

[All Research](#) [Leadership Compass](#)

CIAM Platforms

September 27, 2022



John Tolbert

This report provides an overview of the market for Consumer Identity and Access Management solutions and provides you with a compass to help you to find the CIAM product or service that best meets your needs. We examine the market segment, vendor product and service functionality, relative market share, and innovative approaches to providing CIAM solutions.

1 Introduction / Executive Summary

Consumer Identity and Access Management (CIAM) is a well-established and innovative branch of the broader IAM field. CIAM solutions are designed to address specific technical

[Table of Contents](#)



CIAM systems allow users to register, associate device and other digital identities, authenticate, authorize, collect, and store information about consumers from across many domains. Unlike workforce IAM systems though, information about consumer users often arrives from many unauthoritative sources. Information collected about consumers can be used for many different purposes, such as authorization to resources or for transaction, or for analysis to support marketing campaigns, or Know Your Customer (KYC) and Anti-Money Laundering (AML) regulatory compliance. Moreover, CIAM systems must be able to manage many millions to even billions of identities, and process potentially tens of billions of logins and other transactions per day. SaaS delivery of CIAM services is the norm and will remain so.

CIAM systems can aid in other types of regulatory compliance. Since GDPR took effect in the EU in May of 2018, collecting clear and unambiguous consent from consumers for the use of their data has become mandatory. Many CIAM solutions provide this capability, plus offer consumers dashboards to manage their information sharing choices. Moreover, CIAM systems can help corporate customers implement consistent privacy policies and provide the means to notify users when terms change and then collect acknowledgement.

Improving the consumer experience is often a goal in deploying or upgrading CIAM solutions. With the increasing digitization of Business-to-Consumer (B2C) interactions, consumers are asked to create and use more and more accounts and passwords. Managing the escalating numbers of digital accounts can be burdensome for consumers if the CIAM systems with which they are engaging are not optimally designed, implemented, and continuously tuned.

CIAM platforms are used by both for-profit and non-profit organizations. Some government agencies use CIAM for government-to-citizen (G2C) identity management scenarios. For-profit businesses typically have more consumer data and marketing objectives. Non-profits use CIAM to host the identity information of donors, volunteers, and service recipients. Government agencies use CIAM to manage citizen identities for government interactions, such as paying taxes, fees, or fines; registering for licenses and services; managing applications; and various other use cases. All such organizations need to provide the means for consumers or citizens to register, manage their user profiles, authenticate, and get authorized for different kinds of resource access. Most also need dashboards for monitoring utilization, reports on historical activities, and the ability to collect other metrics.

Table of Contents



digitalization of consumer experiences was well underway in the late 2010s, and the Covid pandemic forced more businesses and other organizations to expedite digital transformation. With every iteration of this report, we observe significant acquisitions of CIAM specialists by others in the market, and entry into the market of new vendors. These trends will continue for the foreseeable future.

1.1 Highlights

- Innovation in CIAM drives the wider IAM market. The “consumerization of IT” is exemplified by the push to use CIAM methods and technologies for registration, authentication, and authorization in workforce IAM.
- Features that were considered innovative in the previous edition of this report are going mainstream.
- The new entrants in CIAM tend to coalesce locally; that is, the startups form to address region or country specific use cases, populations, or government regulations. In other cases, new CIAM businesses offer some new technologies, modifications on deployment methods, or better licensing or subscription models.
- Support for consumer IoT device identity linking is growing. Smart Home, wearable, and entertainment devices are proliferating, thus the need for such integration will increase as well.
- Account TakeOver (ATO) protection is required for all industries and use cases. Some CIAM platforms provide advanced capabilities, and others provide connectors to third-party services. Multi-factor authentication is a primary defense mechanism against ATO.
- Participating vendors indicate that MFA usage remains relatively low among their customers.
- Account Opening (AO) fraud is a persistent problem across many industries, particularly those in finance. Identity proofing services help mitigate against AO fraud, and some CIAM service providers have integrations with one or more identity proofing services.

Table of Contents





Full article is available for registered users with free trial access or paid subscription.

Log in

Register and read on!

Create an account and buy Professional package, to access this and 600+ other in-depth and up-to-date insights

Register your account to start 30 days of free trial access

Register

Get premium access

Table of Contents



Stay up to date

Subscribe for a newsletter to receive updates on newest events, insights and research.

Enter your e-mail

☐ I have read and agree to the Privacy Policy *

☐ I have read and agree to the Terms of Use *

Submit



Insights 

Research 

Table of Contents 

Events

▼

KC Open Select

▼

Company

▼



Switch to dark theme

Imprint

Terms & Conditions

Terms of Use

Privacy Policy

© Copyright KuppingerCole Analysts AG

Go to Market with KuppingerCole

Table of Contents

≡