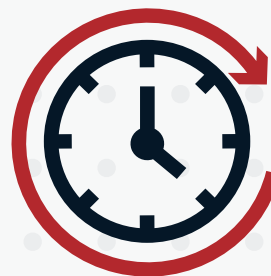
[Getting Started on Your Passwordless Journey](#)



Fast: Don't Make Me Wait

Poor experiences like complicated password requirements aren't just frustrating; they take too much time. Customers simply don't want to go through additional steps or processes when logging in to your site. Of course, in cases where security is crucial—such as banking—it's okay to require more information from customers. But, the key is to never require more than is necessary.

Remember—no one comes to your site to see how great your registration or sign-on experiences are. In fact, the way you know those experiences are amazing is when they're so seamless that they actually go completely unnoticed.



2. Security: Safe and Secure Digital Interactions

1

Convenience

2

Security

3

Privacy

You have to ask your customers for information about themselves in the normal course of business. Every smooth and personalized digital experience depends on this data in order to drive engagement, open up cross-sell and up-sell opportunities and boost revenue.

As your users continue to share data with you, your customer data security strategy needs to evolve to keep up with the rapidly growing fraud and breach landscape, right alongside the need to mitigate your customers' lackluster password habits. Whether justified or not, they are looking to you to secure their data and expect more accountability from you than ever before.

Breaches: Don't Expose My Personal Data

Data breaches are among the most costly events a customer-facing enterprise can experience. A single breach can result in customer abandonment, fines and brand damage that is nearly impossible to quantify. Even if your customer's own bad password habits—such as reusing passwords or using weak passwords—might be the cause of a breach, your customers will still hold you responsible for keeping their data safe from a breach. In fact, **87% of consumers** would not do business with a company if they had concerns about its security practices.

If you're storing user data, you have the responsibility for protecting that data. That includes ensuring that potential bad actors both from outside as well as within your organization can't access the keys to the kingdom. Your customers are trusting you to take the security measures needed by whatever means necessary.

[Multi-factor Authentication for Customers](#)



Fraud: Protect Me, but Don't Treat Me Like a Criminal

The shift to digital hasn't gone unnoticed by fraudsters and bad actors. As more digital channels become available for customers to use, fraudsters are upping their game and evolving their tactics to evade detection. And they're often successful, which has forced companies to respond with additional security checks—which often come at the expense of customers' once-satisfying digital experience.



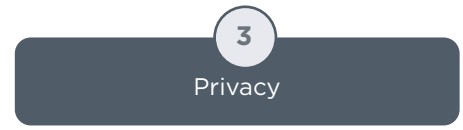
[WATCH THE VIDEO](#)

Fortunately, it doesn't have to be this way. In an ideal scenario, fraud prevention is invisible, adding no friction to the vast majority of user sessions while still effectively protecting the organization from fraudsters and only using friction commensurate to the threat level. To do this, fraud prevention must be integrated fully into the broader customer journey. Fraud tools can work with identity tools to effectively determine whether users are real, or criminals, and take targeted action. When this is done correctly, legitimate users can still enjoy a low-friction experience while fraudsters encounter additional security measures that make it difficult for them to steal from you or your customers.

[The Ultimate Guide to Online Fraud Prevention](#)



3. Privacy



Across industries, customers are becoming more skeptical about companies' ability to protect their privacy. Even as customers are more likely to choose security over convenience in a digital experience, their top priority is that their privacy is maintained—and respected. While regulations like General Data Protection Regulation (GDPR) and [California Consumer Privacy Act \(CCPA\)](#) further support this expectation, being compliant also provides an opportunity for brands to show their customers how they can respect their privacy.

It's all too easy to see compliance as just another hurdle to overcome. But checking the compliance box doesn't simply prevent fines; it also has the power to prevent a negative impact on customer retention and revenue. Point blank, if customers don't feel that you are respecting their privacy, they will leave. 48% of consumers have stopped using an online service because they were concerned ([Source](#)).

By providing your customers with transparent insight and control over the personal data you've gathered about them, you're also giving them the respect they deserve—all while earning their trust in continuing to engage with your brand.

By year-end 2024, 75% of the world's population will have its personal data covered under modern privacy regulations.

Gartner®: 'Top Trends in Privacy Driving Your Business Through 2024', May 5, 2022.



Delivering on Convenience, Security and Privacy Expectations Without Compromise

Customers want it all—convenience, security and privacy—in every digital experience. Finding the perfect balance with those three for your business is challenging, but not impossible. Customer identity can help you design and optimize user journeys that not only span across all of your digital properties but are frictionless, secure and compliant with privacy regulations.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

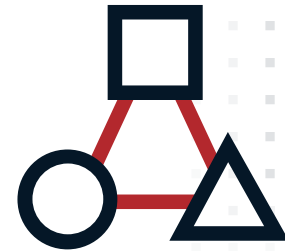
CHAPTER 3

Design Extraordinary Digital Experiences That Have It All

Understanding your customers' expectations is one thing, but translating your organization's ideas into real digital experiences that drive engagement comes with its own challenges. Building such digital experiences using customer identity to exceed user expectations means easing the tension between three seemingly opposing forces: convenience, security and privacy.

When businesses attempt to bring these forces together, one tends to do really well while the other two fall short. For instance, maybe security is top-notch, but the user experience is not convenient nor is their privacy a priority. Customer satisfaction hinges on ensuring neither of these forces impede on each other. If one outdoes the other two, then you will end up providing experiences that neither your customers nor your business will find satisfactory.

Therefore, using customer identity to help you design and build digital experiences without sacrificing convenience, security or privacy is the first step in driving engagement and out-maneuvering the competition.



The Challenges That Get in the Way

You have a vision of the perfect digital experience that will drive engagement for your business by eliminating friction, enhancing security and ensuring compliance with privacy regulations. But what's standing in your business's way of turning that vision into reality?

The Ever-Changing Threat Landscape

Bad actors and fraudsters see the rise in the digital economy as an opportunity. They are continuously improving their attacks, making it harder than ever to detect and mitigate any threats.

Keeping up to date with the latest threat vectors is nearly impossible, so many brands rely on a growing number of fraud and security solutions to protect their customers and businesses. Organizations must find a way to properly manage all these solutions from multiple vendors and bring their insights into a single view to properly evaluate potential risks and initiate mitigation measures in real time.

Legacy and Homegrown Solutions Hold You Back

Legacy and homegrown customer identity solutions were not designed to handle the scale and complexity of the digital experience ecosystems that businesses have to build in order to compete in today's marketplace. These antiquated solutions limit your organization's ability to maintain the flexibility needed to add innovative technologies or update functionality without massive development effort. That's if the legacy solution can even support the updates at all.

While homegrown solutions might work for the customer-facing application they were originally built for, these are typically "point solutions" that don't translate well to other digital channels, leaving your customers with inconsistent experiences and you with another solution to manage.

Integrations and Optimizations Slow You Down

Extraordinary digital experiences don't rely on one service from a single vendor. Instead, they are built on the foundation of multiple business services working together.

Unfortunately, weaving together these services to deliver a cohesive experience takes development hours and custom code, ultimately slowing down your time to market for new products and services. And if you want to simply swap out a service or try new technologies to optimize how your customers engage with your brand, the development effort required to add another integration can disrupt both internal teams and the customer experience overall.

You Don't Have a Single View of the Customer

Personalizing your customer's experience with tailored interactions to make them feel like you understand them requires every digital property to have access to the same customer profile information. However, as many brands have rolled out their digital experiences, profile data ends up stored in different places across the business which leaves customer-facing applications without a single source of truth to tap into to properly personalize interactions. The end results are customers frustrated with generic and inconsistent experiences across your brand's digital properties.

Organizations can overcome these challenges by implementing customer identity solutions that eliminate the data silos for your teams, the result being personalized digital experiences that your customers appreciate. It all starts with synchronizing and consolidating customer data across your organization to create a single view of the customer. This lets you build consistent and personalized omnichannel experiences that help you boost revenue with cross-sell and up-sell opportunities based on what your customers like.



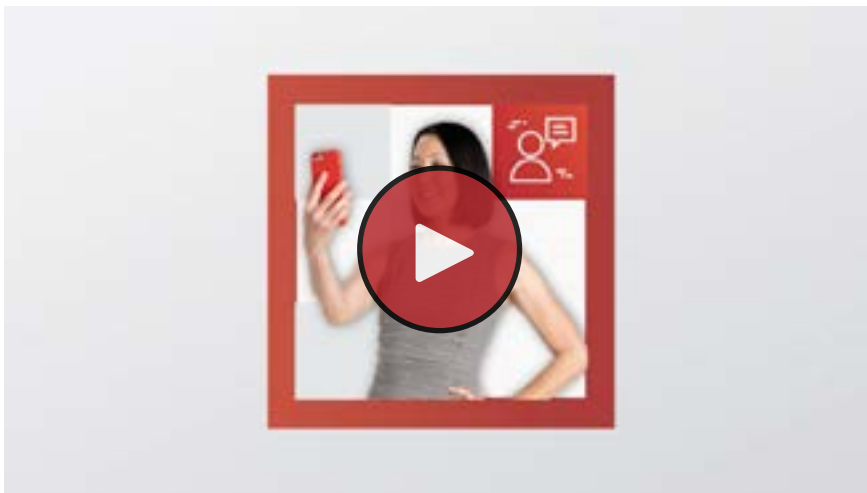
Turn Digital Experience Visions into Reality

Getting rid of complexity in how your organization builds user journeys will translate into smoother, more secure digital experiences for your customers. By simplifying how your teams integrate different services together—i.e. in testing new vendors, business logic or experiences and deploying enhancements—you'll help set that bar for providing digital experiences that other companies will want to replicate for their customers.

Furthermore, you know your customers' expectations when it comes to engaging with your brand online: convenience, security and privacy. You can accomplish this by weaving together customer identity, risk providers, databases and more into one seamless digital experience.

How can you accomplish this?

With identity orchestration.



[WATCH THE VIDEO](#)

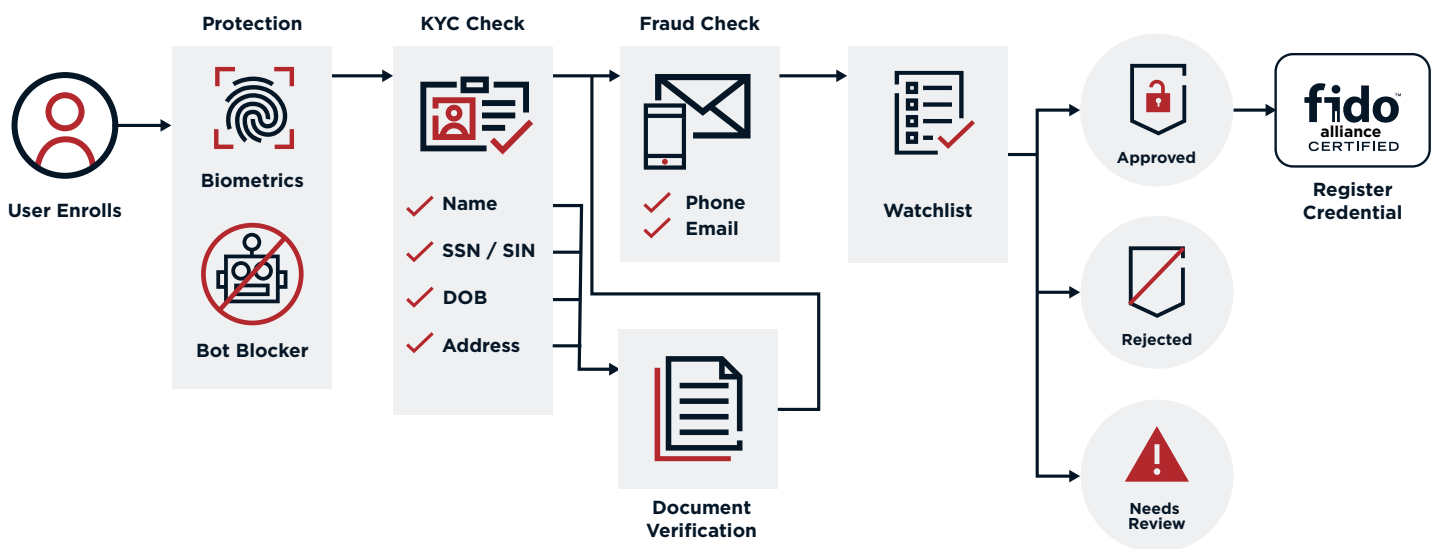
Identity orchestration is essential in removing the complexities and friction required to make smooth customer experiences happen across the entire customer journey.



What Is Identity Orchestration?

Identity orchestration is the flexible approach to designing, testing and optimizing digital experiences. Using a no-code/low-code environment to integrate all the services and applications seamlessly together, identity orchestration takes the friction out for your business to delight and protect customers. For instance, your teams can automate the creation of workflows using a drag and drop canvas to weave together identity services like fraud detection, identity verification and authentication into critical digital touchpoints along your customer journey.

Ultimately, identity orchestration makes it simple for your organization to make security invisible to the customer until it needs to be seen.



Leveraging identity orchestration to create digital experiences provides your organization with the ability to rapidly iterate and optimize the user journey. By taking an intuitive, graphical approach to building out a single view of the entire customer journey, you can:

- Experiment with different experiences to drive engagement
- Swap out or test different vendors to manage cost-effectiveness
- A/B test different workflows to measure performance

Best of all, with identity orchestration, these tests and optimizations can be pushed live so you can get them in front of your customers quickly.

Identity Orchestration Is Your Secret Advantage

Identity orchestration gives your organization the power to design and deploy digital experiences that bring together convenience, security and privacy without compromise. Not only that, but it will become your secret weapon to out-maneuvering your competition. This is because identity orchestration helps you set the bar for digital experiences among your competitors in your industry. They will be eager to replicate what you're providing for your users in order to bring back the customers that have now preferred your brand instead.

Give Your Teams an Agility Boost

Low-code/no-code identity orchestration gives your organization the time to focus on building experiences—instead of the integrations or custom development required to connect to multiple vendor solutions or proprietary systems. Plus, your business can rapidly iterate and test experiences without causing major disruption to your teams, meaning that they can keep focusing on what is important: delivering customer experiences that drive engagement.

Consistent Experiences Across Every Channel

As digital consumption rises, the number of digital touchpoints your business has to design and maintain increases. Identity orchestration makes it simple to optimize across multiple applications, devices and use cases to ensure that your customers have consistent, personalized experiences with your brand—no matter what channel they are engaging with.

Full Control Over Your Customer's Experience

Taking advantage of identity orchestration allows you to use any customer identity or business service to create the perfect digital experience. Your business will have full control over what vendors and services you want to integrate into your digital experience so you can generate the greatest amount of impact and engagement when interacting with your customers.

Turning what you think your customer experience should be into reality is simple with identity orchestration. By seamlessly weaving together the necessary customer identity services with business applications, you can design, test and optimize digital experiences that meet your customers' expectations and deliver business impact that will be the envy of your competitors.

Identity Orchestration
Fundamentals



CHAPTER 4

The Influence of Customer Identity on Digital Experiences

Knowing who your customers are is essential to delivering the seamless, secure and personalized experiences that they not only expect, but also drives engagement for you. Unfortunately, a perfect solution that provides everything your business needs in order to truly get to know your customers doesn't necessarily exist in one neat package.

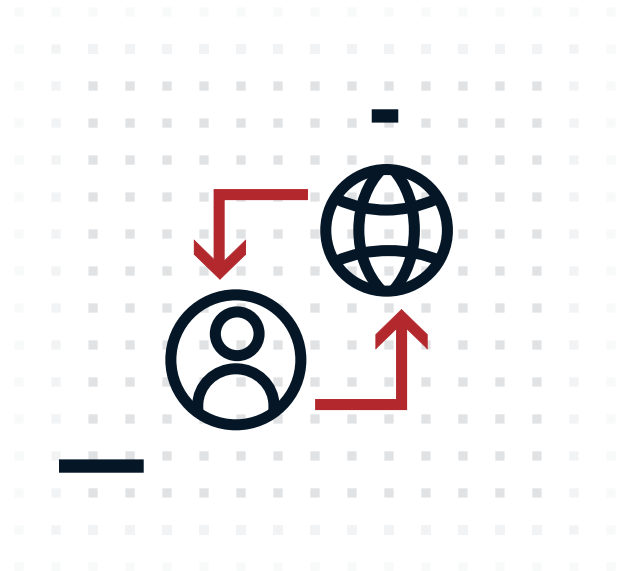
But, there is a way.

Identity orchestration can help your organization get to know your customers all while alleviating the friction, complexities and costs associated with integrating business applications and identity services together.

The result is ensuring your customers have a delightful and secure experience.

How your brand integrates services together is only one piece of the puzzle. Another foundational aspect is understanding how each service impacts how your customers engage with your business online. Recognizing this influence at every interaction point can give your business an advantage to remove friction and make it simple for customers to continue engaging with your brand.

Customer identity services are critical to ensuring your users can securely engage with your brand online. However, approaching customer identity as not just a means to an end for security—but also a key part in driving engagement by removing friction—can help your business deliver the experiences your customers can't turn their back on.



Understanding the Basics of Customer Identity

A common misconception of customer identity is that it is simply a security tool to protect customers and businesses from fraud and breaches. This scoped view will give a business a decent foundation for securing user engagements online. However, this only partially meets customer expectations when it comes to digital experiences and can typically leave users frustrated with long registration forms, complex and confusing password requirements and easily forgotten pin numbers to regain access to an account.

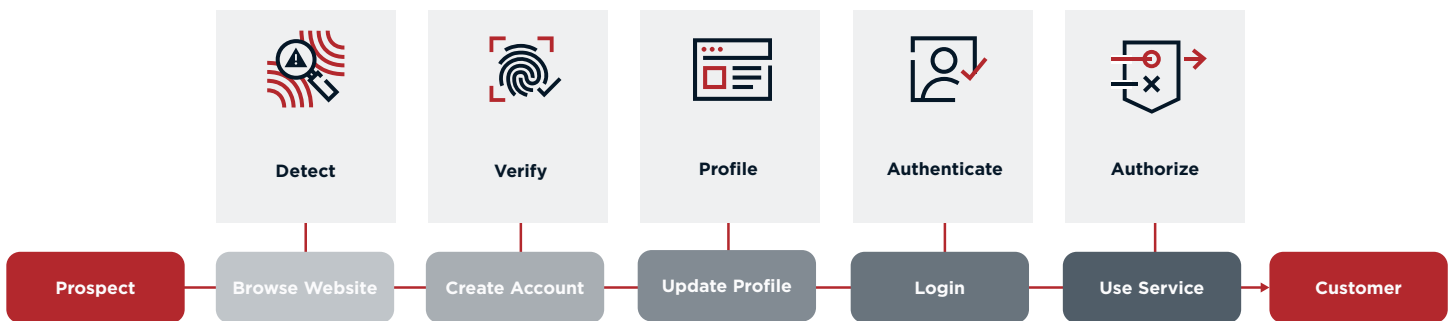
The difficulty comes down to deciding how much friction is the right amount of friction. It is a classic “Goldilocks” problem: too much friction can result in frustration and abandonment while too little results in a breach of trust. Understanding how customer identity influences every step of the user journey can help you identify the right amount of friction you can introduce into an experience. And once you find the perfect level of friction, it actually makes it easier for your customers to put their trust in you.

The Identity Touchpoints in the Customer Journey

From your customer’s perspective, your business is providing them a single experience that they can engage with across all of your digital properties. With the right approach, they shouldn’t see what’s actually happening behind the scenes.

That’s because your customers shouldn’t be able to tell that their digital experiences are actually a series of touchpoints your brand has created by stitching together different services and applications. Without customer identity seamlessly woven into every interaction point, you could inadvertently let your customers in on what is going on under the hood and leave them with a disjointed experience – one that is filled with friction and yet still insecure.

Let’s explore the customer identity capabilities needed at every touchpoint that provide your users a smooth and secure digital experience:



Browse the Website – Detect Online Fraud

The increase in digital touchpoints in the customer journey hasn't gone unnoticed by fraudsters who are seizing this opportunity to defraud customers and businesses. [Protecting your customers and business from fraud](#), therefore, relies on your ability to quickly determine if a visitor to your website is legitimate or a bad actor.

How is this done?

Organizations need to build an agile, open solution that leverages multiple IDPs and detection and risk services to prevent identity fraud, most notably account takeover and new account fraud. The solution needs to evaluate the entire customer journey, from the first interaction to the final transaction. It must provide transparency into the user session to detect fraud, decide what course of action to take, direct mitigation, and defend against future attacks. Incorporating dynamic training and learning capabilities can help organizations stay ahead of ever-changing threats and adjust the response in real time, evaluating attack vectors, device/network telemetry, user attributes, user behavior, and integration vulnerabilities.

A robust threat protection solution should allow you to integrate and orchestrate detection, decisioning, and mitigation services into customized user journey flows that increase customer trust, lead to more conversions, decrease churn, and reduce fraud losses.

Customer identity can provide your business with the insights to rapidly tell the difference between safe and risky users the moment a visitor touches any of your digital properties. By doing so, you can help prevent costly fraud.



Objective

Protect against fraud without impacting the customer experience

How customer identity addresses it:

- Detect bots and bad actors by combining biometrics, behavioral data and device intelligence to rapidly make decisions
- Aggregate fraud and risk signals from multiple sources and pass information directly to identity solutions for mitigation
- Mitigate fraud in real time by assessing risk and automating the response to stop fraud before it occurs
- Design customer journeys that add friction based on the level and type of risk to ensure minimal impact to the experience of legitimate customers

Example: Don't risk losing customers by asking them to prove they're not a bot by completing a CAPTCHA every time they check out. Instead, you can monitor visitor behavior—such as mouse movements, copy/paste usage, auto-complete, etc.—to identify them as a legitimate user.

Creating an Account – Verify Who Your Customers Are

Registration and account creation are pivotal moments of any user journey. It's where your customers decide to start a relationship with your brand and are willing to give you personal information about themselves.

This touchpoint is not only an important opportunity to ask questions in order to learn more information about your customers, but also for you to gain confidence that your customer is the real person they say they are. Make a good impression right from the start by eliminating any unnecessary friction—such as long registration forms or cumbersome identity verification checks—that would otherwise cause new users to abandon the process altogether. This can be done by limiting the information gathered to what's absolutely necessary as well as letting customers register using social media accounts.

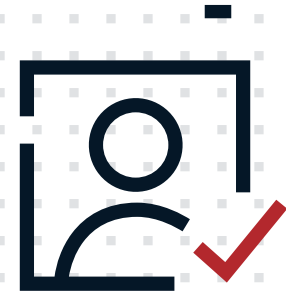
Objective

Make registration or creating an account fast and frictionless

How customer identity addresses it:

- Support for different registration options (social registration, standard fields or registration with other identity providers)
- Easy-to-use identity verification methods that make it simple for customers to prove who they are during registration – issue a reusable verifiable credential based on this and eliminate the cost and time to verify users again in the future
- Giving customers single sign-on (SSO), creating a common registration experience and one set of credentials to use across every digital property
- Customizable registration pages to reflect your business's brand
- Convenient and secure password policies

Example: Allow your customers to create an account using their existing Google or Facebook account, eliminating the need for them to have to fill out a separate (and long) registration form.



Self-Service - Profile Management Made Simple

Your customers don't want to call or email to make basic changes to their account profile. Nor do they want to have to update their information across each of your digital properties whenever they want to make a change. It's up to you to give your customers the ability to view and update their profile information on any digital property and have those changes quickly take effect at every interaction point thereafter.

When you make it simple for customers to have control over their profile information, you can build unified customer profiles that are the single source of truth for all customer data. You can use these unified profiles to build personalized experiences based on each customer's preferences in order to drive cross-sell and up-sell opportunities.

Objective

Make it simple for customers to manage their profile so you can use their preferences to build consistent and personalized omnichannel experiences

How customer identity addresses it:

- Consistent preferences across every digital channel
- A unified customer profile that gives every application access to the same profile and preference data
- Store any custom attributes and unstructured data to capture the necessary information required for a complete customer profile
- Ability to consolidate unified profiles with bi-directional sync, migration and coexistence

Example: When your customer updates their address on your website, they should immediately see the change take effect in their profile in your mobile app. Additionally, when a customer selects they have a certain preference, any of your customer-facing applications should be able to leverage this data to serve up relevant content at every digital touchpoint as a way to keep the customer engaged.



Signing-In – Seamless and Secure Customer Authentication

Anytime your customers visit your digital properties, you have to make sure that they are who they claim to be in order to provide a secure experience. But you can't sacrifice convenience in the name of protecting against fraud or breaches; you need to provide both convenience and security during authentication in order to make it simple enough for your customers to log in, but impossible for hackers to bypass.

Asking customers to perform multi-factor authentication (MFA) to prove their identity is essential to protecting both users and your brand, but you shouldn't require MFA at every interaction point as this will only lead to frustrated customers. Make the right authentication decision by evaluating user behavior and risk signals every time a customer attempts to login. This includes allowing low-risk users to sign in without MFA.

Doing this helps your business confidently ensure your customers are who they say they are, while providing them with the seamless experience they deserve

Objective

Make logging in convenient and secure across every digital channel

How customer identity addresses it:

- Single sign-on (access to all applications with one username and password)
- MFA and adaptive authentication to protect customers while enhancing their experience
- Multiple ways for customers to authenticate (SMS, email, push notifications)
- Passwordless login

Example: Instead of having separate login screens and credentials for different customer-facing applications, single sign-on gives your customer one consistent sign-on experience for all of your brand's services and products.

Passwordless Authentication: Maximizing Security, Minimizing Friction

Your customers don't want authentication to be complicated. They have been trying to eliminate friction on their own by using weak passwords that are easy to remember but also easy to crack, and then they are reusing the same password across multiple sites. This might have made logging in a little easier for them, but has made their account more vulnerable to hackers.

Give your customers the seamless experience they want without putting them at risk, by "forcing" them to replace lazy password methods with other authentication methods that improve digital experiences and enhance security.

While shifting to [passwordless authentication](#) may seem a little out there or unattainable, developing a strategy to phase out passwords on your terms can set your business up for success, making it secure and convenient for your customers to prove their identity.

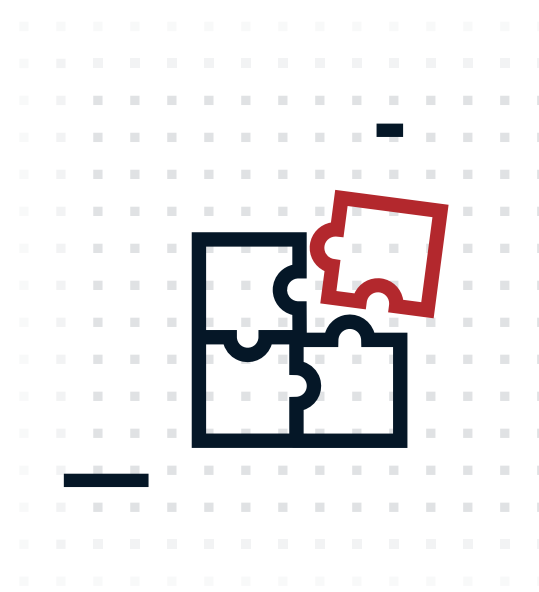
Curious to learn more? [Read the blog](#) to get answers to your questions about passwordless authentication.



Use Services – Authorization for What Customers Can Do

Once your customers have logged in, you need to be able to ensure that they can see and do what they came there to do, while having insights into how their data is being used. If your business leaves authorization up to each customer-facing application team, the experience and privacy of your customers will suffer. This is because customers will encounter inconsistent and disjointed digital experiences that potentially expose their data in ways they wouldn't approve of.

Centralizing authorization in your organization takes a context-aware approach to evaluate access requests in real-time. This is a way to give customers a seamless experience and protect their data.



Objective

Protect customer data with consistent experiences

How customer identity addresses it:

- Dynamic authorization to centrally enforce contextual, fine-grained access policies
- Tailored logic around what customers can see and do to provide seamless, consistent experiences
- Manage and enforce privacy and consent to protect customer data

Example: Instead of forcing customers to do MFA whenever they take any action—from checking a bank balance to setting up a wire transfer—only prompt for MFA when a person attempts a high-risk transaction, such as transferring a certain amount of money over a certain threshold.

Support: Making It Easy for Customers to Get the Help They Need

If your customers are contacting support, it's often because they're experiencing a problem and are frustrated. Don't make an aggravating experience worse by making them go through a tedious process to identify themselves. Instead, make it simple for them to get the support they need without making them tell you what their first car was, their mother's maiden name or answer any other easily forgotten security questions.

This is especially important if your customer has already logged into your site. Once they log in on any of your digital properties and try to access support, it's up to you to start that interaction off on the right foot. Do this by beginning the conversation with a "What can I help you with today?" rather than a "Who are you?".

Objective

Resolve their problem quickly and efficiently; don't add to their frustration

How customer identity addresses it:

- Delegated administration to control which user data support reps can see or edit
- A face scan from a trusted device or other biometric options to verify customer identity
- Persistent sessions across channels to eliminate redundant authentication steps

Example: If your customer is logged into their account and uses the "call customer support" feature, they shouldn't have to provide their password again or remember the answers to security questions. Instead, their initial authentication should suffice. If they called into support directly, you could send a convenient push notification to their phone for authentication. You can also control what information from the customer profile is accessible by customer service reps, so you're able to protect sensitive data.

Respect Customer Privacy Everywhere

Privacy isn't limited to one stage of the customer journey. Businesses must comply with one or more privacy regulations that are applicable at multiple touchpoints in a digital experience, such as EU's General Data Protection Regulation ([GDPR](#)) and Revised Payment Services Directive ([PSD2](#)) and the California Consumer Privacy Act ([CCPA](#)).

Going beyond treating regulatory requirements as a simple "checking a box" initiative not only prevents costly fines, but also gives you the opportunity to earn customer trust and loyalty by giving them [control over and insight into their data](#). Your customers should have the ability to make decisions not only about who their data is shared with and how it's shared, but also what data is shared in the first place. Beyond merely collecting consent, though, you also need to enforce it. Customers should also be given the ability to easily revoke consent at any time. This is how you build trust.

Customer identity solutions can provide your business with centralized authorization authority that enables you to meet always-changing regulations and respect customers' privacy. It all starts by providing users full control and insights into their data.

[Read the blog](#) to discover how customer identity solutions can help you address data privacy challenges and opportunities

CHAPTER 5

Taking the Right Customer Identity Approach for Your Business

As you evaluate the best customer identity solution to use, you may wonder whether or not your current enterprise identity solution can be extended to address customer requirements, before making any other decisions. If not, then you may wonder if you're better off building your own solution.

However, there's also an option that meets the best of both worlds: utilizing a dedicated customer identity solution that can be customized to fit your organization's needs.

To help you navigate this decision, let's take a closer look at your options.

Option A: Extending Your Enterprise Identity Solution

As you consider how to address your customer identity needs, you may look first at your current enterprise identity solution. It may be working well enough for your workforce requirements, and you could be tempted to figure out how you can extend it to address your customer requirements as well.

If your requirements for customer identity are minimal, your enterprise identity solution may be up to the task. To evaluate whether or not your current system is a feasible solution, you'll want to consider your requirements for scale, profile attributes and support:

- **Scale:** Do you need the ability to support spikes in demand? How many customer identities must you support? If you're supporting thousands of customer identities with no expectation of needing to support millions of identities in the future—and you can also expect a predictable volume of demand—then your current enterprise identity solution may suffice.
- **Attributes:** Do you store a lot of different customer attributes? Do you need to support unstructured data or custom attributes? If your profile data consists of basic fields like name, email and address, you may be able to accommodate customer identity with your current enterprise stack.
However, it's worth taking into consideration that in order to provide customers with the best experience, you may need to store custom attributes like opt-ins or premium member status. You may even need to store unstructured data like a JSON blob of preferences or a browser fingerprint.
Traditional identity solutions may not be able to support these types of profile data, which not only limits the experience your applications can deliver to your customers, but how secure those experiences are overall.
- **Support:** Does your IT team have the ability to support app launches and tight deadlines? How many apps will IT need to support? By relying on your current enterprise identity stack, you'll also be relying on your current IT resources. Therefore, you'll want to be sure you have sufficient resources to support the needs of fast-moving development teams.

It's possible you may find that your enterprise identity solution is enough. But for many organizations, this evaluation will reveal many gaps.

Traditional identity security solutions were designed for workforce applications where the main goal of the system was to protect enterprise data and manage internal access. But since these systems were built for non-customer applications and use cases, they aren't intended to accommodate critical customer features such as: self-service registration and account management, social registration and login, detecting online fraud, storing rich customer profiles, handling demand spikes and many others.

Enterprise identity also has little regard for the experience customers demand in general. The features you consider to be optional "nice-to-haves" for your workforce are absolute "must-haves" for your customer use cases. Remember, unlike those in your workforce who will forgive you for clunky login experiences, your customers have specific preferences when it comes to choosing a brand that provides the digital experiences they want. Fail to delight them, and they won't hesitate to go to a competitor.

Bottom Line: Enterprise Identity Often Lacks Critical Capabilities for Customers

Enterprise identity solutions may work for some less-demanding customer use cases. But for many, trying to extend enterprise identity to address customer requirements creates unnecessary risks like:

- Poor customer experience
- No elasticity to accommodate spikes in engagement
- Limited horizontal scalability
- Increased security risks
- No support for online fraud detection or identity verification
- Regulatory compliance challenges
- No customer-friendly methods of multi-factor authentication



[Read the blog](#) to learn about the origins of customer identity and access management.



Option B: Building Your Own Customer Identity Solution

Building your own customer identity solution may seem like a smart way to meet your specific requirements, especially when you have developer resources in-house. And, an enterprise like yours never turns down a good challenge, right? Unfortunately, architecting a homegrown solution can be a massive undertaking that can slow down getting to market.

It may seem that implementing a customer identity solution is little more than a registration and login form. But, should you decide to take up the challenge of building a customer identity solution, you'll soon find that it's a lot harder than it looks. You'll have to find answers to questions that can drastically slow down the time it takes to manage your identity solution and get products to market, like:


- Are you prepared for the complexities of identity standards?
- How will you enable single sign-on for every application, including non-standard and legacy systems?
- What about authentication policies for different apps?
- How will applications be protected from breaches and fraud?
- What about MFA?
- How do you enforce privacy?
- Will customers be able to log in during demand spikes?
- What about passwordless authentication?
- Will development times impact timelines in getting to market?

If you have answers to these questions and ample resources to support a DIY system, then building your own customer identity solution may be an option for you. But most likely, this exercise will produce a lengthy to-do list and illuminate the many disadvantages of trying to undertake a custom build and the maintenance required to support it.

Bottom Line: DIY Solutions Can Create More Problems Than They Solve

Instead of providing the customization you envisioned, building your own DIY solution for customer identity often creates more problems like:

- Lengthy design and implementation
- Ongoing maintenance requires specialized resources
- Potential security gaps
- Lack of standards support
- Inflexible project-specific solutions

[Read the blog](#) to better understand the risks of building vs. buying a customer identity solution. 

Option C: A Purpose-built Customer Identity Platform

Enterprise identity can't always handle the scale and performance requirements, let alone the experience and privacy requirements to meet customer needs. And the other option of attempting to build your own solution is like trying to reinvent the wheel—or a rocket ship. It just doesn't make sense to take on such a risky and overwhelming task when you have the option of using an integrated and dedicated customer identity platform instead.


A purpose-built platform solution that's designed specifically for the requirements of customer identity and developed by identity experts—who've spent decades getting it right—gives you all of the capabilities you need to deliver the seamless and secure digital experiences your customers want. And, it does this without wasting resources on other options that will eventually not meet your needs or will be too difficult to create. With a dedicated customer identity solution platform, you'll be able to:

- Rapidly build, test and optimize customer journeys as a way to keep ahead of the competition with innovative digital experiences
- Give your customers easy-to-use registration, sign-on, support and more so you can acquire more customers and keep them coming back
- Detect and mitigate potential malicious activity to protect you and your customers from fraud or breaches
- Deliver personalized, omnichannel experiences that drive revenue wherever customers interact with your brand
- Give customers insight into and full control over their data in order to adhere to privacy regulations and build trust

Bottom Line: A Purpose-built Customer Identity Platform Provides Everything You Need

A fully integrated customer identity platform provides powerful capabilities like:

- No-code [identity orchestration](#) to design seamless customer experiences by integrating all your chosen identity vendors together with the ability to A/B test to optimize
- Enterprise-grade authentication for [single sign-on](#)
- Adaptive [multi-factor authentication](#) with support for multiple authentication options, including passwordless
- Configuration and customization options to deliver personalized experiences
- Issue verifiable [digital credentials](#) to improve user security and reduce cost
- [Online fraud prevention](#) to detect and mitigate fraud across every channel
- Ability to store identity and profile data how and where you'd like
- Regulatory compliance and consent management
- Handle complex enterprise use cases with custom apps
- Meet scale and security SLAs

Read the [Buyer's Guide](#) to better understand what you should look for in a customer identity vendor. 

	Extend Enterprise Identity to Customers	DIY Customer Identity	Purpose-built Customer Identity
Time to Market	Slow/Medium, need to modify existing or legacy systems to handle customer identity use cases, if possible.	Slow, need to develop baseline identity expertise prior to developing customer identity solution	Fast, use a proven no-code orchestration solution to rapidly design, build and optimize digital experiences
Integrations	Existing systems may not support new technologies that are critical for digital experiences	Requires development time to build and support integrations that can connect to homegrown solution	Use out-of-the-box integrations to business and identity applications to design the experiences you want your customers to have
Customer Experience	Experiences may be less than optimal for customers or not be supported	You will have complete control over the experiences you build	Use pre-built workflows, templates and APIs to choose from to create experiences that align with your business
Scale & Performance	May not meet customer scale and performance requirements	Possible, but requires specific expertise and resources to manage	Build to handle and adapt to changing scale and performance needs
Resources Required	Requires IT resources to support application teams	Requires specialized, technical resources to build and maintain	Resources requirements needed primarily for deployment
Customer Data	May have rigid scheme and limit what type of data you can store	Can architect the customer identity store however you like	Flexible schema to store custom and unstructured attributes
Security	May not meet customer identity security SLAs	Possible, but requires specific expertise and resources to manage	Provides build-in security, particularly in enterprise-grade customer identity solutions
Fraud	May not support online fraud detection and mitigation solutions	Requires time-consuming integrations and difficult to manage multiple fraud vendors and signals	Provides online fraud detection that orchestrates signals from multiple sources to quickly detect and mitigate potential sources of fraud
MFA	May not have customer-friendly authentication methods (i.e. push notifications from a mobile app)	Possible, but time-consuming to build	Many will focus on authentication methods that customers will actually use
Authentication	Most customer identity features not available	Resources required to build single sign-on, passwordless, social login & registration, adaptive authentication, and other use cases	Provides out of the box: <ul style="list-style-type: none"> • Passwordless authentication • Adaptive authentication that looks at user behavior and risk signals to prompt for MFA • Social registration & login • Identity verification

CHAPTER 6

Making the Business Case for Customer Identity

Enhancing the digital journey for customers is a strategic priority for most organizations. But the responsibility for transforming how a customer engages with a brand online rarely falls to a single group. Building smooth, secure digital experiences that successfully drive revenue, increase engagement and inspire brand loyalty, requires a cross-functional effort with collaboration between multiple teams—across an entire organization.

Your business will have to bring together digital experience, product management, marketing, IT, identity and compliance teams to build a cohesive customer journey. However, each of these groups will have varying levels of understanding of how customer identity can help address key challenges in removing customer friction without compromising security and privacy.

You can get ahead of future roadblocks and delays by getting every team on the same page with customer identity before embarking on any digital experience overhaul initiative. By building a business case that's tailored to each team's objectives and needs, you can elevate the value customer identity can bring to an organization—all while ensuring your enterprise is prepared to make a decision regarding a vendor.

Customize Your Business Case For Every Audience

We know that customers demand convenience, security and privacy in every digital interaction with a brand (read [Chapter 2](#) of this guide if you aren't convinced). But teams inside your organization tend to be more focused on a singular aspect of the digital journey. This means they often align objectives with goals that only meet some of the needs of your customers and some of the security requirements of your organization long-term.

With customer experience initiatives, there are generally two groups of teams that will have to work together despite having different objectives:

- **Engagement-Focused:** Building digital experiences that are frictionless to drive engagement.
- **Security & Privacy-Focused:** Ensuring customer security and privacy with resources available.

Optimizing how you make your business case can help bridge the gap between these two groups' objectives, allowing you to align on a customer identity solution that delivers both smooth and secure digital experiences.



Engagement: Drive Business with Delightful Experiences

Engagement-focused teams are tasked by the business to streamline how customers interact with a brand, in order to drive revenue, increase acquisition, reduce abandonment rates and boost customer lifetime value. These teams will look for any opportunity to remove friction in the user experience to meet those business goals. While they do want to ensure every digital experience is secure, they don't want those security or privacy controls getting in the way of revenue or product release timelines.

Conversations with these teams are generally centered around how customer identity is the foundation of seamless digital interactions—from account creation and login to contacting support. Thankfully, it is possible for security to be invisible unless absolutely necessary to avoid abandonment-inducing friction. This can give them peace of mind that customer identity—when done right—enables the business to keep customers coming back for more.

Teams:

Digital Experience, Product Management, Marketing, Business Units

What they care about:

How customer identity impacts top-line revenue, customer acquisition and retention and time to market

How to communicate customer identity's value:

- Build support by providing an analysis of the business value customer identity creates, measured in revenue, customer acquisition and similar metrics
- Share data on current abandonment rates for login and registration forms and explain how identity can improve them
- Provide specific examples of how customer identity can improve user experience by removing friction at every step of the customer journey
- Optimize digital experiences faster to stay ahead of the competition



Calculate the Value of Customer Identity

Customer identity can significantly impact how your users engage with your brand. But what is the impact on your business when you use customer identity to enhance the digital experience? By looking at abandonment rates, average customer lifespan and site visitor data, your business can quantify customer identity's impact on revenue and customer retention.

[Use this calculator](#) to estimate how using customer identity solutions can deliver measurable results and see what is possible for your business.

WATCH THE VIDEO

Security & Privacy: Boost Agility to Protect Customers

For the teams charged with securing digital interactions and ensuring compliance, customer identity is key to preventing data breaches, detecting and mitigating fraud and protecting customer data. These teams are focused on giving the business greater confidence in the identity of who they are engaging with. However, given the focus on customer experience, they know they can't make getting this level of assurance too hard on users.

Adding to the difficulties these teams face is the constant pressure to maintain a high degree of agility in order to be able to adopt new technologies and rapidly evolve the end-user experience while lowering the total cost of ownership at the same time. Conversations with these teams should then be focused on how customer identity can enable businesses to increase their agility to rapidly meet customer security requirements and privacy regulations, without increasing costs and delaying time to market.

Teams:

IT, Security, Identity, Compliance, Fraud

What they care about:

How customer identity meets their security and compliance needs and impacts cost savings

How to communicate customer identity's value:

- Discuss the ways that customer identity makes teams more efficient
- Demonstrate how it offers a lower total cost of ownership (TCO)
- Demonstrate the potential cost savings associated when identity is integrated with fraud and risk management
- Address the need for scale and adaptability and how customer identity meets it
- Identify your various customer use cases and how customer identity supports them
- Address the need for security and how customer identity meets it



Use Customer Identity to Power Engaging Digital Journeys

The rapid rise of digital experiences isn't a temporary trend but rather a paradigm shift in how all brands approach engaging with their customers. In order to remain competitive, businesses have to build customer journeys with smooth and secure digital touchpoints”.

Weaving customer identity seamlessly through every interaction can give your brand an advantage when developing engaging digital experiences that both acquire and retain users. Taking an intuitive approach to customer identity will help you delight and protect your customers, while boosting your teams' agility and flexibility in the long run.

Build, test and optimize your digital experiences for your customers using Ping's customer identity solution, so there's no compromise between convenience, security and privacy. [PingOne for Customers](#) helps your business deliver engaging digital experiences without sacrifices—in order to build loyalty, drive revenue and out-manuever the competition.

If you're ready to give your customers a better experience, start your [free trial of PingOne](#) today.