Leadership Compass Consumer Identity and Access Management (CIAM)

John Tolbert

January 14, 2026



This report provides an overview of the Consumer Identity and Access Management market and a compass to help you find a solution that best meets your needs. It examines solutions that provide an integrated set of account management, access control, security, and regulatory compliance capabilities. It provides an assessment of the capabilities of these solutions to meet the needs of organizations that are looking to deploy CIAM or replace their CIAM solutions.

Contents

Executive Summary 4
Key Findings 4
Market Analysis 5
Delivery Models 5
Required Capabilities 6
Leadership 8
Overall Leadership 8
Product Leadership 10
Innovation Leadership 12
Market Leadership 15
Product/Vendor evaluation 17
Spider graphs 17
1Kosmos – 1Kosmos Customer 19
cidaas – cidaas 22
CoffeeBean Technology – CoffeeBean CIAM 25
Descope – Descope 28
DruID – Identity and Pulse 31
e-trust – HORACIUS CIAM 34
Frontegg – Authentication, Entitlements, AI Security Suite, Frontegg.ai 36
FusionAuth – FusionAuth 39
IBM – IBM Verify 42
Kinde – Kinde 45
LoginRadius – LoginRadius Platform 47
Microsoft – Microsoft External Entra ID / Azure AD B2C 50
Nevis – Nevis Identity Suite, Nevis ID & Authentication Cloud 53
Okta – Auth0 Platform 56
Optimal IdM – OptimalCloud 59
Ping Identity – Ping Identity Platform 62

© 2026 KUPPINGERCOLE ANALYSTS AG

ReachFive – Customer Identity and Access Management 65
SAP – Customer Identity and Access Management for B2C 68
SecureAuth – SecureAuth IAM 71
Thales – Thales OneWelcome Identity Platform 74
Transmit Security – Mosaic Platform 77
TrustBuilder – TrustBuilder.io 80
WSO2 – WSO2 Identity Server and Asgardeo 83
XAYONE – XIAM - Consumer Identity & Access Management 86
Vendors to Watch 89
Avatier 89
Avoco Secure 89
AWS Cognito 89
Beyond Identity 89
Clerk 90
Curity 90
Ergon (Airlock) 90
Google Firebase 90
Login Alliance Login Master as a Service 91
NRI Secure Technologies 91
Ory 91
PRIVO 92
Quasr 92
Relock 92
Simeio 92
Stytch 93
Synacor 93
Ubisecure 93
WorkOS 93

© 2026 KUPPINGERCOLE ANALYSTS AG

Executive Summary

The Consumer Identity and Access Management (CIAM) market continues to grow and mature as digital engagement becomes central to how organizations interact with consumers. CIAM solutions are now foundational to delivering secure, privacy-respecting, and personalized digital experiences across industries such as retail, media, finance, healthcare, and government-to-citizen (G2C) services. These platforms provide core capabilities for user registration, authentication, consent and privacy management, fraud detection, identity verification (IDV), and identity lifecycle management for potentially tens of millions of people.

The primary motivations for adopting CIAM include improving user experience, protecting against account takeover and other forms of fraud, ensuring compliance with privacy regulations, and enabling secure access across web, mobile, and connected device ecosystems. As consumers increasingly expect seamless and secure access to services, CIAM vendors have introduced innovations such as risk-adaptive authentication, behavioral biometrics, Software Development Kit (SDK)-based mobile identity assurance, decentralized identity support, and consent orchestration. While the CIAM landscape is competitive, many vendors differentiate through advanced orchestration; specific innovations in IDV; and support for integrations with external IDV services, consumer Internet of Things (IoT) identity association, Fraud Reduction Intelligence Platforms (FRIPs), Customer Relationship Management (CRM), Customer Data Platforms (CDPs), Consent and Privacy Management (CPM) solutions, payment services, and chatbot services. Although integrations with third-party CPM solutions is desirable, consent and privacy management capabilities are so essential that we expect CIAM solutions to have well-developed built-in features in this area, particularly in the light of expanding global regulatory requirements. The trend toward composable, Application Programming Interface (API)-first CIAM architectures is accelerating, enabling organizations to integrate identity services flexibly across consumer-facing channels. The market is expected to continue its growth trajectory as consumer expectations, fraud threats, and regulatory pressures evolve.

This report will focus on solutions for consumer- and citizen-facing IAM systems. Business-to-business (B2B) CIAM solutions will be covered in a separate Leadership Compass which will be published soon.

For details on how these reports are produced, please see KuppingerCole Leadership Compass Methodology.

Key Findings

- Passkey authentication is accepted by the vast majority of vendors surveyed (88%).
- Basic identity governance and lifecycle management features for consumer accounts are emerging as requirements, and are supported, at least in part, by many of the solutions examined herein.
- Built-in IDV services, including mobile apps for remote onboarding with liveness detection and document processing, are now offered by nearly 40% of solutions.
- Organizations pursuing CIAM solutions are looking for in-platform fraud prevention functions as well as integrations with full FRIPs.

© 2026 KUPPINGERCOLE ANALYSTS AG

- Nearly 80% of vendor solutions surveyed offer at least some basic device intelligence capabilities. Orchestration is an important consideration, with nearly three-quarters of solutions offering graphical orchestration interfaces of varying complexity and quality.
- Only about half of the products and services investigated offer consent and privacy management capabilities that are robust enough to aid in compliance with privacy regulations like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the US.
- Most solutions have varying capacities to support consumer IoT device association and management.
- Artificial Intelligence (AI) agents operating on behalf of consumers are already interacting with CIAM systems, and five of the solution providers in this market are building functionality to meet this emerging technical challenge.

Like most other software companies, some CIAM vendors are rushing to explore and/or implement Generative AI (GenAI) in their products, but currently only about one-third of the solutions are leveraging it in their administrative interfaces.

Market Analysis

The CIAM market continues to grow and diversify. Although CIAM has been around for a long time, there is still much room for expansion by vendors and room for new startups. CIAM systems are adopted to improve consumer experiences and marketing capabilities, add security (generally by offering more and better forms of Multifactor Authentication (MFA)), and increase revenues. Respondents to our surveys indicate that replacing homegrown CIAM systems or re-purposed workforce IAM systems still drives a large percentage of new deals.

Microsoft and Okta may dominate the market, but companies such as Ping Identity, IBM, and Thales command a large share as well. As has been the case since we started reporting on the CIAM market nearly ten years ago, there are still many regional CIAM vendors. These regional vendors tend to specialize by providing integrations with local (country-specific) identity or attribute providers, more granular features for regulatory compliance, or better language support for their target regions. These regional CIAM specialists are likely to remain and grow in their home markets, as well as expand into other regions where language support is needed.

There have been no significant acquisitions in the CIAM market since the previous edition of this report was published in 2024, when the WSO2 acquisition by private equity was still in progress.

Delivery Models

Software as a Service (SaaS) is the primary delivery model for CIAM. In fact, only one vendor in this report does not offer their solution as SaaS. Some vendors have multi-cloud options and can support data residency across multiple continents. The overwhelming majority offer both multitenant and single-tenant hosting options.

© 2026 KUPPINGERCOLE ANALYSTS AG

Two-thirds of the vendors allow customers to host their software on-premises or in private clouds. But of those that do have on-premises or private cloud options, most report that SaaS is still the preferred delivery model.

Required Capabilities

The following is a list of criteria for inclusion and evaluation in this Leadership Compass on CIAM:

- Flexible deployment (SaaS, in PaaS/IaaS, hybrid, private cloud, and on-premises)
- Multitenant and single-tenant options
- Multi-cloud support options
- Microservices architecture
- Orchestration engine and administrative interface for built-in and third-party services
- Self-registration; social login registration; bulk user import for platform migration
- User dashboards for credential, device, user profile, and consent management
- Secure account recovery mechanisms (not security questions)
- Multifactor and passwordless authentication, supporting multiple authenticator types, especially mobile apps, and biometrics
- SDK to enable customers to build authenticators and embed CIAM platform authentication into customer apps
- Authentication policies mapping assurance levels to authenticator types for step-up authentication
- Risk-adaptive authentication: evaluation of runtime environmental parameters, user behavioral analytics, and fraud/threat/compromised credential intelligence
- Support for consumer IoT device identity integration and management
- Support for all major identity federation standards, including Security Assertion Markup Language (SAML), Open Authorization (OAuth), OpenID Connect (OIDC), and JSON Web Token (JWT)
- Support for Single Sign-On (SSO) between all related customer properties and brands
- Collection and presentation of identity analytics
- APIs and connectors for marketing analytics and automation, CDPs, CPMs, CRMs, and other SaaS apps
- Identity verification functions and/or integration with third-party identity verification services
- Integrations with FRIPs
- Integrations with customer Security Information and Event Management (SIEM) systems
- IT Service Management (ITSM) integration (for example, ServiceNow, JIRA Atlassian, BMC Remedy, etc.)
- Reports & dashboards for CIAM system metrics
- Data localization/residency for privacy regulatory compliance
- Reports and support for privacy regulation compliance audits
- Developer support/capabilities
- Standards support, such as Fast Identity Online (FIDO), Kantara Consent Receipt, and JWT

© 2026 KUPPINGERCOLE ANALYSTS AG

The following items are considered as additional and innovative capabilities:

- Ability to utilize national e-IDs, bank IDs, and passports
- Ability to utilize decentralized IDs
- Support for GDPR Data Subject Access Requests
- Support for advanced financial use cases including Anti Money Laundering (AML), Know Your Customer (KYC), and Payment Services Directive 2 (PSD2)
- Applied AI/Machine Learning (ML) for identity analytics
- Applied AI/ML for risk-adaptive authentication
- Advanced support for IoT, Smart Home, connected cars, and wearables use cases
- Intuitive interface for customer admins
- Sophisticated features that allow for granular and proactive user account lifecycle management
- Integrations for payment services

© 2026 KUPPINGERCOLE ANALYSTS AG

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify vendors that should be evaluated further. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept (PoC) or pilot phase, based on the specific criteria of the customer.

Based on our rating, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for:

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

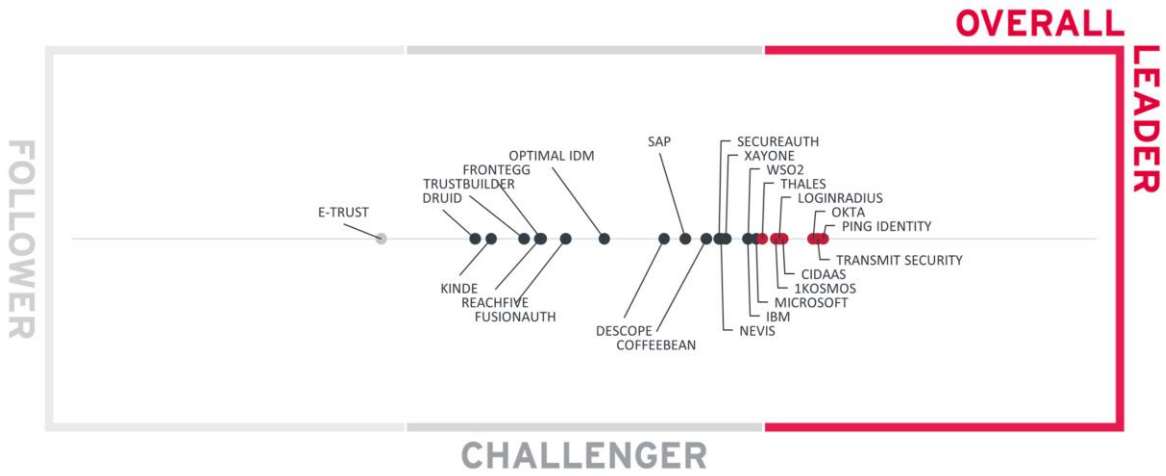


Figure 1: Overall Leadership in the CIAM market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and to see which of your use cases they support best.

The Overall Leaders in this edition of LC CIAM are Ping Identity, Transmit Security, Okta, cidaas, LoginRadius, 1Kosmos, Thales, Microsoft, WSO2, and IBM. Transmit has made enormous strides in product and innovation leadership. Their combined CIAM and FRIP offering addresses nearly all requirements in both fields. Ping Identity has a similar, leading-edge portfolio that provides nearly every feature organizations need for consumer identity

management and fraud prevention. Okta, with its Auth0 product, ranks highly due to the vendor's strong feature sets and innovative provisions for AI agents. cidaas and 1Kosmos likewise have excellent CIAM products with IDV and ATO prevention capabilities, just smaller, regionally-focused customer bases. Thales excels due to the combination of built-in IDV, FIDO/PKI authentication, and consent management features. LoginRadius maintains its Overall Leadership position with continual innovation and addition of functionality, particularly in consent management, and increasing market share. Microsoft is back in this edition of the report and is also an Overall Leader, buoyed by their overwhelming market position. WSO2 is as an Overall Leader due to their innovation in AI agent and Post-Quantum Cryptography, and IBM is an Overall Leader with good authentication options and decentralized identifier support.

XAYONE, Nevis Security, SecureAuth, CoffeeBean, SAP, and Descope are nearly Overall Leaders at the top third of the Challenger rank. Optimal IDM is doing well in the center of the Overall Leaders chart. FusionAuth, Frontegg, ReachFive, TrustBuilder, Kinde, and DruID round out the Challengers. Of these, Frontegg and Kinde are debuting in this iteration of the CIAM LC. Market newcomer e-trust is in the Follower area.

Overall Leaders are (in alphabetical order):

- 1Kosmos
- cidaas
- IBM
- LoginRadius
- Microsoft
- Okta
- Ping Identity
- Thales
- Transmit Security
- WSO2

Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.



Figure 2: Product Leadership in the CIAM market

Ping Identity, Transmit Security, LoginRadius, and Okta are at the top of the Product Leadership chart. 1Kosmos, cidaas, Thales, Nevis Security, SecureAuth, Microsoft, WSO2, CoffeeBean, and IBM are also in the Product Leadership area.

XAYONE, is at the top of the Challenger section. SAP, Descope, and Optimal IDM are near the border between Challengers and Leaders. The majority of vendors are distributed evenly across the rest of the Challenger box.

e-trust is in the upper part of the Follower area, indicating room for product growth.

Product Leaders (in alphabetical order):

- 1Kosmos
- cidaas
- CoffeeBean
- IBM
- LoginRadius
- Microsoft
- Nevis Security
- Okta
- Ping Identity
- SecureAuth
- Thales
- Transmit Security
- WSO2

Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.



Figure 3: Innovation Leadership in the CIAM market

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers' requests but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

Innovative features in CIAM include the use of GenAI for natural language queries, report generation, and policy construction; identification and handling of AI agents operating on behalf of human users; use of ML for anomaly detection and classification; support for Decentralized Identities (DIDs); no-code/low-code admin interfaces; user attribute data transformation logic; built-in IDV functions, including providing mobile apps/SDKs that enable

remote onboarding with high degrees of identity assurance via liveness detection; New Account Fraud (NAF) detection; identity governance and lifecycle management features; advanced device intelligence and behavioral biometrics functions; Account Takeover (ATO) prevention; advanced support for consumer IoT device identity management; and connectors for third-party IDV, FRIP, payment services, CDP, and CPM solutions.

Transmit Security, 1Kosmos, cidaas, Ping Identity, XAYONE, Okta, LoginRadius, Nevis Security, Thales, SecureAuth, and WSO2 are the Innovation Leaders at the end of 2025.

All other participants are scattered throughout the Challenger section of the chart.

Innovation Leaders (in alphabetical order):

- 1Kosmos
- cidaas
- LoginRadius
- Nevis Security
- Okta
- Ping Identity
- SecureAuth
- Thales
- Transmit Security
- WSO2
- XAYONE

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, the number of identities managed, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

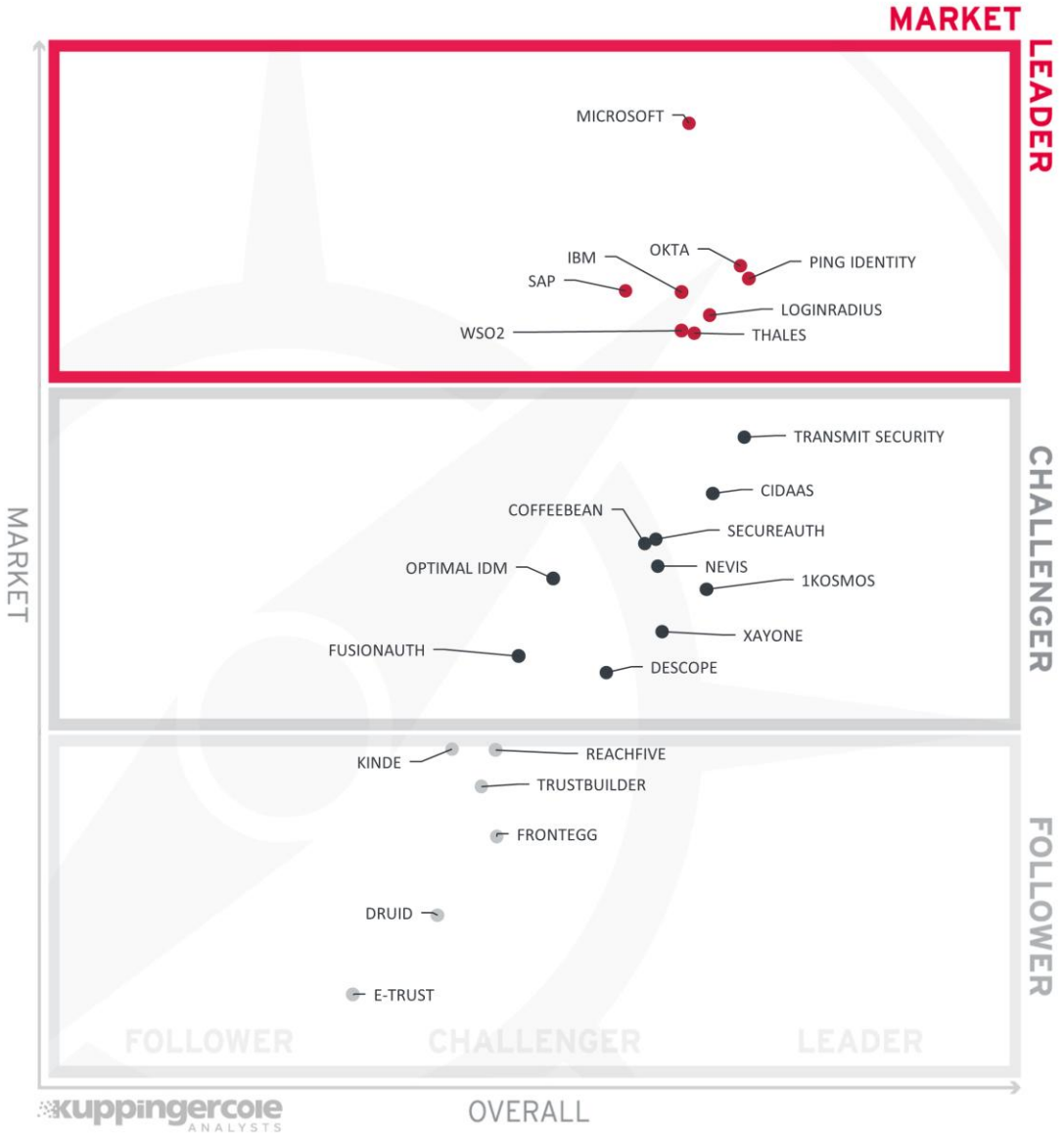


Figure 4: Market Leaders in the CIAM Market

Microsoft has a commanding lead in the market. Okta, Ping Identity, SAP, IBM, LoginRadius, WSO2 and Thales are also CIAM Market Leaders.

Transmit Security, cidaas, SecureAuth, CoffeeBean, Nevis Security, Optimal IDM, 1Kosmos, XAYONE, FusionAuth, and Descope are the Challengers.

Kinde, ReachFive, TrustBuilder, Frontegg, DruID, and e-trust appear in the Follower area, with room to capture larger shares of this always growing market.

Market Leaders (in alphabetical order):

- IBM
- LoginRadius
- Microsoft
- Okta
- Ping Identity
- SAP
- Thales
- WSO2

Product/Vendor evaluation

This section contains a quick rating for every product/service we have included in this KuppingerCole Leadership Compass document. For many of the products, there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For this market segment, we look at the following categories:

Onboarding – this metric examines the registration options available, support for bulk provisioning for migration between solutions, progressive profiling options, mobile device associations with consumer accounts, and IDV options.

Orchestration – this category represents the presence and ease-of-use of graphical tools for orchestrating workflows, including steps for registration, IDV, authentication, authorization, fraud risk checks, the presence of modifiable templates, and the ability to customize workflows. Scriptable or command-line interfaces will also rate here, albeit lower. The variety of APIs supported, the security of API connections, and the availability of pre-defined connectors to third-party apps is also measured under this heading.

Lifecycle Mgmt. – this metric covers the ability to detect and merge similar/duplicate accounts, to detect abandoned accounts and present options for handling them, and account recovery options.

Authentication– this measures the breadth of authenticators accepted, the depth of risk-based authentication factors examined, and the intuitiveness of the authentication policy building interface. One Time Passwords (OTPs) are less secure and have been deprecated in some areas but are still supported. There are many authenticator apps, such as those from Authy, Duo, Google, LastPass, Microsoft, Okta, and SAASPASS; and many of the vendors examined below support multiple third-party apps. Android and iOS biometric authentication (fingerprint and facial recognition) are widely used by CIAM solutions. FIDO2 and passkeys are standard and state-of-the-art. Fortunately, most vendors support these today. SAML, OAuth2, OIDC, and JWT support enables federation. The authentication category also rates the capabilities of vendors' SDKs, including the environments for which SDKs are available, the types of device intelligence that can be harvested from the SDKs, and whether behavioral biometrics are supported , and if so, which modalities are included.

Authorization– this category examines the ability of each solution to implement transaction-level authorization and to enable use cases for fine-grained access controls. Support for Role-Based Access Control (RBAC) is considered rudimentary, while support for Attribute-Based Access Control (ABAC), Policy-Based Access Control (PBAC), and Relationship-Based Access Control (ReBAC) models is considered more advanced and therefore suitable for disparate use cases such as high-value transaction authorization, delegated administration, privilege management, and for the implementation of family management in CIAM scenarios.

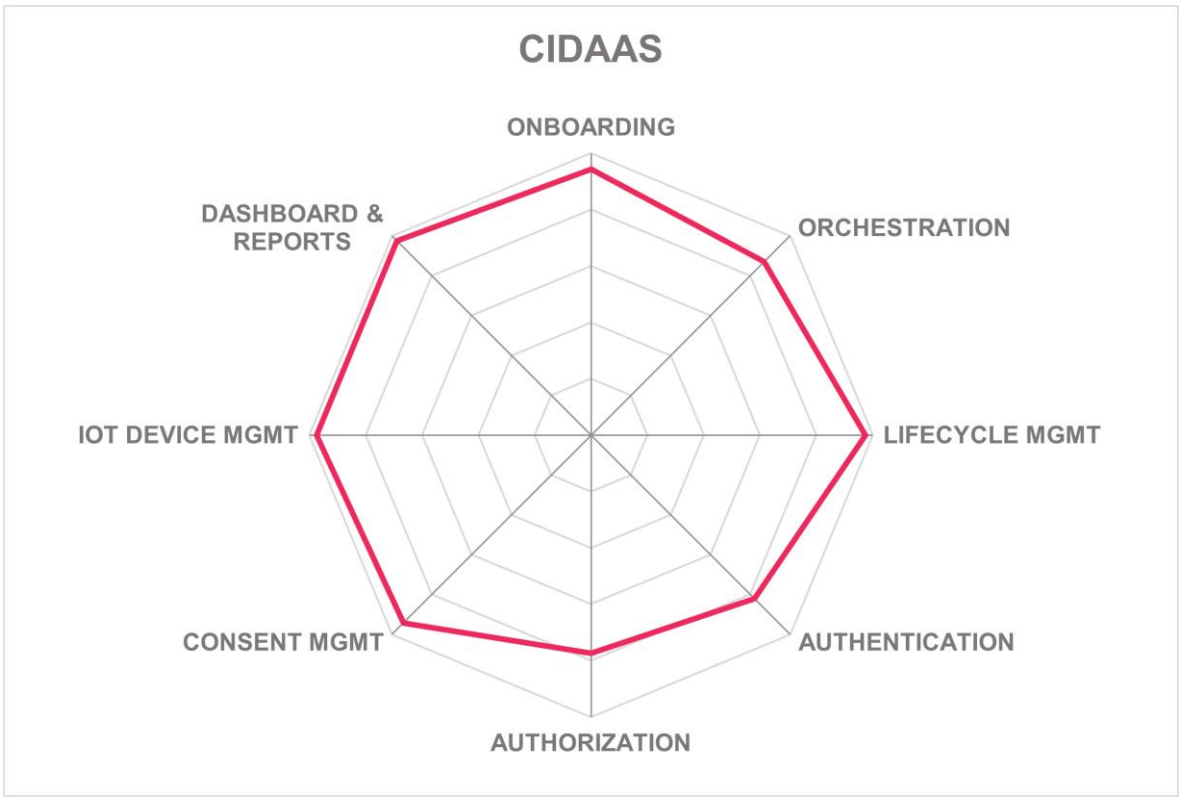
Consent Mgmt. – this rubric covers the facilities within the vendor solution's UI that allow consumers to edit their contact information, and to opt-in/out of services and data sharing, including data sharing between the customer site and third parties. These functions are often constructed as consumer privacy dashboards or self-service portals. For optimal regulatory compliance support, solutions must give consumers the ability to view, edit, export, and delete their profiles as desired. Family management functions are considered here as well. Kantara Consent Receipt is a standard that promotes interoperability in consent collection and management. The provision of Data Subject Access Request (DSAR) templates and the ability to configure Terms of Service (ToS) change notifications is also represented in this category.

IoT device Mgmt. – this category reviews the functionality within CIAM platforms that allows consumers to register, activate, authorize, and monitor usage of home automation and entertainment, wearable IoT devices, connected cars, and so on, by associating consumer identity with device identities. The use of the OAuth2 Device Flow specification is a good first step to achieve this. The ideal solution includes capabilities within the user self-service portal to manage these devices.

Dashboards & Reports - This measures the quantity of information available and quality of the dashboards and reports covering identity analytics, such as logins processed, concurrent sessions, failed login attempts, consumer profile changes, and so on. Most CIAM platforms provide at least basic identity analytics and dashboards within their solutions, as well as the capability to send identity event information to customer SIEM systems via Common Event Format (CEF), Representational State Transfer (REST) API, or syslog. Widget-based dashboards facilitate customization. Dashboards can also be used as starting points for security investigations. This metric also represents the ability of each solution to interoperate with third-party CRM, CDP, and SaaS apps.

© 2026 KUPPINGERCOLE ANALYSTS AG

cidaas – cidaas



Leader in



Widas, a private German company, was established in 1997. In 2018 they launched cidaas, their CIAM product and brand. cidaas is most active in the DACH region in Europe but has been expanding into Benelux and the Nordic countries, as well as gaining some customer traction in the US and India. cidaas is delivered as SaaS, which is hosted on a public IaaS provider and their own facilities, in datacenters in Europe, NA, and Asia. Multitenant and single-tenant options are available. Subscription fees for monthly users are available in four different tiers of service.

cidaas can store the widest variety of data objects in its user database, including photos and videos. It can interoperate with Microsoft AD. Self-registration and registration via OIDC-conformant social network providers are available. Support for LDAP and SCIM allows for migration from and synchronization with other directories. Data normalization is possible via an external aggregation platform. DIDs are accepted, but W3C DID compliance is still in the planning stage. Device registration is present, and customers can configure different workflows for this as needed.

cidaas's AutoIdent service can validate users against 150 document types, including passports, national ID cards, and driver's licenses. Full attribute retrieval is possible via NFC. It performs face matching between selfie ID documents, with both active and passive liveness detection. Customers can also configure connections with eHerkenning, Mitek, MitID, Stripe, and Verimi IDV providers. These high-assurance IDV methods deter new account fraud. Email/SMS/phone OTP, mobile push notifications, and account linking can be used for account recovery procedures. cidaas can identify similar or duplicate accounts and help users merge them, leveraging their built-in fraud detection to prevent account takeovers. It can also send keepalive messages to inactive account holders if customers want to purge abandoned accounts.

For authentication, cidaas supports email/phone/SMS OTPs, mobile push notifications, cidaas/Google/Microsoft authenticator apps, mobile biometric authentication, and all FIDO-certified authenticators, including passkeys. JWT, OAuth2, OIDC, and SAML federation are supported as well. cidaas provides Android, iOS, React Native, Flutter, and Node.js SDKs, which can gather a wide range of device intel attributes for risk decisions. Behavioral biometrics are also evaluated, but the set of modalities examined is quite limited. Customers author registration workflows and authentication policies in a flowchart-style GUI. Templates are provided, which can easily be edited. The risk engine outputs scores for calling applications to consume. cidaas supports delegated administration, privilege management, and RBAC/ABAC/PBAC models.

As mentioned above, cidaas has some FRIP features including device intelligence, User Behavior Analytics (UBA), and imports device and IP reputation information. It has built-in connectivity to third-party sources such as fraud0, Omniac, and RISK IDENT. cidaas supports REST, Simple Object Access Protocol (SOAP), GraphQL, webhooks, WebSockets, and WebAuthn API types. cidaas has connectors for Billwerk, Adyen, and Stripe payment service providers. Eighteen connectors for SaaS apps such as CRM and ITSM are available out-of-the-box. Moreover, cidaas's parallel product, cnips, is an integration Platform as a Service (iPaaS) which allows customers to quickly build integrations to legacy or highly customized systems.

The cidaas user self-service portal allows consumers to manage their digital identities, including preferences, consents, security settings, registered devices, and active sessions. Consumer IoT device identity management extends to consumer electronics and smart home automation use cases. cidaas has advanced support for shopping bots that act on behalf of consumers. Users can export or delete account information in accordance with GDPR and other privacy regulations. cidaas provides DSAR templates, notifies users of terms of service changes, and adheres to the Kantara Consent Receipt standard. It has well thought-out family management features that support complex access control scenarios for video streaming apps, theme parks, and hotel guest management. cidaas also has connectors for OneTrust and Usercentrics CPM.

cidaas has a customizable widget-based dashboard that displays a wide range of identity metrics, including the standards such as login success/failure rates and MFA events as well as registration/conversion funnel statistics and suspicious events. Many report types are present. They are introducing GenAI for natural language queries for investigations, policy authoring, and reporting.

cidaas has completed its ISO 27001 audit and is eIDAS certified, but it has not yet obtained SOC 2 Type 2 certification. They offer onboarding and ongoing support packages. English and German are the supported languages. cidaas has strong features in IDV, authentication,

user management, consent management, and early support for non-human identities (NHIs). Although they are best known in the DACH region, companies in any region that are prioritizing these features, particularly in the retail, media, and entertainment industries, should have cidaas on their CIAM RFP shortlist.

Strengths

- AutoIdent app and SDKs allow for strong, remote IDV, including support for many authoritative documents and active and passive liveness detection
- Good range of authenticators supported
- Built-in NAF and ATO prevention functions
- Excellent API support for easier integrations
- Full featured consent management
- Granular family management for media and entertainment industry use cases
- Includes connectors for payment services
- Innovative use of GenAI for reports and queries
- Supports consumer IoT devices and other NHIs

Challenges

- Limited implementation of behavioral biometrics
- Data normalization for directory sync operations requires external solution
- Additional out-of-the-box connectors for SaaS apps would be helpful, although their cnips product can facilitate such integrations
- SOC 2 Type 2 certification not yet achieved