

DIGITAL AND COMMERCE

Maturity Pathway

Understand the technologies and processes required at each stage of your digital transformation journey.

Contents

The Pathway
to digital trust

4

The Maturity
Pathway

6

Basic
webstore

8

Modern
Webstore

10

Digital Trust:
single brand

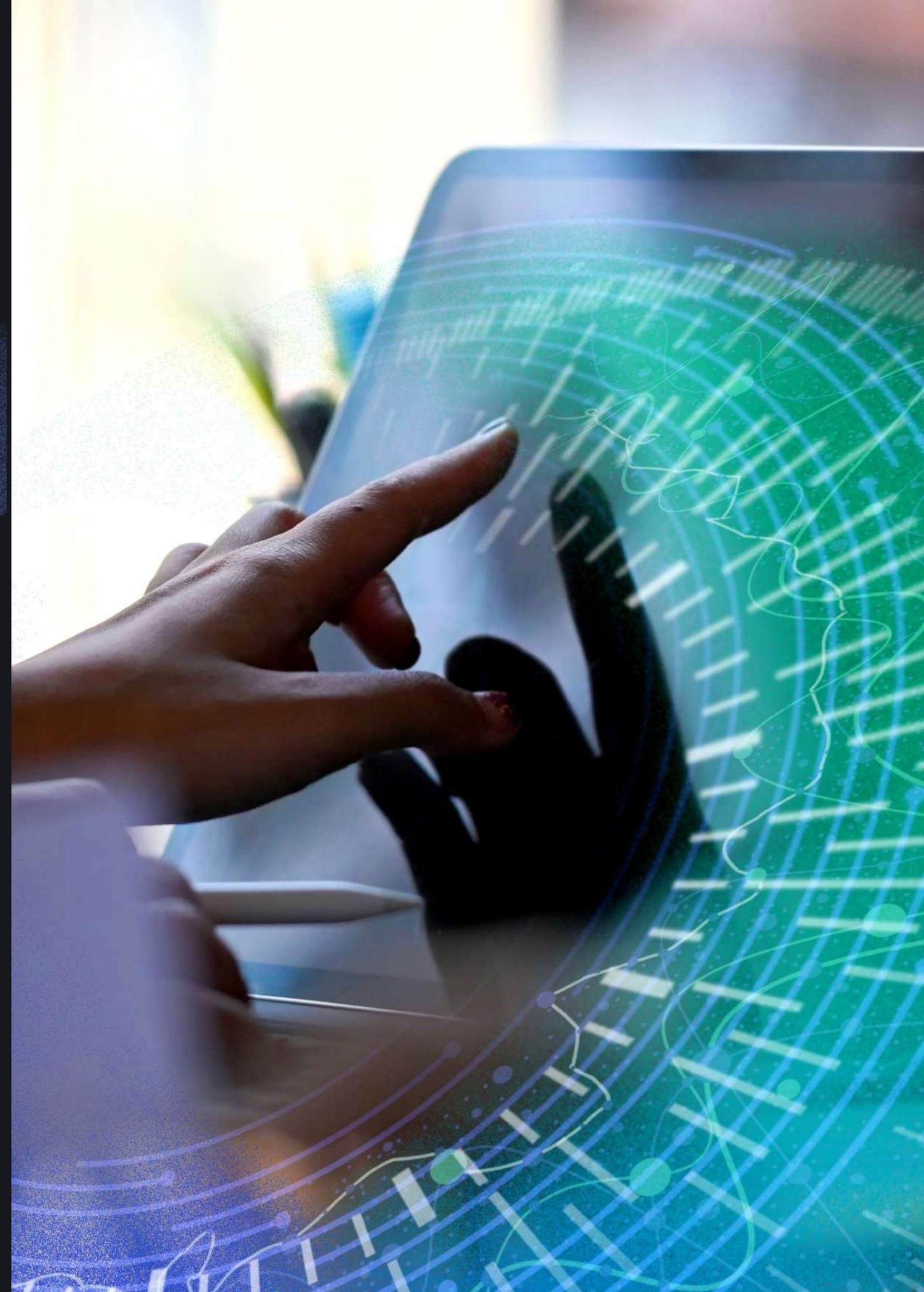
13

Digital Trust:
multiple brands

16

Beyond the
Pathway

18



INTRO TITLE

CURRENT LANDSCAPE

The Pathway to digital trust

Identification, authentication and fraud prevention: the foundations of the future of online transactions

The future of online businesses has never looked brighter.

Understanding and usage of e-commerce sites is growing like never before. Customers of every demographic are opting for the speed and convenience of e-commerce over physical channels; and digital subscription services are the first choice for most consumers.

But an increase in opportunity is shadowed by an increase in risk. And as e-commerce organizations mature digitally, they can find themselves increasingly at risk of bad actors. Card fraud, inventory attacks, and friendly fraud are just a few examples of the challenges that digital businesses have to face. Get it wrong and you risk reputational damage and, in the worst cases, lost customers.

As e-commerce organizations increase the pace of their

digital transformation, new opportunities will emerge – as will new threats.

Businesses that want to be successful need to adopt a new approach. By embracing nascent technologies, they will realize that there is no longer a need to trade user experience for security/fraud prevention. By building a personal digital relationship with each customer, organizations can provide the seamless digital experience users dream of, in the secure way businesses yearn for.

This e-book presents a maturity model which will help you to do just that: mitigate these mounting risks, without missing out on those opportunities, or compromising user experience or compliance.

Whichever level you're at, you'll discover how to build on what you have already achieved – and take the vital next steps.



How to use the Maturity Pathway

The competing pressures of customer experience, fraud prevention and compliance hold many challenges for e-commerce organizations when designing their identification strategy. But they also hold huge opportunities – such as the chance to build digital trust with consumers and gain long-term loyalty.

But the journey towards customer advocacy and outstanding customer experience can feel overwhelming, with tech capabilities to upgrade, cross-functional team cohesion to foster, and much more.

We've created the Maturity Pathway to give you a clear starting point and progression plan, along with guidance on the business attributes and tech capabilities you'll need to develop at each stage.

We refer to each stage on the pathway as a Milestone. If you're comfortable at your current Milestone, that's fine – as long as you have the right technology in place to support your business goals. For many businesses, however, there will be opportunities to advance and progress.

For example, you might have a reliance on guest checkout and digital wallets, but be looking to reduce fraud at the point of payment, or to build out customer engagement programs and tailor online experiences.

Perhaps your intelligent identification and authentication capabilities allow you to offer those personalized experiences, but you have disjointed journeys across brands.

If you're unsure of where you're at, look at the introductory sections of the Maturity Pathway Milestones and see if you recognize your business in any of the groups.



DIGITAL TRANSFORMATION

Your Maturity Pathway



BASIC WEBSTORE

LIMITED TO NO DIGITAL PRESENCE

..... FOCUS ON

Payments

..... ATTRIBUTES

Basic customer accounts

Reliance on guest checkouts

Limited potential to engage with customers

Lack of card-on-file capability

.... CHALLENGES & RISKS

Data breaches & credential stuffing attacks

Cart abandonment

Dispute resolution

OTP costs

Inventory attacks



MODERN WEBSTORE

LIMITED FRAUD DETECTION & PERSONALIZATION

..... FOCUS ON

Logins & Payments

..... ATTRIBUTES

Utilizing card-on-file and digital wallets

Ability to offer basic engagement program

High card abandonment at checkout

.... CHALLENGES & RISKS

Account Takeover (ATO)

Bot fraud

Card Not Present (CNP) fraud

Fake account creation

Friendly fraud (e.g. chargebacks)



DIGITAL LEADER: SINGLE BRAND

CUSTOMER-CENTRIC

..... FOCUS ON

End-to-end customer journeys

..... ATTRIBUTES

Genuine customer detection means personalized experiences

Customers recognized via passive authentication

Tailored incentive schemes

Lower cart abandonment at payment

Diversified payment options

.... CHALLENGES & RISKS

Promocode abuse

Loyalty point fraud



DIGITAL LEADER: MULTIPLE BRANDS

PORTABLE IDENTITY

..... FOCUS ON

Omnichannel customer journeys

..... ATTRIBUTES

Hyper-personalized customer journeys across all brands

Portable omnichannel digital IDs across brands and partners

Reduced cost of customer acquisition

Interconnected incentive schemes and offers

Strategic ability to create new revenue streams

M&A strategy benefits from cross-brand customer identification

.... CHALLENGES & RISKS

Promocode abuse

Loyalty point fraud

MODERNIZE ME

Basic Webstore



Organizations at this phase will at least have an online presence but for many, the ability to recognize returning customers will be limited.

The website and user journeys may be good, but user accounts will be very basic – guest checkouts or accounts with limited information stored, and options such as card-on-file absent.

That limits the ability for the merchant to provide personalized experiences – and in turn, to build loyalty and gain customer trust. Instead, it's the third-party payment wallets and payment systems that benefit from the customer's data. The cost of those lost insights and opportunities quickly adds up.

The chief aim for e-commerce organizations in this stage is to begin to establish ongoing digital relationships with customers. It's a certainty that at least a few of your competitors will be aiming to do so – and if you don't keep pace, it could leave you seriously behind the curve.

Customer Experience

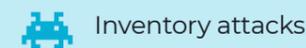
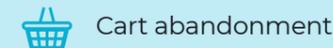
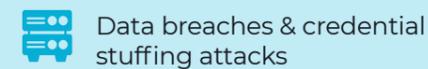
Customers expect highly personalized shopping experiences, not unnecessary friction. But with limited abilities to remember and welcome returning users, customers will be either forced to fill in payment details for every visit, or to use a third-party wallet vendor. Those are extra steps that can swiftly lead to abandoned carts.

That's an issue that goes beyond checkout – it complicates returns and limits the overall functionality of the web service.

FOCUS ON:



CHALLENGES & RISKS:



Fraud and Risk

A reliance on guest checkouts leaves you wide open to attacks from bad actors and friendly fraud. With no ability to identify and weed out bad actors up front, security is left until the end of the shopping process.

- Basic account security leaves businesses unable to distinguish between humans and bots – and as a result, vulnerable.
- In the case of fraudulent chargebacks, wallet vendors invariably side with the customer – to the business's detriment.

- Bots can clear out inventories in seconds, or tie them up with false abandoned transactions.

Compliance

For businesses at this stage of the Pathway, account authentication that's dependent solely on usernames and passwords brings the risk of accounts being easily compromised. This includes attacks such as credential stuffing via credentials that have been exposed in data breaches on other sites.

Cost

Unwelcome cost pressures can arise from out-of-band OTPs, which organizations routinely use to authenticate customers.

Then there are the downstream costs that are less immediately obvious. Acquiring new customers is always more costly than nurturing existing ones. Being unable to recognize returning users means that you can't take advantage of the rich data around their individual spending habits and preferences – leaving you less able to provide tailored offers and incentives.

RISKS AT MILESTONE 1

Callsign helps prevent:

THE PROBLEM:

- Data breaches & credential stuffing attacks
- Dispute resolution
- Inventory attacks

SOLVED BY:

- Behavioral biometrics
- Device fingerprinting
- Location analytics

- Cart abandonment
- OTP costs

- Passive authentication at checkout

User journey augmented by Callsign

1 Customer selects product and proceeds to checkout

2 As shopper enters payment details Callsign confirms that the user's device is free of malware, the user is in a low-risk location, they are not deliberately seeking to hide their identity, and they are not a bot

3 Purchase is complete without the need for an insecure and expensive SMS OTP

Which steps should you take?

Customer accounts need to be as secure and friction-free as possible. The benefits are clear:

- Reduce the risk of fraud at the point of transaction/checkout
- Reduce abandoned carts by storing payment and shipping details, making the shopping process faster

It's vital to put in place technologies that can detect and intercept payment fraud, and to be also able to prevent bots from doing damage – to you, your customers, and your reputation.

Callsign allows you to add passive layered intelligence during the payment process that can help you detect fraudulent activities. Our multi-layered authentication processes combine information sources such as device fingerprinting & location and behavioral biometrics (the way a user types, swipes or holds their device), to positively identify customers.

So, when a user attempts to interact with your service digitally, we ensure that your customers really are who they claim to be without adding any friction to the user journey.

With a greater understating of who your customer are, it also puts you in a better position to consider your move along the Pathway.

DIGITIZE ME

Modern Webstore



Businesses at this Milestone are better able to recognize returning users and offer them secure accounts that allow organizations to personalize customer journeys. This provides the basis for customer incentive programs. These allow valuable data to be collected around preferences and spending habits – data that's essential for building insights to create tailored offers.

Whilst many will be leveraging device checks to detect returning customers, at this stage, usernames and passwords are (still) the main or only method of identification and authentication. That's an outmoded approach to authentication, and one that doesn't provide protection against the challenges that businesses face at this level.

Compliance

Complex payment journeys lead to increases in cart abandonment; yet at this Milestone, user journeys are often still beset by friction. A user account has to offer some tangible benefit to the user, the most obvious of which is the ability to store a card on file to make for a smooth checkout.

Customers like to be welcomed back. Many websites recognize returning customers with persistent cookies, but a reliance on cookies alone is unsustainable. It's also important that any form of personalization considers data and privacy.

FOCUS ON:

Login & Payments

NEW CHALLENGES & RISKS:

Account Takeover (ATO)

Bot fraud

Card Not Present (CNP) fraud

Fake account creation

Friendly fraud (e.g. chargebacks)

Additionally, organizations at this stage may not be fully in a position deal with regulatory compliance such as SCA (Strong Customer Authentication) or 3DS exemptions – impacting customer experiences leading to cart abandonments.

Fraud and Risk

A reliance on passwords alone leaves you wide open to Account Takeover (ATO fraud). You should look to alternate solutions beyond passwords such as behavioral biometrics that are highly secure and reduce customer friction.

There's also still risks of fraud at the point of payment.

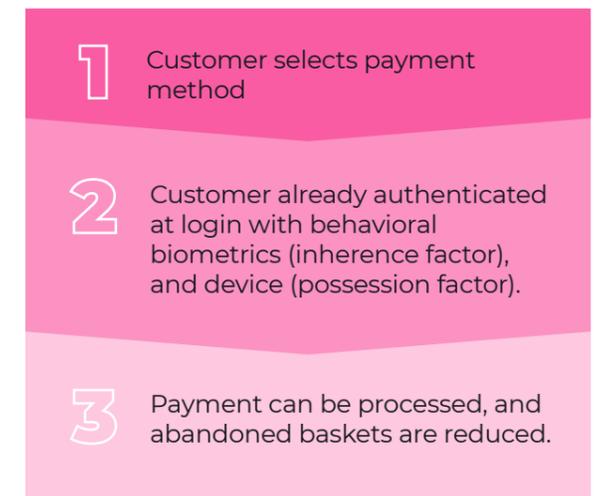
- Fraudulent chargebacks and Card Not Present (CNP) fraud will persist – but greater insights about customers will help you win more than you lose.
- You may also begin to see increases in friendly fraud with customers looking to get that additional 10% off or looking to share their accounts with one too many friends or family.
- Bots also pose a greater risk. Aside from credential stuffing to gain access to legitimate accounts, customers increasingly turning to sniper bots to snap up desirable items to sell on at a profit.

Compliance

Relying on a single authentication factor such as a username and password combination is precarious from a compliance standpoint, as you're at greater risk of stolen details being used to create accounts, or seeing existing accounts breached with data sold on the dark web – putting your reputation at risk.

It also leaves you in a position where you may struggle to deal with regulatory compliance such as SCA (Strong Customer

User journey augmented by Callsign



Authentication) or 3DS exemptions – impacting customer experiences and leading to cart abandonments.

Cost

The risks at this stage, both in terms of fraud and compliance, can result in some costly outcomes. Fraud is an expensive business for both you and your customers; but user journeys that expose the customer to undue friction – and risk – can swiftly lead to cart abandonment.

OTPs are still common at this stage, but with SMS scams on the rise and 45% of consumers losing trust in organizations that are named in scam messages they receive, it's not just the cost of SMS that's at stake – the reputational costs of using antiquated security methods need to be considered.

Which steps should you take?

It's clear that more is needed than the tried, tested, and compromised username and password approach. With layered intelligence, you can better prevent fraud at the point of payment but utilizing it to protect customer accounts can help to drive revenue – and you can begin to move away from relying on blacklists to more robust data signals from devices and other attributes.

This means looking beyond outdated and easily compromised cookies – which limit cross-browser authentication – to device

RISKS AT MILESTONE 2

Alongside the risks in the previous Milestone, Callsign helps prevent:

THE PROBLEM:

- Account Takeover
- Bot fraud
- Fake account creation

SOLVED BY:

- Behavioral biometrics
- Device fingerprinting
- Location analytics

- CNP fraud

- Credential input analysis

- Friendly fraud (e.g. chargebacks)

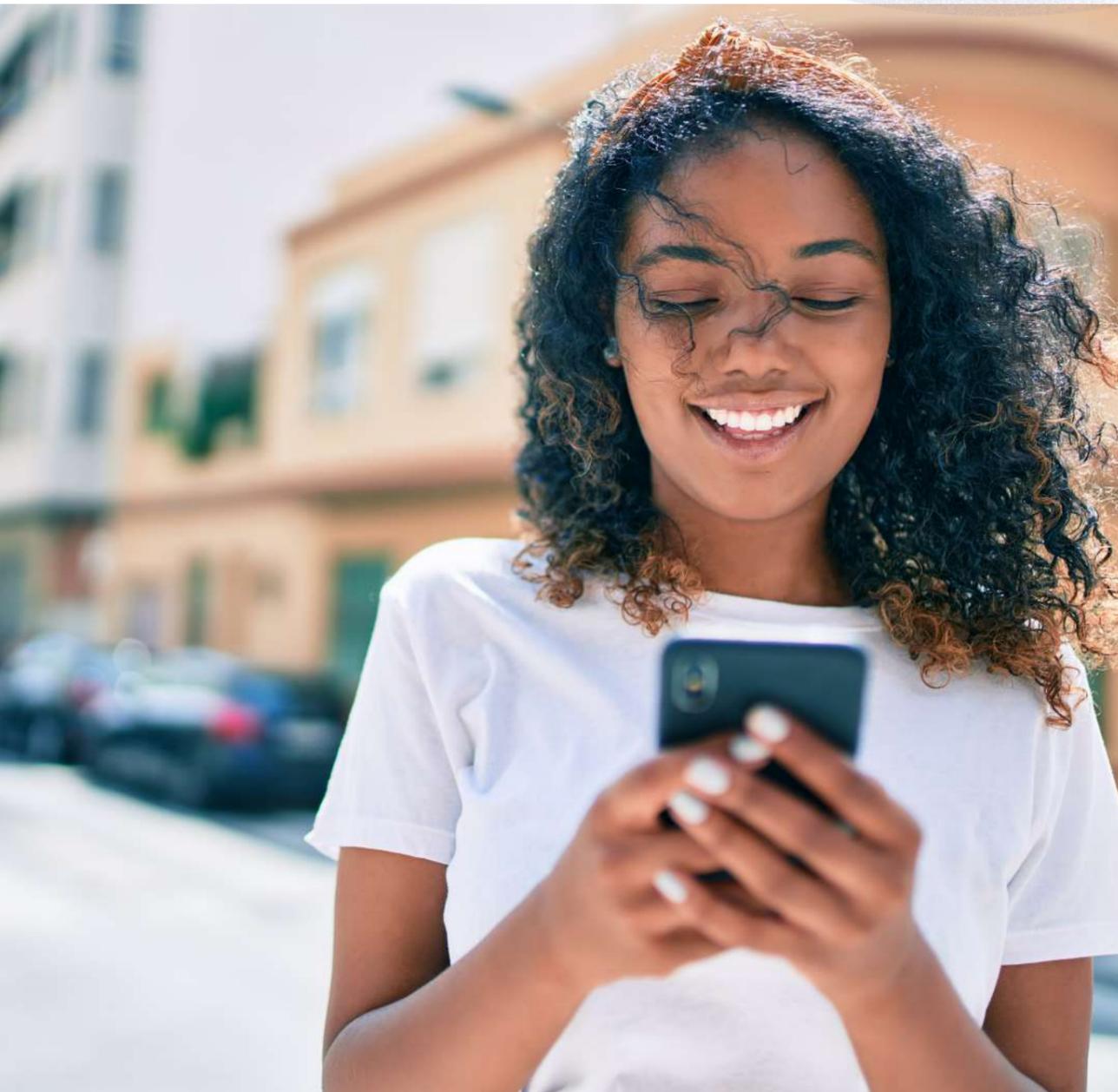
- Dispute resolution enabled on accounts

fingerprinting. Layering device fingerprinting with behavioral biometrics will allow you to recognize and welcome your returning customers, and with a card safely held on file, you'll increase conversion rates and reduce fraud at the point of payment.

With the ability to begin to tailor experiences and authenticate your customers, you're

on the path to crafting unique tailored journeys which in turn enable you gain that competitive edge.

All of which allows you to reach the top of your Milestone and paves the way for moving on to the next one.



CUSTOMER-CENTRIC

Digital trust: single brand

Increasingly secure and compliant, this stage of the Pathway is where an organization truly begins to become a leader in digital e-commerce experiences. Although the customer's journey is now highly evolved, there is still more value that can be gained from it.

The goal at this stage is to tailor and personalize the customer experiences – not just recognizing, but rewarding returning customers with offers and incentives that will resonate with them. That's a factor in eliminating the risk vs. reward conversation, with the risks of friendly fraud reduced and customers kept happy with tailored incentives from the outset.

Customer Experience

Organizations at this Milestone are seeing the positive impact of tools such as AI and Machine Learning, and are able to positively identify customers from the moment they interact – regardless of their device or location – and repay return business through offers and incentives. Furthermore, this recognition lets them understand how those customers shop, and proactively sculpt their interactions accordingly.

With this comes significant brand reputation improvements, as customers genuinely value the brand, committing to them as a result of quick and easy journeys; in other words, returning due to a compelling user experience rather than seeing them as a 'utility' to move on from at will.



FOCUS ON:

 End-to-end customer journeys

NEW CHALLENGES & RISKS:

 Loyalty point fraud

 Promocode abuse

Fraud and Risk

Combatting fraud at this stage requires stepping beyond just detecting fraudulent transactions to positively identifying customers. That may seem like a subtle shift but without that move, it's hard for an organization to offer secure and hyper-personalized experiences.

- Friendly fraud will be an increased risk at this stage, with customers abusing the very incentive schemes designed to reward them. A greater understanding of your customers and how they interact with your business will help you reduce the risks associated with friendly fraud – for example, proactively offering incentives rather than waiting for customers to leave – which reduces call center costs.
- Loyalty points are just as valuable to fraudsters who can sell them on via the

dark web. It's key, from both a cost and reputational standpoint, that organizations at this Milestone protect loyalty schemes with more than just a simple password.

Compliance

At this Milestone you will find yourself increasingly reliant on data to shape and tailor the experiences of your customers, and the more data you collect, the more stringent your protection mechanisms have to be.

This level of data can often make you more of a target to fraudsters looking to gain access to customers' accounts, whether that's for their data or loyalty points. It's important that you ensure you're protecting your customers' data in a privacy-preserving and compliant way, or you run the risk of reputational damage and costly fines.

Cost

At this stage, fraud solutions move away from being a cost center to a ROI reputation maker, with the wider business able to benefit from these technologies to identify genuine users

RISKS AT MILESTONE 3	
Alongside the risks in the previous Milestones, Callsign helps prevent:	
THE PROBLEM:	SOLVED BY:
<ul style="list-style-type: none"> Loyalty point fraud Promocode abuse 	<ul style="list-style-type: none"> Behavioral biometrics Device fingerprinting Location analytics
<ul style="list-style-type: none"> Friendly fraud 	<ul style="list-style-type: none"> Dispute resolution enabled on accounts

User journey augmented by Callsign

- 1 User navigates to webstore, and, based upon passive intelligence, is instantly recognized, without the need to enter any passwords or other credentials
- 2 At payment, Callsign is PCI DSS and GDPR compliant, so payment and personal details are already stored

and offer truly hyper-personalized experiences – something that becomes increasingly pertinent as a business expands its portfolio to encompass multiple divisions and brands.

Which steps should you take?

This is the point where it's important to treat every individual as just that: an individual. Hyper-personalization will let you shape the user journeys, loyalty rewards and product offerings for each customer – and in doing so, improve conversion rates.

By adopting a Start More Certain approach, customers are identified long before they've reached checkout, with the information about their preferences and habits building out a user profile that goes far beyond just ID, with the customer's journey getting more secure every time they log into their account.

Passively identifying a regular customer on a verified device and location will allow you to move them through the security measures quickly and unobtrusively; extra checks for new customers or existing customers in new circumstances can be dynamically called into play where needed.

Callsign can help you put in place the technology that makes this degree of personalization possible. Feeding layered intelligence signals into our Orchestration

Layer will allow you to seamlessly identify users in whichever channel they are using (physical, phone, mobile, or web).

We'll also help you reduce costs. Our multi-tenant Orchestration Layer joins your central systems up, eliminating duplication of functions and processes. This also offers the opportunity to build digital IDs that can be used with any system or

process the business deems necessary – driving customer experience and allowing organizations to benefit from truly integrated partnerships.

For businesses with this as their goal, they have the ability to progress to an extra step in the Maturity Pathway.



PORTABLE IDENTITY

Digital trust: multiple brands



Businesses at this stage will have expanded into omnichannel operations, and will be enjoying successes from a number of sub-brands or divisions. Maintaining those successes and building that digital trust hinges upon unifying customer experiences across those brands and channels.

Here, businesses can benefit from creating portable IDs, which provide opportunities to leverage ID across their entire organization, or their strategic partners, to offer seamless cross-brand user journeys that instill long-term digital trust in their customers.

There are many factors that influence that trust. Fluid, intuitive customer journeys are a given at this stage; it's the very least that a customer expects from a business at this level. And it's not enough for them to just be highly secure – customers need to feel that reassurance at every step.

They also expect to be able to buy and access the products and services that they want, when they want, without having to jump between logins.

The margin for error is very thin at this stage – with your organization's reputation hanging in the balance.

FOCUS ON:

- Omnichannel customer journeys

NEW CHALLENGES & RISKS:

- Promocode abuse
- Loyalty point fraud

Customer Experience

There are a multitude of benefits to be found at this stage – not least of these is the ease of which offers and incentives can be tailored across brands and business units. By recognizing returning users across multiple sites, their loyalty can be rewarded, and they can be presented with relevant and timely offers without having to re-authenticate or log back in.

In other words, the perfect customer experience: and in fact, nothing less is acceptable. Whether that's provided via a web portal or an app, it needs to be intuitive, easy to use and consistent, with the reassurance that secure authentication technologies are firmly in place.

This will be pivotal in creating long-term trust and loyalty from happy, protected customers.

Fraud and Risk

At this stage, many organizations will have the same risks as those at Milestone three. But cross-brand journeys are even more dependent on solid authentication mechanisms; without them, portable identity can't happen. And these mechanisms need to be present in every aspect of the customer's interactions, whether with the organization or wherever their ID is used.

A large and successful organization presents an alluring target for bad actors, and they'll deploy every sophisticated method at their disposal to ply their malicious trade. Equally, friendly fraud becomes more of a risk at this level, with the added complication of any weaknesses in loyalty schemes being targeted.

At this stage it's vital that you ensure that customer data not only remains secure, but that you have 360° visibility of the customer across all of your brands.

Compliance

Having a single source of truth allows you to do just that and avoid record duplication that could lead to costly issues with regulations such as GDPR, CASL and CCPA.

And of course for the customer, the consent journey is all the more important. It needs to allow customers to authenticate and authorize which information can be shared, and to opt in or out whenever they wish.

What are the next steps?

Vigilance is the watchword. Innovation never ceases; nor does competition. New products and services are constantly emerging, along with new challenger brands. But equally, the tactics of the bad actors and fraudsters are also evolving.

It's important to constantly evaluate and re-evaluate where an organization is on the current landscape, where it's going – and what steps it needs to stay secure.

As an organization expands across brands and channels, orchestration becomes vitally important to ensure that fraud signals are shared amongst business units. Callsign's Orchestration Layer allows us to build a secure pipeline between your organizations and brands, and those you'll be sharing information with.

Our comprehensive solutions provide assurance at every stage of the creation of a portable identity. But what makes us truly unique in this space is that we can provide a solution no matter what other technologies you're using and whatever legacy systems or bespoke architectures you have in place, Callsign's technology ensures that ID and authentication is secure and smooth at every step.

RISKS AT MILESTONE 4	
Alongside the risks in the previous Milestones, Callsign helps prevent:	
THE PROBLEM:	SOLVED BY:
<ul style="list-style-type: none"> Loyalty point fraud Promocode abuse 	<ul style="list-style-type: none"> Behavioral biometrics Device fingerprinting Location analytics
<ul style="list-style-type: none"> Friendly fraud 	<ul style="list-style-type: none"> Dispute resolution enabled on accounts

LOOKING FORWARD

Beyond the Pathway

Wherever an organization currently finds itself on the Pathway, there is the opportunity to move further along.

Whether that's reaching the limit of your current Milestone, or moving to the next, it's imperative that momentum is maintained. Customer behaviors and tastes are constantly evolving and changing – along with the techniques of bad actors and criminals.

A mature identity strategy gives you smarter ways to authenticate, stronger decisioning, and a single view of the customer, not to mention a seamless and secure experience for them. But it also has the potential to become a strategic driver for a wide range of other business benefits.

Putting customer ID at the center of customer strategy will involve a positive and future-focused mindset change, which will ripple out across all areas of the business and embed itself in even seemingly unrelated business priorities.

Lastly, and perhaps most crucially, the digital trust created when businesses complete the Pathway will open up

significant and lasting opportunities – from boosting brand reputation and customer loyalty, to using ID data to drive value.

Depending on where you are on your journey, some or all of these tasks might seem complex. But you don't have to do it alone.

Callsign is here to partner with businesses to help them choose and implement the right technology for where they are and where they want to go. We want to get to know your business, forming a strategic and collaborative partnership and working together to find the best journey for you through the Maturity Pathway.

To get that started, please get in touch with a Callsign specialist today, and place your business on the path to digital trust.

How does Callsign work?

Callsign has a simple vision: we want to make digital identification simple and secure, every time, and across any transaction – and our unique layered approach helps businesses do just that.

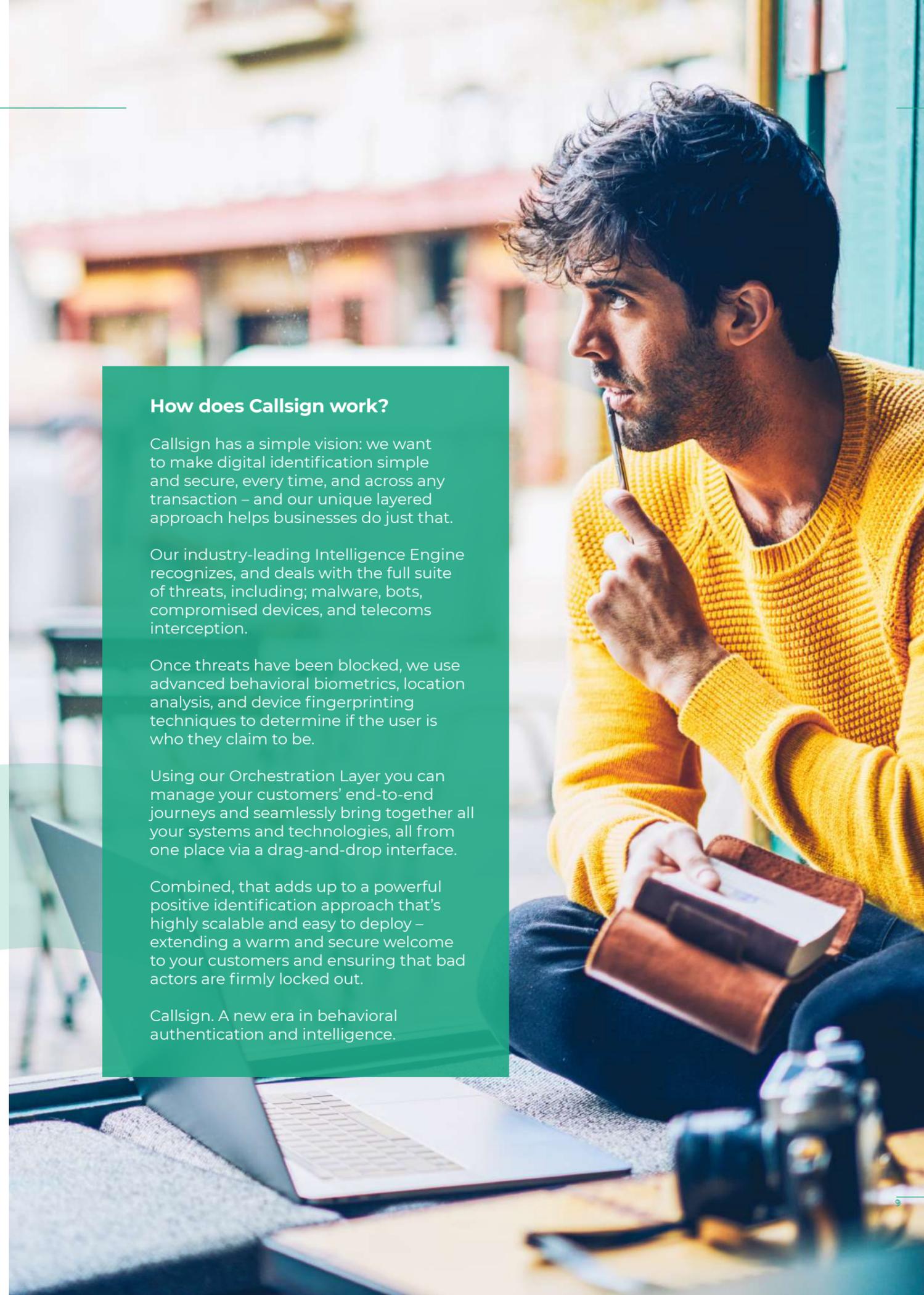
Our industry-leading Intelligence Engine recognizes, and deals with the full suite of threats, including; malware, bots, compromised devices, and telecoms interception.

Once threats have been blocked, we use advanced behavioral biometrics, location analysis, and device fingerprinting techniques to determine if the user is who they claim to be.

Using our Orchestration Layer you can manage your customers' end-to-end journeys and seamlessly bring together all your systems and technologies, all from one place via a drag-and-drop interface.

Combined, that adds up to a powerful positive identification approach that's highly scalable and easy to deploy – extending a warm and secure welcome to your customers and ensuring that bad actors are firmly locked out.

Callsign. A new era in behavioral authentication and intelligence.





callsign[®]

Balancing security, UX & privacy is easier than you think.
Find out how we can help you on your journey to
digital leadership - callsign.com.

Get in touch for a demo of our
capabilities: sales@callsign.com

© 2021 Callsign Inc. All rights reserved.