REPORT

TOP 5 TRENDS IN CIAM TO WATCH

BEYOND IDENTITY

BEYOND IDENTITY

CONTENTS

BEYOND IDENTITY

INTRODUCTION

Customer expectations are ever increasing and regulatory standards are growing in number and scope. In response, Customer Identity and Access Management (CIAM) as an industry is constantly evolving to stay ahead to enable identity and security teams along with developers to deliver seamless customer identity experiences.

Some trends are mere fads while others have the staying power to transform digital identity experiences as we know it today for customer-facing applications.

The trends that are here to stay are worth paying attention to, because recognizing and accounting for them will help you build future-proof CIAM solutions that meet your customer needs, both now and later.

We delved into analyst and reputable third-party research published within the last three years to identify the top five trends in CIAM with the highest promise of longevity along with recommendations for actionable strategies for CIAM planning at your organization.

> "Some trends are mere fads while others have the staying power to transform digital identity experiences as we know it today."

BEYOND IDENTITY

TREND 1: WORLD-CLASS IDENTITY EXPERIENCES

Identity is unique in that it touches 100% of acquired users. It bridges the gap between a visitor and a customer of your product and serves as the gateway for engagement.

But a good experience is not world-class and what's good now is not going to be good enough in a few years.

Upleveling the authentication is important because companies, now more than ever, are competing on the basis of customer experience.

> "Identity bridges the gap between a visitor and a customer of your product and serves as the gateway for engagement."

KEY STATISTICS:

86% of CIOs identified customer experience as their primary competitive differentiator by 2021.
Gartner, 2020

Customer experience identified as the top competitive differentiation across all industries -- financial services in particular outpace other industries in their prioritization of customer experience.
Adobe and eConsultancy, 2019

57% of consumers would prefer passwordless authentication.
Ponemon, 2020

Only 29% of consumers agreed that the second factor was worth the convenience tradeoff.

35% of consumers mentioned difficulties with their second factor not being immediately available when they're trying to login.
Brigham Young University, 2019

83% of consumers are willing to share some data to enable a personalized experience. However, 64% said a brand experience is invasive when the brand had information about a consumer they didn't share knowingly or directly.
Accenture, 2019

WHAT CAN YOU DO TO MEET THIS TREND

1. Eliminate the password from the user interface and database

Passwordless technologies have proliferated in the last decade but not all solutions are created equal.

On the user experience side, a strong passwordless solution allows users to authenticate without picking up a second device for a one-time code (OTP) or push notification for a truly frictionless experience.

On the security side, a passwordless solution should allow you to completely eradicate the password from all user flows (including recovery) and your database to eliminate passwords as an attack vector while taking the target off of your database.

2. Implement frictionless multi-factor authentication (MFA)

Legacy MFA solutions leverage the password and an additional factor leaving the weak factor of passwords in place. Modern, frictionless MFA does not rely on passwords at all and instead authenticates users with strong inherence and possession factors.

When evaluating MFA options, there are three key considerations.

- One, can you trust all the factors used? For instance, passwords are a weak factor and out-of-band methods have known security vulnerabilities.
- Two, what is the user convenience tradeoff if it exists? Requiring second devices for OTP or push notifications introduce additional friction into the user flow.
- Three, can you deploy this easily across all your applications scalably? The cost of texting SMS OTPs add up as you grow your user base and is compounded by user authentication frequency.

3. Deliver identity-driven personalization

Identity doesn't stop at registration and login. Identity programs can help your entire business better understand customers, deliver customized product experiences, and simplify troubleshooting.

When building towards this, some key considerations include ensuring a centralized view into users and their device network, data sharing capabilities between your CIAM system and customer relationship management, support, and product analytics solutions, and maintaining a balance between personalization and privacy.

TREND 2: DOMAIN SHIFT FROM BACKEND TO PRODUCT EXPERIENCE DESIGN

CIAM historically grew out of Identity and Access Management (IAM) and there's a lingering connotation of IAM-related technology as being an enabling technology in the realm of engineering, security, and identity teams.

However, as businesses undergo digital transformation, more people across the organization are paying greater attention to CIAM efforts. This is because authentication has a direct impact on customer acquisition rates and great digital experiences are built from knowing who the customer is.

The domain shift and intensifying focus on CIAM is great news for identity and security professionals. This is because CIAM strengthens the recognition of your team's impact on business metrics that translate directly to revenue..

KEY TRENDS:

Covid-19 has accelerated digital transformation by an average of 6 years across all industries.
Twilio, 2020

During the pandemic, digital acceleration saw a "decades in days" growth.

- Telemedicine grew by 10x in 15 days
- Online delivery saw an increase that would have taken 10 years in 8 weeks.
- Online entertainment saw a 7 year growth in 5 months.

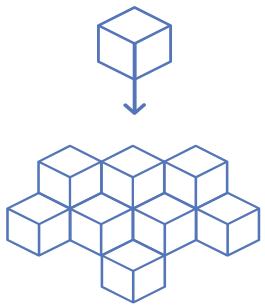
McKinsey, 2020

Buying committee shifting to include marketing, customer experience, and digital transformation.

"As businesses undergo digital transformation, more people across the organization are paying greater attention to CIAM efforts."

WHAT CAN YOU DO TO MEET THIS TREND

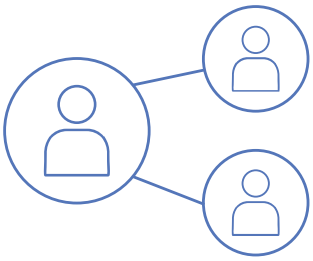
With this shift, there are three things to keep in mind to ensure successful CIAM evaluation and deployment.



Technology

When CIAM is a critical part of your digital transformation and growth strategy, CIAM systems must be able to exchange data with marketing, sales, product analytics, customer support, and eCommerce analytics solutions.

Your specific technology stack may differ but the core principle is that the identity, behavioral, and device data captured by a CIAM solution should inform customer interactions across every touch point.



Process & Stakeholders

Adapting to stakeholder changes means including the right people earlier in the planning process to gather requirements and ensure alignment around success criteria.

The appropriate stakeholders typically come from product, marketing, and customer experience teams. Your specific set of stakeholders may differ. As a general guideline, stakeholders responsible for customer-facing product experience are a good start.

In addition to gathering requirements, ideally the process of stakeholder alignment would enable you to find natural tie-ins to their initiatives which can help your team get buy-in and accelerate implementation.

Impact

CIAM's central role in driving and supporting customer-facing initiatives means that you have a unique opportunity to quantify the impact of your team in success metrics that translate across the organization.

Some key metrics that a strong CIAM program can impact include:

- Acquisition - increase conversions at registration. The drop-off here is a leaky bucket for most companies costing millions in marketing spend.
- Engagement - increase successful logins. Once you've successfully acquired a user, frictionless logins increase loyalty and help customers extract more value from your product.
- Retention - decrease churn from recovery and cart abandonment rates. Research shows that, for returning users, 18.75% abandon cart after forgetting password and having issues with password reset emails.

BEYOND IDENTITY

TREND 3: SELF-SOVEREIGN IDENTITY IN THE AGE OF PRIVACY

There's no question that we're living in the Age of Privacy with the number of privacy regulations passed in the last 5 years alone and increasing consumer scrutiny.

Even if customer demands and regulations weren't as stringent as they are today, investing in privacy is the right thing to do out of respect for customers and their trust in doing business with your company.

It's against this context that we're seeing an increasing interest in the idea of self-sovereign identities. As its core, self-sovereign identity is an approach to digital identity that empowers individual ownership of identity.

In contrast with the most common approach today where an application lets a user create a digital credential used only to access its services, the self-sovereign model introduces the concept of a self-signed, cryptographically verifiable credential that can establish trust in the user's identity and used to gain access across applications.

KEY TRENDS:

By 2023, 63% of the world's population will have our personal information covered under modern privacy laws which is up from 10% in 2020.
Gartner, 2020

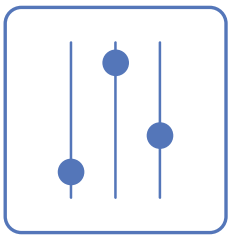
79% of consumers are concerned with how companies are using data collected about them.
Pew Research, 2019

85% of organizations report positive ROI on privacy investment.
Cisco, 2020

"Investing in privacy is the right thing to do out of respect for customers and their trust in doing business with your company."

WHAT CAN YOU DO TO MEET THIS TREND

Self-sovereign identity is a movement that inherently makes it difficult to be fully realized on an individual company basis. However, the core principles of identity ownership can be leveraged in your products to better prepare your organization and customers for digital identity ownership.



1. Transparent access and control

Control and transparency are the antidote to privacy concerns. Customers want to see, understand, and self-manage their devices, privacy & consent settings, and data-sharing permissions.

You can enable customer transparency and control via an easy to find control center. Within this control center you can expose authenticating devices with the ability to add and remove devices, refresh or revoke data sharing permissions for third-party applications, and adjust privacy and consent permissioning.

2. User habit formation

Even if you have a control center, it's a good idea to help customers build the habit of reviewing their device, data sharing, and consent permissioning at a regular interval. Dismissable in-app cues can be a good strategy to build habits for security hygiene and settings review without being an intrusive disruption to the product experience.

3. Technology exploration

There are existing technologies that let you support decentralizing identities. Blockchain may not be the only option.

For instance, Beyond Identity's deployment of asymmetric cryptography backed by proven technologies like X.509 certificates and TLS allows you to extend the chain of trust to the user without cert management and create self-signed, cryptographically verifiable credentials that are owned by no one but the user themselves.

TREND 4: CONTINUOUS, RISK-BASED AUTHENTICATION

Continuous authentication is a method of confirming identity and risk on an ongoing basis. That is, instead of treating authentication as a singular event, it allows you to assess risk and make adaptive access decisions using real-time signals from users and devices.

Authentication as a binary decision based on the ability to reproduce a password accurately is not secure enough to combat increasingly aggressive methods like brute force and bot attacks or the elevated sophistication of phishing attempts.

Without risk-based authentication that accounts for the integrity of a user's identity claim, behavioral patterns, and device security posture at the time of login, companies can be at higher risk for account takeover fraud and breaches.

Zero trust principles are taking off in workforce IAM at the moment but, not to be left behind, companies are also showing an appetite for continuous authentication for customers. This is especially prominent across industry leaders in financial services and eCommerce industries.

The impetus for continuous authentication is different for CIAM. Continuous authentication for the workforce revolves around securing access to company resources across all endpoints regardless of device management status.

In CIAM, continuous authentication allows companies to take the burden of authentication off of users and instead have machines do the work of establishing trust.

KEY TRENDS:

We expect manufacturers to release smartphones that learn from user behavior…The ultimate goal is to make user authentication "continuous".
Gartner, 2018

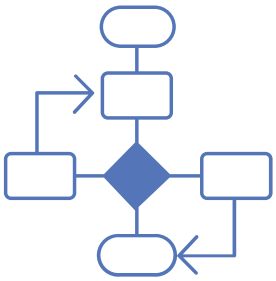
> "Continuous authentication allows companies to take the burden of authentication off of users and instead have machines do the work of establishing trust."

WHAT CAN YOU DO TO MEET THIS TREND

Continuous, risk-based authentication is an ongoing process of data collection around user and device risk signals, actioning on those risk signals, and optimizing risk models over time to make better access decisions. As a sequence of activities, the iterative loop looks like this:

1. Continuous risk assessment

Gather device security posture and user behavioral data captured in real-time at the time of login. This data is fed into a policy engine that assesses user and device risk for access decisioning. Additionally, you can use this data to establish a baseline of risk for user groups, device types, and other segmentation criteria that may be relevant for your business.

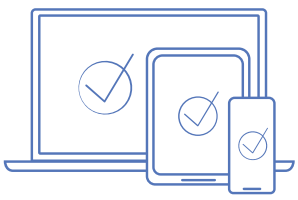


2. Dynamic access decisions orchestrated by a policy engine

Once you have the risk signals in place, you need a way to move beyond data collection to actioning on those risk signals to enforce access policies. For this step, you need a policy engine that can consume those risk signals along with flexible orchestration to create frictionless customer experiences.

Risk is a spectrum and to prevent frustrating lockouts the policy engine should give you the option to orchestrate dynamic biometric step-up authentication to establish further assurance of user identity. You may also want to invoke step-up authentication by default for higher risk actions like money transfers above a certain amount, checking lab results, or accessing payment information.

Ultimately, this leads to a more frictionless user experience as customers are only prompted for step-up when risk is present and detected rather than forcing customers to jump through authentication hoops every time.



3. Ongoing monitoring and risk model optimization

Users, devices, and your security requirements change over time which means risk-based authentication cannot be a static program. To ensure that your risk engine is running optimally, it's important to monitor and review access decisions and perform analysis parsed by user groups, device types, and other meaningful segmentation criteria for your business.

TREND 5: ECOSYSTEM SIMPLIFICATION

Historically, CIAM systems have been developed on a per application basis. This may have worked for the first application but creates an environment where each application becomes a silo.

Application silos lead to interoperability issues stemming from disjointed directories, difficulty with data sharing, and inflexible integrations.

Not to mention, scalability becomes an issue as new applications, acquisitions, and mergers have a multiplier effect on ecosystem complexity.

According to research, both developers and IT leaders are feeling the strain from outdated or overly complex CIAM systems.

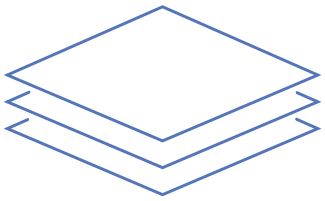
KEY TRENDS:

Developers spent 17 hours/week on code maintenance and refactoring amounting to $85B in annual opportunity cost.
Stripe, 2018

55% of IT budget was allocated to maintanence but leaders want to spend more on innovation.
Deloitte, 2020

"Both developers and IT leaders are feeling the strain from outdated or overly complex CIAM systems."

WHAT CAN YOU DO TO MEET THIS TREND

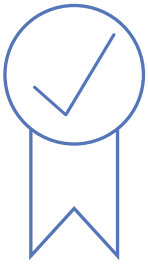


1. Decouple identity from applications

This is the most important guiding principle for ecosystem simplification. When you decouple identity from individual applications you can create a unified security, identity, and privacy layer in your architecture.

The abstracted identity layer helps you deliver consistent, scalable customer identity experiences across all your applications and domains.

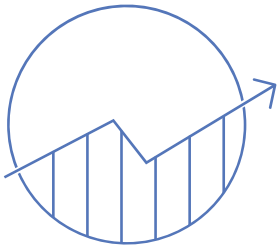
Additionally, it gives much needed flexibility and interoperability for development teams to accelerate time to market for new applications, respond to business needs, and ship innovative features.



2. Leverage proven open standards

If you choose to roll your own CIAM program, there are a number of proven open standards available to ensure secure interoperability across your infrastructure and applications.

These standards include OIDC, SAML, and OAuth 2.0 for authentication and authorization operations as well as SCIM and LDAP for directory and user management.



3. Explore investments in CIAM platforms

With increasingly demanding customer needs and regulations, it is a good idea to explore investing in customer identity platforms designed to handle not only common journeys in the customer identity lifecycle but also edge cases.

Strong CIAM platforms also lower your cost and risk of ownership as they are stress tested to handle enterprise workloads and spikes across global regions.

06 CONCLUSION

The world never stops changing and neither does CIAM. Here we discussed 5 emerging trends that are taking hold in CIAM and strategies to stay ahead.

It's an exciting time as practitioners, technology solutions, and regulatory organizations are pushing for more secure, frictionless, and safe digital experience for all.

Beyond Identity provides the strongest authentication on the planet, eliminating passwords completely for customers at registration, login, and recovery, as well as from your database.

Unique to Beyond Identity, customers never have to pick up a second device to enroll or authenticate, passwords are completely eliminated from user flows and your database, and you can implement risk-based access controls using granular user and device risk captured in real-time. Backed by a cloud-native architecture, our platform reliably handles enterprise workloads and usage spikes for always-on authentication services so you can deploy with confidence.

About the Author

Jing Gu leads product marketing for Beyond Identity's Customer Passwordless solution, responsible for driving its awareness, adoption, and growth. Prior to Beyond Identity, she formed and led the product marketing function at Shutterstock focused on its API/SDK product portfolio and bringing the platform's SAML capabilities to the enterprise market. When not evangelizing zero-friction, strong passwordless authentication, she enjoys exploring New York City, hiking, and building mechanical keyboards.

About Beyond Identity

Beyond Identity provides the most secure authentication platform in the world. Breaking down barriers between cybersecurity, identity, and device management, Beyond Identity fundamentally changes the way the world logs in–eliminating passwords and providing users with a frictionless multi-factor login experience. Beyond passwordless, the company provides the zero-trust access needed to secure hybrid work environments, where tightly controlling which users and which devices are accessing critical cloud resources has become essential. The advanced platform collects dozens of user and device risk signals during each login - enabling customers to enforce continuous, risk-based access control. The innovative architecture replaces passwords with the proven asymmetric cryptography that underpins TLS and protects trillions of dollars of transactions daily. Customers turn to Beyond Identity to stop cyberattacks, protect their most critical data, and meet compliance requirements.

Ready to Explore Passwordless Customer Solutions?

GET A DEMO

beyondidentity.com | info@beyondidentity.com

BEYOND IDENTITY