KuppingerCole Analysts

Ory

John Tolbert

November 4, 2025

EXECUTIVE VIEW

This KuppingerCole Executive looks at the background and options available to IT managers and security strategists to manage Consumer Identity and Access Management. A technical review of the Ory platform is included.

Content

Figures

Introduction

As organizations increasingly digitize consumer and partner engagement channels, the demand for Customer Identity and Access Management (CIAM) solutions has expanded well beyond traditional registration and login capabilities. CIAM platforms now serve as critical infrastructure designed to deliver trust, compliance, personalization, and operational resilience across both Business-to-Consumer (B2C) and Business-to-Business (B2B) environments. Unlike workforce IAM platforms that address provisioning and lifecycle governance for known employees within authoritative directories, CIAM systems are designed to operate in volatile, high-volume, and heterogeneous contexts. They must accommodate millions or even billions of identities derived from scattered, often non-authoritative sources, using a variety of credential types, including email addresses, social networks, national ID systems, mobile devices, and IoT endpoints, all while maintaining privacy and adhering to security standards.

Most CIAM platforms are delivered as multi-tenant Software-as-a-Service (SaaS) solutions built on public Infrastructure-as-a-Service (IaaS) providers. This model allows vendors to offer massive scalability globally, rapid and consistent new feature implementation, and predictable cost structures based on monthly active users or authentication/authorization transaction volumes. However, CIAM requirements vary significantly by industry, geography, and data residency obligations, which necessitates alternative deployment models. Some vendors offer customer-deployable CIAM software suitable for installation in IaaS or Platform-as-a-Service (PaaS) environments, as well as traditional on-premises deployments for clients with strict compliance requirements. This also addresses private cloud or single-tenant SaaS options, which offer logical separation of customer data and dedicated compute and storage resources. These models, which are growing in popularity, appeal to enterprises that prioritize data isolation, performance customization, or contractual service-level agreements beyond what shared environments can offer.

Modern CIAM solutions must serve both B2C and B2B constituencies. B2C use cases dominate numerically, and address the need for secure, user-friendly access to digital properties by consumers, donors, or citizens. In contrast, B2B CIAM supports complex identity relationships involving contractors, gig workers, collaboration partners, resellers, and customer support personnel. These users generally require delegated administration, hierarchical role assignments, and compliance attestation workflows that resemble workforce IAM, but at consumer scale. B2B CIAM introduces added complexity in identity verification (IDV), federated Single Sign-On (SSO), and policy enforcement. Use cases often require integration with external IAM systems, Attribute-Based Access Control (ABAC), and provisioning or de-provisioning capabilities based on contractual relationships, usage, and temporal parameters. Regulatory requirements for Anti-Money Laundering (AML), Know Your Customer (KYC), and sanctions screening are also more prevalent in B2B scenarios, particularly in regulated industries such as financial services, defense, and healthcare.

At a functional level, CIAM platforms provide a distinct but overlapping set of capabilities relative to enterprise IAM. Self-service registration processes must accommodate wide-ranging entry points such as social network identity federation, passwordless registration, QR codes, or document-based IDV. Progressive profiling enables incremental data collection, which reduces registration abandonment rates and improves data accuracy. B2B scenarios may require human resources (HR) background checks, delegated registration, or account linking to external directories. CIAM systems manage dynamic consumer identity attributes, associations with devices and consent objects, account linking, and de-duplication logic. Consumers must be empowered with self-service dashboards for credential management, account recovery, and consent review. Family account structures, parental controls, and device lifecycle management are increasingly required for digital media subscription management, healthcare portals, and smart home device management scenarios.

Multifactor Authentication (MFA) is a core requirement for mitigating Account Takeover (ATO) attacks, yet adoption remains woefully low. CIAM platforms support a wide array of authentication methods including mobile and behavioral biometrics, Fast Identity Online 2 (FIDO2) or Web Authentication (WebAuthn) passkeys, risk-adaptive authentication with step-up triggers, and device fingerprinting and reputation analysis. Most vendors allow their organizational customers (tenants in SaaS) to edit authentication policies to meet their specific requirements based on risk context, business rules, and regulatory mandates. Authorization enforcement often extends beyond binary role assignments. Role-Based Access Control (RBAC), while nearly universally available, is increasingly insufficient to meet the demands of contemporary requirements. Advanced CIAM platforms support ABAC and Policy-Based Access Control (PBAC), delegated administration, contextual access enforcement, and integration with downstream applications via OAuth2 scopes or Security Assertion Markup Language (SAML) attributes.

Regulations such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Brazil's General Law for the Protection of Data Protection (LGPD), and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) mandate that consumer data be collected and processed only with informed, revocable consent. CIAM platforms must provide consent orchestration workflows, version tracking, Data Subject Access Request handling, and account data export or deletion Application Programming Interfaces (APIs). Integration with external consent and privacy management platforms is increasingly common, especially where consent needs to be orchestrated across multiple systems. The proliferation of connected devices, such as smart home devices, consumer electronics, medical monitors, and connected vehicles, has extended the CIAM perimeter to include device identity management. Open Authorization 2.0 (OAuth2) Device Flow, device allowlisting, ownership transfer workflows, and attribute mapping are required to securely link Internet of Things (IoT) objects with user identities and enforce authorization based on device characteristics.

CIAM is not a standalone capability. Well-documented Representational State Transfer (REST), Graph Query Language (GraphQL), and Webhooks APIs are required. Most customer organizations look for out-of-the-box connectors to platforms such as Customer Relationship Management (CRM), Customer Data Platforms (CDP), Consent and Preference Management (CPM), marketing analytics and automation solutions, Identity Verification (IDV), and Fraud Reduction Intelligence Platforms (FRIP). Innovative solutions have connectors for payment services and chatbot applications. Some vendors offer embedded Software Development Kits (SDKs) and orchestration tools that allow real-time evaluation of identity, behavioral, and environmental signals during authentication and transaction flows.

Scalability is not merely an architectural preference: it is a gating requirement for any CIAM solution operating in consumer contexts. Platforms must be capable of supporting tens of millions to billions of digital identities and processing high-volume transaction loads including login requests, session validation, and consent changes. Major product launches, seasonal e-commerce peaks, and public-sector events can trigger unpredictable surges in usage. To accommodate this, best-in-class CIAM platforms employ elastic cloud infrastructure with global distribution to minimize latency, multi-region failover and replication for resilience, dynamic caching and edge processing, rate-limiting and throttling controls to protect downstream systems, and data partitioning and isolation models in single-tenant and private cloud variants. These capabilities are critical not only for user experience but also for Service Level Agreement (SLA) compliance and regulatory reporting in sectors governed by strict availability and disaster recovery requirements.

The evolving CIAM landscape reflects the broader convergence of identity, security, privacy, and digital experience, delivered in accordance with the Identity Fabric model. Whether supporting millions of consumers or complex B2B relationships, CIAM systems must offer flexible deployment models, advanced authentication and authorization, consent management, and interoperability with customers' broader IT and security ecosystem. Success in CIAM requires more than simply managing credentials or logging events. It requires orchestrating a dynamic fabric of identity relationships, contextual trust signals, regulatory obligations, and consumer expectations.

Product Description

Ory started as an open-source project in 2015. Ory Corp was founded in 2019. The company is headquartered in Scottsdale, Arizona in the US, and is backed by venture capital. The Ory ecosystem consists of Ory Kratos, Ory Hydra, Ory Oathkeeper, Ory Polis, and Ory Keto, which are licensed in packages as Ory open source, Ory Enterprise License (OEL), and Ory Network. Ory secures over two billion reported identities across its open-source, OEL (commercial self-hosted), and Ory Network (cloud) offerings. The platform supports organizations of all sizes, from startups to the largest web-scale enterprises.

The Ory ecosystem is a modular identity and access platform that includes solutions for CIAM and workforce IAM. Its modules can be licensed individually or as packages. **Ory Hydra** is the OAuth2 and OpenID Connect (OIDC) compliant authentication server. **Ory Kratos** handles user management. **Ory Polis** provides identity federation, SSO, and directory synchronization. **Ory Oathkeeper** is an access proxy (that can function as a reverse proxy) and remote Policy Decision Point (PDP) for legacy applications. Lastly, **Ory Keto** is a Google Zanzibar-based authorization server that enables Relationship-based Access Control (ReBAC) and Access Control List (ACL) enforcement; ABAC support is planned for 2026. All modules are available as open source. The **Ory Enterprise License** provides 24/7 support and is priced by daily active user charges. **Ory Network** is their SaaS solution, which also includes an enterprise tier for 24/7 support. It is priced by daily active users and per-token creation charges. Most contracts are per annum, but monthly options are available. Ory Network has achieved ISO 27001 and System and Organization Controls 2 (SOC 2) Type 2 certifications.

The open-source and commercial Ory Enterprise License (OEL) versions of the software can be delivered as a binary and can run on any Linux system. Ory recommends using the containerized version for private clouds and in IaaS installation. Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP) are supported. The solution needs a database, and CockroachDB is recommended, although PostgreSQL and MySQL are also supported. Ory Network runs in a single public IaaS provider in two US data centers, one in western Europe, and one in Asia, which enables data residency for those regions. Multi-tenant SaaS is the default option, but single-tenant options are also present.

Ory Kratos allows customers to define custom attributes. Ory Polis can understand and translate SAML to OAuth2 and OIDC, and Ory Actions allows customers to create Webhooks to send user event information to interoperate with other Identity-as-a-Service (IDaaS) and IAM suites. Ory Polis leverages System for Cross-domain Identity Management (SCIM) and cloud service specific APIs for bulk user import and directory synchronization operations. Ory Polis also provides a self-service admin portal that enables enterprise customers to onboard their organizations, configure SSO integrations, and synchronize user directories without developer involvement.

All modules can be customized by customers for brand consistency. Users can self-register with email addresses, and most major social network logins are accepted for registration. Account creation verification notifications are delivered via SMS. Device information can be stored, but there is no formal device registration workflow yet. Customer organizations can set up multiple registration workflows and define and apply logic for data mapping and normalization with synced accounts. Account recovery options include email magic links and SMS OTP.While Ory does not include built-in identity verification (IDV) or native connectors to third-party services, the platform can be extended through Ory Actions/webhooks. This enables customers to integrate IDV providers and other external systems directly into their identity workflows.

Similarly, governance and lifecycle management capabilities such as duplicate or inactive account discovery, automated account de-provisioning are not built-in features but can be implemented through Ory's API-first design and open ecosystem.

Ory Kratos accepts username/password, email and SMS One-Time Password (OTP), most mobile authenticator apps, and FIDO 2 and passkey authentication methods. Mobile biometrics are not directly supported but are supported if using a third-party mobile authenticator app or FIDO authenticator.

Customers can implement risk-adaptive authentication by integrating external risk signals via Ory Actions/webhooks and enforcing step-up policies accordingly. At present, administrators log in with local credentials to access Ory products and services. Federated authentication for administrative accounts is in the final stages of development and expected to be available soon.

Ory Keto is a relationship-based authorization (ReBAC) engine, designed to serve as the Policy Decision Point (PDP) in distributed systems. It provides APIs for evaluating access control decisions based on defined relationships between subjects, resources, and permissions. Integration with gateways like Kong, Nginx, or Envoy is possible by coding those services to query Keto for authorization decisions.

Ory Oathkeeper is an identity- and access-control proxy that enforces authentication and authorization for incoming HTTP requests. It acts as a reverse proxy, validating identity tokens, performing access checks, and forwarding only authorized traffic to backend services. Oathkeeper integrates seamlessly with other Ory components, such as Ory Kratos for authentication and Ory Keto for authorization. Configuration is defined declaratively through YAML or JSON, enabling automated and consistent policy enforcement across environments.

Connectors for FRIP solutions are not offered, but the platform's extensibility through Ory Actions, Webhooks, and REST APIs allows customers to integrate with any third-party FRIP provider.

Ory provides user self-service portals that allow end users to edit their contact information, reset passwords and other credentials, set communications preferences, set consent and data sharing preferences, request account deactivation (but not deletion), and view and edit full consent history. Consumer level account delegation is not supported at this time; thus, family management is not explicitly possible. Ory does not include prebuilt Data Subject Access Request (DSAR) form templates or automated Terms of Service (ToS) change notifications, but the platform's user interface and schema-driven configuration enable organizations to implement these features. Ory supports flexible data schemas that allow administrators to define custom fields and consent attributes during signup or profile updates, enabling organizations to meet privacy and compliance requirements through tailored workflows. Ory is currently building out-of-the-box connectors for third-party CDP, CPM, or CRM solutions.

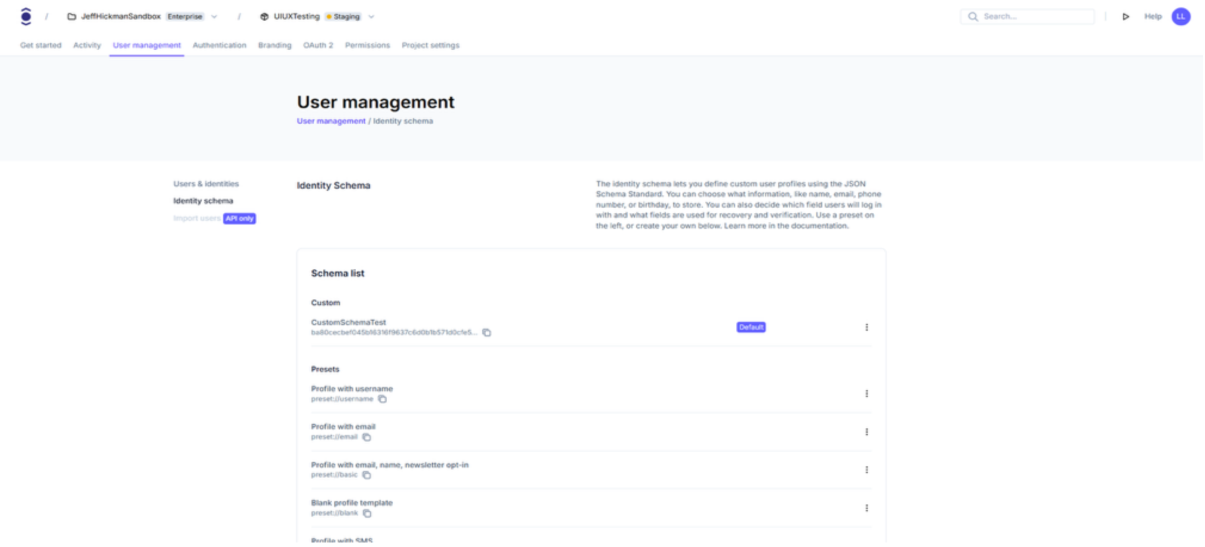
Ory's suite provides many identity analytics features, including the tracking of login success/failure rates, customer profile changes, changes to credentials, ATO attempt indicators, MFA events, consent actions, account recovery actions, administrative changes to platform configurations, and API calls. A customizable widget-based dashboard is available, and although not all the metrics are visible initially, they can be surfaced in searches. Standard reports include user login and sign-up activities, daily active users, and active sessions. The admin interface is designed around the workspace concept. A workspace contains projects that represent either production environments or developer sandboxes. All product modules are operated through a single console that serves as the control plane. Operational visibility centers on sign-ups and logins, presented as primary Key Performance Indicators (KPIs). Each metric links to the underlying event stream for drill-through analysis so teams can trace sequences, inspect payloads, and build timelines. User management provides fast search, record inspection, and edits. Multiple identity schemas can be defined and applied to the project or workspace scope. Customers are not required to use the UI; the platform is API-first, and some key management functions are accessible only via the Command Line Interface (CLI) or REST API.

Ory provides SDKs that make it easy for developers to build and integrate using a wide range of languages and frameworks, including Dart, .NET, Elixir, Go, Java, JavaScript (with Fetch), PHP, Python, React, Ruby, and Rust.

Ory uses horizontal and vertical scaling of workloads, and the spreading of traffic across regions with dynamic load balancing. Ory’s standard SLA for Ory Network guarantees 99.995% uptime, which is above the industry standard.

For B2B CIAM use cases, Ory supports custom individual denylists and federated domain allowlists. Just-in-Time (JIT) account creation via SCIM, SAML, OIDC ID tokens is supported. User accounts can be time-limited. Support for per-customer/partner/contractor authentication and authorization policies is planned for 2026.

Support services are available in English, German, French, and Spanish. Documentation is in English only.



The identity schema lets you define custom user profiles using the JSON Schema Standard. You can choose what information, like name, email, phone number, or birthday, to store. You can also decide which field users will log in with and what fields are used for recovery and verification. Use a preset on the left, or create your own below. Learn more in the documentation.

CustomSchemaTest
ba80cecbef045bf6316f9637c6d0b1b571d0cfe5...

Profile with username
preset://username

Profile with email
preset://email

Profile with email, name, newsletter opt-in
preset://basic

Blank profile template
preset://blank

Profile with SMS

Figure 1: Ory administrative console – user management (provided by Ory)

Strengths and Challenges

Ory’s strength lies in its deployment flexibility and developer accessibility. Organizations can start building at no cost using Ory’s open-source foundation, enabling rapid experimentation and proof-of-concept development. When requirements evolve toward mission-critical deployments, Ory offers commercial solutions that deliver enterprise-grade reliability, advanced security updates, and web-scale performance, ensuring a smooth path from prototype to production.

Ory’s modular, API-first design enables incremental service upgrades rather than “rip-and-replace” migrations, aligning with the Identity Fabric model to make it easier for customers to modernize specific identity services as needed. Ory supports all deployment models from on-premises to full SaaS. Public IaaS-based elastic scaling techniques are employed to manage unpredictable customer demand for its SaaS. Their SaaS has a 99.995% uptime guarantee that surpasses most industry peers. Ory takes an API-first, developer-friendly approach that facilitates integration and customization. Ory has achieved ISO 27001 certification for its commercial solutions, with the Ory Network additionally certified under SOC 2 Type 2. The platform is competitively priced, and the daily active user licensing model helps mitigate the cost volatility often encountered in traditional monthly active user pricing structures. Ory is deployed in regulated industries, supporting environments that require high volumes and high availability.

Ory’s extensible architecture supports emerging AI-driven identity scenarios such as Agent-to-Agent (A2A) and Model Context Protocol (MCP). This allows organizations to securely embed identity and authorization into AI and agentic workflows. Ory is positioned as a business enabler for enterprises building agent-powered digital experiences

Ory is designed for organizations seeking supported open-source CIAM solutions with modular services aligned to the Identity Fabric model. It can be deployed by customers on-premises or in private clouds, and is available as a fully managed service through the Ory Network. Its modular architecture and deployment models allow Ory to address modern CIAM requirements for flexibility, observability, and scalability.

Strengths

- Modular, identity fabrics implementation makes it easier for customers to upgrade services individually
- All deployment models supported, from on-prem to SaaS
- Free, open-source options are available for development and testing.
- Competitive pricing for the managed service
- Uses public IaaS elastic scaling techniques to handle peak customer loads
- OpenTelemetry-based observability enables visibility into system performance and reliability
- Daily Active User licensing model helps alleviate spikes in pricing that some organizations encounter in the more traditional Monthly Active User paradigm
- Developer friendly, API-first platform
- ISO 27001 and SOC 2 Type 2 certifications
- 99.995% uptime guarantee is higher than most competitors

Challenges

- Progressive profiling and device registration not yet available
- No IDV or connectors for third-party IDV services
- Identity lifecycle and governance features have not been implemented
- Device intelligence and behavioral biometrics are not instantiated in the SDKs, but are planned
- Risk-adaptive authentication requires customization through Ory's framework rather than a turnkey feature
- Lacks out-of-the-box integrations for FRIP, CDP, CPM, CRM, and marketing analytics/automation solutions

Related Research

Leadership Compass: Customer Identity and Access Management 2024
Leadership Compass: Customer Identity and Access Management 2022
Buyer's Compass: Customer Identity and Access Management 2024

Buyer’s Compass: Identity Fabrics 2024

Leadership Compass: Identity Fabrics 2025

Blog: A Lean Identity Fabric – Making Identity Understandable

Blog: Identity Fabric 2040: Modular, Orchestrated, Autonomous

About KuppingerCole

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

Copyright

The conclusions, recommendations, and predictions in this document reflect KuppingerCole's initial views. As we gather more information and conduct deeper analysis, the positions presented here may undergo refinements or significant changes. KuppingerCole disclaims all warranties regarding the completeness, accuracy, and adequacy of this information. Although KuppingerCole research documents may discuss legal issues related to information security and technology, we do not provide legal services or advice, and our publications should not be used as such. KuppingerCole assumes no liability for errors or inadequacies in the information contained in this document. Any expressed opinion may change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Their use does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

For further information, please contact clients@kuppingercole.com..