EXPECTATION VS. REALITY AT THE LOG INN:

How to create the identity experience your customers want

With insights from more than 17,000 global IT/marketing decision makers and consumers

auth0

EXPECTATION VS. REALITY AT THE LOG INN

Regardless of your organization's location, industry, or size, there's one commodity that has become synonymous with success when it comes to Customer Identity and Access Management (CIAM): incredible customer experience (CX) backed by bulletproof security.

We're not talking about vanity UX projects that are used to gloss over technical problems at the login: we're talking about seamless, secure, modern identity experiences that act as a portal to profitability.

Why? Because it's what your customers expect from organizations today. Whether you're a digital-first business or you are looking to master omnichannel services, your customers will be anticipating a simple, effortless login experience. Not only that, but they will be expecting the highest level of security. But this isn't always their reality.

Often, customers are spooked by archaic, long-forgotten logins. Logins that require repetitive password resets, endless security questions, and a call to the help desk. Left frustrated, these customers are lost – never to return, never to recommend.

IT'S TIME TO TAKE BACK CONTROL

First impressions are critical: they build credibility and set expectations for users. With logins often being the first interaction your user has with your organization, it's imperative that this experience is as seamless and secure as possible.

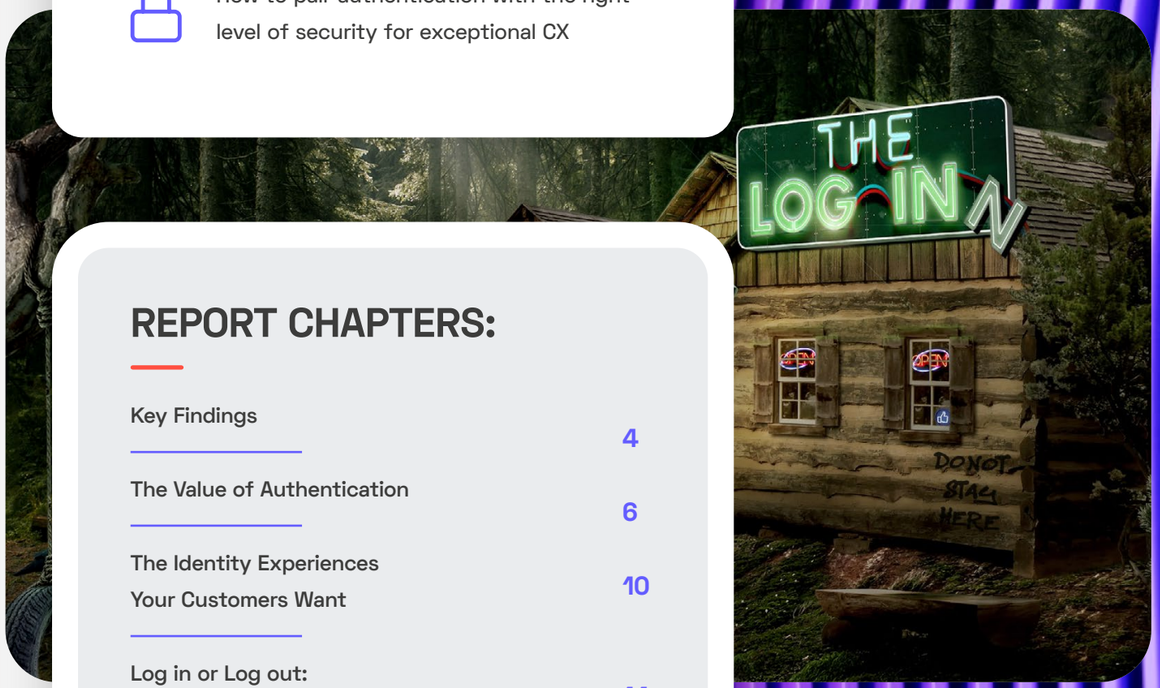
This is why poor identity management can no longer be overlooked by organizations in favor of other digital transformation initiatives. Your login is an incredibly valuable asset. It's up to you how you utilize it for success.

To help you create the identity experiences that customers want, this report shows you how to transform your login and unlock new business opportunities from modern identity management strategies – without compromising on security. Plus, with exclusive insight from more than 17,000 global IT/marketing decision makers and consumers, you'll have front row seats as we reveal the tactics your peers and competitors are utilizing to deliver exceptional identity experiences.

auth0

THIS REPORT EXPLORES:

- How businesses are not meeting their customers' expectations and demands through their current CIAM strategies
- How consumers are currently using logins, and what they expect from future identity experiences
- Why Customer Identity and Access Management (CIAM) technologies and processes minimize consumer frustrations
- How to pair authentication with the right level of security for exceptional CX



REPORT CHAPTERS:

KEY FINDINGS

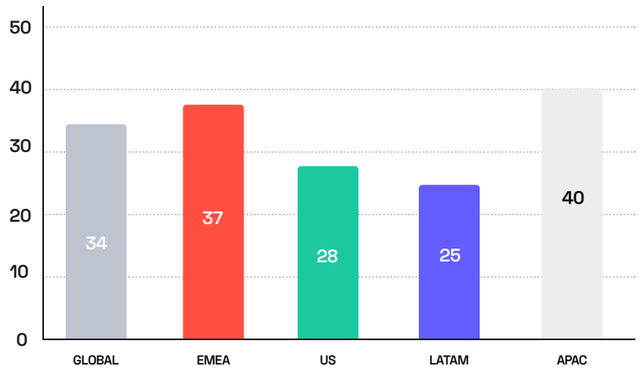
MFA AND SSO

THE LOGIN EXPERIENCES CONSUMERS WANT MOST

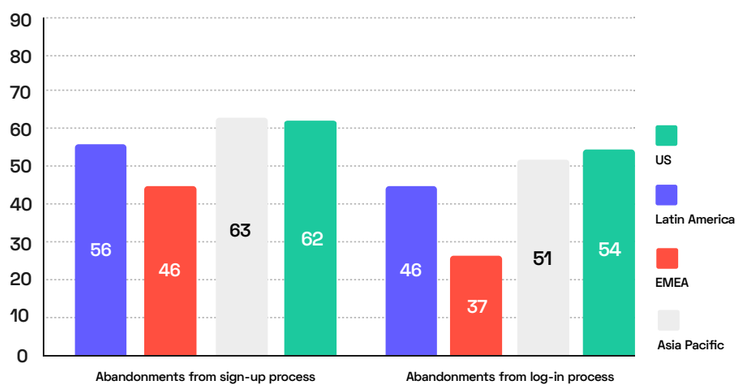
US organizations are ahead of those in APAC, EMEA, and LATAM in offering biometric logins, and ahead of EMEA and LATAM in offering MFA.

> 86% of consumers admit to reusing passwords

% OF CONSUMERS WHO FIND IT DIFFICULT TO IDENTIFY APPS/ SERVICES THAT WILL KEEP THEIR PERSONAL INFORMATION SAFE

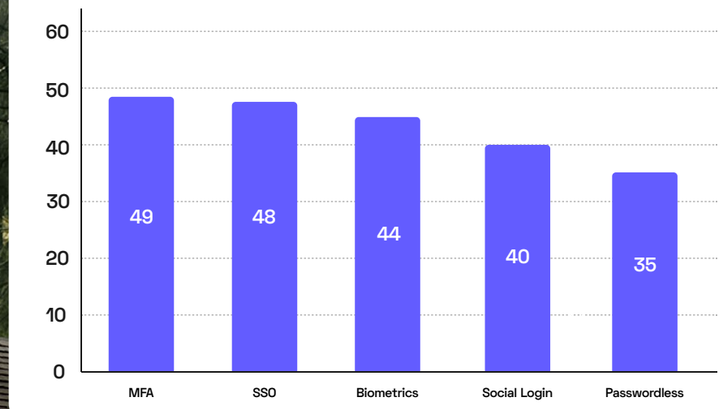


% OF DECISION MAKERS WHO ATTRIBUTE CART OR SIGN-UP ABANDONMENT TO SIGN-UP OR LOGIN PROCESSES

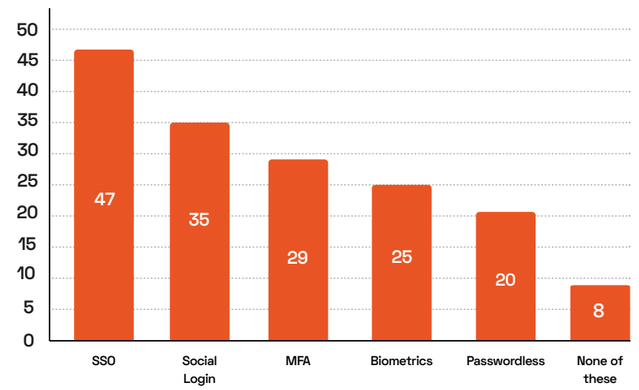


auth0

% OF CUSTOMERS WHO ARE MORE LIKELY TO SIGN UP TO AN APP OR ONLINE SERVICE IF IT OFFERS THESE LOGIN TECHNOLOGIES

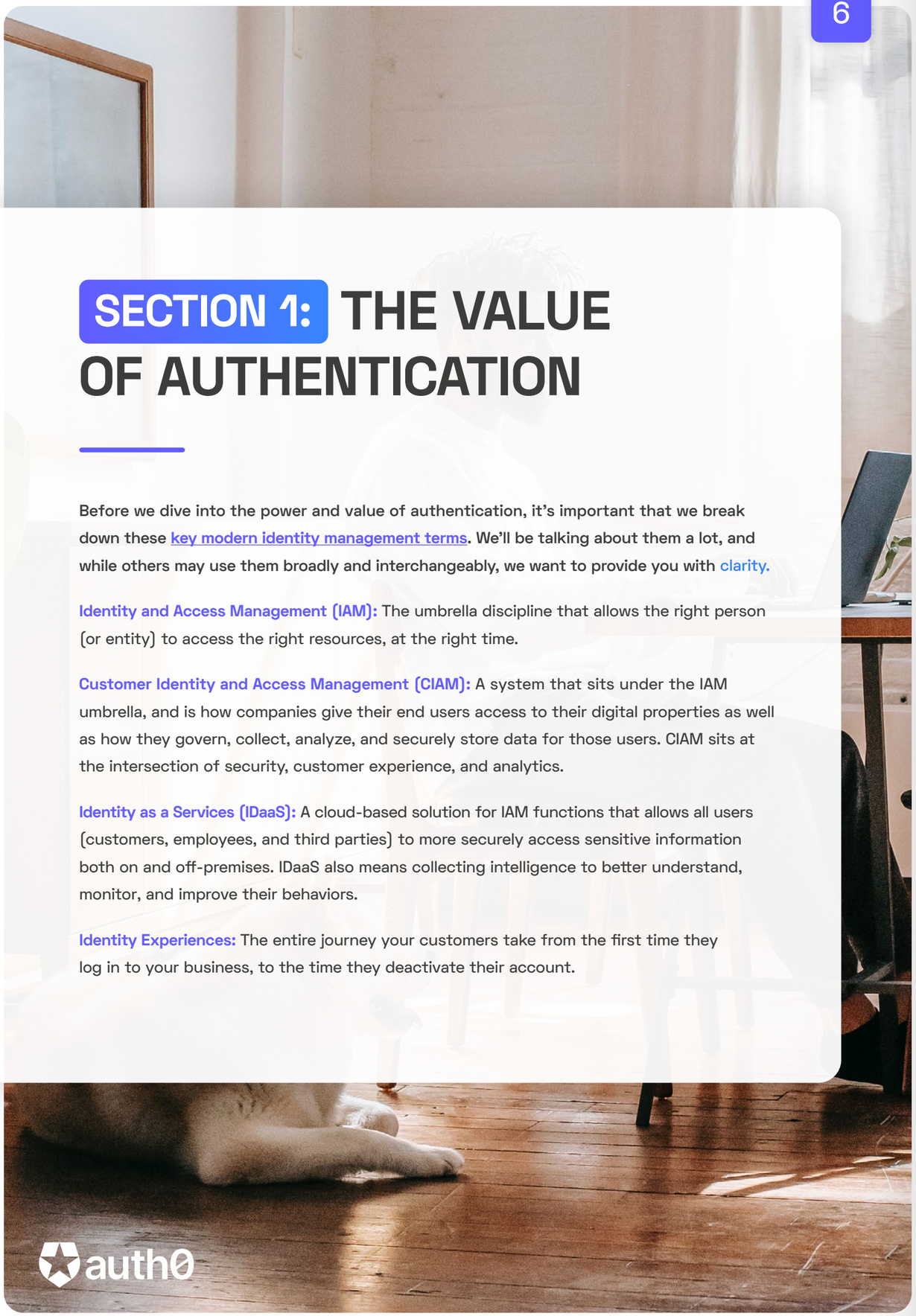


% OF ORGANIZATIONS WHO OFFER THESE LOGIN TECHNOLOGIES



> **87%** of developers see productivity improve when they are able to use the SaaS components they want and need.

> **58%** of development teams expect to add new third-party SaaS components to their application strategy over the next year.



SECTION 1: THE VALUE OF AUTHENTICATION

Before we dive into the power and value of authentication, it's important that we break down these key modern identity management terms. We'll be talking about them a lot, and while others may use them broadly and interchangeably, we want to provide you with clarity.

Identity and Access Management (IAM): The umbrella discipline that allows the right person (or entity) to access the right resources, at the right time.

Customer Identity and Access Management (CIAM): A system that sits under the IAM umbrella, and is how companies give their end users access to their digital properties as well as how they govern, collect, analyze, and securely store data for those users. CIAM sits at the intersection of security, customer experience, and analytics.

Identity as a Services (IDaaS): A cloud-based solution for IAM functions that allows all users (customers, employees, and third parties) to more securely access sensitive information both on and off-premises. IDaaS also means collecting intelligence to better understand, monitor, and improve their behaviors.

Identity Experiences: The entire journey your customers take from the first time they log in to your business, to the time they deactivate their account.

TODAY'S AUTHENTICATION LANDSCAPE

> "Identity has become more important since COVID has made physical boundaries irrelevant[1]."
>
> - ANDRAS CSER, VP, PRINCIPAL ANALYST WITH FORRESTER RESEARCH

In the past, consumer authentication has been overlooked by busy IT leaders: viewed purely as a necessary security function, or as a way to solely manage customer information. Then came the CX juggernauts: brands like Netflix, Amazon, Uber, and Apple who transformed the way we use, engage with, and choose digital authentication experiences.

These rivalries forced brands to compete on the way consumers created and utilized their digital identities. Logins went from being a functional necessity to an opportunity to drive engagement and strengthen brand loyalty.

Then, the global pandemic hit, accelerating the use of digital services across every demographic – changing the authentication market forever.

Faced with these fluctuating pressures and responsibilities, businesses are now leveraging their IAM strategies and CIAM solutions to:

1 MEET EVER-CHANGING CONSUMER BEHAVIORS AND DEMANDS

As we've seen, the way we use digital services can shift overnight – particularly for sectors like banking, healthcare, and e-commerce. CIAM has helped many brands meet the demand for more personalized, streamlined offerings.

[1] https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

2 KEEP UP WITH COMPETITORS AND INNOVATORS

Whether you're B2B, B2C, or B2E, individuals expect the same flawless experience from your business's login as they receive from their phone, their apps, even their streaming services. Your rivals aren't just competitor brands – they're any brand with a digital offering.

3 PROTECT CUSTOMERS (AND EMPLOYEES) FROM CYBER THREATS AND DATA BREACHES

For any organization, data is a highly valuable asset - especially when it's used for things like personalization and customized recommendations. As good data stewards and to prevent non-compliance penalties (and a PR nightmare), your organization has a duty to ensure your customer data and identity are protected from threats like ransomware and data breaches – from the moment users log in, to the moment they delete their account.

> "92% of consumers expect businesses to keep their personal information safe."

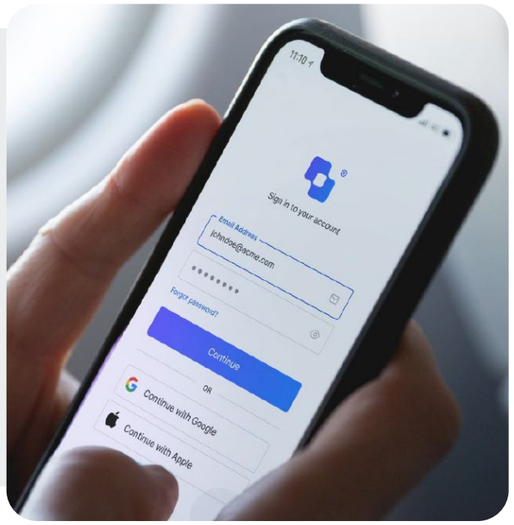
4 IMPROVE OPERATIONAL EFFICIENCY

Data silos, Frankenstein architectures, slow systems, and poor visibility are just some of the challenges IT and operational teams battle on a daily basis. When it comes to developing new services and streamlining processes, it's vital your IAM strategy is robust enough to improve the productivity and efficiency of your workforce.

5 BUILD RECURRING REVENUE

Businesses are looking for ways to open new revenue streams by monetizing customer data: leveraging it to design new loyalty programs, target specific groups like super-users or dormant accounts, and create personalized offerings.

By establishing flexible, responsive authentication solutions, leading organizations have been able to navigate these fluctuating changes and respond to consumer demand through seamless CX. But not all businesses have been able to decipher what their customers want from their identity experience.



SECTION 2: THE IDENTITY EXPERIENCES YOUR CUSTOMERS WANT

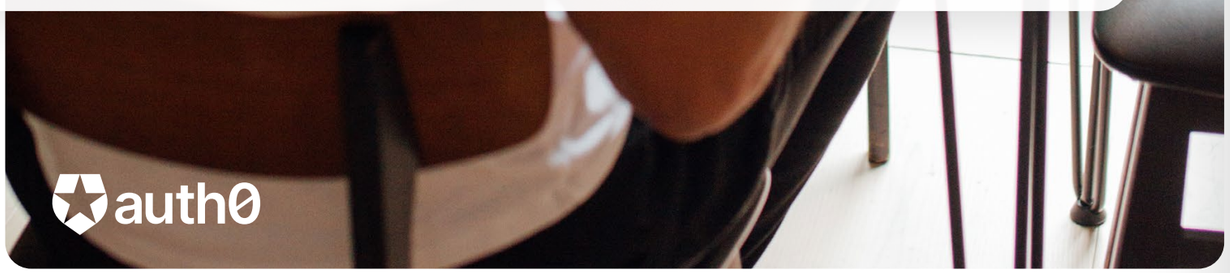
> **The login experience consumers want most is MFA, followed closely by SSO.**

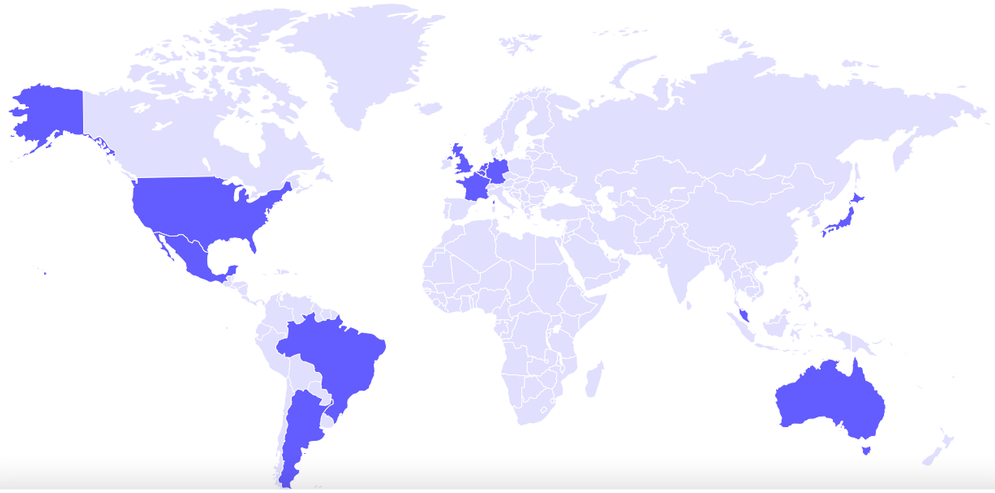
As an IT leader, how confidently can you answer these three questions?

1. ***"How are your customers currently using your login solutions?"***
2. ***"What are their preferred methods for authentication?"***
3. ***"Are you prepared to give them what they want?"***

Luckily for you, we surveyed more than **14,700 global consumers** to help you understand what authentication experiences they really crave. That way, you can learn how to tailor your strategies and invest in the right solutions that'll give you the flexibility and control you need and the experiences they want.

Let's get started.





MULTI-FACTOR AUTHENTICATION (MFA)

A method of verification that requires the user to provide more than one piece of identification – often signing in with a password and a one-time code or confirmation on your phone.

DID YOU KNOW?

MFA, WITH ONE-TIME CODES AND SMS VERIFICATION, CAN BLOCK 99.9% OF ACCOUNT HACKING ATTACKS[2].

How often is it used by consumers?

- **34%** - All the Time /Frequently
- **36%** - Sometimes
- **14%** - Hardly Ever
- **16%** - Never

Expected to grow **16.2%** on average annually through 2026[2], MFA is one of the most commonly used authentication solutions by consumers. In Singapore, it's even more popular, with **52%** of consumers reporting using it frequently/all the time, closely followed by **42%** of Americans. Dutch IT/marketing leaders decision makers surveyed are more likely their French, German and Belgian counterparts to say their companies currently offer customers the ability to log in with Multi-factor Authentication **(NL 37% compared to FR 20%, DE 27%, and BE 24%).**

[2] https://www.globenewswire.com/news-release/2021/05/03/2221402/0/en/The-global-MFA-market-size-is-projected-to-grow-from-USD-11-1-billion-in-2021-to-USD-23-5-billion-by-2026-at-a-Compound-Annual-Growth-Rate-CAGR-of-16-2.html

BIOMETRICS

A cybersecurity process that verifies a user's identity using their unique biological characteristics, such as fingerprints, voice, or face, as their password.

DID YOU KNOW?

UK BUSINESSES ARE FALLING ESPECIALLY SHORT WHEN IT COMES TO BIOMETRICS – ONLY 14% OFFER IT.

How often is it used by consumers?

- 31% - All the Time /Frequently
- 17% - Sometimes
- 12% - Hardly Ever
- 39% - Never

While it may take some consumers a little more time to get used to the idea of biometrics, it's definitely an area to watch. 44% of consumers admit they are more likely to sign up to an app/online service if a company offers biometric authentication.

SOCIAL LOGINS

An option for users to sign in to an app or webpage via their social media credentials such as Facebook, Twitter, Apple, or Google.

DID YOU KNOW?

CONVERSION RATES CAN INCREASE ANYWHERE FROM 20-40% AFTER SOCIAL LOGIN IMPLEMENTATION[3].

How often is it used by consumers?

- 24% - All the Time /Frequently
- 29% - Sometimes
- 16% - Hardly Ever
- 20% - Never

Social logins are growing in popularity with consumers. Brazilian (52%), Argentinian (50%), Mexican (47%), and Singaporean (41%) consumers are more likely to use social logins either all the time or frequently compared to those in Japan (22%), the UK (28%), and Germany (21%). Interestingly, Latin American consumers are more likely to sign up to an app/online service if they are able to use social logins compared to consumers in all other markets (LATAM 61% compared to APAC 42%, EMEA 31%, and US 38%).

[3] https://www.globenewswire.com/news-release/2021/05/03/2221402/0/en/The-global-MFA-market-size-is-projected-to-grow-from-USD-11-1-billion-in-2021-to-USD-23-5-billion-by-2026-at-a-Compound-Annual-Growth-Rate-CAGR-of-16-2.html

SINGLE SIGN-ON (SSO)

A single ID and password consumers can use for multiple related services.

DID YOU KNOW?

48% OF CONSUMERS ARE LIKELY TO SIGN UP TO AN APP OR SERVICE IF THEY CAN USE SSO. THIS NUMBER RISES FOR ARGENTINIAN (63%), MEXICAN (62%), BRAZILIAN (59%), AUSTRALIAN (59%), AND SINGAPOREAN (56%) CONSUMERS.

How often is it used by consumers?

- 31% - All the Time /Frequently
- 29% - Sometimes
- 16% - Hardly Ever
- 24% - Never

One of the reasons for SSO's popularity is that it helps to eliminate the need for multiple passwords or resetting information. In fact, Latin American consumers are more likely to sign up to an app/online service if they are able to use SSO compared to their global counterparts (LATAM 61% compared to APAC 52%, EMEA 41%, and US 47%).

PASSWORDLESS AUTHENTICATION

No need for a password – users are sent a one-time link or code to enter, or can verify their identity using a biometric trait, like a face or fingerprint.

DID YOU KNOW?

86% OF CONSUMERS ADMIT TO REUSING PASSWORDS FOR MORE THAN ONE ACCOUNT WHEN USING ONLINE SERVICES.

How often is it used by consumers?

- 15% - All the Time /Frequently
- 26% - Sometimes
- 25% - Hardly Ever
- 34% - Never

Similarly to biometrics, passwordless is one of the newest forms of authentication, which helps to explain its slower adoption. That being said, 26% of US consumers reported using passwordless either all the time or frequently. LATAM (43%), US (42%), and APAC (40%) consumers are more likely than their EMEA counterparts (29%) to sign up to an app/online service if they are able to use passwordless services.

For those organizations looking to stay one step ahead of their competition, this technology could be a revolutionary investment.

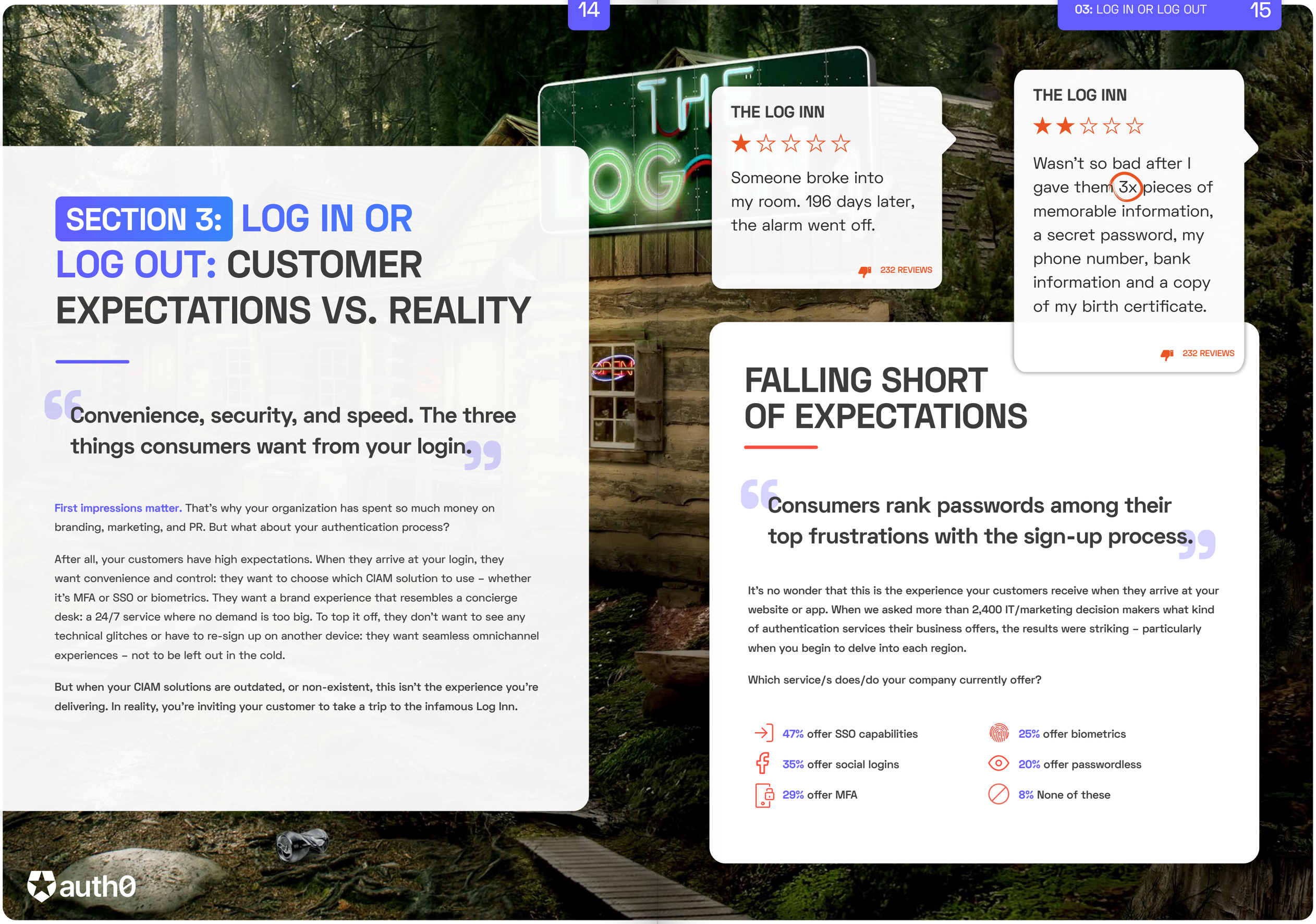
SECTION 3: LOG IN OR LOG OUT: CUSTOMER EXPECTATIONS VS. REALITY

> Convenience, security, and speed. The three things consumers want from your login.

First impressions matter. That's why your organization has spent so much money on branding, marketing, and PR. But what about your authentication process?

After all, your customers have high expectations. When they arrive at your login, they want convenience and control: they want to choose which CIAM solution to use – whether it's MFA or SSO or biometrics. They want a brand experience that resembles a concierge desk: a 24/7 service where no demand is too big. To top it off, they don't want to see any technical glitches or have to re-sign up on another device: they want seamless omnichannel experiences – not to be left out in the cold.

But when your CIAM solutions are outdated, or non-existent, this isn't the experience you're delivering. In reality, you're inviting your customer to take a trip to the infamous Log Inn.



FALLING SHORT OF EXPECTATIONS

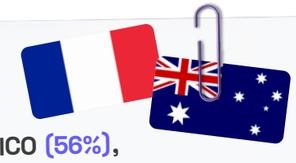
> Consumers rank passwords among their top frustrations with the sign-up process.

It's no wonder that this is the experience your customers receive when they arrive at your website or app. When we asked more than 2,400 IT/marketing decision makers what kind of authentication services their business offers, the results were striking – particularly when you begin to delve into each region.

Which service/s does/do your company currently offer?

- **47%** offer SSO capabilities
- **35%** offer social logins
- **29%** offer MFA
- **25%** offer biometrics
- **20%** offer passwordless
- **8%** None of these

ALL ABOARD SSO



ARGENTINA (59%), MEXICO (56%), AUSTRALIA (53%), AND FRANCE (53%) LEAD THE WAY WITH OFFERING SSO TO THEIR CUSTOMERS.

The numbers don't lie. One in ten companies surveyed that offer online services to customers, don't offer any of these login options. British (21%), together with Japanese (19%) organizations, are much more likely than those in all other countries surveyed to say that they don't offer any of these online login services to their customers.

These striking statistics reveal that organizations just aren't meeting their consumers' demands when it comes to the latest login technology. And it shows. Consumers are fed up, particularly with passwords.

SPEED UP SOCIAL LOGIN

UK IS THE SLOWEST ADOPTER OF SOCIAL LOGINS. ONLY 19% OF BUSINESSES OFFER IT COMPARED TO 35% OF US ORGANIZATIONS.

> **Consumers in Asia-Pacific and Latin America are more likely than those in EMEA and the US to find having to fill in long login or sign-up forms frustrating (APAC 55% and LATAM 51% compared to EMEA 46% and the US 36%).**

TOP CUSTOMER FRUSTRATIONS

1. Having to fill in long login or sign-up forms — 48%
2. Creating a password that has to meet certain requirements (e.g. number of digits, symbols) — 47%
3. Entering private information (e.g. passport number, tax file number) — 46%
4. Having to create a new ID/password for every app or online service — 43%
5. Verifying my account via a One-Time Password sent to my phone/email — 23%
6. None/don't know or not applicable — 14%

auth0

Another top consideration for consumers today is being able to identify apps/online services that will keep their personal information safe. Japanese (50%), together with German (48%) consumers, are more likely than consumers in all other markets surveyed to say they find it difficult to identify apps/online services that will keep their personal information safe. Overall, less than three in ten (28%) find it easy to identify these kinds of secure apps/online services.

LOST CONVERSIONS = LOST REVENUE

> **E-commerce stores lose $18bn in sales per year from cart abandonment alone[4].**

Bad customer experiences like those at The Log Inn cost businesses more than their reputation. **83% of consumers HAVE abandoned their cart or sign-up attempt** because the login process was too arduous (this rises to the highest levels in SG (89%), BR (87%), AU (86%), FR (86%), US (86%), UK (85%), and MX (85%)). IT/marketing decision makers in Latin America are more likely than those in EMEA to attribute these abandonments to both sign-up processes (LATAM 56% vs EMEA 46%) and login-processes (LATAM 46% vs EMEA 37%). They are, however, less likely than those in Asia-Pacific to attribute these abandonments to sign-up processes (LATAM 56% vs APAC 63%).

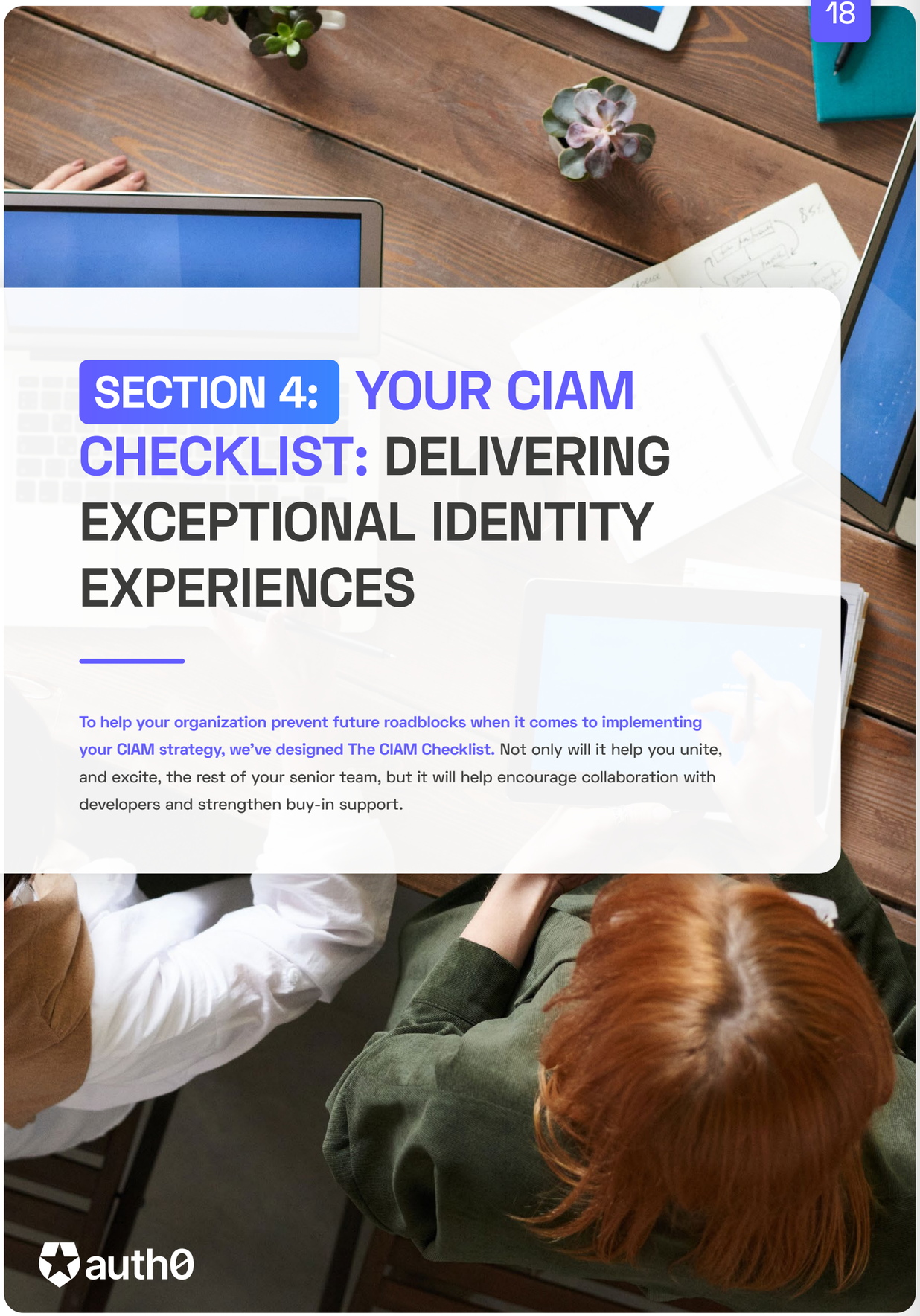
THE CIAM LIFEBOAT

Repairing the damage caused by The Log Inn is vital for every organization. That's why it's critical for organizations to put customer experience and security at the forefront of their authentication strategy. Leading decision-makers are already taking action, utilizing solutions like CIAM to help facilitate change, and meet customer expectations.

> **58% of development teams expect to add new third-party SaaS components to their application strategy over the next year[5].**

SaaS solutions like CIAM have been purposefully designed to help organizations deliver scalable identity experiences – whether it's through things like MFA, biometrics, or SSO. As these solutions work across apps and web pages, they help businesses unlock omnichannel opportunities by breaking down siloed user data: boosting revenue, boosting customer loyalty, and boosting competitiveness. Plus, the additional layers of security of these solutions mean that your organization is less vulnerable to cyber-attacks, data breaches, and identity fraud.

[4] https://www.dynamicyield.com/blog/shopping-cart-abandonment-ebook-announcement/
[5] https://auth0.com/resources/whitepapers/how-development-teams-purchase-saas



SECTION 4: YOUR CIAM CHECKLIST: DELIVERING EXCEPTIONAL IDENTITY EXPERIENCES

To help your organization prevent future roadblocks when it comes to implementing your CIAM strategy, we've designed The CIAM Checklist. Not only will it help you unite, and excite, the rest of your senior team, but it will help encourage collaboration with developers and strengthen buy-in support.

auth0

1 SET UP A CIAM HQ

Familiarize yourself with the quantifiable benefits of CIAM and share with your wider team. In this early stage of the decision-making, you're likely to be the in-house CIAM expert in your business: get these benefits ingrained in your brain.

If you're asked **"Why CIAM?"**, remember that it:

- Delivers a secure and frictionless login experience
- Guides compliance with data privacy laws
- Protects data assets against malicious intrusion
- Derives more specific, meaningful insights from customer data

2 BRING TOGETHER DEVELOPERS, IT TEAMS, AND MARKETERS

> "Getting to choose SaaS components matters to 91% of developers."

Create a meeting point where wider teams can come together and align on how CIAM solutions will be chosen, implemented, and managed, as well as allocate roles and responsibilities. It's vital to include your development team as early on in this process as you can. Our research shows that 87% of developers see productivity improve when they are able to use the SaaS components they want and need. And 88% say it improves their overall job satisfaction[6].

Find out more about the purchasing decisions of innovative companies in our report "How Development Teams Purchase SaaS".

[6] https://auth0.com/resources/whitepapers/how-development-teams-purchase-saas

3

VISIT THE ROI CONSULTANTS

Speak to vendors, peers, and authentication experts so that you can build a business case for the C-Suite. They'll want to see cost vs. return so be sure to come prepared – even if it's an estimated figure at that point. Don't forget, quantifiable results don't just include revenue: they can also include **increased employee happiness, productivity, and satisfaction.**

4

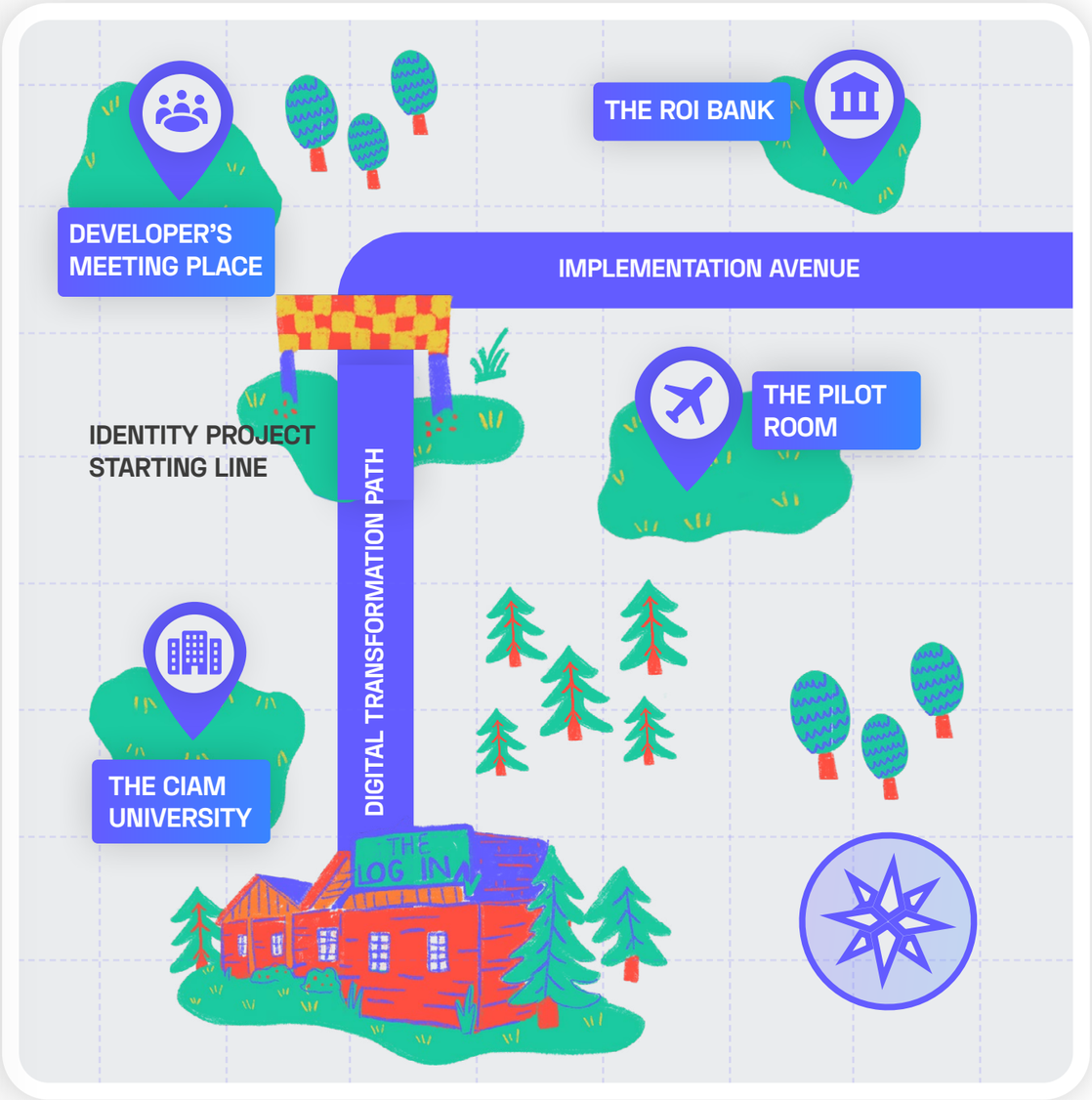
CHOOSE YOUR PILOT (PROGRAM)

> **58%** of teams believe in using third-party SaaS components vs. **11%** who strongly believe in building application processes in house[7].

Before you make a final decision on whether to build vs. buy your CIAM solutions, it's important to establish with your developers and engineers how you plan on testing it. Our research shows that trials and proof of concepts (POCs) are the preferred methods of testing SaaS components by fast-moving organizations. Plus, statistics show that companies who listen to developer feedback early on in the purchase cycle are **more likely to avoid technical obstacles later on.**

THE PATH TO CIAM

For more directions, follow our 'Modern Identity Management Map' where you'll see how you and your team can make a seamless trip along the Digital Transformation Path and Implementation Avenue, towards an incredible CIAM delivery. Below is a just snippet to get you onto the right path. To find out which path to take after Implementation Avenue, and access the whole of The Modern Identity Management Map, click here and download our rewelcome pack.



[7] https://auth0.com/resources/whitepapers/how-development-teams-purchase-saas

SECTION 5: FROM ‘DO NOT RETURN’ TO ‘CUSTOMER FAVORITE’

It’s never too late to take control of your customers’ experience. Take The Log Inn for example. After receiving shocking customer reviews, they used CIAM to transform how their guests checked into the business, to fix security risks, and even to deliver a 24/7 customer service. To find out more, and access the full The Modern Identity Management Map, click here.

If you’d like to find out more about how CIAM can help your business, visit https://auth0.com/b2c-customer-identity-management

ABOUT AUTH0

The Auth0 Identity Platform, a product unit within Okta, takes a modern approach to identity and enables organisations to provide secure access to any application, for any user. Auth0 is a highly customisable platform that is as simple as development teams want, and as flexible as they need. Safeguarding billions of login transactions each month, Auth0 delivers convenience, privacy, and security so customers can focus on innovation.

Auth0’s Customer Identity and Access Management (CIAM) solution balances convenience, privacy, and security for 5-star logins.

METHODOLOGY

The study was conducted online by Auth0 and YouGov from February to August 2021. The research consisted of two surveys, questioning more than 14,700 consumers and 2,400 IT and marketing decision-makers who work for businesses that offer an app/online service to customers (excluding sole-traders) across 12 global markets: The United States, United Kingdom, Belgium, France, Germany, the Netherlands, Australia, Singapore, Japan, Argentina, Brazil, and Mexico. The data for the consumer study was post-weighted by age, gender, and region to reflect the latest population estimates in each market.


auth0