Does your customer identity and access management (CIAM) inspire trust?

The way you manage your customers' digital identities is part of the quality of their total experience with your brand.

Many do not gain the full value of consumer identity and access management (CIAM) because they confuse it with traditional Enterprise IAM, which focuses heavily on regulatory and security challenges and usually affects the CISO and Chief Risk Officer.

CIAM, on the other hand, is a critical component of digital transformation which affects the business success of an organization, and requires working with new and different stakeholders (CMO, CDO, profit centers), different users, different tools.

Why should the business executive care?

- To serve your customers well, you need to know them.
- Companies lose money when transactions and interactions get dropped or interrupted — for example, when customers forget their passwords.
- Security breaches cost money and reputation.
- Today's savvy consumer expects data privacy and control.
- Reaching for a tech solution is NOT the answer — unless you want a vendor to set your customer experience strategy.
- Treat CIAM as a critical component of enhancing your customers' experience.

Why should the security pro care?

- Access-related breaches top the list of known security breach causes.
- Verifying identity has expanded beyond the individual to include their devices and data.
- Increasing privacy regulations make compliance an ever-more-challenging mandate.
- A piecemeal approach can result in fragmented security, risking unauthorized access and compromise of organizational and consumer data.
- Educate executives on how CIAM can help increase the quality of the customers' total experience.

Security and marketing, previously considered strange bedfellows, are a match made in digital heaven with consumer identity and access management (CIAM).

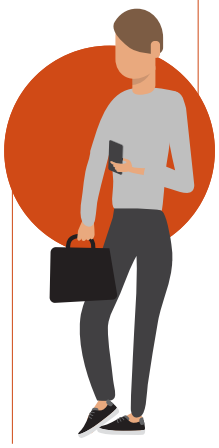
Designed primarily to protect applications and websites from bad actors, CIAM can be invaluable for marketing, brand management and digital initiatives, as well. At its heart, the technology vets and verifies user identity to secure applications and devices. But certain CIAM solutions can also

provide a comprehensive view of your customers' preferences and online behaviors — helping you to personalize digital experiences, reduce irrelevant communications, and improve customer interactions.

Today's most sophisticated CIAM offerings provide a full range of consumer services, including privacy protection, data collection and data analytics as well as identity verification,anti-fraud features, and more. These help to solve a host of business problems, bolster consumer trust and boost efforts to increase revenue.

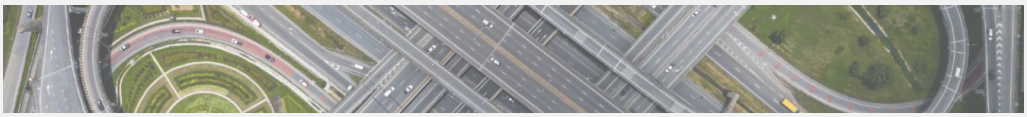
But not all CIAM software is created equal. Before shopping for a solution, it's important to know what CIAM is, what it is not, and how it can best support your business objectives.

CIAM is built around the customer's needs



- **Data collection**
- **Data analytics**
- **Privacy protection**
- **Identity verification**
- **Anti-fraud**

I generate data, therefore I am



CIAM has evolved with our changing notions of identity, a term that no longer refers only to the individual. In the digital age, identity also encompasses smartphones and the other computing devices a person uses, their finance/payment cards and medical records, and other data reflecting their preferences, habits and purchases.

Managing consumer identity for security's sake, therefore, means managing data.

The need to secure access to websites and applications grows more urgent by the year. According to F5 Labs, access-related breaches constituted the largest known security-breach type **(52%) in 2019**, increasing by 5 percent from 2018.

Think of CIAM as a digital handshake that verifies and manages an organization's external users or customers. With 82 percent of the world population covered by privacy regulations in place or imminent, according to **PwC analysis**, safeguarding customer data is no longer an option — it's a must.

But modern CIAM goes beyond security, access control and compliance. Today's smart solutions also feature a single view of the customer and customer intelligence across omnichannel interactions and transactions. It is built around the customer at different stages of the individual's relationship with an organization or brand.

These capabilities are designed to answer digital customer demands. People expect easy and convenient online shopping that's secure, private, efficient and smooth, even when they're using multiple devices. They want ads and promotions that speak to their wants, needs and lifestyles. And, increasingly, they want control of their personal information. Using a CIAM solution helps businesses meet these needs without having to build the features themselves.

CIAM is woven into every stage of the customer's relationship with your organization

Guest browsing and checkout
Consumers prefer to browse services anonymously or as a guest before they commit to a brand. Implementing a platform that motivates them to engage further is the first step

Registration, progressive profiling
Quick and easy registration that requires minimal information is preferred (e.g. registration through linking to social accounts, incremental data collection)

Secure self service functions
A flexible, secure solution tailored to manage credentials, update profile attributes and passwords is an enabler. Trust and Security through multiple factors and channels (e.g. SMS, Email, Authenticator App, Voice) is expected

One click / easy access across channels
A passwordless but secure login creates a strong incentive for users to access the platform more often. Saved profiles and preferences, linked coupons & reward redemptions create a seamless checkout experience. Credential prompts only when necessary

Transparency - Privacy and data collection
Consumers want to have digital options to delete, modify, or download their data. Failing to provide these capabilities creates dissatisfaction

Excitement and buzz around personalized offerings
Opportunities to actively and passively communicate

- Monthly activity and rewards statements
- Test and pilot offerings
- Market specific offerings

There's strength in unity

Various solutions exist to meet different CIAM needs, but a fragmented, piecemeal approach can result in disjointed experiences for customers — and the loss of their business. One in three US consumers (32%) are willing to walk away from a brand they love after just one bad experience, according to a PwC survey. This figure is even higher in Latin America, at 49%.

Cobbled-together CIAM technologies can't deliver the easy transitions and continuity that consumers want or the comprehensive "360-degree view" of customers' behaviors that businesses need to serve their customers well. To do CIAM properly, a unified approach works best.

Digital healthcare, for example, has become the new normal, and patients expect their data and transactions to be available to themselves and to other healthcare providers. At the same time, they want their information to be secure and private whether they're using their phone, laptop or tablet. Enabling their doctors, therapists, nurses and other practitioners to view and track their overall health over time may provide them with higher-quality, holistic medical care.

Financial services firms, including payment processing companies, must safeguard consumer information and accounts while providing customers with continuous access to their balances and funds. But even though these services may be isolated from one another — a credit card account may be completely separate from the consumer's bank account, which is separate from their investment accounts, for instance — financial institutions want to incentivize loyalty with rewards, and that requires holistic insight into every transaction. At the same time, consumers want to be able to seamlessly manage their money on demand, and to have secure experiences while doing so.

Topping the long (and getting longer) list of CIAM features:

1. **Consent management**: Letting customers choose how their private information is used (or not).
2. **Adaptive authentication:** Continually verifying user identity based on biometrics, behaviors and other indicators.
3. **Preference management:** Using consumer data to engage with customers wherever they are.
4. **Multichannel access:** Providing customers with multiple ways to interact with your organization.
5. **Simplified registration and progressive profiling:** Making it easy to sign up, then continuing to collect user data to improve customer profiles.
6. **Transparent data collection:** Notifying consumers that their data is being collected, processed and used, and for what purposes — which 41 percent of US consumers said would make them more likely to use mobile applications and buy a particular business' products and services.
7. **Secure self-service functions:** Letting users enroll in multi-factor authentication, manage passwords and other security features, and access and manage their customer accounts.
8. **Modern customer advocate workflows:** Tracking marketing and service initiatives all the way to results for a truly customer-centric business approach.

Solving your identity crisis: Six steps

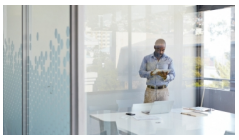
CIAM is catching fire in healthcare, retail and finance, in particular — but any entity with a digital presence can reap its rewards for itself and its customers. Here's how to begin.

1. Bring the right people to the table.

The business leaders responsible for the customer experience are in different parts of your organization. Assemble a multi-functional team of supporters from your security, privacy, customer experience, marketing and other relevant areas of the business, and solicit their input on features that would serve your entire organization best.

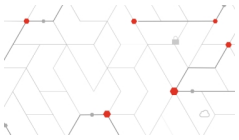
Exceptional customer support is already a mainstay with leading businesses, and the leading CIAM solutions help them manage customer identities and data while merging security, privacy management and compliance from login all the way through post-purchase support and service.

Related content



Cyber risk quantified. Cyber risk managed.

Quantifying the financial risks of different cyber threats can increase the bang for the cyber buck: it enables you to direct resources to the greatest risks.

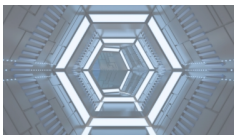


2021 Global Digital Trust Insights

Perspectives of over 3,200 business and technology executives on what's next in cybersecurity.

Digital evolution: What corporate directors and executives think

Corporate director and company management perspectives on the digital evolution of their companies differ on timelines, knowledge, rate of adoption and more.



What's next in cyber? Video podcast series

Hear from CISOs, cybersecurity, privacy and forensics subject matter specialists discuss the relevant issues and best practices.

Follow us

Get in touch

Required fields are marked with an asterisk(*)

First Name*

Last Name*

Joseph Nocera
Cyber & Privacy Innovation Institute Leader, PwC US
Email

Richard Kneeley

× Hide

Company Name*

Job Title*

Job Function*

- Please select

Email address*

Location*

- Please select

I agree PwC can email me about its insights, newsletters, events, services, products, and offerings.*

- Yes
- No

By submitting your email address, you acknowledge that you have read the Privacy Statement and that you consent to our processing data in accordance with the Privacy Statement (including international transfers). If you change your mind at any time about wishing to receive the information from us, you can send us an email message using the Contact Us page.

Managing Director, Cybersecurity and Privacy, PwC US

Email

Scott MacDonald

Principal, Cybersecurity, Privacy and Fraud, PwC US

Email