KUPPINGERCOLE ANALYSTS

Customer Identity and Access Management - CIAM

John Tolbert

June 3, 2024

LEADERSHIP COMPASS 2024

This report provides an overview of the Customer Identity and Access Management (CIAM) market and a compass to help you find a solution that best meets your organization's needs. It examines solutions that allow users to register, associate device and other digital identities, authenticate, authorize, collect, and store information about consumers from across many domains and help organizations to comply with privacy regulations. A good CIAM solution can improve the customer experience.

Contents

Executive Summary

The Customer Identity and Access Management (CIAM) market continues to grow and evolve. CIAM is a well-established and innovative branch of the broader IAM field. CIAM solutions are designed to address specific technical requirements that consumer-facing organizations have that differ from traditional “workforce” or business-to-employee (B2E) use cases. CIAM encompasses business-to-consumer (B2C), business-to-business customer (B2B), and government-to-citizen (G2C) use cases and functions.

The main reasons organizations acquire CIAM solutions are to:

- Provide identity management for consumers and customers
- Improve customer experiences through personalization
- Enable stronger authentication and authorization
- Improve defenses against fraud
- Convert unknown users into known users and customers
- Gain insights for targeted marketing
- Increase account acquisitions and revenue and improve retention
- Provide mechanisms to allow users to consent, revoke consent, and/or request deletion in accordance with privacy regulations
- Manage regulatory compliance

CIAM systems allow users to register, associate devices 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 transactions, or for analysis to support marketing campaigns, or Know Your Customer (KYC) and Anti-Money Laundering (AML) regulatory compliance. In B2B customer scenarios, the CIAM systems increasingly need to pull authoritative attribute information from partner, contractor, and customer IAM systems. 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. Privacy regulations and the requirement to collect consent have been a strong driver for CIAM implementations. For example, GDPR took effect in the EU in May of 2018, and CCPA took effect in California in 2020, the need to collect consent from consumers for the use of their data has become mandatory in many jurisdictions. 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 consent.

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. 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 B2B customers, consumers, or citizens to register, manage their user profiles, authenticate, and get authorized for different kinds of resource access. CIAM deploying organizations need dashboards for monitoring utilization, reports on historical activities, and the ability to collect other metrics.

The CIAM market continues to grow in terms of numbers of vendors, numbers of organizations deploying CIAM, and the numbers for consumer engagement. The trend toward 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.

All kinds of organizations buy CIAM solutions: from small-to-medium size businesses to large enterprises and governments agencies. Any organization that needs to interface digitally with consumers, customers, or citizens, whether for-profit or non-profit, can benefit from CIAM. Some solution providers are themselves global businesses, while others are regional specialists. Organizations across most all industries can improve their customer experiences and security with well-implemented CIAM platforms. Moreover, CIAM is useful to the deploying organizations regardless of their longevity, from startups to long-established institutions.

To better understand the fundamental principles this report is based on, please refer to KuppingerCole's Research Methodology.

Key Findings

- Innovation in CIAM requires adherence to industry standards and capabilities to interoperate and integrate with many different and discrete service functions.
- Some of the leading services embrace the Identity Fabrics architecture and deliver IAM and CIAM as flexible microservices.
- CIAM solutions are increasingly catering to B2B customer use cases as well as consumer and citizen use cases. Services that include these features are considered innovative.
- Identity verification (IDV) capabilities, primarily through integration with service providers, are becoming more common across the CIAM market, with 65% of solutions offering IDV connectors.

- Fraud prevention functions and/or connectors to Fraud Reduction Intelligence Platforms (FRIP) are becoming more common due to customer demand and the expanding threat landscape.
- Decentralized Identities (DIDs) are not widely supported by CIAM solutions due to very low demand. Services that include these features are considered innovative.
- Customers increasingly need Identity Governance and Administration (IGA) and identity lifecycle management capabilities within their CIAM systems. Services that include these features are considered innovative.
- Some CIAM solutions are innovating by providing connectors to third-party solutions for Customer Data Platforms (CDPs), payment services, AI chatbot interfaces, and Consent and Privacy Management (CPM) systems. Services that include these features are considered innovative.
- FIDO has gained acceptance, and the use of passkeys is growing, due to their security and convenience.
- Consent and privacy management features are a must, and more advanced solutions provide Data Subject Access Request (DSAR) portals, family management, support Kantara Consent Receipt, and offer integration with third-party Consent and Privacy Management (CPM) solutions.

Market Analysis

Though there are many large software service vendors in this market, the CIAM space is dynamic because we observe new vendors emerging in between the editions of this report, with different specialties and in different regions of the globe.

- The acquisition of Ping Identity and ForgeRock and subsequent combining of the products and services in their portfolio has created a larger entity ostensibly to compete better against the other market leaders.
- Thales' acquisition of OneWelcome expanded their IAM portfolio and makes them a strong contender for market leader.
- SecureAuth's acquisition of Cloudentity improves both their former positions in IAM and CIAM. Cloudentity's prior focus on complex authorization and CIAM should complement the SecureAuth portfolio well.
- Microsoft was in the middle of phasing out Azure AD B2C and preparing for the launch of Entra External ID and was unable to participate in this round.
- Customer organizations have increasing technical expectations for CIAM, which has forced CIAM vendors to develop additional integrations to serve these requirements.
- Though the CIAM market is mature, startups are still able to enter and carve out a niche by focusing on technical innovations and/or addressing particular use cases well.
- Several CIAM solution providers started out and continue to focus on certain geographic regions and language support.
- There are a number specialized CIAM solutions that serve one or a few related industries and have grown to significant size just focusing on those target customers.

- Customer Data Platforms (CDPs) and CIAM systems are still mostly distinct from one another, although integrations between them are more commonly used.
- B2C CIAM vendors are beginning to offer connectors to payment services and AI chatbot interfaces.
- Consumer devices can be managed via some CIAM platforms, and a few of the solution providers serve this important set of use cases well.
- Support for DIDs has not become a deciding factor in CIAM purchases. At present, 27% of vendors surveyed have built-in DID support.
- B2B CIAM use cases require specialization, and demand for these features is growing.

Market Size and Segmentation

Based on our current research the CIAM market size was last estimated at $3.57B with an annual growth rate of 19.9%.

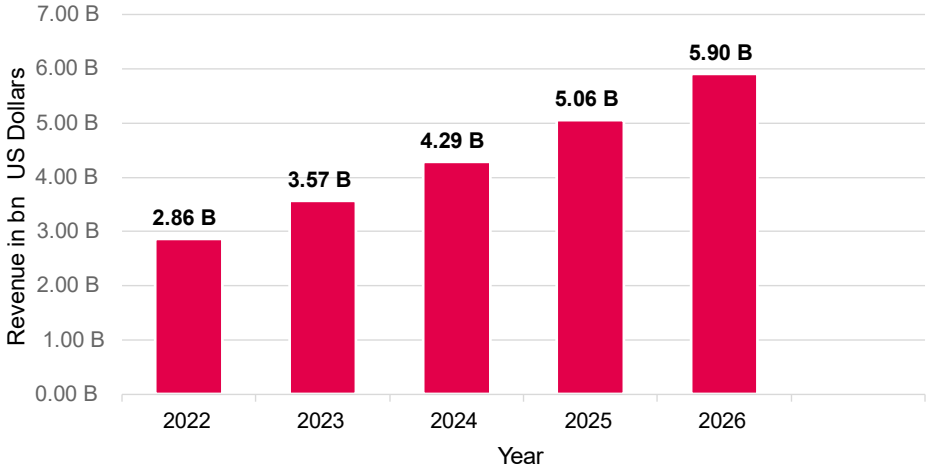


Figure 1: CIAM market size predictions 2022-2026

The CIAM field is segmented in multiple ways. Historically, the “C” in CIAM was generally assumed to stand for consumers. CIAM first evolved to meet the demands that consumer-facing applications have that are functionally different from workforce/enterprise IAM. These are still the largest types of use cases that CIAM solutions cater to. However, CIAM systems have been adapting to B2B customer scenarios as well. Some vendors report that the B2B CIAM segment is growing faster than pure B2C implementations. Moreover, with the many organizations shifting to the Identity Fabrics model, it is necessary that CIAM solutions address both B2B and B2C use cases equally well. This means there will be a greater need for more integrations with identity verification services, Fraud Reduction Intelligence Platforms (FRIP), and SaaS applications like CRM, CDPs, payments services and financial applications, and others.

CIAM is also segmented geographically in some cases. Newer entrants into the field tend to focus on the legal, regulatory, and business requirements in specific regions. We see this

especially in the EU where CIAM vendors leverage support for eIDAS/national IDs and provide more fine-grained consent collection and management options.

We also observe that some CIAM solutions tend to focus on and therefore be more strongly aligned functionally with certain industries. Examples here include those that emphasize support for finance and banking, insurance, media, retail and ecommerce, and healthcare.

Delivery Models

Most CIAM solutions are delivered as SaaS, and this delivery model is likely to continue growing. Some vendors provide both SaaS as well as customer deployable software. A significant number of SaaS vendors provide single-tenant options, where the vendor spins up and runs dedicated instances for each customer. This maximizes logical separation and data privacy and security. Single tenant SaaS options are generally more expensive than paying for service within their multi-tenant infrastructure. For most cases where the vendor solutions are implemented and maintained by customers, the software is delivered such that it can be deployed on-premises or in private clouds.

To accommodate the various deployment methods, many of the vendors in this space have moved to the microservices-based Identity Fabrics service delivery model.

The most common licensing model in CIAM delivered as SaaS is per-user per-month, specifically Monthly Active Users (MAUs). Some solutions charge per registered monthly user and per-feature or per-application. For on-prem solutions, standard licensing mechanisms are per-server, per-VM, and generally include blocks of users for additional fees. A few CIAM solutions have more convoluted licensing schemes, which tends to lower perceived usability. A small number of vendors charge fixed rates, which could be advantageous for their customers.

Required Capabilities

These are the capabilities that KuppingerCole views as foundational for CIAM:

- Flexible deployment (SaaS, in PaaS/IaaS, hybrid, on-premises).
- Micro-services architecture.
- Self-registration; social login registration; bulk user import facilities.
- User dashboards for credential, device, user profile and consent management.
- Secure account recovery mechanisms (excluding security questions).
- Multi-factor 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, if no SDK, then well-documented APIs for easier integration.
- Orchestration for onboarding, authentication, and maintenance workflows; inclusive of third-party services.
- Integrated compromised credential intelligence.

- 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.
- Support for all major Identity Federation standards, including SAML, OAuth, OIDC, and JWT.
- Support for Single Sign-On (SSO) between all related customer properties and brands.
- APIs and connectors for marketing analytics and automation, CRMs, and other SaaS apps.
- Identity proofing functions and/or integration with third-party identity proofing services.
- Integrations with Fraud Reduction Intelligence Platforms.
- Integrations with customer SIEMs.
- ITSM integration.
- Collection and presentation of identity analytics.
- Reports & dashboards for CIAM system metrics.
- Data localization/residency for privacy regulatory compliance.
- Reports and support for privacy regulation compliance audits.

Features that are innovative and up-and-coming include:

- Integrations for payment services and chatbots.
- Integration with third-party Customer Data Platforms (CDPs) and Consent and Privacy Management solutions (CPMs)
- Single tenant SaaS options.
- Multi-cloud deployments.
- Low-code/no-code administration.
- DID, eID, and digital wallet support.
- Mobile apps for remote onboarding.
- Flowchart style onboarding process and authentication policy definition.
- Advanced identity governance and lifecycle management, such as duplicate account detection and merging options, and identification and processing of inactive accounts.
- B2B CIAM use case support, including delegated administration, attribute-based access controls (ABAC), compliance checks and sanctions screening, compromised credential detection, per-customer communications channels, per-application Terms of Service (ToS) display, customizable consent options, dedicated per-customer management portals, custom roles and entitlements, and time-limited accounts.

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 shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of 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

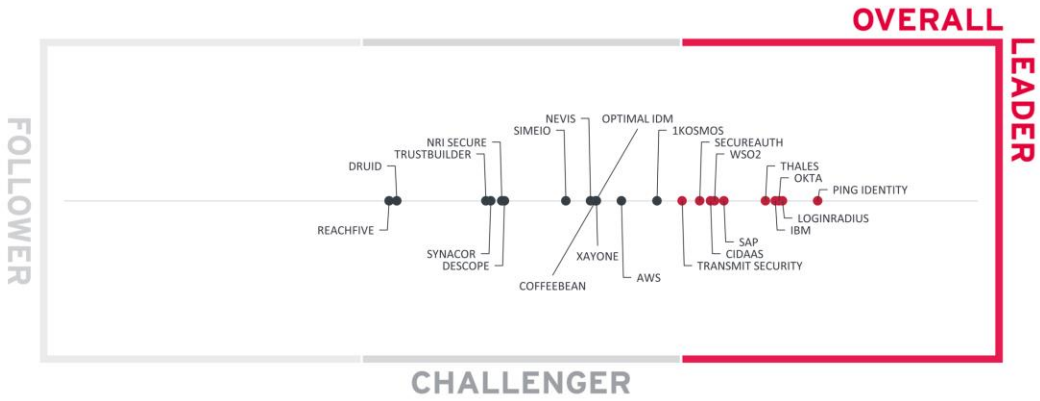


Figure 2: Overall Leadership in the CIAM market

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 from each other 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 which of your use cases they support best.

Ping Identity is in front in the Overall Leaders. The representation of “Ping Identity” on these charts includes both pre-merger Ping Identity and ForgeRock offerings. LoginRadius, Okta, IBM, SAP, Transmit Security, and WSO2 retain leadership status as they continue to improve their products and attract customers. The acquisition of OneWelcome by Thales has improved their chart position since the last Leadership Compass edition, reflecting not only product enhancements but also greater market reach. Strong innovation and successfully executing on their product roadmap has pushed cidaas into the Overall Leader area this year. SecureAuth, with the former Cloudentity, appears as an Overall Leader. This pairing of

IAM and CIAM vendors will result in greater opportunities for SecureAuth going forward as well.

1Kosmos is on the verge of Overall Leadership. Amazon Cognito debuts as a top Challenger in this report. Optimal IdM, XAYONE, CoffeeBean, Nevis, and Simeio are also approaching the leadership threshold. Descope, NRI Secure, Synacor, TrustBuilder, DruID, and ReachFive round out the list of Overall Challengers.

Overall Leaders are (in alphabetical order):

- cidaas
- IBM
- LoginRadius
- Okta
- Ping Identity
- SAP
- SecureAuth
- 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 3: Product Leadership in the CIAM market

In this 2024 edition of the Leadership Compass on CIAM, Ping Identity and Login Radius top the list for Product Leadership. Thales, IBM, Okta, cidaas, SecureAuth, WSO2, and 1Kosmos are in close proximity far above the Leadership threshold. Nevis, SAP, CoffeeBean Technology, and Transmit Security are all north of the dividing line between challengers and leaders here. These solutions are the most complete in terms of functionality, internal product security, deployment options, interoperability, usability, and integrations available.

XAYONE, Optimal IdM, Descope, AWS, and Simeio are at the top of the challengers for Product Leadership. TrustBuilder, NRI Secure, Synacor, DruID, and ReachFive are in the middle of the Challenger pack. The challengers need to add features and functions as will be elaborated upon in this report.

Product Leaders (in alphabetical order):

- 1Kosmos
- cidaas
- CoffeeBean Technology
- IBM
- LoginRadius
- Nevis
- Okta
- Ping Identity
- SAP
- 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.

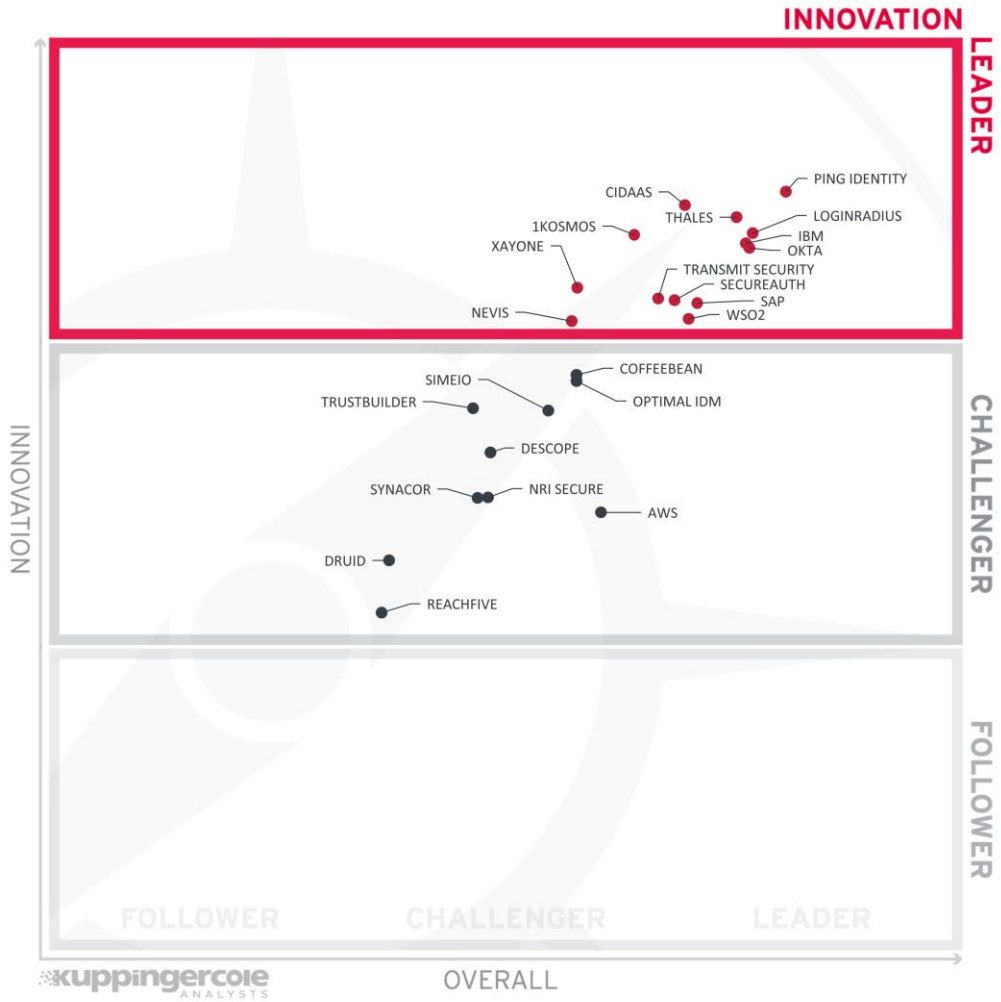


Figure 4: Innovation Leadership in the CIAM market

Innovation Leaders are those vendors that are delivering transformational 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.

Ping Identity, cidaas, Thales, 1Kosmos, LoginRadius, IBM, and Okta form the uppermost tier of Innovation Leaders in CIAM. XAYONE, Transmit Security, SecureAuth, SAP, WSO2, and Nevis are also in the Innovation Leader area, each offering advanced capabilities that appeal to deploying organizations.

CoffeeBean, Optimal IdM, TrustBuilder, and Simeio are the top Challengers in Innovation, exhibiting significant advancements but slightly behind those above. Next, we find Descope, NRI Secure, Synacor, and AWS, followed by DruID, and ReachFive. Each of these vendors have specific innovations, likely targeted at their existing customer base.

Innovation Leaders (in alphabetical order):

- 1Kosmos
- cidaas
- IBM
- LoginRadius
- Nevis
- Okta
- Ping Identity
- SAP
- 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 transactions evaluated, the ratio between customers and managed identities/devices, 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.

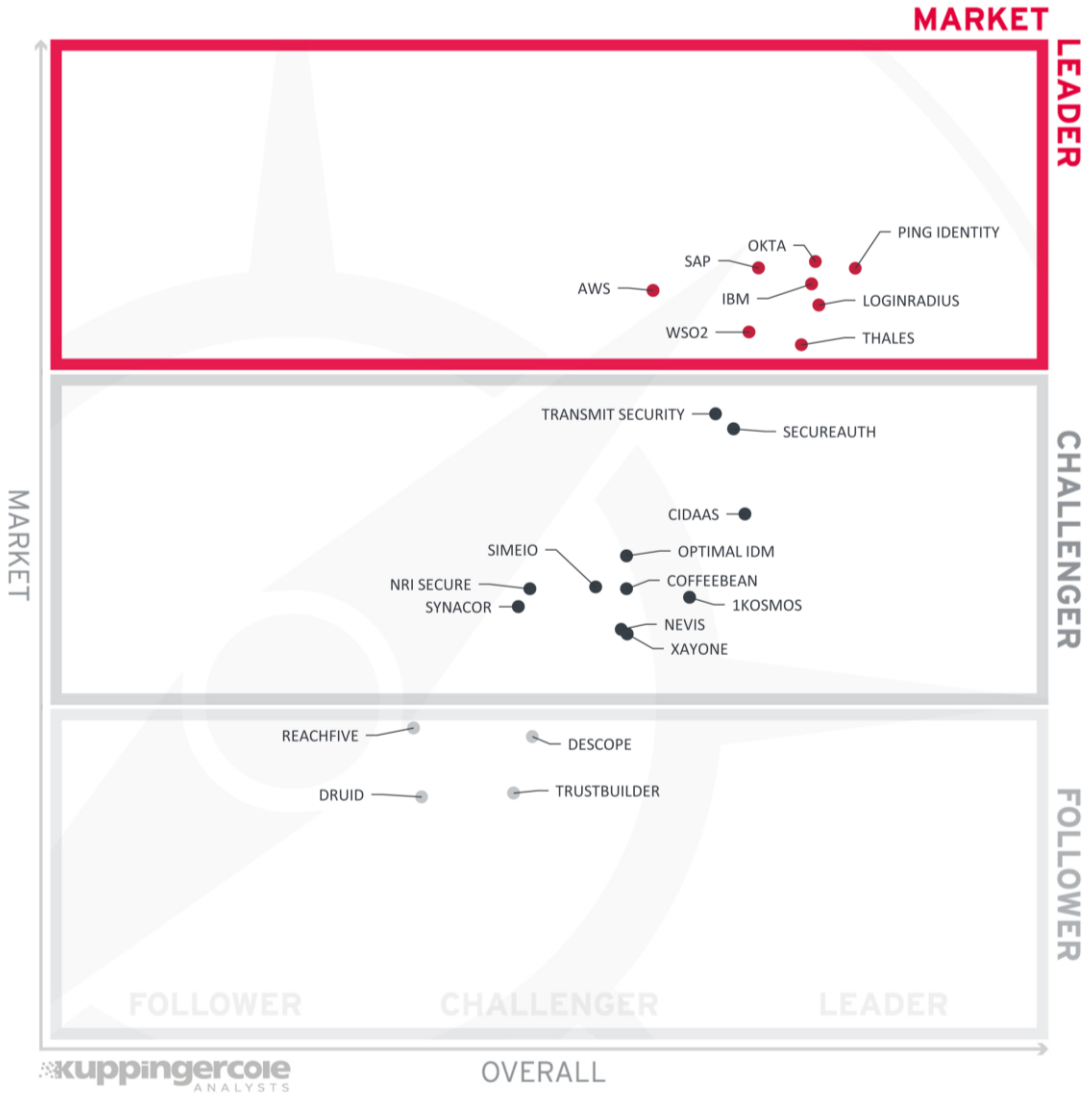


Figure 5: Market Leaders in the CIAM Market

The CIAM Market Leaders are companies with global sales and support operations. AWS, IBM, and SAP are large IT vendors with a huge catalog of other products, and their CIAM offerings are often the front door for other parts of their portfolios. Okta, Ping Identity, and WSO2 are growing their CIAM as well their long-established IAM/IDaaS products. LoginRadius is the largest pure CIAM specialist in this group. Thales' addition of OneWelcome has enabled them to move into CIAM alongside their high-security IAM and related products.

Transmit Security continues to move up toward CIAM market leadership. SecureAuth (now with Cloudentity) is also positioned near the top of the challengers in market. cidaas has made some gains in market share. Optimal IdM, Simeio, CoffeeBean, NRI Secure, 1Kosmos, Synacor, Nevis, and XAYONE are also challengers in the CIAM space.

ReachFive, Descope, TrustBuilder, and DruID are all coming closer to challenger status. Each of these vendors is geographically limited but they have a lot of room for growth.

Market Leaders (in alphabetical order):

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

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this Leadership Compass. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name

Vendor	Security	Functionality	Deployment	Interoperability	Usability
1Kosmos	Strong Positive	Positive	Strong Positive	Positive	Strong Positive
AWS	Strong Positive	Neutral	Strong Positive	Neutral	Positive
cidaas	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
CoffeeBean	Positive	Positive	Positive	Positive	Positive
Descope	Positive	Neutral	Neutral	Neutral	Positive
DruID	Positive	Neutral	Neutral	Weak	Neutral
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
LoginRadius	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Nevis	Strong Positive	Positive	Positive	Neutral	Strong Positive
NRI Secure	Neutral	Neutral	Neutral	Neutral	Neutral
Okta	Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Optimal IdM	Positive	Neutral	Neutral	Neutral	Positive
Ping Identity	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
ReachFive	Positive	Weak	Neutral	Neutral	Neutral
SAP	Strong Positive	Positive	Strong Positive	Positive	Positive

SecureAuth	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Simeio	Strong Positive	Positive	Positive	Neutral	Strong Positive
Synacor	Positive	Neutral	Neutral	Neutral	Positive
Thales	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Transmit Security	Strong Positive	Positive	Strong Positive	Positive	Strong Positive
TrustBuilder	Positive	Neutral	Weak	Neutral	Positive
WSO2	Strong Positive	Positive	Strong Positive	Strong Positive	Strong Positive
XAYONE	Strong Positive	Positive	Positive	Positive	Positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
1Kosmos	Strong Positive	Neutral	Neutral	Neutral
AWS	Neutral	Strong Positive	Strong Positive	Strong Positive
cidaas	Strong Positive	Neutral	Neutral	Weak
CoffeeBean	Positive	Neutral	Neutral	Neutral
Descope	Positive	Weak	Neutral	Weak
DruID	Neutral	Weak	Weak	Weak
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive
LoginRadius	Strong Positive	Strong Positive	Positive	Strong Positive
Nevis	Strong Positive	Neutral	Neutral	Weak
NRI Secure	Neutral	Neutral	Positive	Weak
Okta	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Optimal IdM	Positive	Positive	Positive	Neutral
Ping Identity	Strong Positive	Strong Positive	Strong Positive	Strong Positive
ReachFive	Neutral	Weak	Weak	Weak
SAP	Strong Positive	Strong Positive	Strong Positive	Strong Positive
SecureAuth	Strong Positive	Neutral	Neutral	Neutral
Simeio	Positive	Neutral	Positive	Positive
Synacor	Neutral	Neutral	Positive	Weak
Thales	Strong Positive	Positive	Strong Positive	Strong Positive
Transmit Security	Strong Positive	Positive	Positive	Positive
TrustBuilder	Positive	Weak	Neutral	Weak
WSO2	Strong Positive	Positive	Positive	Strong Positive
XAYONE	Strong Positive	Weak	Neutral	Weak

Table 2: Comparative overview of the ratings for vendors

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, the presence of modifiable templates, the ability to customize workflows, and account recovery options.

Identity assurance – capabilities in this category provide Account Opening (AO) fraud reduction and AML/KYC compliance features. Identity assurance is facilitated primarily by API level interoperability with third-party identity proofing services and by remote onboarding applications (mobile and web-based) that perform selfie-to-ID photo matching, validation of authoritative documents, and issuance of digital credentials.

Authentication – this rubric measures the variety and usefulness of authentication methods present within each solution. Almost all CIAM solutions support username/password and various OTP methods. MFA is a leading mechanism to prevent ATOs. Passwordless authentication improves usability and security. Risk-based analysis of authentication context, including subject and environmental attributes, credential and device intelligence, user behavioral analysis, and behavioral biometrics can improve login and transaction security while reducing the need for obtrusive “login” actions. Many CIAM solutions have mobile and web SDKs that facilitate customer development of applications that integrate with CIAM authentication and risk analysis service. MFA and risk-adaptive authentication are required for EU PSD2 use cases. MFA, passwordless, and risk-adaptive authentication techniques that are supported by each vendor will be called out in the entries below.

Administration – this category evaluates the presence of functions that aid customers in administering the CIAM solution. This includes functions for identity governance and lifecycle management as well as B2B CIAM use cases that require complex delegated administration and dedicated consoles and reports.

Consent management – this rubric covers the facilities within the vendor solution’s UI that allow consumers 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 requested. Family management functions are considered here as well. Kantara Consent Receipt is a standard that promotes interoperability in consent collection and management.

IoT device management – this category reviews the functionality within CIAM platforms that allow consumers to register, activate, authorize, and monitor usage of home automation and entertainment, wearable IoT devices, connected cars, etc., by associating consumer identity with device identities. The use of the OAuth2 Device Flow specification is a good first step to achieve this.

Identity analytics - 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, etc. 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 Security Incident and Event Monitoring (SIEM) systems via CEF, REST API, or syslog.

Marketing integration – harvesting consumer data for marketing purposes is a key driver for the adoption of CIAM solutions. Some CIAM platforms provide built-in marketing analytics, but most make the data they can obtain available to third-party data analytics, CRM, and marketing automation services via APIs and dedicated connectors. This category rates the types of APIs available of each CIAM platform and availability of pre-packaged “integrations” (connectors) for external marketing analytics and automation services.

1Kosmos – BlockID Customer

1Kosmos was founded in 2018 and is headquartered in New Jersey. The company is VC funded and profitable. Most customers are in North America, but they have some operations in the APAC region. They address the consumer and workforce identity management markets with blockchain ID solutions. BlockID Customer is their CIAM offering, and BlockID Verify handles identity proofing and KYC. Beyond providing consumer authentication, 1Kosmos is a decentralized identity (DID) and distributed identity attribute aggregator. 1Kosmos' solutions are hosted as SaaS across multiple public IaaS data centers in multiple regions. It is primarily multi-tenant, but customers can select single tenant options. They have simplified their licensing options to just per-user.

LDAP user stores are supported. BlockID has its own no-SQL database directory that can support multiple data types in consumer profiles. It offers integrations with many IAM and IDaaS solutions. Users can self-register and most social network credentials are accepted. As implied by their name, 1Kosmos supports DIDs. User journeys can be customized in the AdminX GUI. Device registration includes SIM binding options. Consumers can manage their profiles via their digital wallets. BlockID allows account recovery via their LiveID. It does not have any account lifecycle management capabilities.

BlockID Customer has its own app for strong/MFA and identity verification which leverages their own LiveID biometrics scanning technology, which includes liveness detection. 1Kosmos also accepts email/phone/SMS OTP, mobile push, other authentication apps, and FIDO 2.0 authenticators. SAML, OAuth2, OIDC, and JWT can be used for federation. They offer SDKs for iOS, Android, JavaScript, and Node.js, which can harvest the most common device intelligence attributes. BioCatch is their partner, and customers can add on their behavioral biometrics if desired. Customers can craft granular risk-based authentication policies in the no-code flow-chart style interface.

In addition to their own identity verification, 1Kosmos BlockID Verify and LiveID, 1Kosmos can integrate third-party identity verification service providers including AAMVA, Amazon Cognito, Daon, LexisNexis, OneSpan, Ping Identity, and ZenKey. 1Kosmos leverages internal credential intelligence to help prevent ATOs and they provide this information to partners via API. BlockID has connectors for FRIP solutions such as Amazon Fraud Detector, BioCatch, Broadcom, Deduce, Equifax, Experian, ID Data Web, LexisNexis, OneSpan, Outseer, Ping Identity, Telesign, and TransUnion. 1Kosmos API support includes REST, Webhooks, WebSockets, and WebAuthn.

For consent management, 1Kosmos BlockID Customer enables users to control privacy and approve consent requests, and view and approve or reject sharing their data. All personally identifiable information (PII) is encrypted. Only the user has access to their data, not 1Kosmos nor their customer. Data Subject Access Request (DSAR) templates are also available. It supports the Kantara Consent Receipt specification. Family management is not currently supported, and integrations with external Consent and Privacy Management solutions are not available. 1Kosmos supports OAuth2 Device Flow but does not provide IoT device identity management. 1Kosmos has all the standard identity analytics report types and can export audit log data. However, it does not have connectors for CRM, marketing automation, payment services, chatbots, CDP, or some other common SaaS apps.

1Kosmos BlockID Customer can be used for B2B CIAM, and includes features for checking PEP and sanctions lists, custom deny lists, compromised credential checks, delegated administration, B2B portals, per-customer communications channels, and dedicated dashboards.

1Kosmos BlockID Customer uses role-based access controls and interoperates with SIEM solutions. 1Kosmos is NIST CSP IAL2 certified by Kantara and is also certified to UK DIATF specifications. They also have achieved FIDO, ISO 27001, and SOC 2 Type 2 certification. Additionally, their biometrics have been tested by iBeta and certified to DEA EPCS and ISO/IEC 30107-3 standards. They can provide incident response assistance if needed but this is not part of their standard offering. 1Kosmos is focused on identity assurance and strong authentication but does not have integrations with CRMs, CDPs, and marketing products. 1Kosmos is also a Product and Innovation Leader in Access Management. Thus, organizations looking for strong identity verification functions that are built-in to the CIAM platform as well as modern MFA should consider what 1Kosmos BlockID Customer has to offer.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 3: 1Kosmos' rating

Strengths

- Built-in NIST IAL2 certified identity verification app with liveness detection.
- Excellent support for decentralized identities.
- FIDO 2.0 certified.
- Good range of other authenticators accepted.
- Mobile SDKs pick up common device intel attributes.
- Long list of FRIP integrations available.
- Detailed consent management.
- Includes B2B CIAM features for managing complex relationships.
- Interoperates with many IAM and IDaaS solutions.

Challenges

- No identity governance and lifecycle management features.
- Family management is not available yet.
- Lacks integration with third-party Consent and Privacy Management products.
- No IoT device identity management.
- Does not have connectors for CRM and marketing tools.

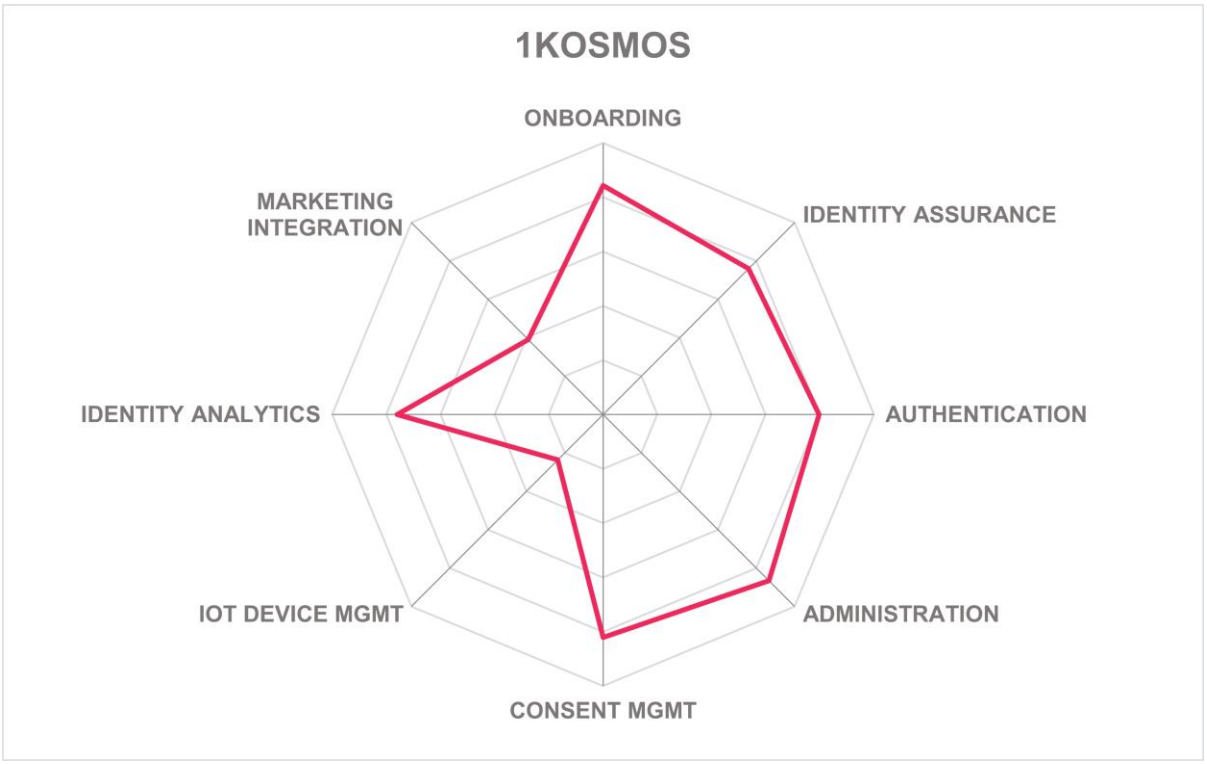
Leader in

OVERALL
LEADER


PRODUCT
LEADER


INNOVATION
LEADER

MARKET
LEADER


1KOSMOS
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

AWS – Amazon Cognito

Amazon Web Services (AWS) was founded in 2006 as a subsidiary of Amazon.com, Inc., aiming to provide cloud computing platforms and APIs to individuals, companies, and governments. Its global headquarters is in Seattle, WA, USA. AWS offers a broad array of services, including compute power, storage options, networking, database management, and security services, such as data encryption and identity and access management, catering to a wide array of IT requirements for customers around the globe. Amazon's CIAM offering is Amazon Cognito. AWS is the world's leading cloud service provider. Cognito is hosted across twenty-nine regional data centers of their infrastructure. Licensing is based on numbers of monthly active users (MAU).

AWS supports user import using its SDKs and from .csv files but not over LDAP or SCIM. Self-registration is available. Some social network credentials can be used for registration. DIDs can be accepted if third-party solutions are in place. The onboarding can be customized leveraging serverless Lambda functions that can be dragged and dropped into the workflow studio in Application Composer. Users can register their devices. Users can manage their passwords, tokens, and attributes in a dedicated UI. Cognito can integrate with 1Kosmos and Transmit Security IDaaS platforms. Account recovery options are limited to email and SMS OTP. Cognito can identify and merge duplicate user accounts, but automatic keepalive messages and de-provisioning are not directly supported.

Amazon Cognito accepts email and SMS OTP, any major TOTP authenticator apps, Android and iOS biometrics, and FIDO 2/WebAuthn/Passkeys. SAML, OIDC, and JWT tokens can be processed for federated authentication. Their Amplify mobile SDK collects basic device intel. Additional attributes can be harvested but doing so requires coding. Behavioral biometrics are not part of the Cognito offering, although contextual behavioral analysis informs the risk-adaptive engine.

Identity verification is only available via third-party integrations, such as itsme. For credential intelligence, Amazon Cognito Advanced Security Features (ASF) are available for an additional cost. Amazon Cognito ASF uses a non-public proprietary compromised credential database. Amazon Fraud Detector can be used for FRIP, and Amazon Cognito also has integrations with F5, Imperva, and Transmit Security. Other third-party WAF connections can also be configured using lambda extensions or proxy integrations, which require coding by the customer. Additional services can be integrated using their REST, CLI, .NET, Java, JavaScript, Python, and Ruby APIs.

Consent management is lacking and there are no out-of-the-box connectors for external consent and privacy management solutions. AWS IoT can leverage Cognito as an authentication provider through their SDKs, but full device identity management is currently not offered in Cognito. Adjacent product AWS WAF can distinguish between malicious and consumer bots. All identity-related actions can be monitored and/or exported via AWS CloudTrail and CloudWatch, although the configuration process is labor intensive, and it does not adhere to any standard CRM formats. There are no pre-built connectors for CRM, marketing automation, CDPs, payment service providers, or chatbot service providers.

B2B CIAM features are not present but could be customized and coded. Role-based access controls are supported, but delegated administration would need to be built using their SDKs. Security logs can be passed to SIEMs using syslog. AWS has many security certifications, including ISO 27001, SOC 2 Type 1/2/3, PCI-DSS, HIPAA, FINMA, US DOD CC SRG, and US FedRAMP. Organizations looking for basic CIAM functionality with excellent security, high performance, and virtually unlimited scalability may want to consider Amazon Cognito.

Security	Strong Positive
Functionality	Neutral
Deployment	Strong Positive
Interoperability	Neutral
Usability	Positive

Table 4: AWS' rating

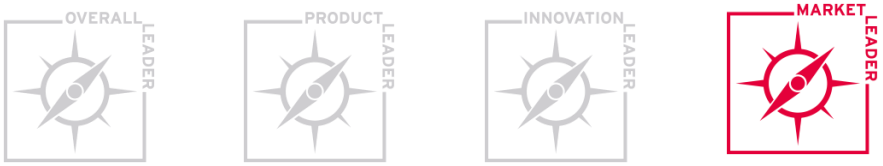
Strengths

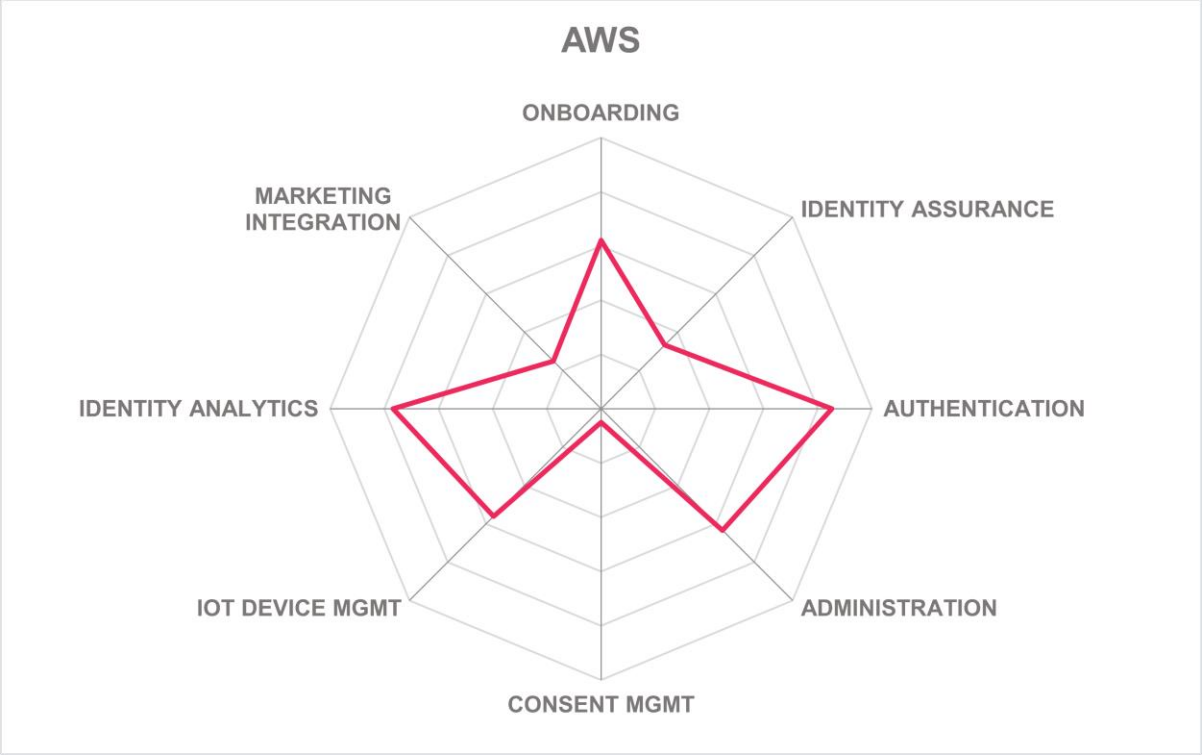
- Massive scalability and high performance for all global regions.
- Excellent admin UI for setting up onboarding workflows.
- Extensive list of security certifications.
- Accepts FIDO 2/WebAuthn/Passkeys.
- Great API exposure and documentation enable extensibility.

Challenges

- Does not support migrations using LDAP or SCIM.
- Missing some account recovery techniques.
- Limited device intel; no behavioral biometrics options for authentication.
- Lack consent management and connectors for CPM solutions.
- Full device identity management is not available.
- Identity analytics requires AWS CloudTrail and/or CloudWatch.
- No integrations with CDP, CRM, or marketing automation solutions.
- Does not directly support delegated administration; customization required.

Leader in




AWS
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

cidaas – cidaas

Widas, a private company, was founded in Germany in 1997, and 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 hosted primarily as SaaS. Their SaaS is hosted in multiple public IaaS providers and their own facilities. Their hosted service is globally distributed for high availability and scalability. Licensing/subscription options include pricing for monthly active or registered users, or by feature sets with blocks of users included.

LDAP, SCIM, and custom APIs are available for migrating users from other directories. User data can be mapped and normalized during migrations. Self-registration and social network registration from all OIDC compliant identity providers is supported. Customers can use DIDs, although the W3C DID specification is not supported. cidaas runs on NoSQL databases that enable storage of complex, non-standard customer data profiles if needed. It can interoperate with Microsoft Active Directory and Azure Active Directory. User and device registration workflows can be customized. All common account recovery methods are supported. cidaas enables customer identity lifecycle management, including account de-duplication and the ability to set different criteria for sending keepalive messages and automatic deprovisioning.

Many authenticator types are supported, including email/phone/SMS OTP, mobile push notifications, Google and Microsoft authenticators, Android and iOS biometrics, and any FIDO compliant solution. The cidaas mobile authenticator app offers its own facial and voice recognition biometrics as well. JWT, OAuth2, OIDC, and SAML tokens are accepted for identity federation. cidaas provides SDKs that enable customization of the registration and authentication experience, and most of the common device intelligence attributes can be evaluated. Passive biometrics are limited to keyboard and mouse usage analysis via JavaScript. Customers can set up authentication policies in the flow chart style interface. Risk factors are configurable, but most customers use the defaults which rely on ML detection of anomalous behavior.

cidaas has a mobile ID verification app, which is an eIDAS compliant Auto Ident solution that does remote onboarding for clients. It can also be used for authentication. Users scan their government-issued ID documents, such as passports, national IDs, and driver's licenses, and then it performs uses facial recognition against selfie photos (with liveness detection) to validate the user. cidaas does not have integrations with third-party IDV service providers, but customers can configure connections via Webhooks. cidaas leverages in-network credential intelligence with their Fraud Detection System. Connectors for third-party FRIP services are planned to be available in their upcoming cidaas marketplace. In addition to Webhooks, cidaas supports REST, WebSockets, WebAuthn, and GraphQL API types.

cidaas has full-featured consent and privacy management with granular options for handling attributes and account deletion requests. Family management is implemented, allowing parents to control kids' access to streaming services. Advanced family management use cases such as sharing hotel, theme park, and event ticket access are configurable. It

supports Kantara Consent Receipt. cidaas accommodates leading-edge IoT device identity management scenarios such as home automation and consumer electronics and provides geo-fencing options for event management. The platform provides a range of identity analytics reports and has connectors for third-party CRM, marketing automation, and other SaaS apps that can be easily configured in “cnips”, their low-code Integration Platform-as-a-Service. cidaas innovatively offers integrations with payment service providers such as Billwerk, Chargebee, and Stripe.

cidaas is used for B2B CIAM and supports hierarchical delegated administrative schemes, per-organizational customer authentication and authorization policies, and per-customer reports. cidaas supports both RBAC and ABAC and has obtained ISO 27001 certification. It can send CIAM event data to SIEM systems. They provide initial setup and incident response services if needed. cidaas is best known in the DACH region of Europe, but their CIAM solution is world-class. Any organization that is looking for CIAM should have cidaas on their shortlist.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 5: cidaas’ rating

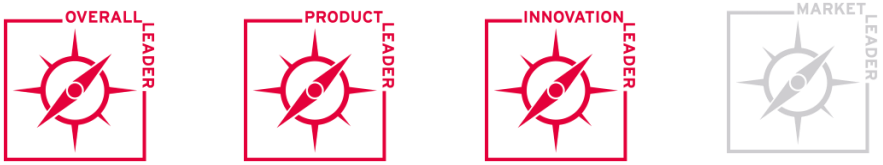
Strengths

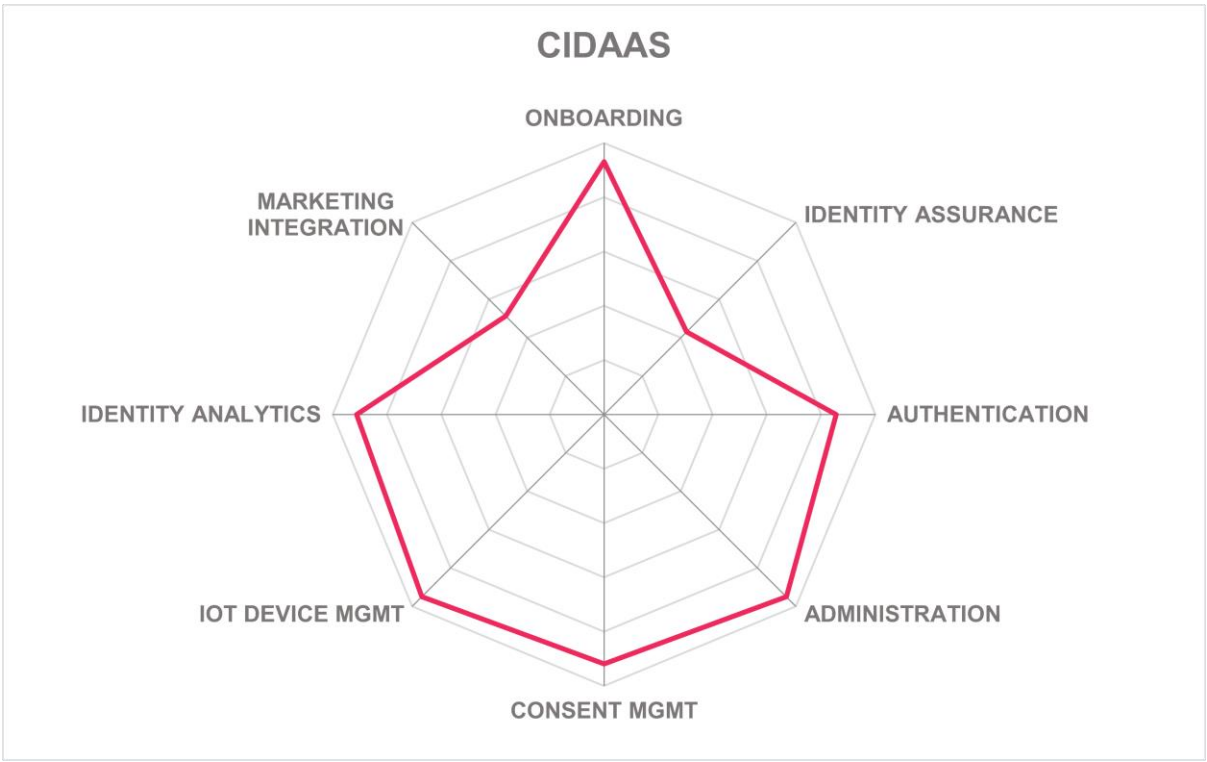
- eIDAS compliant identity verification app included
- Good range of MFA options available including FIDO passkeys and mobile SDK for customer app development
- Robust consent and privacy management
- Granular family management capabilities for advanced use cases such as streaming service subscriptions and physical access controls
- Integrations with some payment service providers
- Features for B2B CIAM relationship management
- New cnips facility is a low-code/no-code Integration Platform-as-a-Service (IPaaS) interface

Challenges

- Limited use of behavioral biometrics
- Additional service hosting options would be beneficial
- Most of their customers are in the DACH region, but they are expanding

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


CIDAAS
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

CoffeeBean Technology – Identity Platform

CoffeeBean Technology was founded in 2008 in the San Francisco Bay area and have operations in Germany and a large development center in Brazil. They have customers in all three regions though most are in Latin America. The company is privately held. CoffeeBean focuses on helping customers realize ROI via marketing integrations, captive Wi-Fi portal integration, and improving consumer identity security. CoffeeBean can be installed on Linux for on-premises deployments, or in Amazon, Azure, or Oracle Cloud IaaS. Most customers use their SaaS, which is hosted in multiple regions of a public IaaS provider. Subscription fees are per active or registered monthly user, and fixed cost options are available.

Users can be migrated over LDAP or SCIM. Decentralized identities are supported, as are all major OIDC-based social network credentials. CoffeeBean has registration-as-a-service and onboarding workflows can be customized in a new visually intuitive drag-and-drop workflow interface. Users can register their devices. Their backend databases can accept complex data types for consumer profiles, and they are compatible with IBM, Microsoft AD and AAD, and Oracle IAM systems. The solution offers user self-service portals for attribute and consent management. A wide range of account recovery mechanisms can be used. CoffeeBean has identity lifecycle management features such as detecting, de-duplicating, and merging similar accounts with proper security controls; the ability to send “keepalive” messages, and options to automatically suspend or delete accounts after configurable time periods.

CoffeeBean accepts an impressive array of authenticators, including all the major apps, FIDO 2 and passkeys, and Google Titan and YubiKey tokens. JWT, OAuth2, OIDC, and SAML support enables identity federation. They offer a mobile SDK that allows customers to leverage their authentication services within their own apps. It facilitates collection and evaluation of the most common device intel characteristics, as well as a subset of behavioral biometrics modalities. CoffeeBean supports risk-based authentication, but the risk engine can be modified only via configuration files.

CoffeeBean does not have identity verification features, and there are no out-of-the-box connectors to third-party services. They report that customers do routinely connect to them via APIs, however. The platform uses in-network plus third-party services like Have I Been Pwned for compromised credential intelligence. They have connectors for Experian and Kaspersky FRIP services. REST, Webhooks, WebSockets, and WebAuthn API types are supported.

CoffeeBean has a good range of consent management features to help customers comply with CCPA, GDPR, and LGPD, including the presentation of DSAR portals. Family management is not provided. There are connectors for OneTrust, SAP, and Twilio Segment as external CPM solutions. It does not manage consumer device identities. On the plus side, CoffeeBean has engagement plug-ins for mobile apps and Wi-Fi captive portal features such as ad and content management. Retailers and facilities operators can use these Wi-Fi captive portal features to interact with consumers in real-time, both when they are online or are in customer facilities such as shopping malls, airports, and restaurants. The platform provides good reports on identity analytics and has integrations for CRM and marketing tools

including Adobe Analytics, Amazon SES, BigCommerce, Facebook Advertising, Freshsales, Google Analytics / Marketing Platform / Tag Manager, HubSpot, IBM Campaign. Mailchimp, Magento, Microsoft Dynamics, Salesforce, SendGrid, Tableau, and more. It does not currently have connectors for CDPs.

CoffeeBean has a few features for B2B CIAM, such as the ability to grant time-limited accounts, discrete application control, and per-customer organization reports. CoffeeBean is ISO 27001 and SOC 2 Type 2 certified. Customers can plumb CoffeeBean event information into their SIEMs via syslog. CoffeeBean provides initial setup and incident response services if customers need it. CoffeeBean reports comparatively quick implementations for customers. They are strong in the Latin American market and are continuing to grow in North America and Europe. CoffeeBean still needs to add consumer IoT device identity management and could use additional connectors for third-party solutions. CoffeeBean has a good platform with differentiating features in identity governance and lifecycle management as well as dedicated functions for customers in the education, retail, and hospitality industries. Organizations looking for these types of capabilities should look at CoffeeBean's solution in more detail, regardless of their geography.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 6: CoffeeBean Technology's rating

Strengths

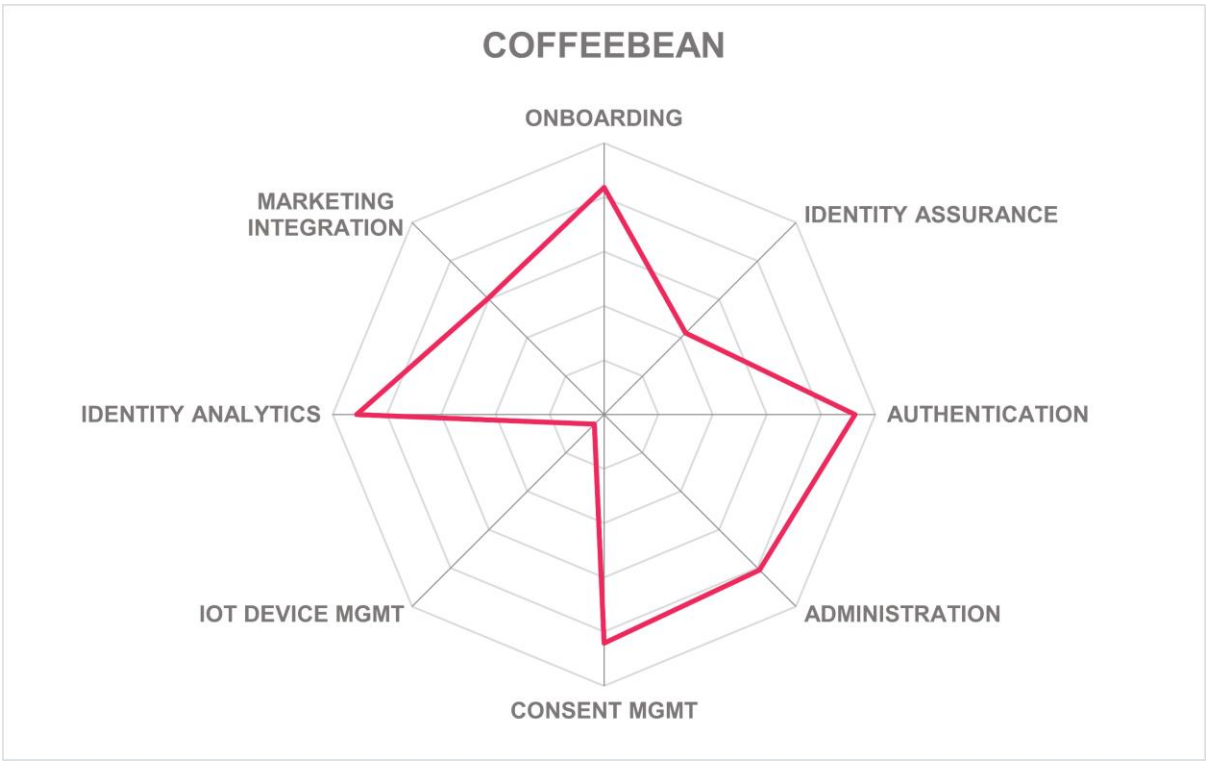
- Registration-as-a-service
- Comparatively fast deployments
- Rich identity governance and account lifecycle management features including multiple account detection and de-duplication
- Accepts most authenticator types, including FIDO 2 and passkeys
- Engagement plug-ins for mobile apps and Wi-Fi captive portals
- Connectors for a few of the most common CPM solutions
- Many integrations with CRM, email automation, and marketing intelligence tools

Challenges

- No identity verification features or out-of-the-box integrations
- Additional FRIP integrations would be useful
- Lacks consumer IoT device identity management
- Delegated administration not supported

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


COFFEEBEAN
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

Descope – Descope

Descope is a well-funded early-stage startup based in Los Altos, CA. They emerged from stealth in early 2023. Delivering CIAM as SaaS is their sole focus. Their customer base and support ecosystem are surprisingly well-diversified geographically considering their recent launch. Their SaaS runs in a single Tier 1 IaaS provider in the US and EU. Descope is fully subscription based, but has multiple options for MAUs, applications, and federations.

Customers can migrate to Descope using SCIM and their custom API. Self-registration and social network registration options are available. DIDs are not supported. Any SAML or OIDC compliant identity provider (IdP) can be accommodated. User and device registration flows and terms of service screens can be customized in their easy-to-use graphical workflow editor. Most common account recovery methods are available. Descope has several IGA and lifecycle management functions, including detection of similar/duplicate accounts with secure account merging and automatic time-based de-provisioning. Account keepalive messaging is not present.

Descope supports nearly every authenticator, including all the major authenticator apps, Android and iOS biometrics, and FIDO, including passkeys. Descope supports JWT, OAuth2, OIDC, and SAML for federation. They offer an SDK so customers can embed their authentication services into their apps. It can collect IP addresses and geo-locations for runtime risk assessments. It does device fingerprinting but does not consider behavioral biometrics. Building risk-based authentication policies is very intuitive using their drag-and-drop editor, which also support A/B testing, branching paths, and multiple user-facing screens.

Descope has integrations with Telesign for phone number verification and Amazon Rekognition for image-based verification of identity documents. It does not use in-network credential intelligence for risk evaluations, but it does have connectors for AbuseIPDB and Have I Been Pwned. Customers can also add reCAPTCHA to their flows, and Descope partners with Traceable for additional fraud prevention services. Customers can extend Descope via their REST, Webhooks, and WebAuthn APIs.

For consent management, Descope allows customers to view and change their attributes and consents, select individual attributes that can be shared, and opt-in/out of data sharing. No DSARs are provided, and customers must leverage their SDKs to enable account deletion. Kantara Consent Receipt and family management are not supported. It does not have integrations with third-party consent and privacy management solutions. Descope supports OAuth2 Device Flow, allowing customers to add steps to the user journey for machine-to-machine authentication, but there is no dedicated user interface for managing IoT device identities. A plethora of identity analytics are available through the easily editable dashboard and reports, but customer admins cannot currently drill down into forensics from the dashboard. Data export is constrained to .csv format. Connectors for Amazon SES and SNS, HubSpot, Intercom, SendGrid, Twilio, and WhatsApp are available. An integration with DevRev's PLuG widget enables chatbot style passcode validation for emails. There are no connectors for payment services.

Their platform supports B2B CIAM through the same interface, which allows configurable registration deny lists, sanctions, and embargo screening, compromised credential checks, per-customer communications options, per-application authorization, delegated administration per-application or per-customer, time-limited accounts, and dedicated per-customer or per-partner reports.

Descope has obtained ISO 27001, SOC 2 Type 2, CSA Star Level 2, and HIPAA certifications. Descope reports that their customers achieve fast implementations. One of their strengths is that they serve as a federation hub for customers with complex many-to-many business relationships. They offer initial setup and incident response assistance. Organizations that are looking for a lightweight, easy-to-use consumer IAM with authentication flexibility and good B2B CIAM features should look at Descope's offering.

Security	Positive
Functionality	Neutral
Deployment	Neutral
Interoperability	Neutral
Usability	Positive

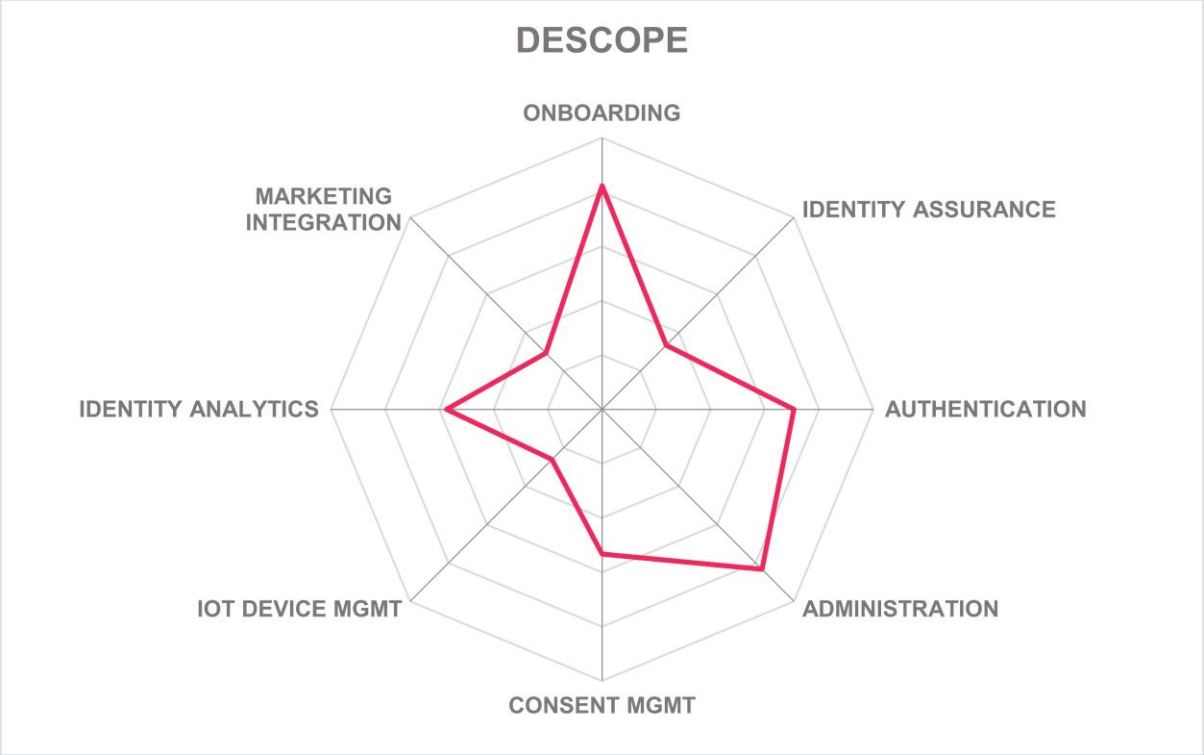
Table 7: Descope's rating

Strengths

- Rapid deployments
- Excellent customer admin interface makes it easy to build and edit onboarding workflows
- IGA and lifecycle management including secure merging of duplicate accounts
- Extremely flexible in terms of authenticators accepted
- FIDO Alliance member
- Supports complex B2B CIAM use cases with granular MFA and authorization policies

Challenges

- Limited use of device intelligence in risk-based authentication
- Consent management model is incomplete; no integrations with external CPMs
- Could use more connectors for third-party services
- Syslog to SIEM not supported
- Early-stage startup but well-supported and growing quickly


DESCOPE
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

DruID – Identity & Pulse

DruID was launched in 2020 from the Genetsis Group and is now an independent startup. They are headquartered in Madrid, Spain. Most of their customers are in Southern Europe although they are beginning to expand in Latin America, mainly in Mexico. They are focused on CIAM and CDP. Their Identity and Pulse services are deployed via Kubernetes, and therefore can run on any OS and/or IaaS instance that supports that. DruID launched a SaaS version recently, utilizing western European data centers of three public IaaS providers. Nearly any kind of data can be stored in user profiles due to their flexible user database. It can interoperate with Microsoft Azure AD. Licensing is primarily by container or server instances, and fixed cost options are offered as well.

DruID offers custom APIs for migration, as LDAP and SCIM are not supported. User self-registration is supported, including via social network credentials. DIDs are not supported yet due to lack of demand. User devices can also be registered; however, the workflow customization is limited. Setting up account recovery is a manual process, and account governance and lifecycle management is constrained to de-duplicating leads via linking accounts. Users can manage their accounts in the DruID user portal.

The MFA types accepted are email/phone/SMS OTP, any RFC 6238 TOTP compliant mobile app, and an integration with Facephi for biometrics. Only OAuth2 is supported for federation. They provide SDKs for Android and iOS. DruID can collect limited device intelligence attributes such as IP, location, time zone, etc., but behavioral biometrics are not included. Risk-based authentication is not configurable.

Identity verification is not built-in, but they leverage Facephi in an OEM arrangement for biometric verification. In-network compromised credential intelligence is used for fraud reduction, but there are no out-of-the-box connectors for other FRIP services. DruID supports REST APIs and Webhooks.

DruID provides consent and privacy management, including giving users the ability to grant/revoke consent, edit profiles, and delete their profiles. DSAR templates are available. Family management is not present yet but is on the roadmap, and Kantara Consent Receipt is not supported. No integrations for third-party CPMs are offered. DruID Pulse, the CDP module, can support some consumer IoT device identity management use cases. Identity and Pulse provide detailed dashboards for identity and marketing analytics. It is designed to serve as a CDP as well as CIAM for their targeted industries, which provides granular cross-channel customer segmentation via manual and ML-enhanced processes. Moreover, there are many connectors for CRM and other marketing tools such as Drupal, Facebook Leads and Custom Audiences, Google Analytics and Tag Manager, HubSpot, Mailchimp, Salesforce Marketing Cloud and Commerce Cloud, WordPress, Xeerpa, and Zoho CRM. DruID provides a connector for Shopify for e-commerce and payment services integration.

Their platform can provide some B2B CIAM features, including setting up custom deny lists, per-customer communications, delegated administration, and per-customer reports. DruID reports that they have obtained ISO 27001 but not SOC 2 Type 2 certification. They state that customers can rapidly create instances to get up and running. SIEM integration is possible over REST API but not syslog. They offer initial setup and incident analysis services

for customers if needed. Their solution is a consumer identity solution with extensive industry-focused customer data platform features such as identity analytics, lead and beats management, ML-powered market segmentation, and the ability to drive sales campaigns. DruID sees identity as necessary but just a step toward marketing analysis and automation. Retail and sports organizations that are looking for CIAM with CDP, particularly those in Spain, Portugal, and Latin America, should take a closer look at what DruID has to offer.

Security	Positive
Functionality	Neutral
Deployment	Neutral
Interoperability	Weak
Usability	Neutral

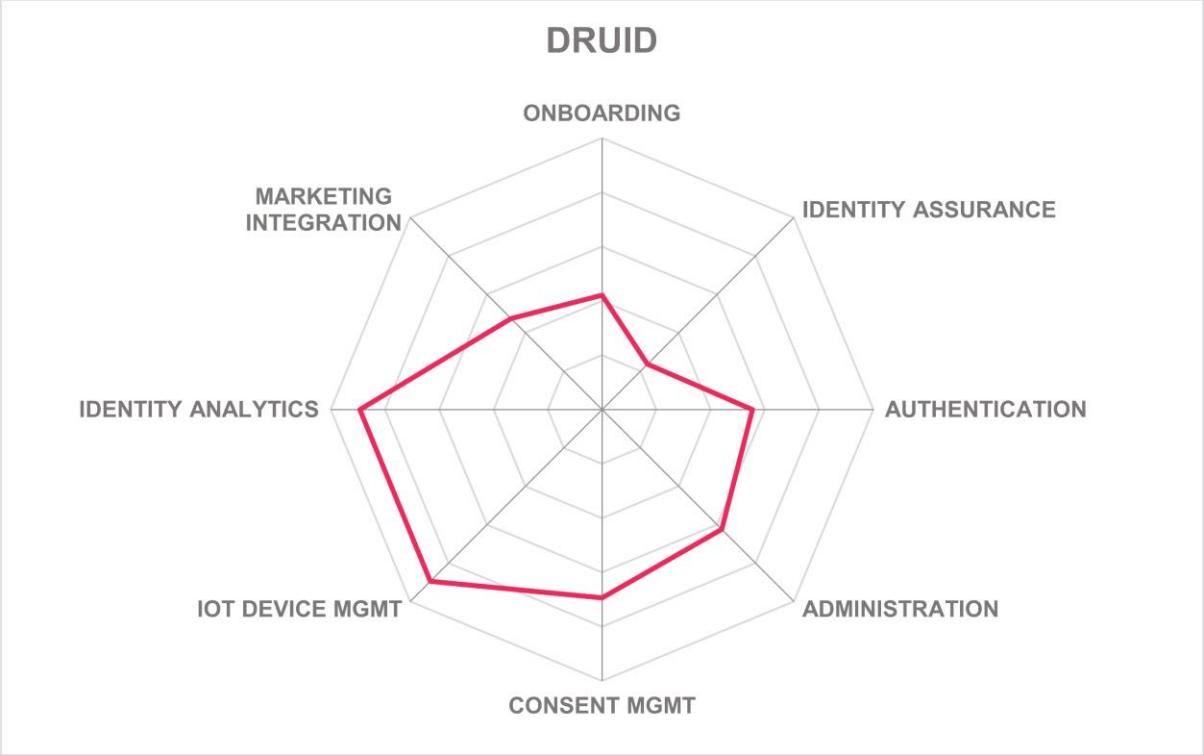
Table 8: DruID's rating

Strengths

- Fast deployments
- Fixed price options
- Extensive customer data platform features are present within the standard CIAM offering
- Direct integration with Shopify for e-commerce and payment services
- Good number of connectors for third-party CRM and marketing tools
- Supports IoT device identity management

Challenges

- Does not support LDAP or SCIM for migrations
- Needs account recovery features
- Risk-based authentication could be improved
- Adding FIDO authentication and federation protocol support should be prioritized
- No built-in identity verification and only a single external service provider is supported
- No connectors for FRIP or CPM services
- Does not handle family management


DRUID
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

IBM – Security Verify

IBM is a global technology and consulting company headquartered in Armonk, New York, USA. Founded in 1911, IBM has evolved from a computing hardware manufacturer into offering a broad range of software solutions and infrastructure, hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, and, of course, information security and IAM. IBM Security Verify is their CIAM solution, and it addresses B2B, B2C, and B2B2C use cases. IBM Security Verify is containerized and can run in any supporting environment: on-premises or in any IaaS. IBM also has SaaS offerings, which are multi-cloud hosted in data centers around the globe. IBM offers management of dedicated per-customer instances for customers that prefer maximum isolation for security and performance. IBM's customer and support network are distributed around the globe. Multiple licensing/subscription options are available.

Customers can migrate from existing solutions via LDAP and SCIM. Organizations can set up data normalization and mapping as needed. It can integrate with Microsoft AD and Azure AD. User self-registration, including registration from OIDC-compliant social networks and DIDs is possible. Security Verify can create and validate digital identity wallets. Users can register devices, and user onboarding processes can be easily modified with their workflow/journey time orchestration engine in the drag-and-drop flow builder. All possible account recovery mechanisms can be used. Security Verify has a full complement of IGA and lifecycle maintenance functions, including duplicate account detection, secure account mergers, automatic de-provisioning of abandoned accounts, and the ability to send keepalive messages, which are configurable.

Customers can use just about any authenticator type, including email/phone/SMS OTP, almost all authenticator apps, Android and iOS biometrics, and FIDO U2F/2.0/passkeys. All federation protocols are accepted. IBM provides an SDK that customers can use to embed their authentication services into their own apps. The SDK enables collection of rich device intel attributes that can, along with the gamut of behavioral biometrics harvested through JavaScript, inform their risk engine. Risk-based authentication policies are edited in the intuitive admin console, which has elements of drop-down, drag-and-drop, and a flow-chart style interface.

IBM does not have built-in identity verification functions, but instead partners with ID Data Web and other standards-based identity verification providers. A remote onboarding app facilitates selfie-to-document matching. IBM supports the OpenID identity assurance specification. Customers routinely use Webhooks, configured in the orchestration builder, to link additional IDV service providers into the workflow. Compromised credential intelligence comes from IBM Security X-Force. X-Force, IBM Trusteer, and connectors for external FRIP services can be brought in for fraud protection. IBM has robust API support including REST, SOAP, Webhooks, WebSockets, and WebAuthn.

IBM Verify has a self-service portal that allows users to grant/revoke consent and select attributes for sharing. It does not allow customers to opt-out of data collection after registration, however. DSAR templates are provided. Customers can delete their accounts if requested. It does not support Kantara Consent Receipt, and family management is not

built-in but could be configured as a delegated administration model. There are no connectors for third-party CPM systems. IBM supports device identity management, including complicated use cases for home automation and other consumer scenarios. All identity events are auditable, and multiple reports are available, but the report interface could be updated. Marketing analytics and BI functions are available in other IBM products or via the many integrations for third-party SaaS applications. No connectors are currently present for payment services, chatbot apps, or CDPs.

The solution has some B2B CIAM features, including per-customer communications channels, per-app authorization and terms of service, delegated administration, time-limited account creation, dedicated per-customer admin consoles and reports, and per-customer authentication policies.

IBM Security Verify has obtained many security certifications including ISO 27001, SOC 2 Type 2, PCI-DSS, HIPAA, OpenID FAPI, and multiple other OIDC profiles. IBM was a leader in all four categories in our Leadership Compass on Access Management. Customers can export identity events via syslog to SIEMs. Setup services are provided, and different tiers of support for incident analysis are available. The consent management portion needs some improvement. IBM Security Verify is a flexible and scalable solution with many good security features that should be on the short list for any organization shopping for CIAM.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 9: IBM's rating

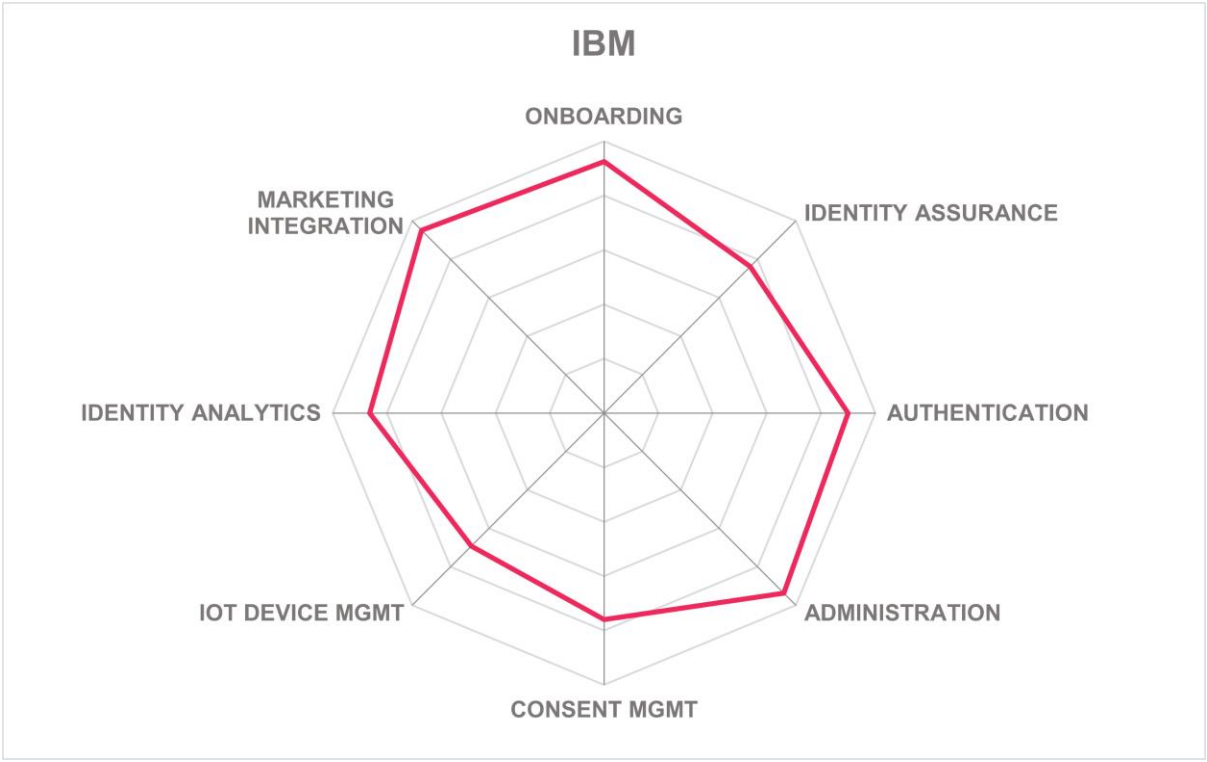
Strengths

- Support for Verifiable Credentials, DIDs, and wallets
- Identity verification integrations with ID Data Web, IDEMIA, and any OIDC Identity Assurance compliant service provider
- Full range of authenticators supported
- Highly scalable containerized, multi-cloud architecture
- Single tenant options available
- IGA and account lifecycle management functions
- Lots of connectors for SaaS apps
- Multiple security certifications

Challenges

- Complicated licensing/subscription models
- More connectors for IDV and third-party FRIP service providers would be useful
- Consent management is missing a few functions; family management must be configured as a delegated administration model
- Reports interface could use improvements to increase usability

Leader in



LoginRadius – CIAM Platform

Established in 2011, LoginRadius is a privately owned CIAM vendor that was founded in Vancouver, BC but now headquartered in San Francisco, CA. They have customers around the world and in many different industries. The company provides CIAM as SaaS via a multi-cloud model hosted in globally distributed data centers. Customers can deploy on-premises on RHEL or Ubuntu or run it in any of the major IaaS providers. Single tenant SaaS options exist for customers who want maximum separation. Subscription costs are based on the number of active users and/or logins, and fixed cost options are available also.

SCIM and use of provisioning APIs enable customer migrations. Users can register with email or social network credentials. DIDs are not accepted yet but are on their 2024 roadmap. Customers can use templates or modify user and device registration flows in the straightforward GUI. Conditional workflows allow for data mapping and normalization if needed. Most account recovery methods can be utilized. LoginRadius can detect duplicate accounts and offers secure means to merge them. It can send keepalive messages to registered users but does not automatically de-provision accounts.

For authentication, in addition to their own app, LoginRadius accepts email/phone/SMS OTP, many popular authenticator apps, Android and iOS biometrics, and FIDO 2 authenticators. All federation methods are supported. They provide SDKs for Android, iOS, React Native, PhoneGap, and Xamarin, which enable the platform to harvest device intel attributes including device type, health, IP address, and geo-locations. Behavioral biometrics are not available. The risk policy interface is characterized by drop-down menu selection with some flow-chart style features. Customers can adjust risk factor weightings, but it does not output a visible risk score.

LoginRadius does not have built-in identity verification but has integrations with nearly fifty third-party IDV service providers. It uses both internal and external compromised credential intelligence sources. Connectors are available for Arkose Labs, Broadcom, Deduce, OneSpan, Ravelin, Transmit Security, and TransUnion FRIP solutions. REST, Webhooks, WebSockets, and WebAuthn APIs are supported.

In terms of consent management, LoginRadius provides customizable user self-service screens for granting/revoking consent, sharing and editing attributes, and DSARs. Family management is supported, but Kantara Consent Receipt is not. It also has connectors for third-party CPMs including OneTrust, Thales/OneWelcome, Piwik Pro, Tealium, and Twilio Segment. LoginRadius facilitates consumer IoT device identity management including use cases for home automation, consumer electronics, wearables, smart speakers, and connected cars.

All auditable identity events can be viewed in the modifiable dashboard, and many reports are available, including for demographic analysis. Furthermore, LoginRadius has an astonishingly long list of integrations for CRM, marketing analysis and automation, and many other SaaS apps. Their platform has connectors for the following payment service providers: Amazon Pay, Billwerk, PayPal, Paysafe, Recurly, Shopify Payments, Square, Stripe, and SynchronEX. Integrations for chatbot services include Ada, Atlassian JIRA, Customer.io, Freshworks, Google Dialogflow, HubSpot, IBM watsonx Assistant, Intercom, Olark,

Salesforce Einstein Bots, SAP, and Zendesk. LoginRadius also has integrations for nearly a dozen of the most popular CDP solutions.

For B2B CIAM, LoginRadius supports compliance checks for customers, partners, and contractors; per-customer communications and reports, per-application terms of service, delegated administration, time-limited accounts, and granular authentication and attribute-based access control policies. LoginRadius has many security certifications including ISO 27001/27017/27018, SOC 2 Type 2, CSA, and multiple OpenID profiles. Identity event data can be exported to SIEMs over syslog. LoginRadius offers support for setup and incident analysis. LoginRadius is a global CIAM solution provider that addresses most all use cases at scale. They provide excellent documentation and are much more developer-friendly than in the past, although it is primarily a low-code/no-code SaaS. The number of connectors for third-party services of every kind make LoginRadius easy to integrate with existing infrastructure. Any organization looking for a flexible, but intuitive CIAM should have LoginRadius near the top of their shortlist.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 10: LoginRadius' rating

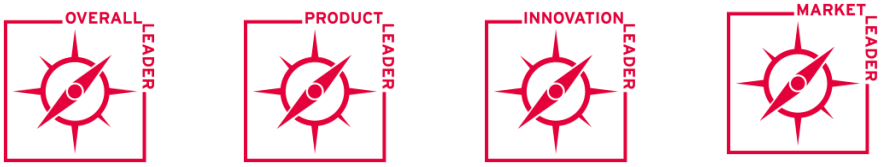
Strengths

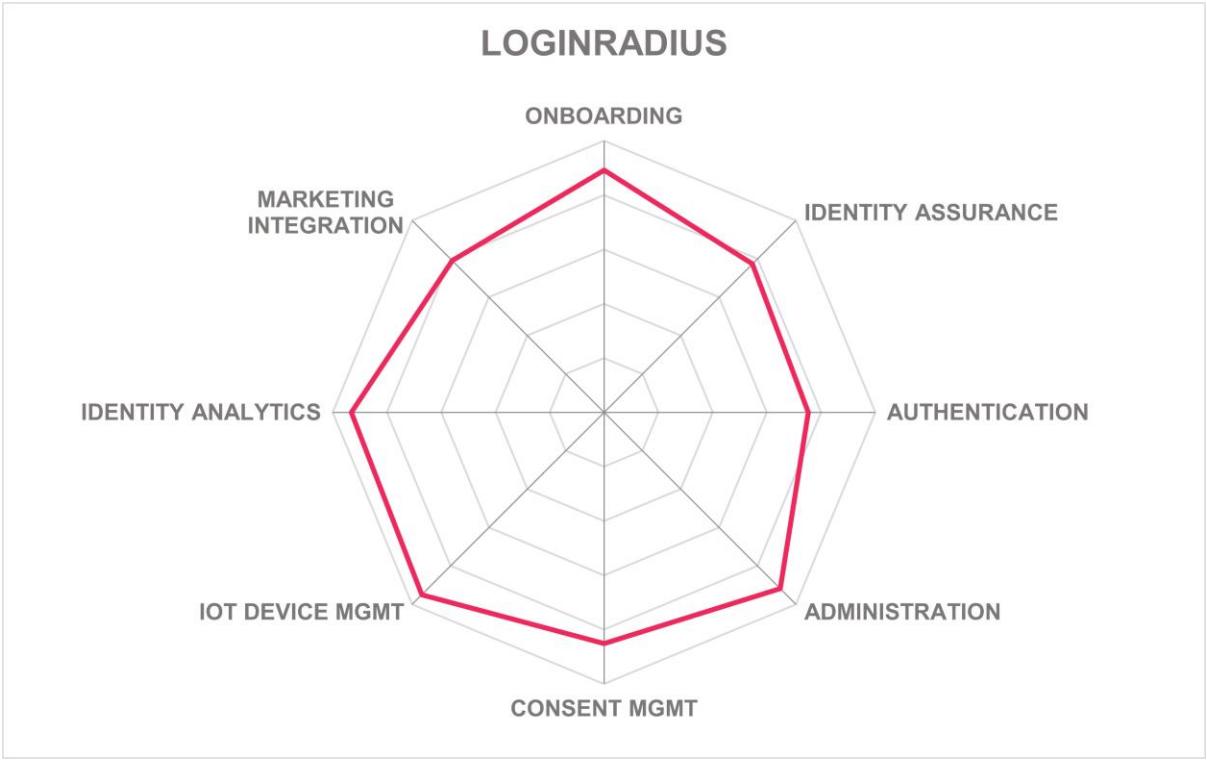
- Single tenant options present
- Clean and intuitive interface for designing workflows and authentication policies
- Duplicate account detection and secure account merging
- Broadest range of third-party IDV service providers in the field
- Multiple FRIP connectors
- Good range of device intel parameters are examined at authentication time
- Thorough consent management implementation including family management provisions and connectors to third-party CPMs
- Excellent connectivity to CDPs, chatbot services, payment services, and SaaS apps enables maximum extensibility
- Designed as an easy-to-use turnkey SaaS

Challenges

- Does not have behavioral biometrics
- Risk scores not visible to admins
- Consumer profile storage constrained to standard attributes and free text types

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


LOGINRADIUS
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

Nevis – Identity Suite & Identity Cloud

Nevis is a private company owned by IHAG Holdings, headquartered in Zurich. Their product focus is on CIAM. Most of their customers are in the EU, specifically the DACH region, but they have a foothold in the US and Singapore. Identity Suite can be installed on Linux on-premises, as well as in private clouds like Open Shift or other cluster types, or in Microsoft Azure. Identity and Authentication Cloud are available on the Azure Marketplace through the "pay as you go" model. Nevis also operates both Identity Cloud and Authentication Cloud as SaaS from Azure in globally distributed data centers. Licensing and/or subscription prices are calculated according to the numbers of annual active users or annual registered users.

Customers can migrate to Nevis using LDAP, SCIM, or several other APIs or input methods. It can interoperate with Microsoft AD and Azure AD. Users can self-register with other IdP credentials, including social networks, but DIDs are not supported yet. Nevis allows for customization of user and device onboarding flows. Data mapping and normalization rules can be set up to expedite migrations. All major account recovery mechanisms are available. The platform has identity governance and lifecycle features including the detection of and secure de-duplication of similar accounts, and automatic de-provisioning.

This solution supports almost all authenticator types including apps, tokens, and FIDO including passkeys. Nevis also can leverage WhatsApp, Signal, and Threema for out-of-band authentication: users text and receive OTPs over these channels. Nevis also has its own Access App and SDK, which enable mobile biometrics and FIDO UAF. This app runs in the Trusted Execution Environment (TEE) on Android for higher security. The SDK facilitates examination of device intel including type, fingerprint, health, IP address, and geo-location. Behavioral biometrics are limited to typing analysis through a partnership with LexisNexis® BehavioSec®. Other behavioral biometrics are avoided due to GDPR concerns. All federation protocols are supported. Risk-based authentication policies with customer editable weightings are authored in a drag-and-drop flow-chart style interface. Customers can test environment or policy changes in either canary or A/B mode.

There are no built-in identity proofing features, but Nevis has integrations with Jumio and PXL Vision. It does not utilize compromised credential intelligence. For fraud prevention, Nevis has connectors for LexisNexis, GeoComply, MaxMind, and IP2Location. Customers can extend this with their support of REST, RPC, SOAP, JMS, AMQP, Webhooks, WebSockets, and WebAuthn APIs.

Identity Suite and Cloud do not provide user dashboards, so there are no out-of-the-box means by which users can view/grant/revoke consents or share or edit their attributes. These features are reachable via their APIs, but customers must construct this. The underlying directory supports multi-tenancy. Delegated administration is possible and supports complex relationships such as family management. Nevis has CPM integrations with OneTrust, Sourcepoint, TrustArc, and Twilio Segment. Nevis allows customers to manage their IoT device identities and supports OAuth2 Device Flow. Basic identity analytics are present, but customer admins cannot drill down into details through their interface. It can export to SIEMs or Business Intelligence (BI) tools for external analysis. Many connectors for third-party CRM, marketing analysis and automation, and other popular SaaS programs are

available. Integrations for CDPs include Adobe, Oracle, Salesforce, and Twilio. They do not have any for payment services or chatbot apps.

For B2B use cases, Nevis can require compliance checks against sanctions lists and allows customers to define deny lists. It also offers per-customer communications channels, terms of service per application, delegated administration, time-limited accounts, per-customer admin portals in which fine-grained authentication and ABAC policies can be defined, and per-customer usage reports.

Nevis has not finalized their ISO 27001 or SOC 2 Type 2 certifications yet. Setup and incident analysis support services are available. Nevis has several high security features which make their solution appealing to customers in the finance and insurance industries. The solution needs to offer dedicated user self-service portals so that users can review and edit their consents and attributes. They are branching out but are still mostly localized in central Europe. Organizations in those regions that need strong security in their CIAM should consider Nevis.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Strong Positive

Table 11: Nevis' rating

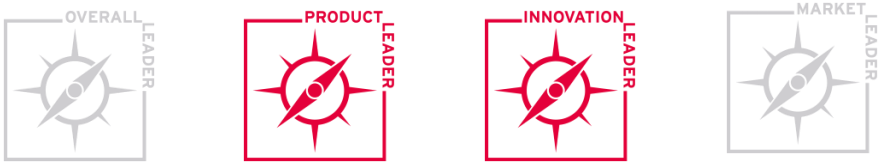
Strengths

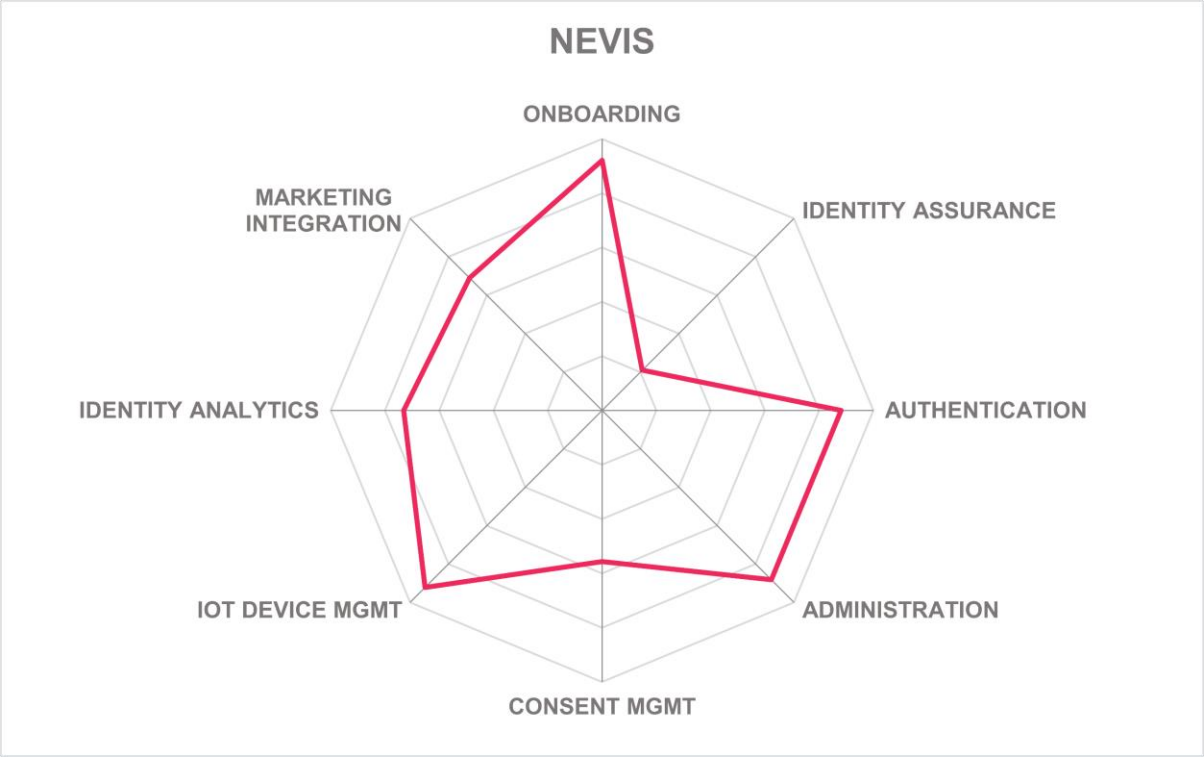
- Easy to configure authentication policy testing in both canary and A/B modes
- Dedicated WhatsApp, Signal, and Threema channels for receiving out-of-band OTPs
- Secure SDK; integrated Arxan app shielding and threat detection
- Excellent selection of authenticator types available
- Support for HSMs for financial transactions
- Integrations for several CDPs and CPMs
- Good support for B2B CIAM scenarios

Challenges

- Most customers are in the DACH region of the EU, but they are expanding in the NA and APAC
- Working on ISO 27001, have not started SOC 2 Type 2 certification yet
- Limited use of behavioral biometrics
- Few IDV and FRIP integrations
- Compromised credential intelligence is on their 2024 roadmap
- Incomplete consent management model - lacks built-in user interfaces for managing consent and profile attributes

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


NEVIS
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

NRI Secure Technologies – Uni-ID Libra

NRI Secure Technologies was founded in 2000 as a subsidiary of Nomura Research Institute. NRI Secure also provides security consulting. Uni-ID Libra is their CIAM product, which was first launched in 2008. They only operate in Japan. Uni-ID Libra can be installed on-premises in CentOS or RHEL or in the top tier IaaS platforms. NRI also has SaaS options hosted on public IaaS in data centers in Japan. Licensing costs are determined by the number of monthly registered users.

Users can be imported via SCIM. They can also self-register with email addresses and most social network credentials. NRI supports DIDs as well. Uni-ID can interoperate with Microsoft AD. Device registration is supported but the processes cannot be modified. Onboarding workflows can be customized but only through editing supplied templates; there is no GUI for this. Email/phone/SMS are the choices for account recovery methods. In terms of identity lifecycle management, Uni-ID can send keepalive messages at frequencies determined by customers.

Accepted authentication methods include email/phone/SMS OTP, Google and Microsoft Authenticators, Android, and iOS biometrics, FIDO UAF/U2F/2.0 and passkeys. JWT, OAuth2, OIDC, and SAML federation protocols are supported. Mobile SDKs are not offered. NRI features risk-based authentication via an older style drop-down policy builder interface. Device intelligence and behavioral biometrics are not analyzed.

Uni-ID does not have identity verification functions itself, but it does have an integration with TRUSTDOCK, the e-KYC IDV service in Japan. Uni-ID does not leverage internal or external compromised credential intelligence and has no connectors for FRIP services. NRI offers REST and WebAuthn API types only.

Uni-ID provides good consent management via its user self-service dashboard. Users can select which data attributes to share, edit their profiles as necessary, and delete their accounts. The user self-service interface allows for family management scenarios. It does not have any integrations for CPMs. Uni-ID follows the OAuth2 Device Flow specification and provides interfaces for customers to manage their IoT devices. Sophisticated device identity management use cases such as connected vehicles and consumer electronics are supported. Uni-ID provides some identity analytics information in their admin console, but it does not enable detailed examination of logged data. All identity events can be exported in .csv files for examination in external solutions. It does not have connectors for CRM, marketing automation, business intelligence, popular SaaS tools, payment services, chatbot apps, or CDPs.

Uni-ID can be used for B2B and includes features such as per-application terms of service, self-service portals for B2B users, and a central console for prime customers to manage all their customers. It does not permit delegated administration or support attribute-based access controls in B2B relationships.

NRI is ISO 27001, 27017, and 27018 certified, but they have not obtained SOC 2 Type 2. Initial setup services are offered, but incident handling services are not. Customers can send identity event data from Uni-ID Libra to their SIEMs over syslog. NRI continues to add some innovative features. The solution is missing some key CIAM functionality as outlined above and would benefit especially from additional out-of-the-box integrations with CRM, marketing, and other SaaS apps. NRI is still focused on Japan and continues to grow within

that market. Any organization in Japan that is looking for CIAM should consider NRI Uni-ID Libra.

Security	Neutral
Functionality	Neutral
Deployment	Neutral
Interoperability	Neutral
Usability	Neutral

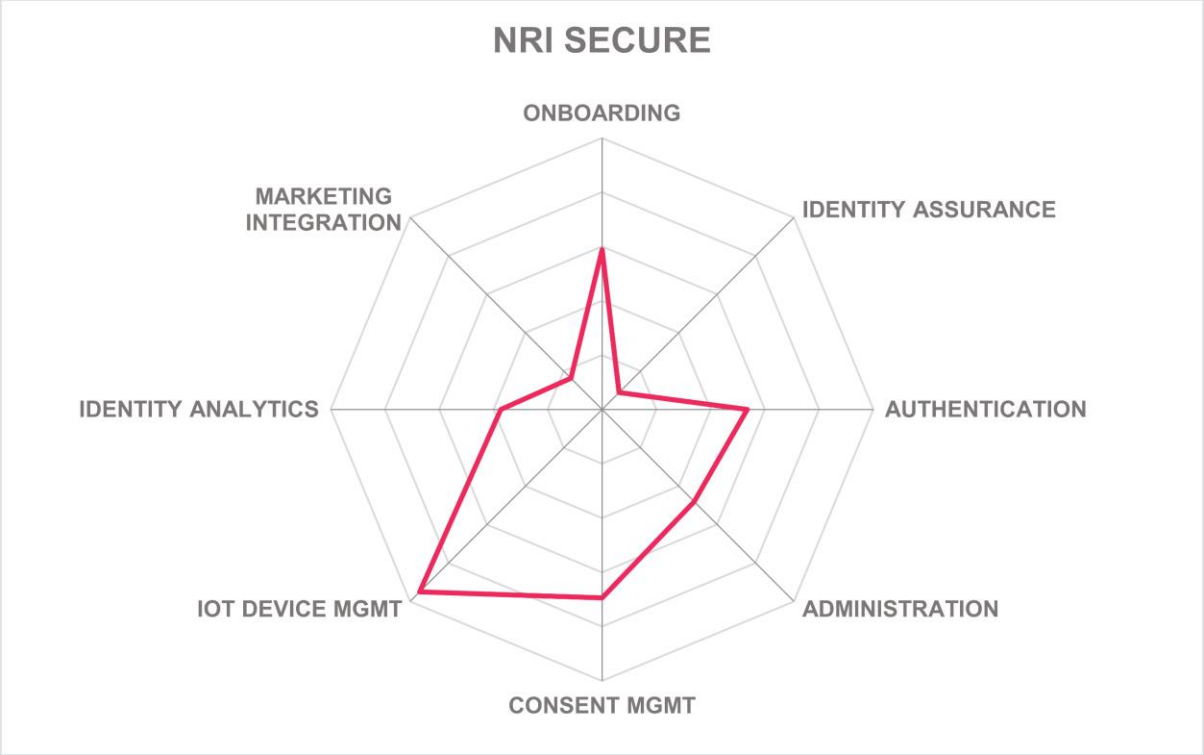
Table 12: NRI Secure Technologies' rating

Strengths

- Support for DIDs
- Integration with TRUSTDOCK for IDV
- Automated de-provisioning at customer-set intervals
- Excellent selection of authenticator choices including all variants of FIDO
- Good consent management implementation
- Provides consumer IoT device identity management for complex use cases such as connected cars and home electronics

Challenges

- Lacks GUI for editing onboarding processes
- Account linking for recovery not supported
- Does not detect and merge similar accounts
- No mobile SDKs or use of device intel or behavioral biometrics
- Does not use compromised credential intelligence
- No connectors for FRIP services, CRM, or other third-party tools
- Limited identity analytics in-platform
- Sales and support limited to Japan


NRI SECURE
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

Okta – Customer Identity Cloud powered by Auth0

Okta was established in 2009 in San Francisco as an enterprise IDaaS provider. In 2021, Okta acquired Auth0, a developer focused IAM and CIAM vendor. Okta offers a full range of identity services, including governance, lifecycle management, and API access management. Okta solutions are SaaS, hosted in public IaaS, and they offer private cloud options as well. Okta has global operations, leveraging data centers on six continents, but most of their sales and support are currently in the US. Pricing is by number of monthly active users.

New customers can migrate to Okta/Auth0 over LDAP or SCIM or migrate their entire custom databases in a bulk or ongoing process using management APIs. Self-registration is possible, and any OIDC compliant credentials, including social network credentials, and DIDs can be used. Onboarding processes can be customized as needed through Okta Workflows and Okta Customer Identity Cloud Actions interfaces, which are easy-to-use no-code editors where customer admins drag-and-drop tasks into flows. Moreover, incoming data can be mapped and normalized if required. Customer profiles can accept complex data types. Most major account recovery mechanisms are present. Okta can interoperate with other IAM and IDaaS services, including 1Kosmos, CyberArk, IBM, Microsoft AD and Azure AD, One Identity, and more. Customer Identity Cloud has deep identity governance and lifecycle management functions including detection and secure merging of similar accounts, sending keepalive messages through integrated marketing email tools, and customer configurable automatic de-provisioning.

Okta accepts a broad range of authenticators: email/phone/SMS OTP, most major authenticator apps, and FIDO U2F/2.0/passkeys. All standard federation token types are supported. They offer over 40 different SDKs to enable customers to manage authentication and authorization for different types of applications from web, mobile, APIs, or input-constrained devices. These SDKs can take in a subset of the common device attribute types, but it does not collect behavioral biometrics. The risk engine is customer configurable and adaptive MFA policies can be set up in the intuitive GUI or extended with custom logic available through Actions functions.

Okta does not provide identity proofing services itself, but it does have integrations with IDV services such as 1Kosmos, Acuant/GBG, ID Data Web, ID.me, LexisNexis, Persona, Signicat, Stripe, and tru.ID. The solution uses both in-network and multiple third-party sources of compromised credential intelligence. Okta has several out-of-the-box integrations with FRIP services including Arkose Labs, Deduce, Forter, Telesign, and Verosint. Their solution supports REST, Webhooks, WebSockets, and WebAuthn API types.

For consent management, Okta provides self-service features that allow users to view and edit their attributes and grant/revoke consents. It supports account deletion requests and the Kantara Consent Receipt format but does not provide DSAR templates or forms. Family management can be accomplished with the Delegated Administration Extension. Their platform has connectors for third-party CPMs including DataGrail, DataGuard, Ethyca, OneTrust, Tealium, Transcend, and Twilio Segment. Okta supports OAuth2 Device Flow specification and sophisticated consumer IoT device identity use cases, including home automation, connected cars, and home electronics. The dashboard has modifiable widgets and reports covering the usual metrics are provided. All auditable events can be streamed to analysis services. Okta/Auth0 has hundreds of connectors for various CRM, marketing automation and analysis, and other SaaS apps. Furthermore, they have connectors for

Charge Bee, PayPal, Shopify Payments, and Stripe payment service providers, and the WordPress chatbot app.

For B2B CIAM use cases, Okta enables compliance checks and sanctions screening for account requests. It also allows for per-app terms of service, compromised credentials screening, delegated administration, granular authentication and authorization policies, and time-limited accounts. Some B2B features such as custom roles and entitlements, and time-limited accounts are not in place yet.

Okta has achieved ISO 27001, SOC 2 Type 2, OpenID FAPI, CSA Star Level 2, PCI-DSS, US FedRAMP Moderate and High compliance. Setup and incident support are available. Okta is keeping the Auth0 brand distinct for CIAM. Auth0 is known for its developer focus, and they continue to provide code snippets and other tools that make building identity around existing apps easier. Okta has been the target of high profile cyberattacks in recent months and is still recovering from those. Okta is a leader in all four categories in our Leadership Compass on Access Management. Okta is highly scalable and has a lot of developer-focused features for CIAM. It is one of the most extensible CIAM solutions on the market. Organizations that need scalable and flexible CIAM solutions will want to consider Okta/Auth0 Customer Identity Cloud.

Security	Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 13: Okta's rating

Strengths

- Accepts DIDs
- Extensive attribute mapping and data normalization capabilities
- Excellent interface for designing onboarding processes and authentication and authorization policies
- Works with multiple IDV and FRIP services
- Many connectors for third-party CPMs and payment services
- Hundreds of integrations for CRM, marketing, and other SaaS apps
- Supports consumer IoT device management, including sophisticated use cases
- Developer focused product with good API exposure and documentation

Challenges

- Only harvests a limited amount of device intel
- No behavioral biometrics
- Needs more B2B CIAM features

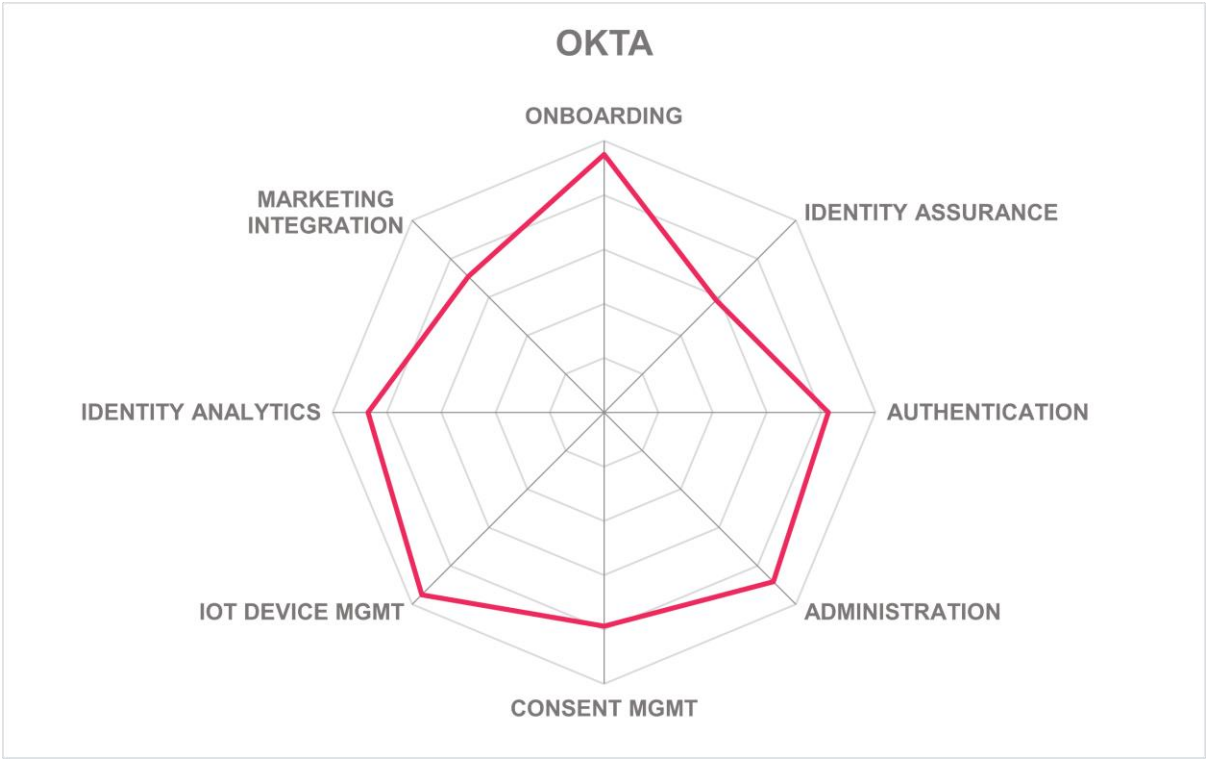
Leader in


OVERALL
LEADER


PRODUCT
LEADER


INNOVATION
LEADER


MARKET
LEADER


OKTA
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

Optimal IdM – The Optimal Cloud

Privately held Optimal IdM was established in 2005. They are headquartered in the Tampa, FL area. The company is an identity specialist, offering full enterprise IAM, CIAM, and IGA products and managed and hosted services. While the majority of their business is in the US, they have customers in western Europe and Australia and New Zealand. Optimal IdM can be installed on-premises on Windows, or in any Tier 1 IaaS provider. Optimal Cloud is their SaaS, which is hosted on public IaaS providers. Single tenant options are available. Optimal Cloud can interoperate with CyberArk, Microsoft AD and Azure AD, and SecurID IAM systems. In Optimal Cloud, customers can choose which geographic regions in which they want their consumer data stored. Licensing and/or subscription pricing options include monthly active users, quarterly/annual registered users, or monthly flat fees for privately hosted tenants.

Optimal Cloud supports LDAP, SCIM, and multiple cloud service APIs for customer migrations. Users can register via social network credentials. User onboarding flows including device registration can be customized by Optimal IdM staff. Optimal Cloud can map and normalize user attribute data if needed. Self-service portals for customers are present. Most major account recovery methods can be selected. For identity governance, Optimal Cloud can send keepalive messages and automatically de-provision accounts if desired.

Optimal IdM accepts an excellent array of authenticators, including most mobile authenticator apps, iOS and Android biometrics, and FIDO U2F/2.0/passkeys. SAML, OIDC, OAuth2, and JWT are understood for identity federation. They do not offer a mobile SDK, so device intel cannot be evaluated. Optimal IdM uses TypingDNA for behavioral biometrics and continuous authentication. Risk-based authentication policies can be drafted in the admin console, although Optimal typically helps customers write the policies.

This solution does not have either built-in identity proofing or connectors for third-party IDV services yet, but they plan to find IDV partners. It also does not use compromised credential intelligence or have integrations with FRIP services. Optimal IdM supports REST, SOAP, Webhooks, and WebAuthn APIs.

Optimal IdM offers good privacy and consent management through its user self-service portal, where customers can view/edit/delete attributes and consent actions. It adheres to the Kantara Consent Receipt specification and allows for family management. It does not have connectors for third-party CPM solutions, however. There are no provisions for consumer IoT device identity management. All expected metrics can be viewed in the intuitive and customizable dashboards. Data can be exported as .csv or PDF, but there are no connectors for CDP, CRM, marketing automation, payment services, chatbots, or other SaaS apps.

Optimal IdM handles B2B CIAM cases with sanctions screenings, per-customer communications channels, per-app terms of service, delegated administration, support for ABAC, and dedicated per-customer admin portals. It also features integration with HR service provider Paylocity.

Optimal IdM has obtained ISO 27001 and SOC 2 Type 2 certification. It does not support direct integration with customer SIEMs. Optimal IdM emphasizes service delivery so that customers do not have to staff up to support their CIAM solution. They provide not only initial setup and incident support, but also full CIAM managed services. Optimal has a lot of good authentication choices and a good consent management solution. It is missing some standard features, particularly around IoT device identity management, and needs more connectors for various kinds of third-party apps. Organizations that are looking for managed CIAM services with a wide range of authenticators and consent management should check out their offering.

Security	Positive
Functionality	Neutral
Deployment	Neutral
Interoperability	Neutral
Usability	Positive

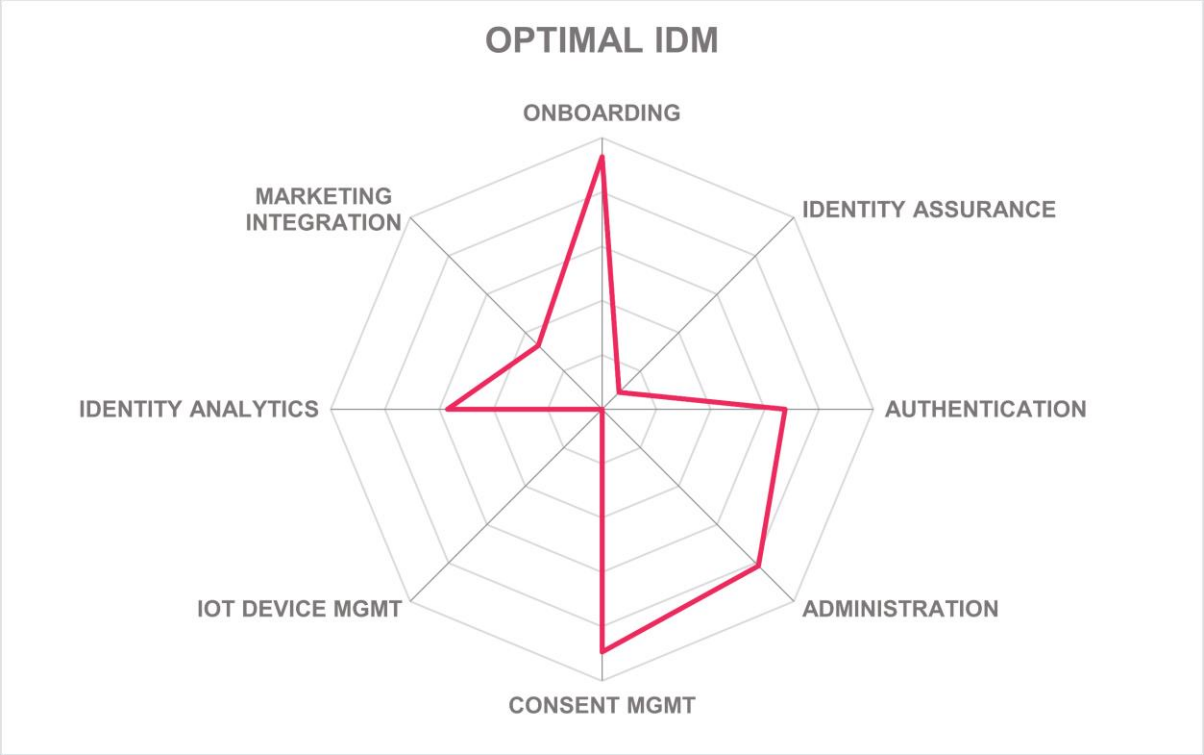
Table 14: Optimal IdM's rating

Strengths

- Managed service offering decreases customer costs
- Wide range of MFA methods are available at no extra charge
- Single tenant options
- Good implementation of consent management, including family management
- Dashboards provide a wealth of information
- Provides some advanced features for B2B CIAM use cases

Challenges

- Lacks duplicate account detection and merging functions
- No identity verification functions or connectors for IDV services
- No mobile SDK; no device intel for risk evaluation
- Does not use compromised credential intel or have integrations with FRIP
- No support for customer IoT device identity management
- No connectors for CRM or marketing analysis and automation tools


OPTIMAL IDM
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

Ping Identity – Platform

Ping Identity has been a pioneer in identity federation and access management since its founding in Denver in 2002. Ping Identity was acquired by Thoma Bravo in 2022, which also acquired ForgeRock in 2023. Since then, the ForgeRock brand has been deprecated but the Ping Identity and ForgeRock products and services still exist and will continue to exist and be supported distinctly. They have customers, operations, and support around the world. Ping Identity was among the first of the enterprise IAM vendors to offer CIAM. Packages for SaaS, on-premises, and in-IaaS installation are available for Linux, Windows, Docker containers. Any public or private space in any IaaS is supported. The Ping Identity Platform is SaaS-hosted in Tier 1 IaaS provider in data centers across five continents. Their solutions can interoperate with 1Kosmos, Broadcom, IBM, Microsoft AD and Azure AD, Oracle, and SecurID IAM systems. Licensing and/or subscription prices are calculated by numbers of active users per month/quarter/year, or per-login/session.

Customers can migrate to Ping using LDAP, SCIM, SPML, or using cloud service proprietary APIs. Attribute data can be normalized and mapped as needed during migrations. Users can register with any OIDC-compliant social network credential or DIDs. They provide excellent support for DID standards. Onboarding flows for users and their devices can be easily customized through their low-code/no-code visual designer interface, and many templates are available. All the common account recovery mechanisms are present. Ping Identity Platform can detect and allow manual merging of similar accounts and can detect inactive accounts. Customers can choose to attempt notifications and de-provision them if desired.

Ping accepts just about all authentication types: most major authentication apps, email/phone/SMS OTP, and all flavors of FIDO including passkeys. All federation tokens, from JWT to OIDC to SAML are supported. Android, iOS, IoT, and web SDKs are available for integrating customer apps to Ping's CIAM services. These enable the analysis of device intel factors such as device type, fingerprint, health, IP address, and geo-location, and a wide range of behavioral biometrics for continuous authentication. The platform supports granular authentication and authorization policies.

Ping Identity offers an IDV mobile app which examines more than 13,000 identity documents (most are government-issued) and takes selfies with liveness detection for matching. Furthermore, the Ping Identity Platform has many out-of-the-box connectors for third-party IDV services, which can easily be dropped into onboarding workflows in Ping's orchestration builder, Da Vinci. The Ping Identity Platform relies on internal fraud detection capabilities rather than traditional lists of compromised credentials from external sources. Ping has integrations with multiple FRIP services, and supports customers building integrations for those not on the list. Ping supports development to REST, RPC, OData, SOAP, Webhooks, WebSockets, WebAuthn APIs, so if desired, customers could configure connections to third-party sources via those APIs.

Ping's platform UI offers a self-service dashboard that allows users to view/grant/revoke consents and edit their attributes. Users can request account deletion in accordance with GDPR and other privacy regulations. Customers can configure terms of service and DSAR screens in Da Vinci, but no templates are provided. Family management within the Ping

Identity Platform is well-developed, providing the ability to grant permission to children to make purchases on parents' accounts. Ping has connectors for external CPM solutions as well. Their solution facilitates device identity management in sophisticated use cases for both consumers and B2B CIAM including connected vehicles, healthcare devices, telecom service providers, and manufacturing devices. All user interactions are logged and can be presented in the dashboards or numerous report types or sent to third-party systems like SIEMs for analysis via syslog or Webhooks. Da Vinci supports analysis of A/B testing for changes to policies. Their platform has numerous connectors for CRM, marketing, and other SaaS apps. They have a few integrations with CDPs too.

Ping has outstanding support for B2B CIAM, including integrations with third-party HR service providers Checkr, First Advantage, GoodHire, HireRight, Paylocity, SpringVerify, and Sterling. Moreover, it offers per-app terms of service and policies, time-limited accounts, delegated administration, and per-customer management portals.

Ping Identity is ISO 27001, SOC 2 Type 2, PCI-DSS, and HIPAA certified. Ping is keeping both cloud and software offerings from each pre-merger company, with the former ForgeRock Identity Cloud being rebranded as PingOne Advanced Identity Cloud. Both Ping and ForgeRock were leaders in all four categories in our Leadership Compass on Access Management. It is probably for the best that they remain separate offerings for their current customers. Ping's combined portfolio is among the strongest in the industry and make them a viable CIAM choice for any organization anywhere.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 15: Ping Identity's rating

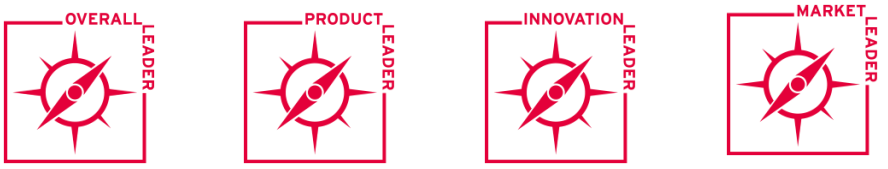
Strengths

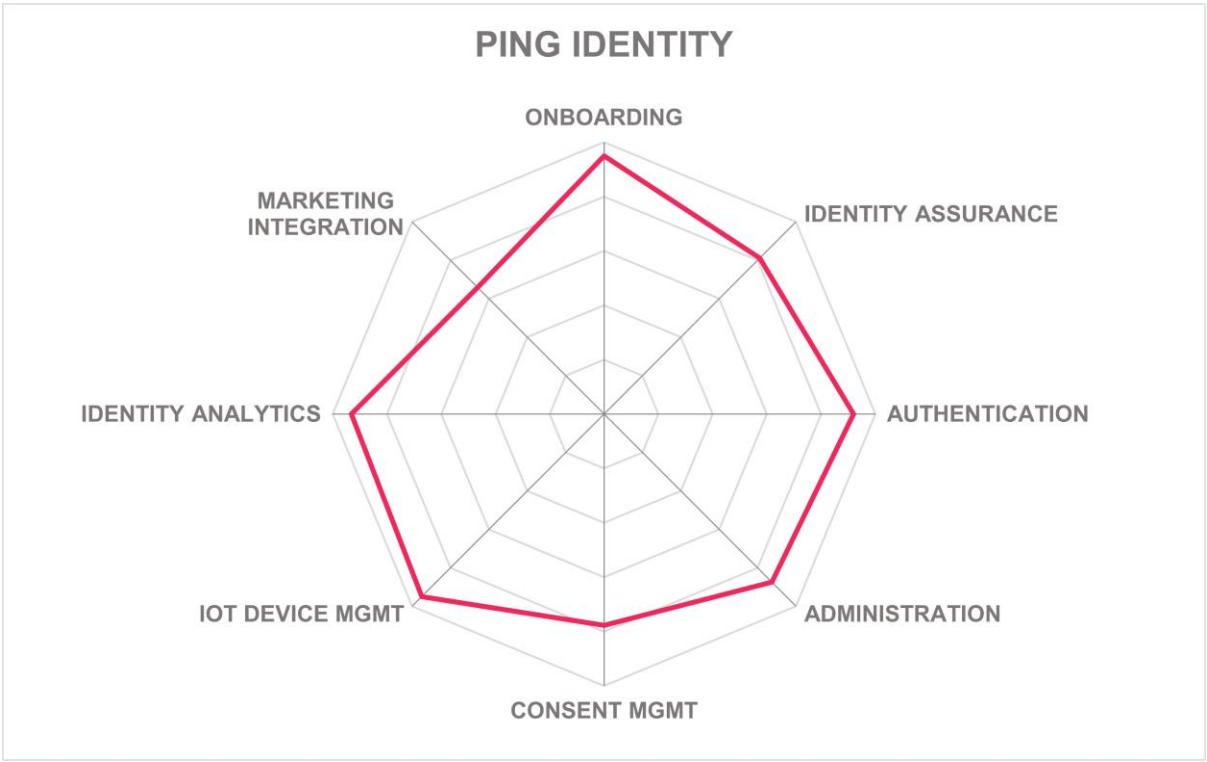
- Many inbound migration and synchronization paths
- Thorough support for existing DID standards
- Low-code/no-code Da Vinci orchestration engine makes it easy to design, visualize, and test onboarding workflows which include third-party callouts
- Many connectors for IDV and FRIP services
- Support for broad range of API types
- Excellent coverage of authenticators
- Good user self-service dashboards enable advanced family management functions, plus connectors for some CPMs
- Comprehensive device identity management
- Sophisticated B2B CIAM use case support, including HR services integrations

Challenges

- Account lifecycle maintenance could use additional automation
- No in-network compromised credential intelligence, although PingOne Fraud module (sold separately) can be used
- Does not provide DSAR templates or functions outside of DaVinci.

Leader in





ReachFive – Customer Identity and Access Management

ReachFive is a small, private, venture backed CIAM company that was founded in 2014 in France. Their CIAM, which is the company's focus, was launched in 2017. Retail businesses are their primary target. Most customers are in France, but they have picked up customers in eastern and southern Europe as well as the US and Asia. One of their goals is to help European orgs do consumer-facing business in China and South Korea. The offering is SaaS and is hosted in top tier IaaS providers. Service prices are calculated by the number of active or registered user profiles. ReachFive has some fixed price single tenant options also.

ReachFive supports SCIM for migration and synchronization, and allows users to register with social network credentials, but DIDs are not supported. It can interoperate with Microsoft AD and Azure AD, Google, and Ping Identity IAM systems. Device registration is limited to 90 days at a time. The orchestration interface does not feature a flow-chart view, but onboarding workflows can be modified somewhat. The user attribute schema can be extended with custom fields. Email/phone/SMS OTP and account linking enable account recovery. Their platform can detect similar accounts and presents opportunities for manual merging of those accounts.

ReachFive's CIAM accepts OTPs, Android and iOS biometrics, and FIDO 2 authenticators. Passkey registration is possible, but their process is manual and not currently user-friendly. They plan to improve it and make pure passwordless options for customers. OIDC enables some federation capabilities, but SAML is not supported. An SDK is provided that can pull device type/fingerprint and IP address for analysis. It does not include behavioral biometrics. These limited factors are available to the risk engine for determinations if step-up authentication is required. The policy authoring interface requires admins to choose attributes and values from drop-down lists.

Their solution does not have identity proofing features and there are no integrations with third-party IDV services yet. It does use internal compromised credential intelligence. ReachFive integrates with Akamai for FRIP. REST, Webhooks, and WebAuthn API types are supported. Users can grant/revoke consent and manage data in their profiles. DSAR templates are not included. It follows UMA but not Kantara Consent Receipt specifications. The solution does not have connectors for CPMs or chatbots. It does have integration with Microsoft Dynamics Customer Insights and Imagino CDPs, and Salesforce Commerce Cloud and PayPal. Some device identity management features are available. ReachFive does not have specific features for B2B CIAM.

ReachFive has not yet sought ISO 27001 or SOC 2 Type 2 certification. The solution has some omissions in terms of core CIAM functionality as related above. However, European organization that are looking for a basic CIAM may want to consider ReachFive, especially those that are eager to attract consumers in the APAC region.

Security	Positive
Functionality	Weak
Deployment	Neutral
Interoperability	Neutral
Usability	Neutral

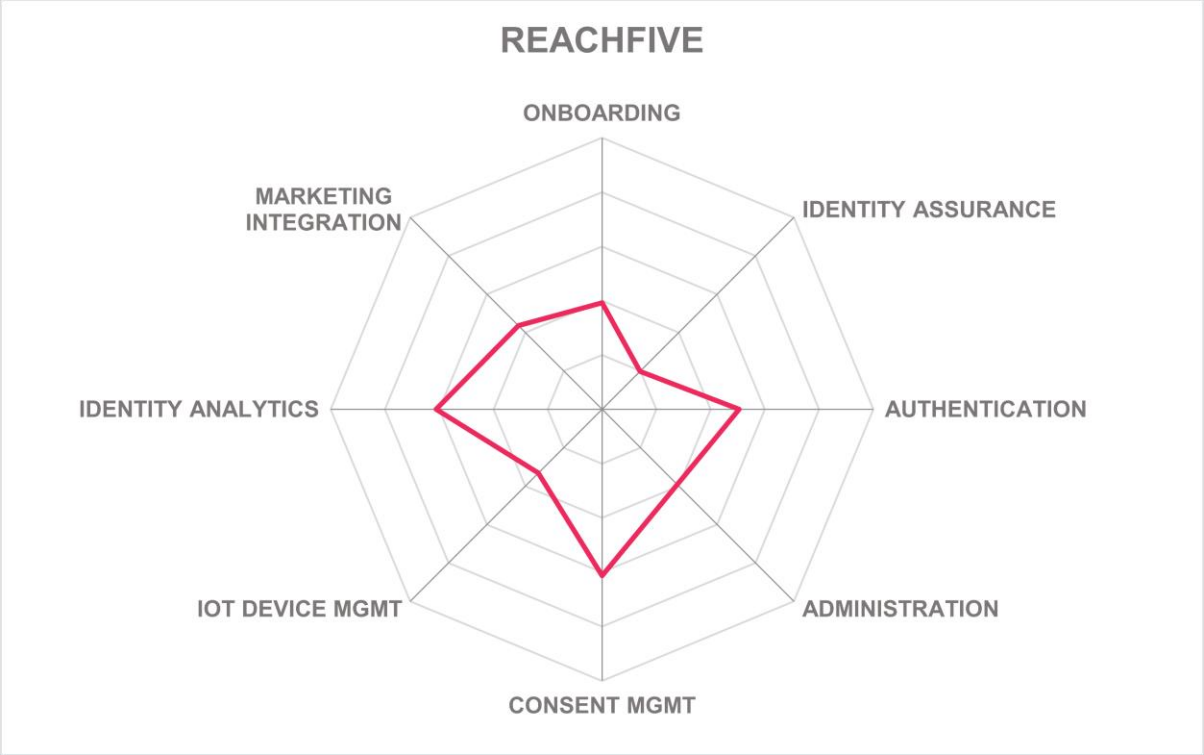
Table 16: ReachFive's rating

Strengths

- Innovative work with selected clients on CIAM to metaverse integration
- Integration with PayPal for payment services
- Supports UMA (User Managed Access) specification from Kantara
- Integration with two third-party Customer Data Platforms

Challenges

- Limited device registration periods
- Few identity governance and lifecycle management features
- SAML is not supported
- No behavioral biometrics for risk-based authentication
- No identity verification services built-in and no integrations available
- No integrations with CRM or marketing automation
- Most customers are in France, but they are expanding


REACHFIVE
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

SAP – Customer Identity and Access Management

SAP was originally founded in Germany in 1972. It has grown into one of the largest software companies in the world, with products and services for many different business sectors. Gigya was a leading CIAM solution and was acquired by SAP in 2017. SAP have integrated the former Gigya into their own suite of solutions and expanded the feature set, providing a common experience for SAP B2B, B2C, and B2B2C customers. SAP CIAM is delivered as SaaS hosted across many data centers distributed globally in multiple top tier IaaS platforms. SAP CIAM is priced by the number of contacts within each customer instance, where a contact is defined as the unique record of customers, prospects, business partners, and/or constituents within the context of the SAP CIAM cloud service.

Customers can migrate using SCIM, REST API, or SAP's ETL Batch capabilities. Most major OIDC compliant social network credentials are accepted, but they do not support DIDs yet. Their user database has a flexible schema that supports complex attribute types, including photos and binary objects. It does not directly interoperate with IAM systems. Flow Builder is the facility within which customers create and edit user and device onboarding journeys in a low-code/no-code drag-and-drop flow chart interface. Customers can choose to map and normalize incoming data if needed. Their user self-service portal allows full viewing and editing of attributes and consents, preference management, and profile data download. All major account recovery methods are available. SAP CIAM features duplicate account detection and secure merging, and inactive and abandoned account detection. Customers then could use an external email marketing solution to send keepalive messages.

SAP CIAM accepts email/phone/SMS OTP, Google and Microsoft Authenticator apps, Android and iOS biometrics, FIDO 2, and passkey authentication methods. SAML, OIDC, OAuth2, and JWT support enable identity federation. SAP offers SDKs that can collect device intel parameters including device type, fingerprint, and health, IP address and geo-location for risk evaluation. It does not have behavioral biometrics capabilities. The risk engine is configurable through the same easy-to-use GUI, although customers cannot change the risk factor weightings.

At present, SAP does not have identity verification functions or out-of-the-box connectors for third-party IDV services. It does not use in-network credential intelligence but does allow customers to create callouts to third-party services. SAP CIAM does have connectors for Arkose Labs, F5 Distributed Cloud, reCAPTCHA, and TransUnion for FRIP. REST, RPC, Webhooks, and WebAuthn API types are supported.

SAP has comprehensive consent management, as hinted above. Moreover, it features DSAR templates, ToS templates and customization, and full account deletion upon request. Family management is supported. There are no connectors for third-party CPMs, however. SAP CIAM supports OAuth2 Device Flow and customer device identity management, but there are no dedicated user interfaces for this.

The dashboard provides key metrics and identity insights at-a-glance. Event details need to be exported as JSON for additional analysis in external solutions. Many connectors for marketing analysis and automation are available. Other connections can be configured by customers over Webhooks. SAP CIAM can integrate well with their Customer Data Platform

and Emarsys, but there are no other specific CDP integrations. It does not have connectors for payment services or chatbots currently.

SAP CIAM is designed for both B2C and B2B. Customers wishing to use it for B2B can enforce compliance checks and sanctions screening, set up per-app ToS, delegated administration, per-customer authentication policies, and define per-customer roles. Customers can output event information to AWS CloudWatch, Datadog, Dynatrace, Elastic Cloud, New Relic, Splunk, and Sumo Logic; syslog is also supported.

SAP has obtained ISO 27001, SOC 2 Type 2, HIPAA, and CSA Star Level 1 certifications and/or attestations. Support for more FRIP services, identity verification services, and behavioral biometrics would make the platform more compelling. SAP's strengths in CIAM also include robust consent and preference management as well as identity and marketing analytics. Given the scalability and consent capabilities, SAP should be evaluated by any company that is looking for cloud hosted CIAM with needs for scalability and privacy regulatory compliance.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive

Table 17: SAP's rating

Strengths

- Excellent customer admin interface for designing registration workflows
- US COPPA compliance
- Similar/duplicate account detection and secure merging
- Thorough implementation of consent and preference management to facilitate privacy regulatory compliance
- Family management
- Good built-in identity and marketing analytics capabilities which can be augmented via integrations with their CDP and many third-party tools
- Many B2B CIAM features, and more on the way

Challenges

- Complex licensing scheme
- Does not have built-in behavioral biometrics
- No built-in identity proofing or integrations with third-party ID verification services
- Does not leverage internal compromised credential intelligence
- Few connectors for fraud reduction intelligence platforms

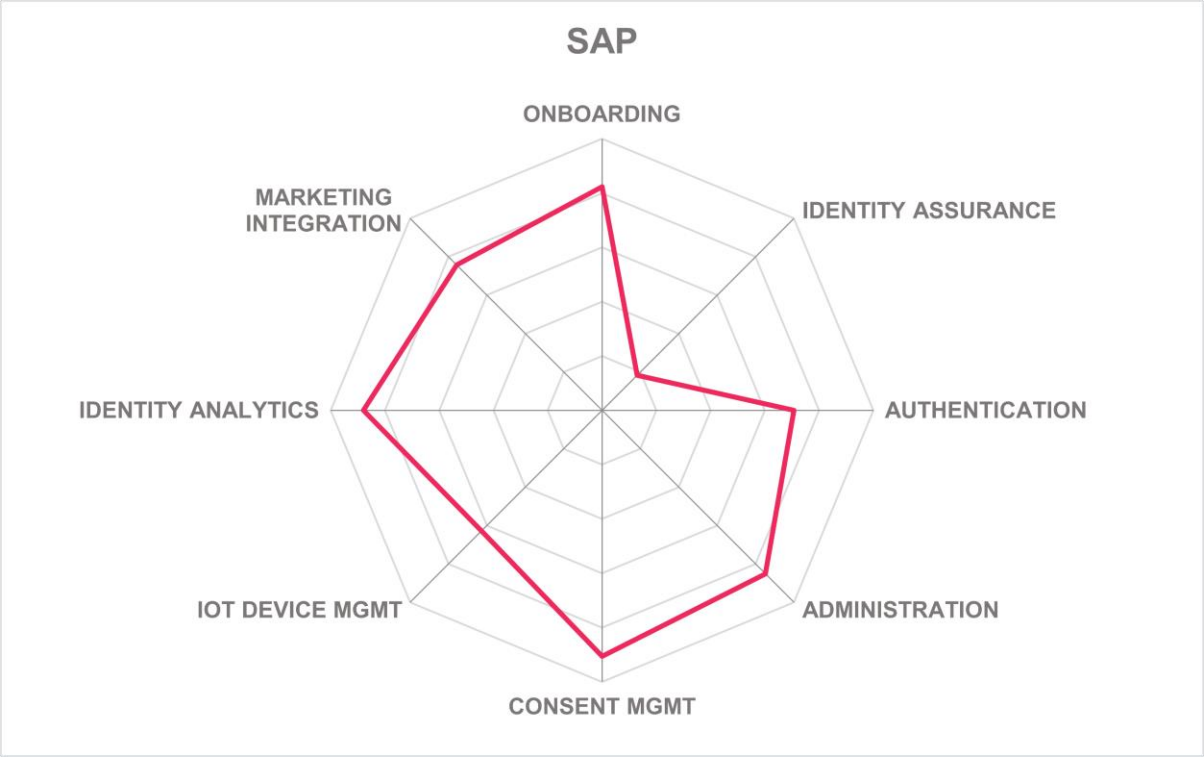
Leader in


OVERALL
LEADER


PRODUCT
LEADER


INNOVATION
LEADER


MARKET
LEADER


SAP
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

SecureAuth – SecureAuth Customer

SecureAuth was established in 2005 and is headquartered in southern California. In 2024, they acquired Cloudentity, which was founded in 2018 and is headquartered in Seattle. SecureAuth is well-known for their workforce IAM and MFA authentication solutions. Cloudentity has a full-featured CIAM and IDaaS solution. Their approach is cloud-first and one of their primary objectives is scalability; thus, they were an early adopter of micro-services architecture. Cloudentity focuses on Dynamic Authorization as the core element for CIAM. Cloudentity utilizes many of the latest container and orchestration technologies, such as Docker, Kubernetes, and Istio, to deliver their services. Their solution can run on-premises on most Linux OSes; and it is cloud-agnostic so it can be deployed to public IaaS environments such as AWS, Azure, or GCP. They also offer their solution as SaaS delivered from a Tier 1public IaaS across multiple regions including US, UK, Europe, Australia. Integration with workforce IAM systems such as CyberArk, Microsoft AD and Azure AD, Okta, and OneLogin is possible. The combined SecureAuth and Cloudentity have most of their customers and support in North America but are well-positioned to grow internationally. As of April 2024, SecureAuth offers two solutions: Workforce IAM and CIAM. The CIAM solution is based on the Cloudentity platform and is focused on use cases where the end-user is a customer outside of the direct control of the business, as in B2C, B2B2C, or B2P2C (business-to-partner-customer) scenarios. Both offerings now include the orchestration, passwordless, and continuous authentication capabilities previously offered and marketed as the Arculix product. SecureAuth's subscription pricing is based on monthly authorization grant volume, with a tiered model incentivizing higher volumes and performing specific authorizations for each sensitive transaction rather than only once per authenticated session.

SecureAuth supports provisioning from LDAP, SCIM, or REST API to enable customer migrations. Their "Identity Pools" construct allows customers to dynamically create and manage different user repositories into a single unit and/or arrange them into an organizational hierarchy for delegated management across complex business/partner ecosystems. Users can self-register with any OIDC-compliant credential; DIDs are supported also. User and device registration flows can be tailored as needed in the drag-and-drop style SecureAuth Orchestration Engine; editable templates are available. It supports data mapping and normalization for inbound user information. All expected account recovery mechanisms are present. SecureAuth can detect similar/duplicate accounts and securely merge them. The orchestration engine can send keepalives to inactive accounts and automatically de-provision them if customers require that.

In addition to SecureAuth's risk-driven continuous passwordless technology authentication, email/phone/SMS OTP, most major authenticator apps, Android and iOS biometrics, and all flavors of FIDO (including passkeys) are accepted. SAML, OIDC, and OAuth2 support enable federation. Mobile SDKs are available and can harvest all the expected device intelligence attributes. Behavioral biometrics are not gathered or processed. Risk-based authentication and authorization policies can be configured in the interface, which features a standard drop-down list approach.

SecureAuth does not have identity proofing but does have integrations with Experian, Facephi, Jumio, LexisNexis, and Ping Identity. It does not use in-network compromised credential intelligence, but customers can leverage external services. Connectors for FRIP services include Akamai, LexisNexis, Pindrop, Ping Identity, Plaid, Ravelin, and Telesign. REST, Webhooks, WebSockets, and WebAuthn APIs are supported.

For consent management, self-service portals allow users to view and change attributes and grant/revoke consents. Customers can opt-out of data processing after registration. DSAR templates are not provided. Account deletion requires coding to their APIs; it is not directly available to end users. Family management can be supported using Relationship-Based Access Control (ReBAC) and fine-grained authorization features based on an embedded Zanzibar implementation (SpiceDB by AuthZed) and can be consumed using OAuth specification methods such as the on-behalf-of and token-exchange flows. No connectors for third-party CPMs are present. IoT device identity management is only possible for devices that support machine-centric OAuth credential flows such as mTLS, JWT-bearer, and client credentials.

Basic identity analytics are available through the console and can be exported via .csv or JSON. There are some out-of-the-box integrations with SaaS apps, but it could use more for CRM and marketing analytics and automation. Although there are no integrations at present for payment services or chatbots, their professional services team can build them on demand. It does have connectors for Salesforce and Twilio CDPs.

SecureAuth excels at B2B CIAM. Their solution allows compliance checks and sanctions screening, custom deny lists, granular authorization, complex delegated administration for hierarchical business relationships, per-customer communications, per-app ToS, and dedicated per-customer portals. It supports RBAC, PBAC, ReBAC, and ABAC. Graphical representation of these multi-level business relationships is planned.

SecureAuth is ISO 27001 and SOC 2 Type 2 certified. SecureAuth's recently acquired Cloudentity was a Product and Innovation Leader in our Leadership Compass on Access Management. Customers can send identity events to their SIEMs over syslog or by using Webhooks. SecureAuth states that they rigorously test for scalability and processing speed to exceed customer requirements. Though there are some areas for improvement on the B2C side, SecureAuth and the predecessor Cloudentity product seem well-suited for complex authorization scenarios in B2B CIAM use cases. Organizations that have sophisticated supply chain, collaboration, or advanced authentication and authorization requirements should carefully evaluate SecureAuth's CIAM solution.

Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 18: SecureAuth's rating

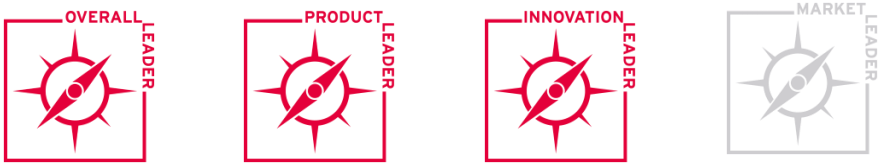
Strengths

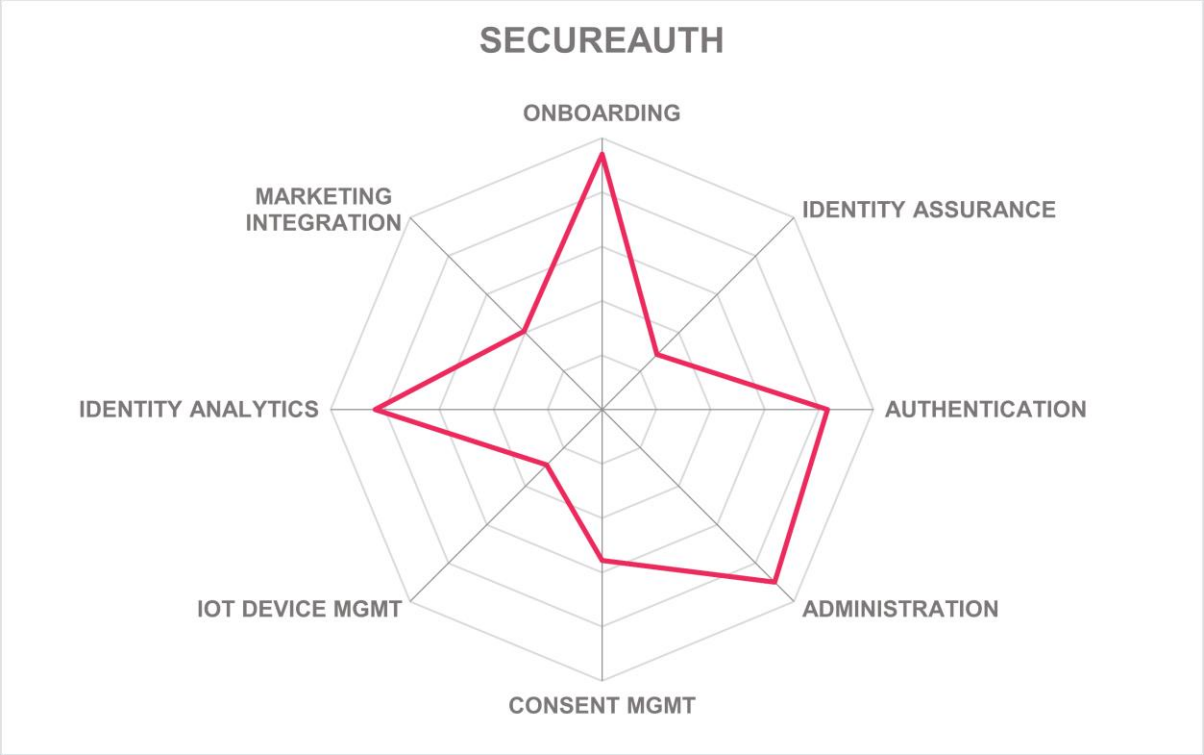
- Free tier available
- Excellent B2B CIAM use case support
- Accepts DIDs
- Wide range of authenticators supported
- Deep authorization capabilities
- Modern, secure architecture
- Developer-friendly CIAM that can be easily extended

Challenges

- Behavioral biometrics not included
- Does not use internal compromised credential intelligence
- Incomplete implementation of consent management
- Needs more connectors for SaaS apps, particularly CRM and marketing tools

Leader in




SECUREAUTH
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

Simeio – Identity Orchestrator - Customer Identity and Access Management

Simeio was founded in 2007 in Alpharetta, GA, US, providing IAM consulting and system integration services. It is a privately held company. Simeio launched their IDaaS and CIAM services in 2017. Simeio serves both B2C and B2B use cases for customers in the North America, EMEA, and APAC regions. Identity Orchestrator is delivered as a managed SaaS, hosted in North American and European data centers in public IaaS platforms. It can be deployed on-premises on Linux, and it can run in most IaaS providers. Pricing for the service is according to the numbers of monthly/quarterly/annual registered users.

Simeio supports migration and synchronization over LDAP, SCIM, or REST APIs. It interoperates with many IAM and IDaaS solutions. Users can register with email address, social network credentials, and DIDs. Customers can modify onboarding flows for users and their devices with the low-code/no-code visual flowchart editor, Identity Orchestrator. Inbound data can be mapped and normalized if needed. It is very flexible in terms of the types of data objects that can be stored with the user profiles. Simeio supports all the common account recovery mechanisms. They have a chatbot that can assist users with access requests. Their solution enables customers to identify inactive and abandoned accounts and de-provision them if desired. It also can detect similar accounts and workflows can establish correlations between them.

Their CIAM service accepts most major authenticators, including email/phone/SMS OTP, mobile push notifications, Android and iOS biometrics, voice recognition, eTAN and mTAN, many authenticator apps, and FIDO 2.0 and passkeys. JWT, OAuth2, OIDC, and SAML can be used for identity federation. SDKs are offered to allow customers to build authentication and device intelligence into their apps. Signals available for risk evaluation include device type, device fingerprint, some device health attributes, IP address, geo-location, and IMEI. It collects environmental data like network characteristics but does not have full behavioral biometrics capabilities. The risk engine can be configured by customers, enabling the weighting of individual risk factors in policies.

Simeio has a mobile app for identity verification and allows customers to select identity proofing services to integrate into onboarding processes, and for subsequent KYC actions if needed. Third-party IDV sources available include 1Kosmos, Jumio, Mitek, Onfido, and Ping Identity. Compromised credential intelligence is not available by default, but LexisNexis and PingOne Risk can be orchestrated in if customers require it. It does not have connectors for FRIP services. Simeio supports REST, RPC, SOAP, Webhooks, WebSockets, WebAuthn, and GraphQL API types.

For consent management, Simeio has user self-service portals that allow the viewing and editing of attributes and granting and revoking of consents. DSAR templates are available. Family management, including granular actions such as the ability for parents to set permissions for children, is possible within their solution. It does not have connectors for third-party CPMs. Simeio follows OAuth2 Device Flow and can be used for device identity management. Customizable dashboards can show a multitude of identity events and metrics. There are no integrations with SaaS apps like CRM, marketing automation, business intelligence, or payments services. Simeio does integrate with Twilio’s CDP.

Simeio CIAM can be used for B2B use cases. It enables compliance checks and sanctions screening, per-customer communications channels, per-app ToS, delegated administration, time-limited accounts, and dedicated customer dashboards. It supports custom role definition and ABAC. It can output to customer SIEMs over REST or syslog. Simeio's solution is ISO 27001 and SOC 2 Type 2 certified.

Simeio reports fast deployments by customers. Since it is primarily a managed SaaS, customers do not need to staff up internally to support the CIAM solution. As a systems integrator and IAM vendor, they have a lot of experience helping clients connect legacy business applications to their IAM solutions. Simeio was a Product and Innovation Leader in our Leadership Compass on Access Management. Organizations that need CIAM and would prefer it as a managed service should put Simeio on their list of solutions to evaluate.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Strong Positive

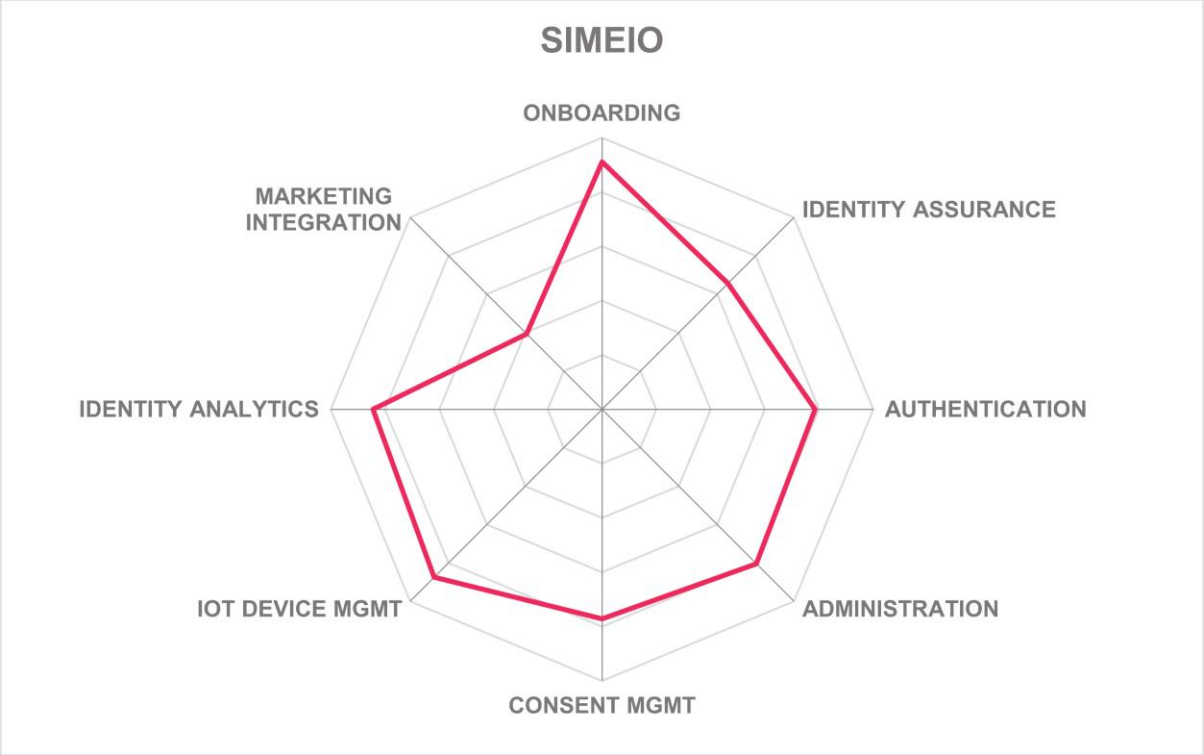
Table 19: Simeio's rating

Strengths

- Fully managed service offering reduces implementation time and customer costs
- Good selection of authentication methods present
- Flexible Identity Orchestrator interface for customizing onboarding and adding third-party IDV services
- Excellent API support

Challenges

- Limited behavioral biometrics
- No connectors for FRIP services
- No compromised credential intelligence by default
- No out-of-the-box integrations with popular SaaS apps, CRM, email automation, marketing, etc.


SIMEIO
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

Synacor – Cloud ID Media Connect, Cloud ID Passkey Connect, and User Lifecycle Management

Synacor was founded in Buffalo, NY in 1998. Synacor was acquired by Centre Lane Partners, a private equity company, in April 2021. Their Cloud ID service's main focus is enabling consumer identity integration with IoT devices, particularly set top boxes (STBs), smart TVs, and home alarm systems. Their target market is US-based media outlets; they have many large streaming media service providers as customers. Synacor hosts Cloud ID as fully multi-tenant SaaS in a public IaaS platform from data centers within the US and Canada. Subscription costs are determined by numbers of monthly active users.

Customers can migrate to Cloud ID using their standard REST API. LDAP and SCIM are not used. Users can self-register and link their devices, generally using email addresses and/or the accounts from their media customers. They do not support DIDs, and they have largely removed sign-up via social network credentials due to lack of demand from their customers. Customization of onboarding processes is not directly available through an admin console but can be accomplished with professional services. Account recovery methods include knowledge-based authentication and email/SMS links. For account lifecycle maintenance, Synacor can detect similar or duplicate accounts, and their support staff can manually move or merge them as needed. Automated de-provisioning takes place when customers close their accounts or bills go unpaid.

Cloud ID accepts username/password, email/SMS OTP, and FIDO authenticators. Passkey Connect is a new feature that will allow their customers to bring passwordless authentication to their media subscribers, enabling them to provide passkey support to hosted login pages, either as the identity provider (IdP) or proxied to the customer's IdP. Alternatively, customers can add passkey support to their own login pages through a low-code web component model, where Synacor manages the passkey in their cloud, but the customer uses their own IdP(s). Home and device-based authentication are also admitted. JWT, OAuth2, OIDC, and SAML tokens are accepted. SDKs are no longer offered as that functionality is available via REST, RPC, SOAP, Webhooks, and WebAuthn APIs. Synacor does not evaluate device intelligence or use behavioral biometrics. It does adhere to the principles of risk-based authentication, but their admins handle the setup and maintenance of the rules. The risk engine can require step-up via MFA as well as the normal permit/deny responses.

Cloud ID does not do identity proofing and does not have integrations with external IDV or FRIP services. It does not use in-network compromised credential intelligence, but they are considering partnering with a third-party provider.

Synacor allows users to view and change permissions associated with accounts. For the cases where Cloud ID is the primary system of record, there is an interface, called Account Hub, for end-users to view and edit their profile information. If Synacor is not acting as the primary system of record, end-users usually go to the self-service portal of their media service provider, i.e., Synacor's customer. DSARs are not provided since this would typically fall under the purview of their media customers. They have fairly detailed family management implementation which allows end-users to manage access and subscription utilization for all members of a household. Integration with CPMs is not available yet but is on their near-term roadmap. Cloud ID offers extensive device identity management capabilities, including supporting OAuth2 Device Flow, particularly for media delivery devices like smart TVs and speakers and STBs. A fairly good range of identity metrics is present in the reporting portal. For additional analysis, Kafka log transport is available, and data can

also be exported as .csv. It does not have connectors for CRM, marketing automation, payment services, chatbots, or CDPs.

Cloud ID is designed to help their customers with B2C; thus it does not have traditional B2B CIAM features. It does support role-based access controls. Synacor has SOC 2 Type 2 and PCI-DSS certification. Customers can pass identity event information to business analytics or SIEM systems with log streaming.

Cloud ID is still missing some key features for general purpose CIAM as outlined above, but the solution is targeted at the digital media, content, and broader consumer IoT device management market. Synacor has excellent capabilities in that part of the CIAM market. Their Passkey Connect authentication proxy approach enables customers to add strong, user-friendly authentication in front of IdPs of their choice. Organizations in the media industry as well as any organization that may have advanced use cases involving consumer IoT devices should consider Synacor Cloud ID for CIAM or as an adjunct to existing IAM/IDaaS solutions.

Security	Positive
Functionality	Neutral
Deployment	Neutral
Interoperability	Neutral
Usability	Positive

Table 20: Synacor's rating

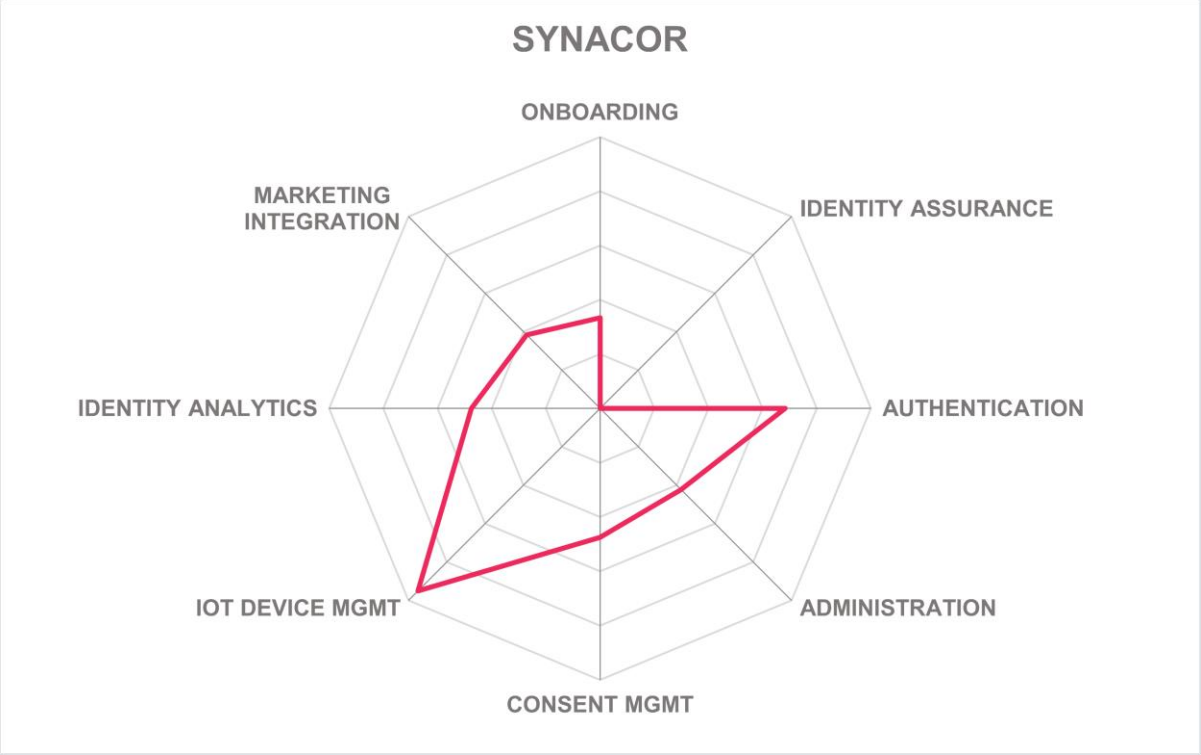
Strengths

- Device and "home"-based authentication increase usability and improve consumer experiences
- Very granular options for permissions and management of household media subscriptions
- Excellent device identity management features for media delivery devices
- Passkey Connect aims to bring user-friendly passwordless authentication to media subscription services
- Passkey Connect allows customers to add strong authentication in a proxy model so that customers can leverage their own IdPs

Challenges

- Restricted registration options and customizing onboarding workflows requires professional services
- Limited account recovery mechanisms
- Narrow range of authenticators accepted
- No IDV or FRIP partner integrations

- Lacks connectors to CDPs, CPMs, CRM, marketing automation, and other SaaS apps
- Does not have B2B CIAM functions



Thales – OneWelcome Identity Platform

OneWelcome launched as a new brand in 2021 after iWelcome and Onegini (both founded in 2011) joined together. OneWelcome specializes in CIAM and B2B CIAM, including gig worker scenarios. The Thales Group acquired OneWelcome in 2022, and it remains the distinct brand for Thales' CIAM. The OneWelcome Identity Platform is composed of multiple discrete services: Identity & Access Core, User Journey Orchestration, Consent & Preferences, Delegated User Management, Identity Verification, Identity Broker, Fraud Prevention, Externalized Authorization and Mobile Identity. The solution is primarily SaaS, hosted in a Tier 1 IaaS provider across multiple data centers in the EU, APAC, and NA regions. OneWelcome supports strict data residency requirements. Multiple pricing schemes are available, including by monthly registered users, fixed cost models for enterprises and MSPs, per-module costs, and per identity verification request.

LDAP, SCIM, and proprietary APIs can facilitate migrations to OneWelcome Identity Platform. The user repository has an extensible schema that enables customers to store a variety of data types in user profiles. The solution can interoperate with other identity providers, such as Ping Identity and Microsoft AD / Azure AD. Users can register with email address, eIDs for many countries, identity wallets (ID.me, IDIN, DataKeeper, Yivi, and itsme), or social network credentials. Other DIDs can easily be added through the Identity Broker app based on demand. Mobiles and computers can be associated with user accounts. Their User Journey Orchestration module provides templates and allows for onboarding process modification; a graphical flow-chart style interface is coming later in 2024. OneWelcome Identity Platform provides all standard account recovery mechanisms. For IGA and account lifecycle maintenance, OneWelcome Identity Platform can detect similar/duplicate and inactive accounts but leaves it to the customer to decide how to manage these situations. It can also send keepalive notices to inactive customers.

Thales provides maximum flexibility for authentication, accepting email/phone/SMS OTP, Android and iOS biometrics, all listed authenticator apps, and FIDO U2F/2.0/passkeys in addition to their own SafeNet brand authenticators. JWT, OAuth2, OIDC, and SAML are supported for federation. They offer a mobile SDK to enable customers to build their CIAM services into their own apps. The SDK can harvest device intel attributes such as device type, device fingerprint, device health, IP address, and geo-location. Behavioral biometrics are also evaluated, including keystroke/mouse, swipe, touchscreen, and gesture analysis modalities. The risk-adaptive authentication engine is configurable, but the interface is still of an older style with drop-down policy builder lists, which makes it less intuitive for business users.

Thales has built-in identity verification services that provide document proofing against more than 8,000 sources such as driver licenses and passports, OCR extraction, barcode and NFC reading, and facial recognition with liveness detection. It also has integrations with many third-party IDV services. It does not leverage internal or external compromised credential sources. A connector for LexisNexis is available for third-party FRIP integration. Thales acquired Imperva recently, and additional fraud detection technologies from Imperva products are likely to be available soon within OneWelcome Identity Platform as a result. OneWelcome supports REST, Webhooks, WebSockets, WebAuthn, and GraphQL API types.

OneWelcome was always well-known for their thorough implementation of consent and preference management capabilities, instantiated in the module of that name. It facilitates full

GDPR compliance, including MyPage portals that enable viewing/editing of attributes and granting and revoking of consent, export of profile data, and full account deletion upon request. The Consent and Preference Management module is offered as a standalone CPM that can work alongside other CIAM solutions, although it does not offer cookie consent features. OneWelcome Identity Platform supports OAuth2 Device Flow and provides consumer IoT device identity management features for smart home applications as well as IoT devices used in B2B scenarios. OneWelcome Identity Platform includes dashboards and reports for both identity and marketing analytics. It leverages Google Tag Manager to collect details for analysis. Another connector for Adobe Analytics is also available. It does not have integrations for payment services, chatbots, or CDPs.

For B2B CIAM, OneWelcome Identity Platform supports compliance checks and sanctions screenings, per-customer reports and communications channels, per-application ToS, delegated administration for complex hierarchical supply chain relationships, time-limited accounts, per-customer portals, custom roles, and attribute-based access controls.

Thales has certifications in ISO 27001, SOC 2 Type 2, EHerkenning (part of eIDAS), FSQS-NL, FIDO U2F, FIDO 2.0, and ISO 30107 iBeta PAD Level 2 (biometrics with Presentation Attack Detection). Thales offers setup, incident response, and fully managed services. Customers can export identity info to SIEMs via syslog.

Thales has an excellent CIAM offering, with a great range of authenticators available, support for customer IoT device identity management, and a well-constructed consent and privacy management module. It still could benefit from having more connectors of various types available out-of-the-box, and compromised credential intelligence should be considered by default. The acquisition of OneWelcome by Thales has extended their marketing and sales reach and combined top-notch FIDO certified authentication and identity verification into an already high-quality CIAM offering. Organizations anywhere that want a CIAM solution with an emphasis on regulatory compliance should have Thales OneWelcome on their shortlist for evaluation.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 21: Thales' rating

Strengths

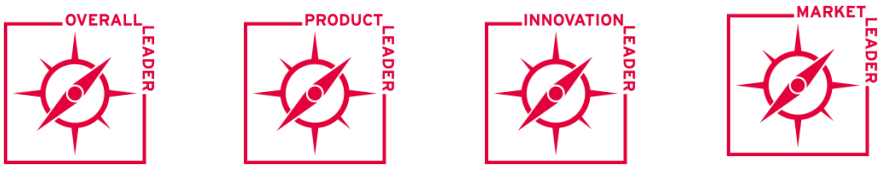
- Multiple security certifications, including FIDO and biometrics
- Enables compliance with strict data residency requirements
- Widest possible authentication support, including Thales' own SafeNet FIDO certified authenticators and passkeys
- Good utilization of device intel and behavioral biometrics

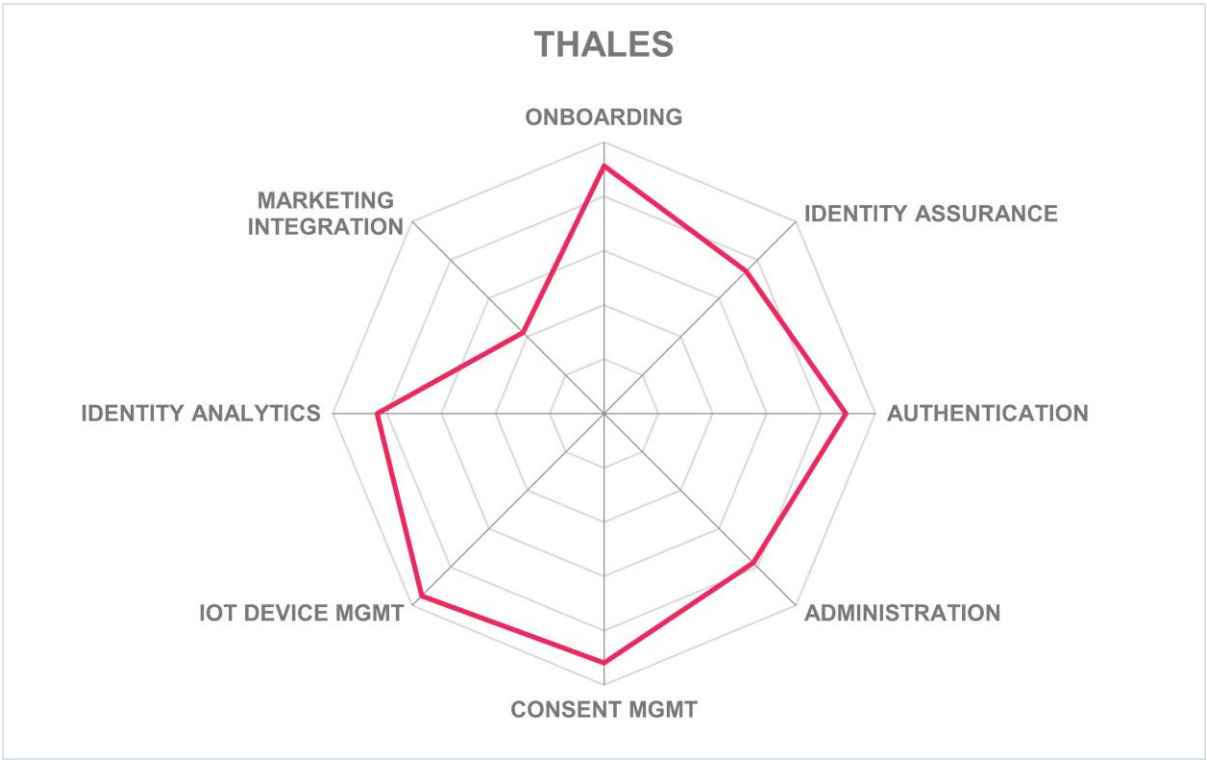
- Excellent built-in identity verification services and multiple connectors for third-party IDV services are available as well
- Robust Consent and Preference Management module provide excellent privacy regulatory functions and can function as a CPM solution (minus cookie consent) working alongside competitor CIAM systems
- Very good built-in identity and marketing analytics capabilities
- B2B CIAM relationship management with advanced features

Challenges

- Policy builder interface needs an update
- Does not use compromised credential intelligence
- Additional FRIP connectors could be helpful for customers
- More connectors for third-party CRM, marketing analytics and automation tools, and other SaaS apps needed
- Comparatively expensive

Leader in





Transmit Security – Platform

Transmit Security was founded in 2014 and is headquartered in Tel Aviv and Boston. They are a well-funded privately held company. Transmit Security also competes in the Enterprise Authentication, Identity Verification, and Fraud Reduction Intelligence Platforms markets. Transmit Security Platform is container-based and can be installed on-premises on most any Linux or in any container-supporting CSP. Transmit operates the products for customers as SaaS spanning APAC, EU, and NA regions, hosted in multiple public IaaS providers for high availability. The user repository is flexible and can support some non-standard data types. It can interoperate with most of the common enterprise IAM solutions. Multiple licensing and/or subscription models are offered.

Customers can move to Transmit from other service providers via LDAP. Self-registration with other IdPs, email addresses, and social network credentials is supported; DID and digital wallet support is under consideration. Orchestration for onboarding journeys for both users and devices can be customized as needed via the many templates or the low-code/no-code visual editor, which includes options for conducting security and usability testing of workflows. The visual editor can export flows as code for easy embedding into apps. All major account recovery options are present. For IGA and account lifecycle maintenance, Transmit Security Platform can detect similar accounts, but it does not support secure account merging techniques yet, and it can auto de-provision accounts if customers configure this capability.

Transmit Security Platform accepts email/phone/SMS OTP, all major authenticator apps, Android and iOS biometrics, and FIDO 2 including passkeys. JWT, OAuth2, OIDC, and SAML are available for federation. They offer mobile SDKs for Android and iOS which can process device intel attributes such as device type/fingerprint/health, IMEI, IP address, and geo-location. It also evaluates most behavioral biometric modalities using JavaScript. The risk engine allows customers to select weightings for risk factors and is configured via a flow-chart style interface.

Transmit offers some built-in IDV solutions which are accompanied with a mobile app for remote identity verification based on facial recognition with liveness detection and document analysis. Out-of-the-box integrations are available for more than ten other IDV services. Compromised credential intelligence from third-party sources can be used but is not on by default. Transmit has its own robust fraud prevention features which are built into the platform. They were Overall, Product, and Innovation Leaders in the last Leadership Compass on FRIP. Moreover, connectors for third-party FRIP services are available. Transmit supports REST, Webhooks, and WebAuthn API types.

In terms of consent management, Transmit offers limited functions for user self-service such as editing their own attributes. Other functions are addressable through their APIs. No DSAR templates are present. Family management features are present but pertain to financial account maintenance. Connections to third-party CPMs require customization. Consumer IoT device management is possible due to their support for OAuth2 Device Flow, but these capabilities would need to be developed by customers. Identity analytics and security insights can be viewed in the dashboard. A conversational analytics tool allows admins to ask questions of a dedicated Large Language Model (LLM) to guide security and fraud investigations, which can provide extensive identity insights for IAM leaders and SOC personnel as well as fraud analysts. Full audit log details can be exported as .csv files for analysis in third-party systems. Transmit has integrations with email automation solutions

including Microsoft Exchange, Gmail, Mailgun, Sendinblue (now Brevo), and Twilio. There are no pre-defined connectors for payment services or chatbots or CDPs.

Transmit Security Platform enables B2B CIAM and supports use cases such as custom registration deny lists, delegated administration, time-limited accounts, ABAC, and custom roles. Additional features in this area would make it more suitable for B2B CIAM deployments.

Transmit has achieved SOC 2 Type 2 certification but has not yet gotten ISO 27001. Transmit allows active-active configurations with other IdPs for high availability. Transmit offers connectors for Grafana, IBM QRadar, Loggly, Microsoft Sentinel, Prometheus, and Splunk. They offer initial setup and incident analysis services. Their targeted customers are banks and financial institutions. It is missing some features that are most likely beyond the scope of what their primary audience needs, such as advanced IoT device identity integration and dedicated CRM connectors. Large organizations in the finance industry that need strong fraud prevention technology included should check out Transmit Security Platform for CIAM and FRIP.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 22: Transmit Security's rating

Strengths

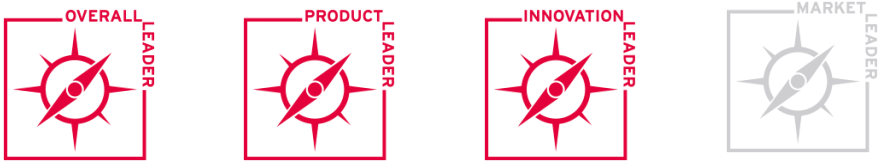
- Excellent range of authentication options present
- Device intelligence and behavioral biometrics inform the risk engine
- Built-in identity verification functions plus integrations with other IDV service providers
- Fraud prevention is part of their platform, and it has connectors for third-party FRIP services
- AI-chatbot interface for starting full identity lifecycle security and fraud investigations / insights
- Highly scalable, and resilient (active-active) multi-cloud deployment
- Comprehensive identity orchestration engine

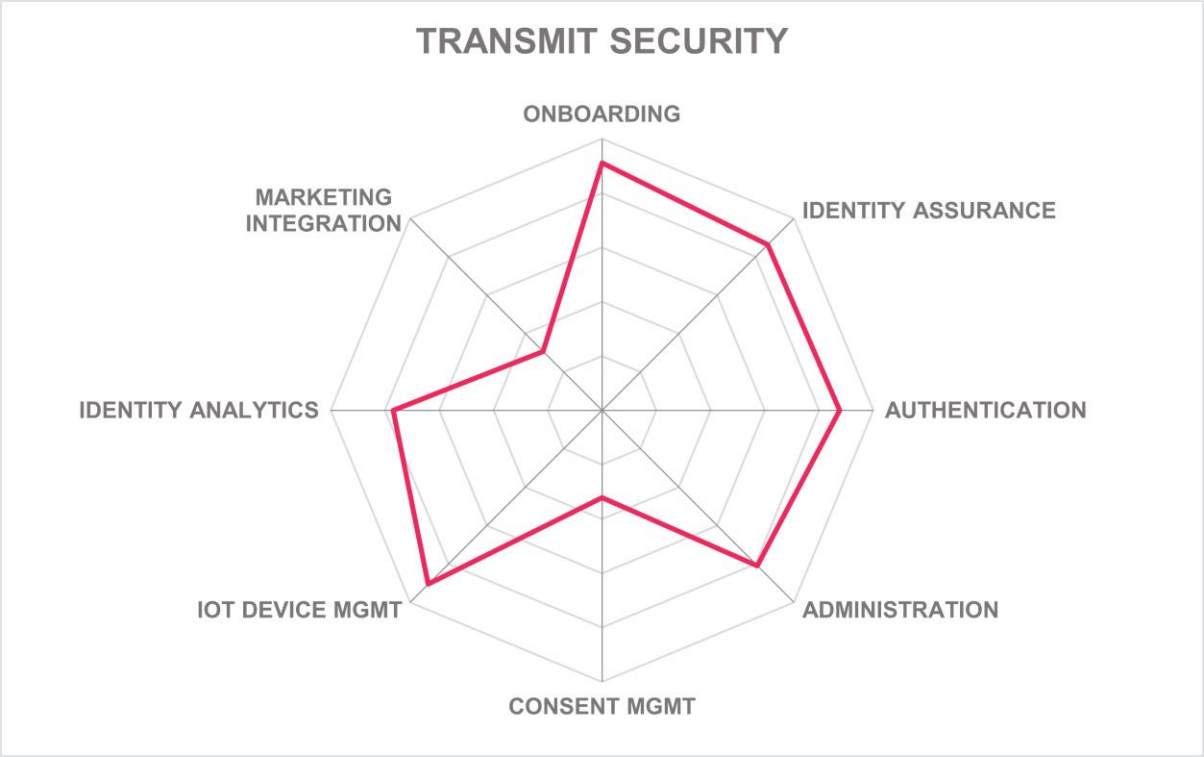
Challenges

- Additional IGA and account lifecycle maintenance features would be useful
- Compromised credential intel not used by default
- Limited consent management capabilities

- More out-of-the-box connectors for CRM, marketing analytics, and other SaaS apps are needed; the identity orchestration engine does allow for this type of customization
- B2B CIAM feature set is evolving to be more complete
- Does not support syslog

Leader in





TrustBuilder – TrustBuilder.io

TrustBuilder started up in 2016 in Belgium. In 2022, they merged with Paris-based InWebo, a strong, MFA solution provider. They are private equity owned and specialize in customer centric IAM. TrustBuilder has offices in Belgium, France, Netherlands, Germany, the UK, and US. The majority of their customer base is in France and the Benelux region. TrustBuilder.io offers two modules: TB Access Manager and TB Authentication Manager. TrustBuilder is delivered as SaaS and runs in a single public IaaS platform hosted in Belgium and France. They also offer an option where they manage customer instances in private IaaS instances. Services are priced per user and/or by blocks of transaction counts.

LDAP support enables customer migrations. Users can register themselves and their devices with social network or DID credentials. Onboarding processes can be customized through their drag-and-drop / flow-chart style interface. Most administrative tasks are handled by TrustBuilder. Data mapping and normalization are not supported. A full range of account recovery mechanisms are present. TrustBuilder can detect similar/duplicate accounts and can apply identity verification techniques for secure account merging. Alternatively, TrustBuilder supports multiple personas per user. It can also send keepalives and automatically de-provision accounts if requested.

For authentication, they accept email/phone/SMS OTP, many mobile authenticator apps, and FIDO 2. JWT, SAML, OIDC, and OAuth2 can be used for federated relationships. They offer a mobile authenticator app and SDK. The SDK can pull some device intel characteristics including device type/fingerprint, IP address, IMEI, and geo-location. Device health can be assessed with third-party Promon product. LexisNexis BehavioSec behavioral biometrics are available as an add-on. Risk-based authentication is possible but setting it up and making changes requires TrustBuilder's assistance.

For identity verification, TrustBuilder OEMs Veridas into their solution. TrustBuilder has connectors for BankID, EHerkenning, Experian, FranceConnect, HID Global, ID.me, InfoCert, Itsme, LexisNexis, Ping Identity, Onfido, OneSpan, Signicat, Thales, Trulioo, etc. It does not leverage compromised credential services. Integrations with FRIP services are limited to OneSpan, Trapets, and Veridas. TrustBuilder has broad API support, including REST, SOAP, Webhooks, WebSockets, and WebAuthn.

Consent management capabilities are somewhat lacking, although end-users can choose attributes for sharing and edit them and screens for opt-in/out data sharing can be presented. Family management can be set up as a form of delegated administration. DSAR templates are not available, and fulfilling account deletion requests requires customization in customer apps. There are no connectors for third-party CDPs. Device identity management is possible through OAuth2 Device Flow, but no dedicated user interfaces are provided. Basic identity analytics reports are available. It does not have out-of-the-box integrations with CRMs, payment services, chatbots, CDPs, or other SaaS apps.

TrustBuilder works for B2B CIAM by providing the ability to do compliance checks and sanctions screening, create custom deny lists, offer per-customer communications and per-app ToS, define time-limited accounts, and delegate administration. It supports attribute-based access controls.

TrustBuilder has obtained ISO 27001 and ANSSI certifications. Setup and incident response support are available through their professional services department. Their platform allows identity information to be passed to customers SIEMS via syslog. TrustBuilder has some

functional gaps as outlined above, most apparent in their implementation of consent management and lack of connectors. On the positive side, it has identity governance, B2B CIAM, and integrations with regional IDV services. Organizations in the western European countries they serve may want to consider TrustBuilder.

Security	Positive
Functionality	Neutral
Deployment	Weak
Interoperability	Neutral
Usability	Positive

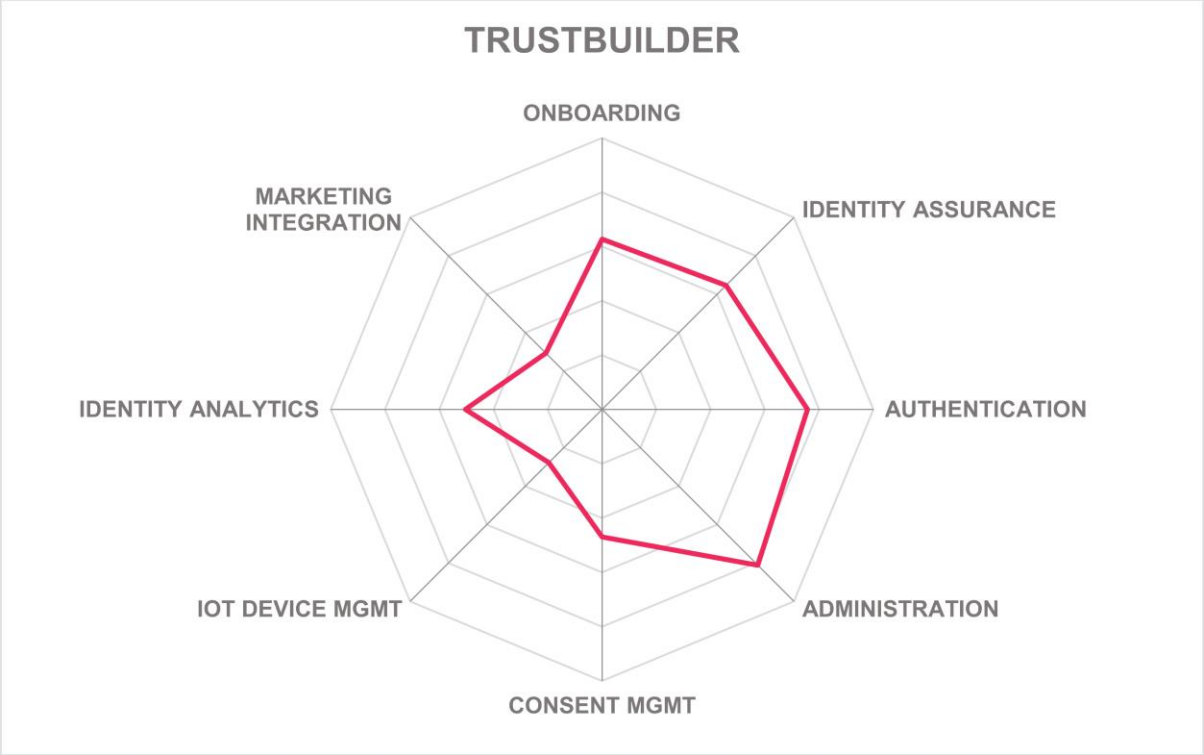
Table 23: TrustBuilder's rating

Strengths

- IGA and lifecycle maintenance functions available
- Good interface for orchestration
- Many connectors for EU-based IDV services
- Support B2B CIAM use cases

Challenges

- Smaller vendor mostly operating in western Europe
- Behavioral biometrics only available as an add-on
- No compromised credential intelligence
- Additional fraud prevention service integrations would be useful
- Consent management needs to be expanded
- Limited IoT device identity management
- Needs connectors for CRM, marketing analytics, and other SaaS apps


TRUSTBUILDER
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

WSO2 – Identity Server, Private Identity Cloud, and Asgardeo

WSO2 was founded in 2005 in Sri Lanka and is headquartered in Austin, TX. They are a venture-backed open source IAM/CIAM solution provider. Their target market is identity architects and developers, who can take advantage of their API-driven and highly customizable product. They have customers and support around the world. Related products include WSO2 API Manager, WSO2 Micro Integrator, and Choreo. Identity Server is the on-premises and self-hosted version, and it can run on Linux or Windows, or any top-tier IaaS platform. Asgardeo is their SaaS, which is hosted on a single IaaS provider in data centers in the US and EU. WSO2 Identity Server is licensed per core, and Asgardeo is priced by the number of monthly active users.

Multiple migration paths, including LDAP, SCIM, and proprietary APIs, are available for new customers. Users can register with email, social network, other IdP, or DID credentials. Mobile device registration is not supported currently. Both products have user self-service portals for attribute maintenance. User onboarding journeys can be modified with a graphical workflow tool or through their APIs. Customers can create data mapping and normalization rules. Email/SMS OTP and account linking are the account recovery methods present. WSO2 has some IGA functions, including detecting similar/duplicate accounts and applying identity verification techniques for secure account merging. It can identify inactive or abandoned accounts and automatically de-provision if desired. It does not send notifications for inactive accounts, however.

WSO2 Identity Server and Asgardeo accept email/SMS OTP, mobile push notifications, many authenticator apps, Android and iOS biometrics, and FIDO U2F/2.0/passkeys. JWT, OAuth2, OIDC, and SAML are admitted for federation. They have a mobile SDK which follows PKCE. It does not directly collect device intelligence attributes, but the highly integrated product from WSO2-spinoff and strategic partner Entgra can, for additional fees. WSO2 does not have behavioral biometrics built-in, but it partners with TypingDNA for some biometric modalities. Customers can create and tweak authentication and fine-grained authorization policies in the intuitive interface.

WSO2 can do basic email verification and has integrations for Evident, iProov, Daon, and Onfido as third-party IDV services. Compromised credential intelligence is not present out-of-the-box but customers can add their own subscriptions and add those checks as steps in the onboarding process via Choreo. Likewise, there are no pre-defined connectors for FRIP services, but customers can configure those on their own. WSO2 is easily extensible via APIs; REST, RPC, OData, SOAP, Webhooks, WebSockets, WebAuthn, and GraphQL are supported.

Users can view and edit their profiles and consent information in the self-care app. They can also granularly select attributes for sharing, opt-in/out of data collection processes, and delete their accounts. WSO2 provides DSAR templates and notifications for ToS changes. It supports Kantara Consent Receipt. Family management is not yet there, but it is on the roadmap. No connectors for CDPs are available yet. Consumer IoT device management is possible through OAuth2 Device Flow support, but they do not provide dedicated interfaces for managing those devices. WSO2 captures a wealth of identity and marketing analytics and makes these metrics visible through their ELK-powered dashboard. Customer admins can drill down into investigations from the console if needed. It provides good support for audit, compliance, and reporting. Moreover, WSO2 offers many integrations for CRM, email

automation, marketing analytics, and other SaaS apps. No connectors are present yet for payment services, CDPs, or chatbots.

For B2B CIAM use cases, WSO2 enables compliance checking and sanctions screening configurations, custom deny lists, per-customer communications, delegated administration for complex hierarchical relationships, custom attributes and entitlements, time-limited accounts, and per-customer management portals.

WSO2 is ISO 27001, PCI-DSS, and SOC 2 Type 2 certified. They offer assistance with implementation and incident analysis if needed. Customers can send identity event information to their SIEMs over syslog. WSO2 Identity Server has been around for a long time and has accumulated most of the mainstream CIAM capabilities. Asgardeo, the SaaS offering, is newer and is catching up. Feature parity is expected soon, according to their roadmap. WSO2's offerings are missing some features as described above, but they cover many functions very well. Their solutions are designed for developers and as such are very extensible. Any organization that needs a modern, dev-centric CIAM should have WSO2 on their shortlist.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 24: WSO2's rating

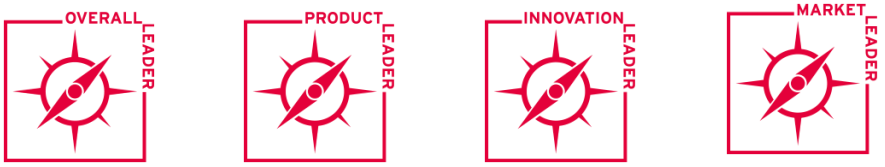
Strengths

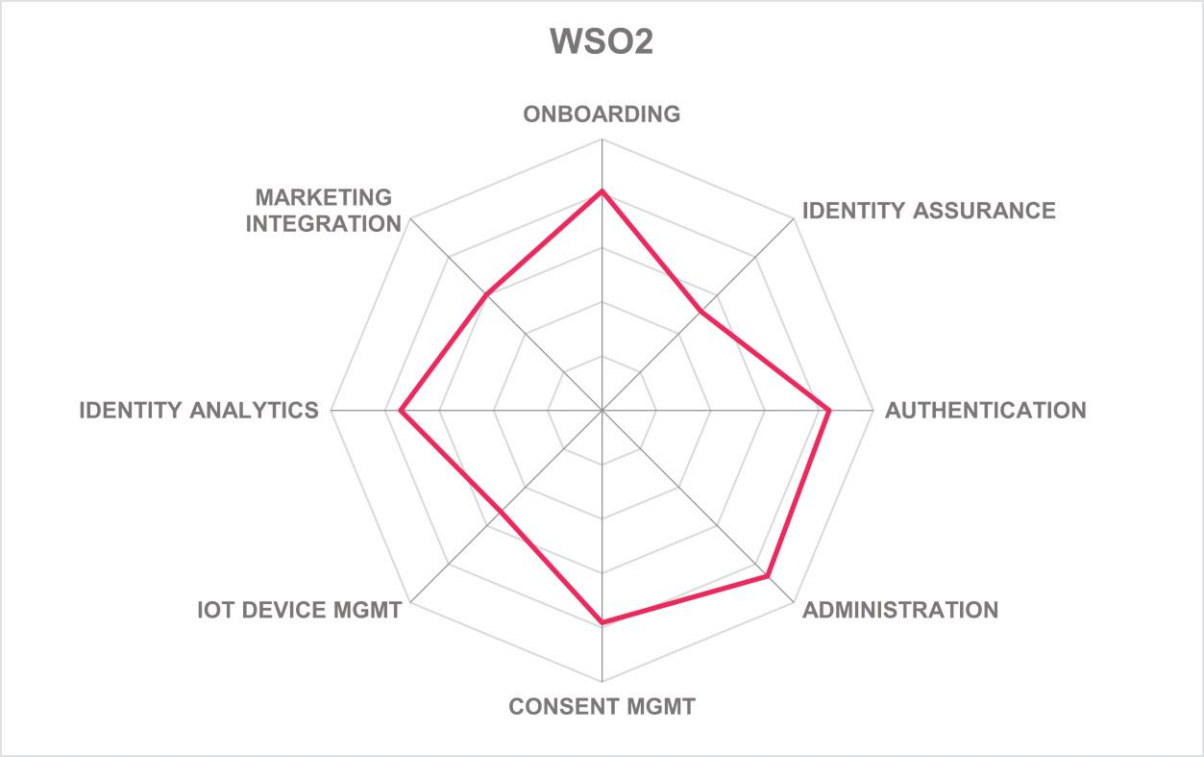
- Global sales and support
- Broad support for migration and registration processes
- Nice interface for designing workflows and authentication/authorization policies
- IGA use case support including duplicate account handling
- Large array of authenticators can be used with their platform
- Excellent API coverage and documentation
- Developer-friendly service with excellent documentation
- Good consent management capabilities, minus family management
- Many connectors for CRM, email automation, and marketing integration

Challenges

- Does not support device registration
- Does not send notifications to inactive users
- Device intelligence is available as an add-on
- Does not harvest behavioral biometrics
- Compromised credential intel is not built in
- No out-of-the-box connectors for FRIP services

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


WSO2
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

XAYONE – Platform

XAYONE Solutions was founded in 2012 as Oxyliom Solutions. They are headquartered in Morocco, Luxembourg, and the UAE. They are a mid-stage, privately owned startup. Most of their customers are in the Middle East and Africa, but they are growing in Southern Europe and Benelux. In addition to CIAM services, XAYONE Platform has B2E IAM, Data Governance, and Trust Management including electronic signatures and key management features. XAYONE Platform can be installed on-premises on Linux or Windows or on most Tier 1 IaaS platforms. XAYONE Platform is offered as SaaS and operates from a single cloud provider in Luxembourg. On-prem deployments are licensed per-user, and SaaS is charged by MAUs.

Customers can migrate to XAYONE from other solutions using LDAP or SCIM. SAML Just-in-Time (JIT) is also supported. Integration with Microsoft AD, Azure AD, Broadcom, Oracle, France Connect, and LuxTrust are available out-of-the-box. Users can register with email, phone, or social network credentials. DIDs are not currently accepted. Onboarding workflows include device registration and can be crafted in the GUI-based editor, which allows admins to drag-and-drop steps into the registration flow. All major account recovery mechanisms can be used. XAYONE offers a full range of governance and lifecycle functions including duplicate account detection and secure merging, sending keepalive messages and automatic de-provisioning.

XAYONE has a mobile authenticator, plus it accepts email/phone/SMS OTP, mobile push notifications, several of the popular authenticator apps, Android, and iOS biometrics, and FIDO 2 authenticators. Their SDK can gather device type, health, Wi-Fi and mobile network identifiers, and IP address information for evaluation by the risk engine. Behavioral biometrics are not collected. XAYONE allows customers to set up fine-grained authentication policies through an intuitive interface, weighting risk factors with slider controls, defining thresholds and overrides, and adding CAPTCHA bot detection if needed.

XAYONE provides identity verification services based on comparing identity documents against facial recognition with liveness detection and validating holograms. Their platform also has integrations with EHerkenning, HID Global, Shufti Pro, Thomson Reuters Clear ID, and TransUnion. XAYONE uses compromised credential intelligence and shares it with industry and government partners. For fraud prevention, their platform has integrations with Broadcom, F5, IBM, and LexisNexis. It has built-in bot detection and management capabilities. REST, Webhooks, WebSockets, and WebAuthn APIs are available.

XAYONE has a user-self-service portal for managing attributes and consents. It supports DSARs and account deletion requests but does not have integrations with third-party CPM systems. It adheres to Kantara Consent Receipt and allows for family management. XAYONE enables consumer IoT device identity management including use cases such as home automation and vehicle certificate management. It follows the OAuth2 Device Flow specification. Dashboards show a wealth of operational statistics including all the information types that identity administrators need to see; moreover, admins can drill down into all details about identity events. Connectors are available for eMarketer, Oracle CRM and Unity CDP, Salesforce CRM, Data Cloud, and Zoho CRM. There are no connectors for chatbots or payment services.

For B2B CIAM use cases, XAYONE offers per-customer communications and reports, delegated administration, time-limited accounts, B2B user self-service, and granular per-

customer authentication and attribute-based access control policies. It can output to customer SIEMs via syslog. XAYONE can help customers comply with PCI-DSS but has not yet achieved ISO 27001 or SOC 2 Type 2 certification. Implementation and incident analysis support options are available. The remote onboarding app that accepts any ICAO passport is a differentiator for XAYONE. Their marketing focus has been on the finance sector. Organizations in the finance industry, particularly those in the regions well-served by XAYONE, should review their capabilities when searching for CIAM solutions.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 25: XAYONE's rating

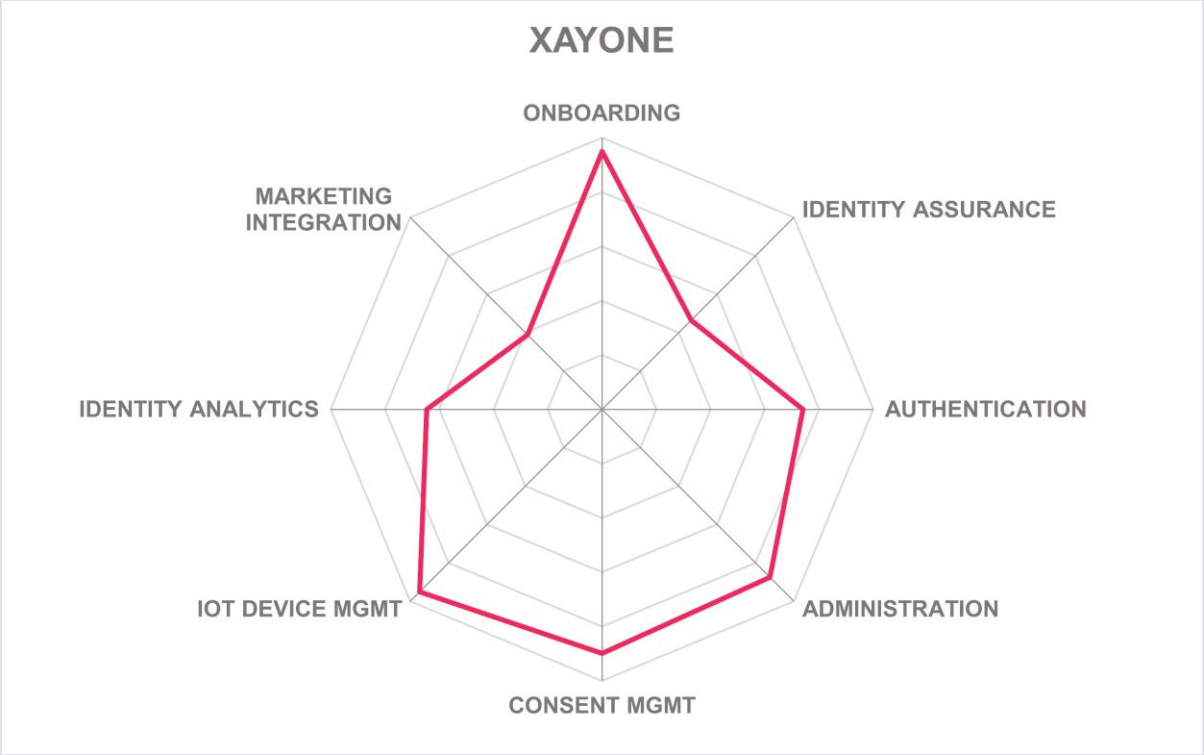
Strengths

- Good orchestration engine
- Excellent interface for designing registration workflows and authentication policies
- Many identity governance and lifecycle management features
- Built-in identity verification services that recognize many identity document types
- Multiple integrations with third-party IDVs and FRIPs
- Full-featured consent management including family management and DSAR support
- Connectors for two CDPs

Challenges

- Does not collect behavioral biometrics
- Not yet ISO 27001 or SOC 2 Type 2 certified
- Missing some B2B CIAM features
- Small but growing company with limited geographic presence outside of several countries in EMEA

Leader in


XAYONE
ONBOARDING
IDENTITY ASSURANCE
AUTHENTICATION
ADMINISTRATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons, but nevertheless offer a significant contribution to the market space.

Avatier

California-based Avatier is an enterprise IAM vendor that supports some CIAM use cases. Their focus is on rapid deployment of basic IAM services to customers. Avatier has mostly been deployed on-premises but is being run in IaaS by some customers. Avatier supports authentication mechanisms including Knowledge-based Authentication (KBA), email/phone/SMS OTP, Symantec VIP, Duo, Google Authenticator, RSA SecurID, HID, Smartcards, CipherLock, and Microsoft MFA. The Avatier mobile app features fingerprint, voice, facial recognition biometrics, but does not support FIDO. Avatier provides API access for ITSM and SIEM integration. The product does federate with Salesforce and NetSuite SaaS. KuppingerCole monitors Avatier and information about their other IAM products is available in other reports.

Why worth watching: Avatier has a solid IAM governance solution that has many functions that make it amenable to CIAM use cases, including processing social logins and accepting biometric authenticators.

Beyond Identity

Beyond Identity was founded in early 2019. They are headquartered in New York and have offices and customers around the world. Beyond Identity Customers is their CIAM offering. It excels at passwordless authentication.

Why worth watching: Beyond Identity can enable their customers to introduce truly passwordless authentication to their customers and consumers, which improves user experiences and decreases account takeover fraud. Their solution is compliant with EU PSD2.

Curity

Curity was founded in 2015 and is headquartered in Stockholm, Sweden. They are a venture-backed firm specialized in providing identity services for users and APIs. Most of their customers and support ecosystem are in the EU, particularly the Nordic region, but they also have a presence in North America. Their Identity Server can run on-prem on Linux or in any IaaS. They do not offer a SaaS version, but they have partners that run it as SaaS.

Why worth watching: Curity Identity Server has some B2B CIAM features, and delegated administration is supported. Curity is OIDC and GSMA Mobile Connect certified. Curity accepts DIDs and has a wide range of authenticators available.

Ergon (Airlock)

Ergon Informatik was established in 1984 in Zurich. They provide customer IAM solutions for major finance and insurance institutions. Ergon is an employee-owned business. Though historically they have been focused on the DACH region of Europe, they have been branching out and have customers in NA and APAC as well. Their suite of products can be deployed on-premises in containers, on Linux, or on any IaaS platform. They also plan to host it as SaaS from data centers in Switzerland.

Why worth watching: Airlock IAM, Airlock 2FA, and Airlock Secure Access Hub are well-integrated CIAM and WAF solutions used by leading finance and insurance companies in the DACH region. Airlock supports a broad range of authenticators and has B2B CIAM features.

Frontegg

Frontegg is a mid-stage startup founded in 2019 and headquartered in Mountain View, CA. They specialize in user management for B2B CIAM with fine-grained application controls. Frontegg accepts social logins and MFA methods including some passwordless authentication mechanisms. It provides SSO with OAuth, OIDC, and SAML, and it supports REST APIs and Webhooks for customer app integration.

Why worth watching: In the admin portal, Frontegg provides capabilities to establish sub-tenants, define subscriptions, and collect payments directly.

FusionAuth

FusionAuth is a privately held company that was founded in 2007 and is headquartered in Denver. FusionAuth debuted in 2018, and the SaaS version launched in 2019. FusionAuth is a developer-focused customer authentication and authorization platform. They have many customers in the finance, retail, B2B, and gaming markets. The platform can be deployed in Docker containers and can run on premises or in any cloud environment controlled by the customer. FusionAuth is also hosted as SaaS on a public IaaS across multiple continents. Customers can create and isolate multiple individual instances for increased security for B2B2C scenarios. Licensing and/or subscriptions are priced by the number of monthly active users. A free version with basic features is available for both development and production depending on feature and support requirements.

Why worth watching: FusionAuth is SOC 2 Type 2 certified. FusionAuth offers several specialty features, such as advanced family management, and granular home entertainment controls. FusionAuth customers can create separate B2B and B2B2C instances for their customers and their consumers to enhance performance and security. These capabilities are tailored to fit their current target markets in gaming and retail.

Google Firebase

Firebase is a mobile app development platform that has some key CIAM features. Firebase allows app developers to manage users and groups, store user data, and provides some authentication options including Google authentication as well as many other major social network providers. Connectors for other SaaS apps are available. Admins can also use Google Analytics for identity and marketing analyses.

Why worth watching: Google is a major cloud platform with lots of business productivity applications and customers. It would be easy for Google to pivot into offering full-scale CIAM.

Login Alliance Login Master as a Service

Login Alliance Syntlogo was founded in 2001 near Stuttgart. Login-Master can run on-premises in Windows or various flavors of Linux, or in AWS/Azure/GCP IaaS; they also offer it as SaaS running in AWS in the EU region. They can host consumer profile data including complex data types using NoSQL databases. Customer admins can opt for complex role-based delegated admin models.

Why worth watching: They have leveraged their experience in IAM consulting to create Login-Master (CIAM) and Keycloak Sentinel (IAM security) solutions. They are strongest in the DACH region of Europe in terms of sales and support.

Microsoft – Entra External ID

Microsoft Entra External ID is Microsoft's next generation customer identity and access management solution for securing all external identities. This offering is designed to meet the core CIAM needs of both large and small organizations. It is built to scale to millions of customers and B2B users and manages over one billion logins per day. Azure is one of the global leaders in the cloud infrastructure market. Microsoft Entra External ID has a core offering based on number of monthly active users with premium features offered as add-ons.

Why worth watching: Microsoft was unable to participate fully in this report due to the timing of the general availability of Microsoft Entra External ID (May 1) and that new customers will not be able to purchase Azure AD External Identities effective May 1, 2025. The Azure platform is CSA Star Level 1 and 2 certified, HIPAA/HITRUST, ISO 27001/27018, PCI-DSS, and SOC 2 Type 2 attested and/or certified. Microsoft has the infrastructure to enable massive scalability.

Pirean (now Exostar)

Pirean was founded in 2002 with offices in London and Sydney. In 2018, Pirean was acquired by Exostar, an IAM and collaboration solutions provider for highly regulated industries such as Aerospace & Defense and Life Sciences. In July 2020, Exostar was acquired by Thoma Bravo. Pirean provides a Consumer and Workforce IDaaS platform called Access: One. Driven by the industries they serve, Pirean offers multiple MFA options, risk-based analytics, and consent management.

Why worth watching: Exostar has a long history of providing essential identity services for the A&D industry, where security is paramount.

PRIVO

Privacy Vaults Online, better known as PRIVO, was founded in 2001 and is headquartered in the Washington, DC area, with an office in the UK and satellite locations globally. They provide a customer identity and consent management platform engineered specifically to address commercial minors' privacy use cases and minors-associated data. The platform delivers cloud-based, configurable, end-to-end, jurisdiction-aware, minor's identity and privacy services, packaged with tech-enabled privacy assurance programs to help companies comply with US COPPA (Children's Online Privacy Protection Act), GDPR, including the UK Children's Code, and emerging children privacy regulations happening throughout the US and globally. PRIVO is SaaS-delivered, residing in public IaaS distributed across multiple data centers in the US.

Why worth watching: PRIVO serves a specific subset of the CIAM market – helping customers comply with regulations that govern minors' online activities. The company is a member of the Age Verification Providers Association and s US FTC-approved COPPA Safe Harbor.

Quasr

Quasr is an early-stage CIAM startup, founded in 2021, and headquartered in Antwerp, Belgium. Quasr accepts social logins, some authenticator apps, OTP, and some passwordless forms of authentication. It is a developer-centric SaaS. They provide consent management, including time-limited consents and scopes.

Why worth watching: Quasr offers a free tier in certain circumstances. Quasr considers their solution to be a Customer Identity and Privacy Platform.

Stytch

Stytch is a small but well-funded identity startup headquartered in San Francisco, CA. The company launched in 2020. Most of their business is in North America, followed by the EU region. They are developer-focused and specialize in passwordless authentication and user experience improvements for B2B customer and consumer use cases.

Why worth watching: Stytch offers the highest uptime SLA in the industry, and has a wide variety of passwordless authentication methods, and uses external compromised credential intelligence to protect customers from ATOs.

Ubisecure

Ubisecure was founded in 2002 in Finland. Ubisecure is a CIAM and IDaaS provider with additional services. Ubisecure is ISO 27001 compliant. Their Identity Platform provides good

basic CIAM functionality, including registration, MFA, and identity relationship management. It is designed to facilitate customer compliance with EU regulations such as GDPR and PSD2.

Why worth watching: Ubisecure supports KYC and Know Your Business, with leading edge accommodation for LEIs, B2B CIAM and supply chain management.

Related Research

Leadership Compass: Fraud Reduction Intelligence Platforms

Leadership Compass: Passwordless Authentication

Leadership Compass: Identity Fabrics

Executive View: cidaas CIAM

Executive View Thales OneWelcome Identity Platform

Executive View NRI Secure Uni-ID Libra

Whitepaper How to Build the Modern CIAM: For Customers, Consumers, and Citizens

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

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 making 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.

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