KuppingerCole Report

LEADERSHIP COMPASS

By John Tolbert

September 27, 2022

CIAM Platforms

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

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction / Executive Summary

Consumer Identity and Access Management (CIAM) is a well-established and innovative branch of the broader IAM field. CIAM solutions are designed to address specific technical requirements that consumer-facing organizations have that differ from traditional “workforce” or Business-to-Employee (B2E) use cases.

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

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

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

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

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.

1.1 Highlights

- Innovation in CIAM drives the wider IAM market. The “consumerization of IT” is exemplified by the push to use CIAM methods and technologies for registration, authentication, and authorization in workforce IAM.
- Features that were considered innovative in the previous edition of this report are going mainstream.
- The new entrants in CIAM tend to coalesce locally; that is, the startups form to address region or country specific use cases, populations, or government regulations. In other cases, new CIAM businesses offer some new technologies, modifications on deployment methods, or better licensing or subscription models.
- Support for consumer IoT device identity linking is growing. Smart Home, wearable, and entertainment devices are proliferating, thus the need for such integration will increase as well.
- Account TakeOver (ATO) protection is required for all industries and use cases. Some CIAM platforms provide advanced capabilities, and others provide connectors to third-party services. Multi-factor authentication is a primary defense mechanism against ATO.
- Participating vendors indicate that MFA usage remains relatively low among their customers.
- Account Opening (AO) fraud is a persistent problem across many industries, particularly those in finance. Identity proofing services help mitigate against AO fraud, and some CIAM service providers have integrations with one or more identity proofing services.
- Consent collection and management requirements are expanding as more jurisdictions enact privacy regulations. However, consent management capabilities within CIAM platforms differ in the quality of consent management features provided, with some offering turnkey regulatory support while others deliver a Do-It-Yourself (DIY) consent collection base that needs customization.
- The Overall Leaders in CIAM in alphabetical order are ForgeRock, IBM, LoginRadius, Microsoft, Okta, OneWelcome, Ping Identity, SAP, Transmit Security, and WSO2.
- The Product Leaders in CIAM are cidaas, Cloudentity, ForgeRock, IBM, LoginRadius, Okta,

OneWelcome, Ping Identity, SAP and WSO2.

- The Innovation Leaders in CIAM are 1Kosmos, cidaas, Cloudentity, ForgeRock, IBM, LoginRadius, Okta, OneWelcome, Ping Identity, SAP, Transmit Security, and XAYONE
- The Market Leaders in CIAM are ForgeRock, IBM, LoginRadius, Microsoft, Okta, Ping Identity and SAP.

1.2 Market Segment

The CIAM market is growing and there is room for much further expansion, with many vendors offering mature solutions providing standard and deluxe features to support millions of users across every industrial sector. As will be reflected in this report, the solutions in this space are quite diverse. Some vendors have about every feature one could want in a CIAM product, while others are more specialized, and thus have different kinds of technical capabilities. For example, some smaller vendors are targeting the government-to-citizen (G2C) market as well as business-to-business-to-consumer (B2B2C). Businesses in finance have AML and KYC requirements, which drives the technical need for higher identity and authentication assurance solutions. We more commonly see support for onboarding consumers by validating digital accounts against national e-IDs, passports, driver's licenses, and x.509 certificates at registration time using mobile apps that do selfie photo matching and data retrieval over NFC. Select companies in the hospitality industry, especially the short-term rentals market, are looking for CIAM solutions with the ability to verify credentials at the time of booking. The types of customers that require higher assurance identity proofing also tend to need higher assurance authentication mechanisms as well.

Furthermore, KuppingerCole research indicates that the particular market segments that vendors choose to target often has a direct effect on the type of features available in their CIAM solutions. For example, CIAM vendors that are primarily pursuing retail and media companies as clients tend to not have as much customer-driven pressure to support high assurance identification and authentication and complex attribute-based access controls.

Additionally, CIAM solutions can be somewhat regionalized, in that, some vendor products/services are specialized in meeting the particular regulatory requirements of a country or a group of countries. For example, there are a few vendors that rely upon the national IDs or bank IDs of the Nordic region of Europe, and provide interoperability with service providers in that area, and help customers adhere to GDPR. Likewise, we find vendors that have solutions tailored to the business and regulatory conditions within Latin American countries or APAC countries, with regionalized language support and excellent interoperability with service providers in those areas. These features are competitive advantages for these vendors and may be especially attractive solutions to customers in these areas.

The number of vendors in the CIAM market is rising, in response to the increasing market size. Many of them are built from the ground up as purely consumer-oriented identity solutions. Other vendors have

modified their traditional LDAP-based, Web Access Management (WAM) components to accommodate consumers. All the major players in the CIAM segment are covered within this KuppingerCole Leadership Compass, as well as the specialized regional players. This Leadership Compass will examine solutions that are available for both on-premises and cloud-based deployment. However, most new vendor solutions are built in the cloud, and most customers are looking for cloud delivered solutions.

1.3 Delivery Models

In the CIAM market, solutions are offered mainly as SaaS. Some vendors have products for installation in IaaS, PaaS, or for on-premises deployment. Pure-play SaaS solutions are mostly multi-tenant by design. There are a few vendors that offer single-tenant and single-instance cloud-hosted platforms, which provides additional logical separation for data privacy as well as performance and SLA upgrades.

For SaaS offerings, the licensing/subscription model is often priced per user, either active users in a given time period or by the number of registered users. For managed services or PaaS, the licensing costs can be per instance, or per managed identity. The cloud delivered variants sometimes charge per-session or per-transaction fees. For on-premises deployments, licensing costs can be measured in a couple of different ways, such as per-user or per-server. There are other more complex licensing or subscription options offered by some vendors, although these are generally perceived as cumbersome by customers and prospects.

1.4 Required Capabilities

- Deployment options: SaaS-hosted; IaaS, PaaS, hybrid, or on-premises installation
- Social logins: Allow users to register and login using OIDC credentials from social network operators such as Facebook, Apple, Twitter, Google, Amazon, etc.
- Seamless branding: White-labeled solutions allow customers to have a brand-consistent look and feel.
- Progressive profiling: The collection of consumer or customer information on an as-needed basis, rather than requesting it all up front.
- Identity proofing service integration: The ability to increase identity assurance at the time of account registration and/or subsequent interactions is required in financial use cases, and increasingly for other businesses as well. Many identity verification services exist across the globe, and some CIAM vendors provide either out-of-the-box connectors or the ability to integrate with such service

providers over APIs.

- Multi-factor authentication: mobile biometrics, behavioral biometrics, mobile apps and SDKs, FIDO2 & WebAuthn, etc. Email/phone/SMS OTP are prevalent as MFA methods but are not recommended. Best used as part of an overall risk-adaptive authentication approach.
- Account recovery mechanisms: When consumers forget passwords, lose credentials, or change devices, they need ways to get access to their accounts. Account recovery techniques include email/phone/SMS OTP, “magic links”, mobile push notifications and applications, and account linking. Knowledge-Based Authentication (KBA), the use of “security questions”, is to be avoided since this method is even less secure than password authentication.
- Ability to include and process 3rd-party fraud intelligence: Runtime evaluation of internal or external cyber threat or fraud information, such as known bad IP addresses/domains, compromised credentials, accounts suspected of fraud, fraud patterns, botnet behavior, etc., for the purpose of reducing the risk of fraud at the login and transaction level. Many specialist FRIP services are present in the market; CIAM platforms should allow customers to plumb these FRIP services into their authentication policies and risk analysis processes.
- Identity analytics: Dashboards and reports on common identity attribute activities including failed logins, consumer profile changes, credential changes, registration tracking, etc.
- Secure and well-documented APIs and support for communications standards: CIAM vendors have trended away from packaging comprehensive identity and marketing analytics functions within their platforms. Support for REST APIs, Webhooks, syslog, etc. allows customers to process identity event information outside of the CIAM platform in other tools that are specialized for such data analysis and actions; specifically, Business Intelligence (BI), Customer Relationship Management (CRM), and marketing analytics and automation systems.
- Privacy and consent management: Explicit user consent must be received for the use of their information. Consumer account dashboards are common mechanisms for providing users with consent monitoring, granting, and withdrawal options. Family management, or the ability to set up specialized delegated account administration for heads of households, parents, guardians, children, and other relationship types is increasingly needed in the CIAM landscape.
- IoT device identity association: As IoT devices increase in popularity, consumers and business customer users will have greater need to associate their IoT devices with their digital identities. These identity associations between subject and IoT object will allow for more secure use of Smart Home, wearables, fitness, medical, and digital media devices. Basic functions for IoT device identity association require support for OAuth2 Device Flow and the ability for consumers to add/remove/validate devices in the self-service interfaces provided by the vendors.

The criteria evaluated in this Leadership Compass reflect the varieties of use cases, experiences, business rules, and technical capabilities required by KuppingerCole clients today, and what we anticipate clients will need in the future. The products examined meet many of the requirements described above, although they sometimes take different approaches in solving the business problems.

When evaluating the services, besides looking at our standard criteria of

- overall functionality and usability
- internal product/service security
- size of the company
- number of tenants/customers and end-user consumers
- number of developers
- partner ecosystem
- licensing models

We've also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other offerings available in the market. Features that are considered innovative are listed below.

- Multi-cloud, multi-region deployments for SaaS-delivered solutions. The more coverage, the better the SLA uptime.
- Options for separate instances per customer for maximum data separation and processing scalability.
- Onboarding orchestration: flexibility in designing consumer registration and identity verification processes. The most advanced solutions have graphical workflows that allow customer admins to orchestrate steps, including collection of additional information from consumers, running identity verification processes on consumer devices, executing attribute queries against authoritative sources, and invoking 3rd-party identity proofing services.
- Built-in identity verification capabilities, usually instantiated within mobile apps that have the ability to utilize national e-IDs, bank IDs, passports, driver's licenses as authoritative documents for registration and KYC; and perform document photo to selfie matching.
- Granular risk adaptive authentication and authorization: Evaluation of runtime device and environmental parameters, user behavioral analytics, and fraud intelligence to match the appropriate authentication mechanisms to the level of business risk or as required by regulations. Includes ability to interoperate with customer line-of-business applications.

- Availability of pre-packaged connectors for 3rd-party Business Intelligence (BI), Customer Relationship Management (CRM), and marketing analytics and automation tools.
- SDKs that harvest a broad range of device attributes and environmental information for analysis by the risk engine.
- Built-in fraud detection functions, such as the use of credential intelligence from in- and out-of-network sources.
- Advanced consent and privacy management functions. Some solutions facilitate compliance with EU GDPR, Canada's PIPEDA, Brazil's LGPD, and California's CCPA, by providing templates and custom controls. Consent and privacy management can also be augmented by API-level integration with specialized 3rd-party services. Additional features in this area include family management that allows parents/guardians to control minors' access to content for digital media.
- Advanced support for IoT, Smart Home, connected cars, digital media devices, fitness and wearables use cases. This may include dedicated interfaces for popular devices, extensive API integration with IoT vendor digital services, and family management that allows parents/guardians to control minors' usage of devices.

Please note that we only listed a sample of features, and we consider other capabilities per solution as well when evaluating and rating the various CIAM platforms.

2 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 evaluation, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

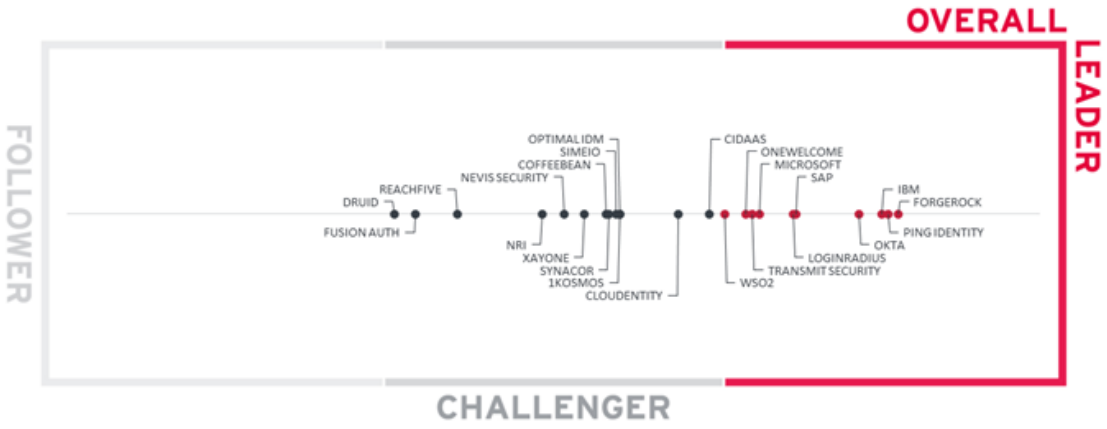


Figure 1: Overall Leaders in CIAM

The Overall Leadership rating is a combined view of the three Leadership categories, i.e., Product Leadership, Innovation Leadership, and Market Leadership. This consolidated view provides an overall impression of our rating of the vendor's offerings in this market segment. We strongly recommend looking at

all Leadership categories, the individual analysis of the vendors and their products to gain a comprehensive understanding of the players in that market segment.

CIAM is a mature market segment with a well-defined feature set. The market itself is quite large and continues to grow. The Overall Leaders in CIAM are ForgeRock, Ping Identity, IBM, Okta, SAP, LoginRadius, Microsoft, Transmit Security, OneWelcome, and WSO2.

The top Challengers are cidaas and Cloudentity. Also in the Challenger section we find Optimal IDM, 1Kosmos, Simeio, Synacor, CoffeeBean Technology, XAYONE Solutions, Nevis Security, NRI, ReachFive, FusionAuth, and DruID.

Leadership does not automatically mean that these vendors are the best fit for a specific customer environment. A thorough evaluation of organizational requirements and a mapping of product functions and features will be necessary.

Overall Leaders are (in alphabetical order):

- ForgeRock
- IBM
- LoginRadius
- Microsoft
- Okta
- OneWelcome
- Ping Identity
- SAP
- Transmit Security
- WSO2

2.2 Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of service features and the overall capabilities of the various services.

Figure 2: Product Leaders in CIAM

Product Leadership, or in some cases Service Leadership, is where we examine the functional strength and completeness of services. Ping Identity and ForgeRock are at the top of the product leadership chart, along with IBM, Okta, LoginRadius, cidaas, OneWelcome, Cloudentity, WSO2, and SAP.

We see a good distribution across the Challenger section with many near the boundary. Microsoft, CoffeeBean Technology, Transmit Security, 1Kosmos, and XAYONE Solutions are closest to the border with the leaders. Simeio, Nevis Security, Optimal IDM, Synacor, and NRI are in the center. FusionAuth and ReachFive round out the Challengers. DruID is at the top of the Follower section.

Product Leaders (in alphabetical order):

- cidaas
- Cloudentity
- ForgeRock
- IBM
- LoginRadius
- Okta
- OneWelcome
- Ping Identity
- SAP
- WSO2

2.3 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.

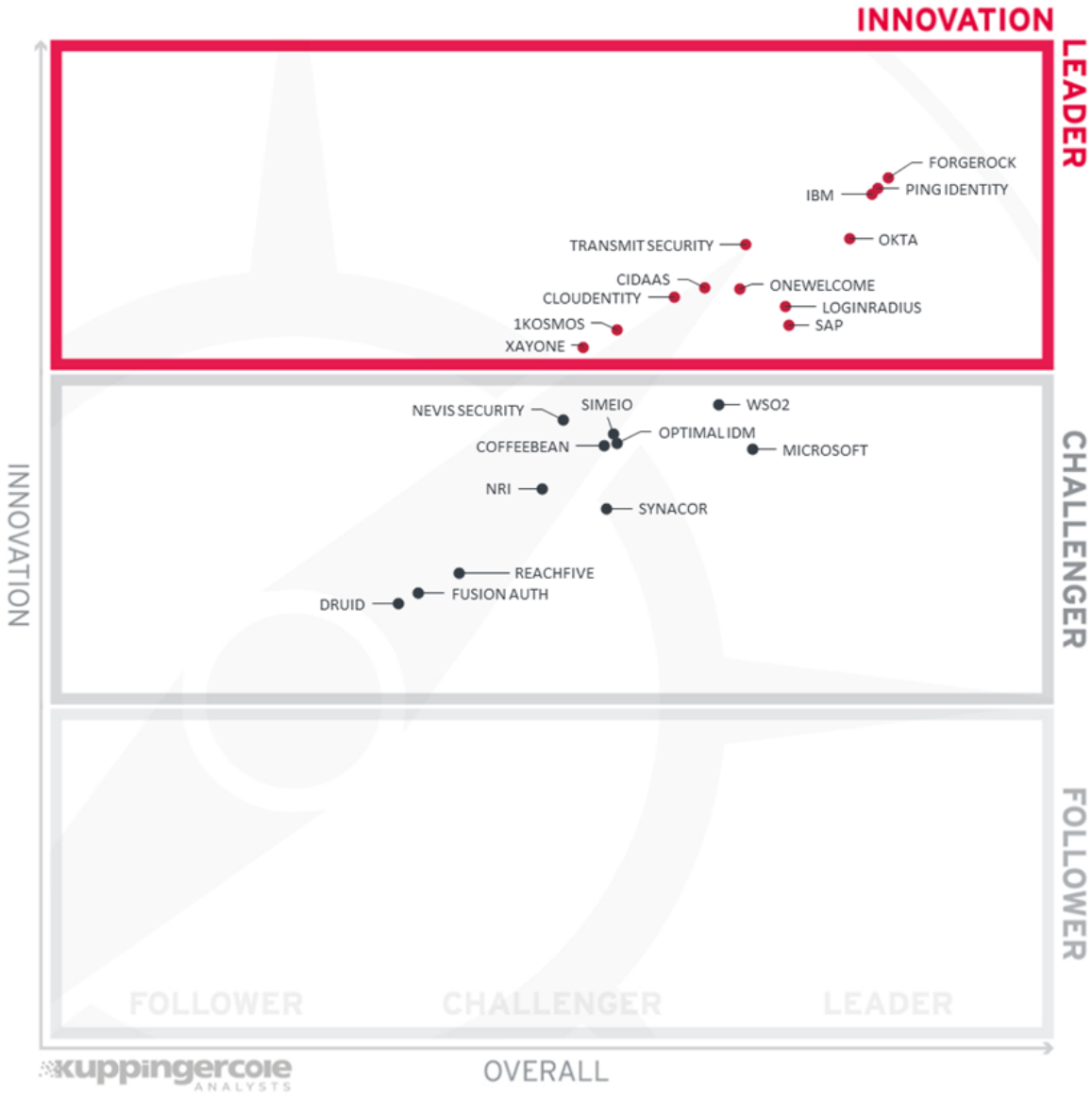


Figure 3: Innovation Leaders in CIAM

As a mature discipline, CIAM has many features that are expected and several features that are innovative enough to set some vendors' solutions apart from the rest. Among the noteworthy innovative developments in CIAM as of this report are mobile identity assurance apps, mobile SDKs, use of device and credential intelligence, the ability to define onboarding workflows and advanced orchestration, granular risk engines for assessing authentication context risk, and packaged integrations for fraud reduction and other identity and security services.

ForgeRock, Ping Identity, and IBM are clustered at the top of the Innovation Leadership chart. Okta, Transmit Security, cidaas, OneWelcome, Cloudentity, LoginRadius, SAP, 1Kosmos, and XAYONE Solutions

also appear as top Innovators in this edition.

The Challengers are spread across the center section: WSO2, Nevis Security, Simeio, Optimal IDM, CoffeeBean Technology, Microsoft, NRI, Synacor, ReachFive, FusionAuth, and DruID.

Innovation Leaders (in alphabetical order):

- 1Kosmos
- cidaas
- Cloudentity
- ForgeRock
- IBM
- LoginRadius
- Okta
- OneWelcome
- Ping Identity
- SAP
- Transmit Security
- XAYONE

2.4 Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, 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 financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

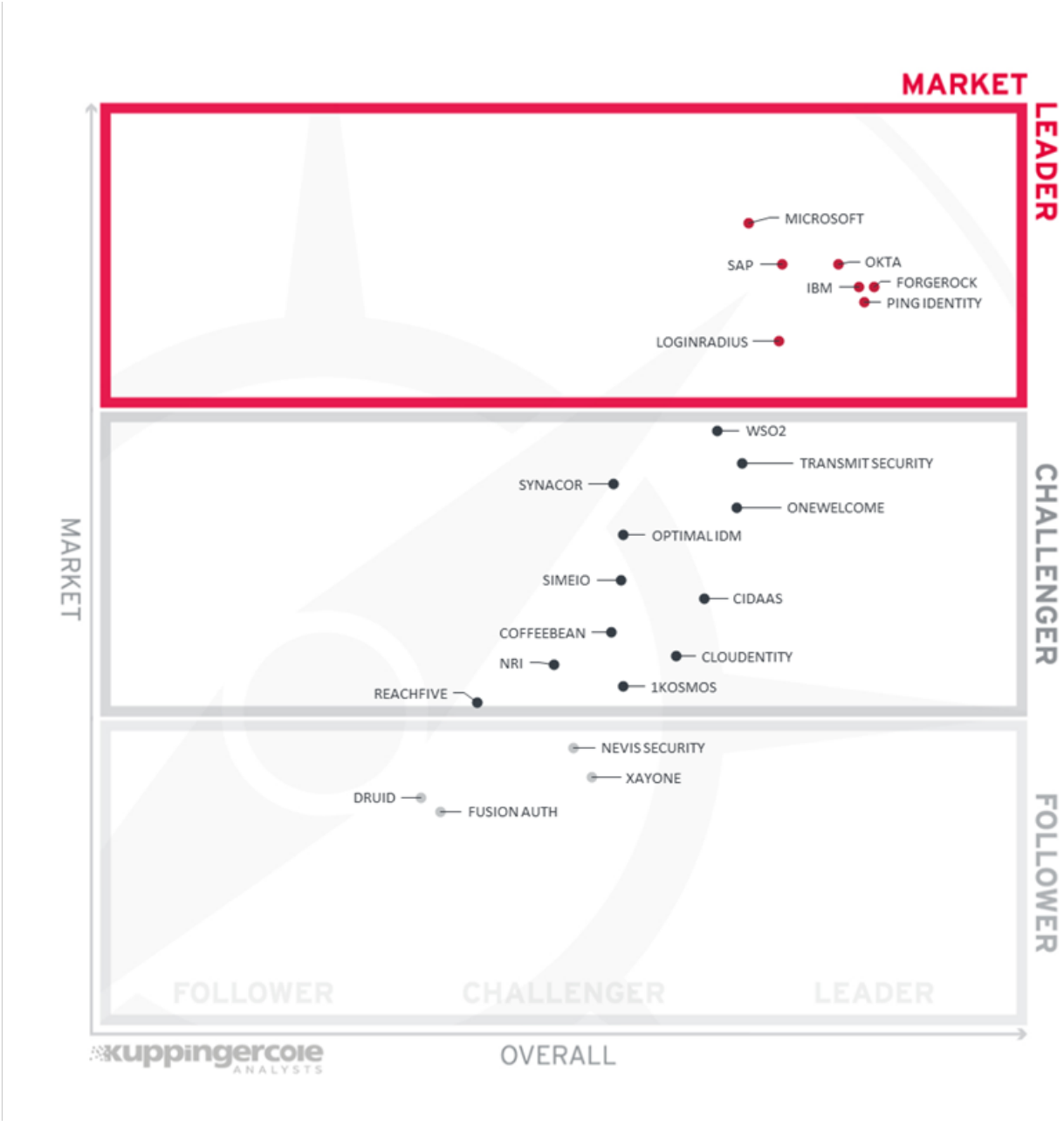


Figure 4: Market Leaders in CIAM

Market Leadership in CIAM is determined by many factors, including overall vendor financial position, company sizes, numbers and geographic distribution of customers, number and geographic distribution of ecosystem partners such as system integrators, and levels of regional support.

Microsoft, Okta, SAP, IBM, ForgeRock, Ping Identity, and LoginRadius are the Market Leaders in CIAM in 2022.

The Challengers are spread very evenly: WSO2, Transmit Security, Synacor, OneWelcome, Optimal IDM, Simeio, cidaas, CoffeeBean Technology, Cloudentity, NRI, 1Kosmos, and ReachFive.

The Followers in this market are more geographically limited but have room to grow: Nevis Security, XAYONE Solutions, DruID, and FusionAuth.

Market Leaders (in alphabetical order):

- ForgeRock
- IBM
- LoginRadius
- Microsoft
- Okta
- Ping Identity
- SAP

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The first of these correlated views contrasts Product Leadership and Market Leadership.

3.1 The Market/Product Matrix

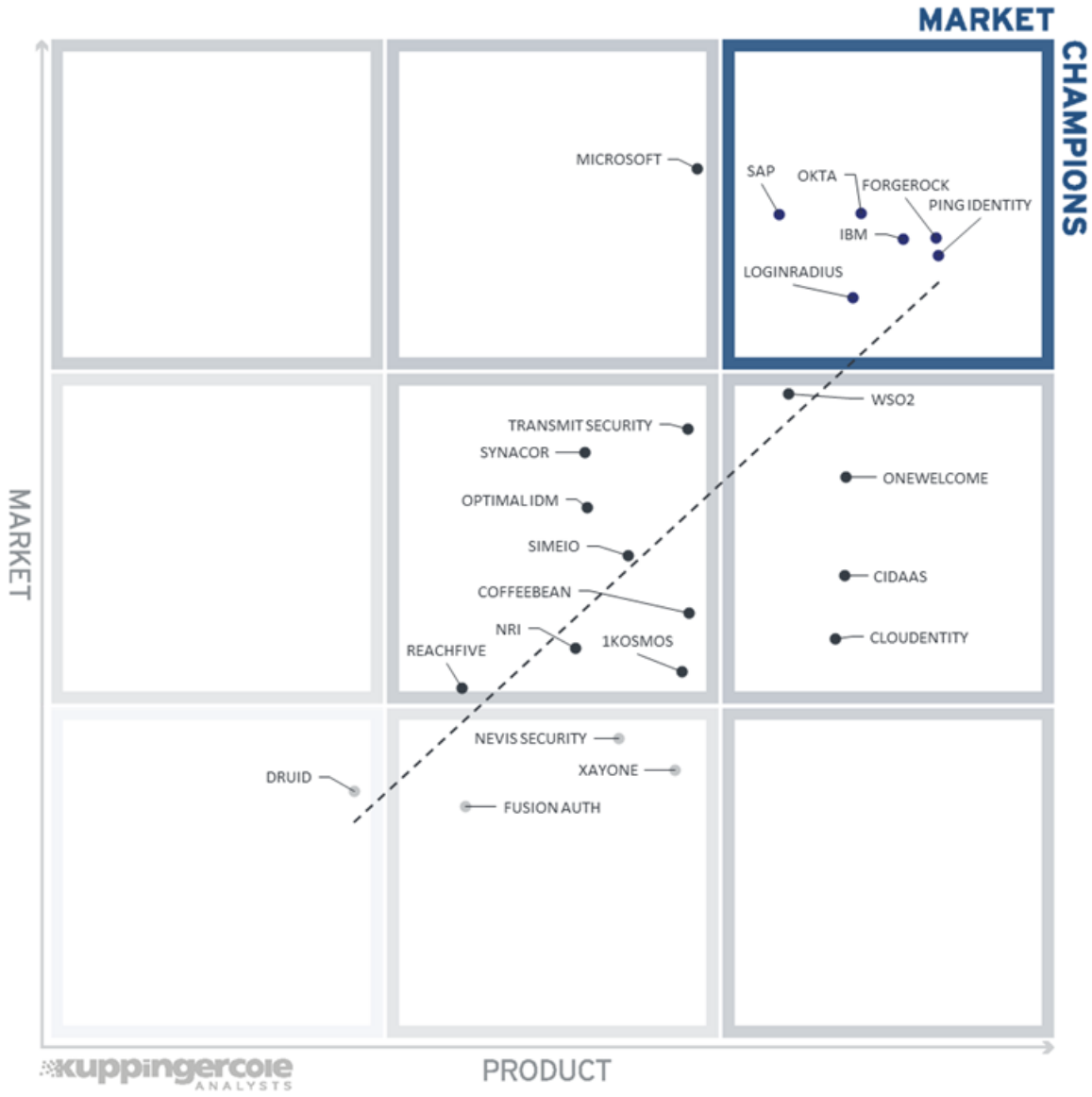


Figure 5: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership.

All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.
The Market Champions are (in alphabetical order) ForgeRock, IBM, LoginRadius, Okta, Ping Identity, and SAP. Microsoft is in the top center with a sizable share of the CIAM market. WSO2, OneWelcome, cidaas, and Cloudentity are in the right center below the line, indicating excellent growth potential in relation to the

strength of their solutions.

Transmit Security, Synacor, Optimal IDM, Simeio, and ReachFive are in the center box above the line. CoffeeBean Technology, NRI, and 1Kosmos are in the center below the line.

In the lower center, we find Nevis Security, XAYONE Solutions, and FusionAuth. DruID is in the lower left area.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

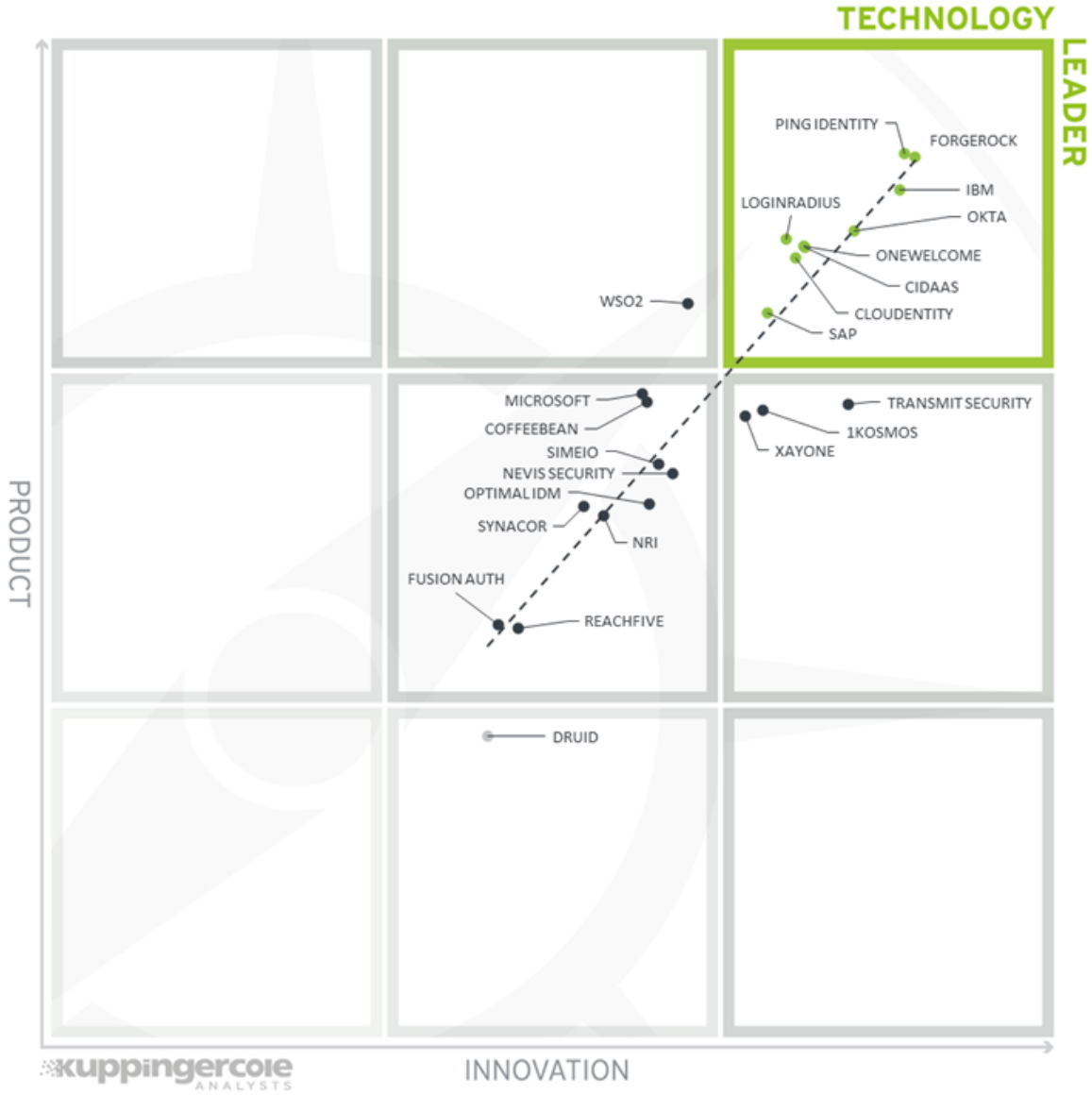


Figure 6: The Product/Innovation Matrix

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.
The Technology Leaders are (in alphabetical order) cidaas, Cloudentity, ForgeRock, IBM, LoginRadius, Okta, OneWelcome, Ping Identity, and SAP.

WSO2 is in the top center box. Transmit Security, 1Kosmos, and XAYONE Solutions are in the center right section below the line.

In the center of the grid, we see Microsoft, CoffeeBean Technology, Simeio, Nevis Security, Optimal IDM,

Synacor, NRI, FusionAuth, and ReachFive.
DruID is in the lower center section.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

Figure 7: The Innovation/Market Matrix

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

The Big Ones in CIAM are (in alphabetical order) ForgeRock, IBM, LoginRadius, Okta, Ping Identity, and SAP. Microsoft is in the top center. Transmit Security, OneWelcome, cidaas, Cloudentity, and 1Kosmos are in the center right box.

WSO2, Synacor, Optimal IDM, Simeio, CoffeeBean Technology, NRI, and ReachFive are in the center

section.

XAYONE Solutions is in the lower right. Nevis Security, DruID, and FusionAuth are in the lower center box.

4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on CIAM Platforms. 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.

Product	Security	Functionality	Deployment	Interoperability	Usability
1Kosmos BlockID Customer and BlockID Verify	strong positive	positive	positive	strong positive	positive
cidaas	positive	strong positive	strong positive	strong positive	strong positive
Cloudentity	strong positive	strong positive	positive	strong positive	strong positive
CoffeeBean Technology Identity and Access Platform	positive	positive	positive	positive	positive
DruID Identity and Pulse	neutral	weak	weak	neutral	neutral
ForgeRock Identity Platform	strong positive	strong positive	strong positive	strong positive	strong positive
FusionAuth	neutral	neutral	positive	neutral	neutral
IBM Security Verify	strong positive	strong positive	strong positive	strong positive	strong positive
LoginRadius CIAM Platform	strong positive	strong positive	strong positive	strong positive	strong positive
Microsoft External Identities	strong positive	positive	strong positive	neutral	positive
NEVIS Security Identity Suite and Authentication Cloud	strong positive	neutral	positive	neutral	neutral
NRI Secure Uni-ID Libra	neutral	neutral	neutral	neutral	neutral
Okta CIAM	strong positive	strong positive	strong positive	strong positive	strong positive
OneWelcome Identity Suite	strong positive	strong positive	positive	strong positive	strong positive
Optimal IdM OptimalCloud	positive	neutral	neutral	positive	neutral
Ping Identity PingOne Cloud	strong positive	strong positive	strong positive	strong positive	strong positive
ReachFive	positive	weak	neutral	weak	neutral
SAP CIAM (B2B and B2C)	strong positive	positive	strong positive	positive	positive
Simeio Identity Orchestrator	strong positive	positive	positive	neutral	positive
Synacor Cloud ID	positive	neutral	neutral	positive	positive
Transmit Security CIAM Platform	strong positive	positive	strong positive	strong positive	positive
WSO2 Identity Server	strong positive	positive	strong positive	strong positive	positive
XAYONE Solutions	strong positive	positive	neutral	positive	positive
Legend		critical	weak	neutral	positive	strong 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	weak
cidaas	strong positive	neutral	weak	weak
Cloudentity	strong positive	neutral	weak	neutral
CoffeeBean Technology	positive	neutral	weak	neutral
DruID	weak	weak	weak	weak
ForgeRock	strong positive	strong positive	strong positive	strong positive
FusionAuth	neutral	weak	weak	weak
IBM	strong positive	strong positive	strong positive	strong positive
LoginRadius	strong positive	strong positive	neutral	positive
Microsoft	positive	strong positive	strong positive	strong positive
NEVIS Security AG	positive	weak	weak	weak
NRI Secure Technologies	positive	neutral	positive	weak
Okta	strong positive	strong positive	strong positive	strong positive
OneWelcome	strong positive	positive	strong positive	positive
Optimal IdM	positive	positive	positive	neutral
Ping Identity	strong positive	strong positive	strong positive	strong positive
ReachFive	neutral	weak	weak	neutral
SAP	strong positive	strong positive	strong positive	strong positive
Simeio Solutions	positive	neutral	positive	positive
Synacor	neutral	positive	positive	strong positive
Transmit Security	strong positive	strong positive	positive	strong positive
WSO2	positive	positive	positive	positive
XAYONE Solutions	strong positive	weak	weak	weak
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

This section contains a quick rating for every product/service we've 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 the LC CIAM, we look at the following eight categories:

- **Onboarding** – this metric examines the registration options available, support for bulk provisioning for migration between solutions, progressive profiling options, phone/computer associations with consumer accounts, 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 3rd-party identity proofing services and by remote onboarding applications (mobile and web-based) that perform validation of authoritative documents and issuance of digital credentials.
- **ATO protection** – this category evaluates the presence of functions that help prevent consumer account takeovers. ATO protection features include credential intelligence, device intelligence, user behavioral analysis, behavioral biometrics, and bot detection. Some CIAM solution providers deploy these capabilities within their platforms, and some partner with 3rd-party Fraud Reduction Intelligence Platforms (FRIP).
- **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.

- **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 optimum 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 3rd-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.

5.1 1Kosmos

1Kosmos was founded in 2018 and is headquartered in New Jersey. The company is small but profitable and growing. 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 in public IaaS data centers across multiple regions. It is multi-tenant, and customers can create sub-tenants under their control. Per-transaction/session and per-user annual subscription pricing models are available.

1Kosmos BlockID Customer allows for customizable user registration workflows and supports social network registration (except Amazon and Apple) and bulk user imports via LDAP. The 1Kosmos LiveID mobile app can do identity proofing by comparing selfies to consumers' government issued ID docs. It is designed in accordance with eIDAS and US NIST 800-63-3 IAL3. 1Kosmos also works with Mitek, Socure, and Zenkey ID proofing services. 1Kosmos' mobile app uses fingerprint and facial recognition and performs liveness detection. Live Biometrics and other mobile-based methods are used for account recovery. Other authenticators supported include Duo, Google, OneSpan, Thales, TrustKey, and Yubikeys. JWT, OAuth2, OIDC, and SAML are supported for federated access. 1Kosmos provides SDKs, which can collect a full range of device intelligence signals and some behavioral biometrics attributes. The BlockID risk engine evaluates SDK telemetry and credential intelligence and then outputs a score. Step-up options are configurable on a per community basis in the AdminX portal. Advanced policy authoring is on the roadmap.

1Kosmos has integrations with Fraud Reduction Intelligence Platforms including BioCatch, Cleafy, HID Global, LexisNexis, OneSpan, Outseer, and TransUnion; and a variety of SaaS apps and SSO platforms. BlockID can also integrate with other apps such as marketing analytics and automation tools via REST API, Webhooks, and WebAuthn. Identity analytics are produced and can be viewed as standard reports or exported and analyzed in 3rd-party solutions such as Informatica, Oracle BI, SAP, and Tableau. CEF and syslog enable connectivity to customer SIEMs.

BlockID allows customers to view, granularly select attributes, and edit profile information in the mobile app or via the AdminX console. The AdminX console can be presented to consumers as a self-service portal. Each user can create multiple personas, which can be deleted within the app. Family management and Kantara Consent Receipt are not currently supported but planned. IoT device identity to consumer account linking is also planned for 2022.

1Kosmos has obtained ISO 27001 certification and SSAE 18 SOC 2 Type 2 is in work. The BlockID Platform is W3C compliant, and 1Kosmos is a member of Trust Over IP, Decentralized Identity Foundation, and Hyperledger Indy. Their server implementation is FIDO2 certified. Visual policy editor, support for IoT device integration, and family management are on their roadmap. 1Kosmos has excellent mobile authentication and profile management features. Integration with identity and marketing analytics and automation requires customization. Organizations shopping for CIAM solutions that have requirements for strong, standards-based consumer authentication capabilities will want to consider 1Kosmos.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●○

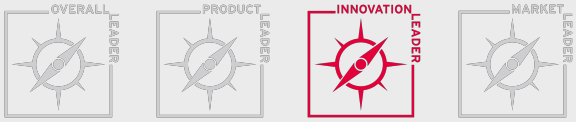
Strengths

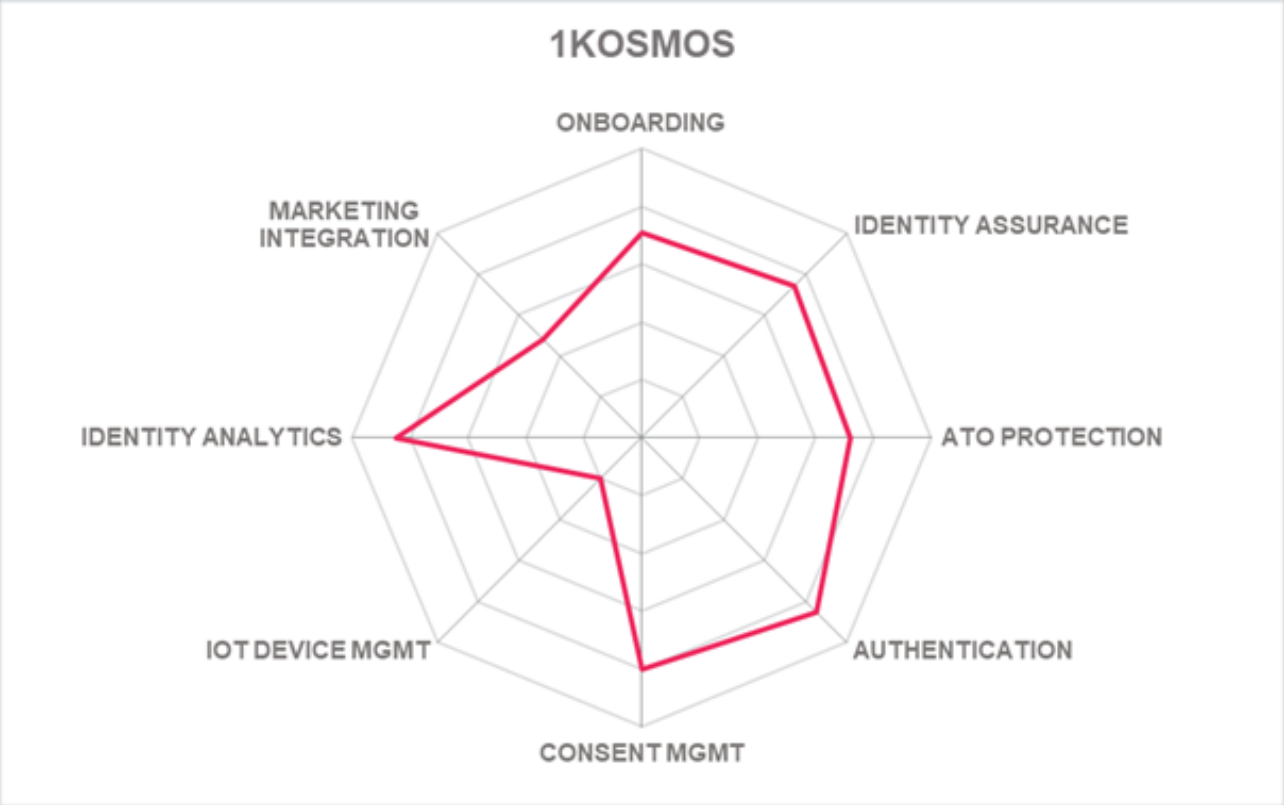
- Build-in identity proofing features and remote onboarding app
- Blockchain-based verifiable credentials
- FIDO2 server certified
- eIDAS and NIST 800-63 IAL3 support
- LiveBiometrics for strong authentication
- Multiple FRIP integrations available

Challenges

- Visual policy editor slated for later in 2022
- Family management not supported
- IoT device identity integration in work
- Limited connectors for marketing analytics and automation but apps can be integrated via APIs
- Sales and support concentrated on North America with some in APAC, no EU presence

Leader in




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

5.2 cidaas

Widas was founded in Germany in 1997, and in 2018 they launched cidaas, their CIAM product and brand. cidaas is hosted primarily as SaaS, but customers can run it in most IaaS platforms. 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 by either monthly active or registered users.

cidaas allows bulk import of users via LDAP and REST API. All OIDC-based social logins are supported. Account recovery options run the gamut of common techniques. Registration workflows can easily be customized using the graphical process editor. cidaas' Autoident is a mobile identity proofing app that performs selfie/video matching against eIDAS-compliant government issued ID documents. cidaas authenticator leverages Android and iOS biometrics. cidaas' biometrics can be used for Physical Access Controls for consumer scenarios. Other authenticators supported include FIDO UAF/U2F/2.0, OTPs, mobile push, and popular apps such as Authy, Google, LastPass, Microsoft, OneSpan, SaaSPASS, and SafeNet. All federation protocols are supported. cidaas' SDK collects device intelligence and has some behavioral biometrics functions. The solution considers in-network credential intelligence. Authentication and authorization policies are easily configured in the flow-chart style admin GUI.

cidaas supports gRPC, REST, WebAuthn, Webhooks, and Websockets APIs. Connectors for some SaaS apps are available on their marketplace. For CRM and business analytics, integrations are available for Emarsys, Hubspot, Microsoft Dynamics 365, Salesforce, and Tableau. cidaas ships with many useful identity and marketing analytics reports. Customers can integrate 3rd-party FRIP sources, but connectors are not pre-built due to lack of demand. CEF and syslog enable communications with customer SIEMs.

cidaas provides consumer self-service portals where consent can be granted, managed, and revoked in accordance with GDPR. Data Subject Access Request templates are provided. cidaas' portal also has built-for-purpose family management, as well as the more common approach of adapting a delegated administration model. Kantara Consent Receipt is supported. IoT device identity association and management are handled in the consumer UI, and encompasses home automation, wearables, and consumer electronics device types. cidaas consumers can authorize their devices to “act on behalf of” the user for certain use cases. Advanced use cases include storing and present event tickets, geo-fencing and Bluetooth beacon integration.

cidaas has attained ISO 27001 audit certification. Additional security certifications would be beneficial. Their service architecture should enable high performance and scalability. cidaas’ primary area of operation is the DACH region of the EU, but they are growing rapidly due to their innovative product. cidaas has excellent identity proofing, authentication, consent management, and device identity management capabilities. Packaged connectors for 3rd-party FRIP services would be appealing. cidaas enables some avant-garde use cases such as the remote onboarding app, advanced consumer IoT device management, and physical access controls for event management. Organizations that need an innovative CIAM platform will want to consider cidaas.

Security	●●●●○
Functionality	●●●●●
Deployment	●●●●●
Interoperability	●●●●●
Usability	●●●●●

cidaas®

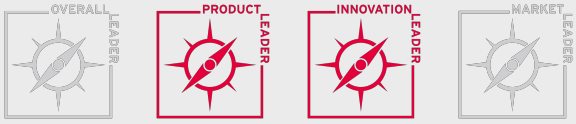
Strengths

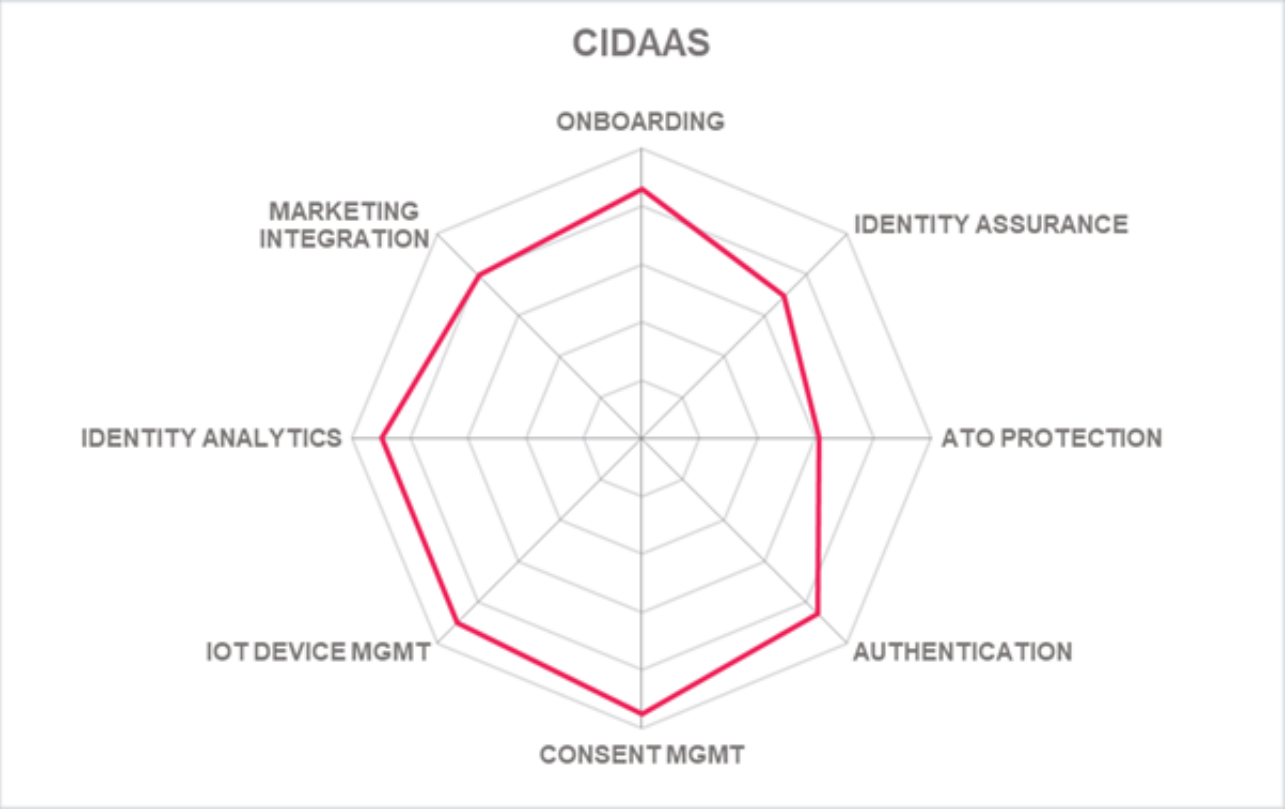
- Customizable registration workflows
- Mobile app for eIDAS-compliant high assurance identity proofing, with 200 authoritative document types supported
- Excellent admin interface for policy construction
- Self-service portal facilitates consumer privacy management
- Family user relationships are easily managed
- Advanced IoT device identity association and management, and geo-fencing
- Supports leading-edge physical access controls use cases such as event management

Challenges

- Supports FIDO but not certified
- Third-party identity proofing and FRIP integrations not present
- Need additional connectors for external marketing analytics & automation services
- Mostly focused on DACH region, but growing

Leader in




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

5.3 Cloudentity

Cloudentity was founded in 2018 and is headquartered in Seattle. 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 CentOS, RHEL, or SUSE; and it is cloud-agnostic so it can be deployed public IaaS environments such as Alibaba, AWS, Azure, or GCP. They also offer their solution as SaaS delivered from public IaaS across multiple regions including US, UK, Europe, Australia. Cloudentity's subscription pricing is based on the number of authorization grants performed per month regardless of how many active or eligible users the customer serves.

Cloudentity customers can import users via LDAP, REST, and SCIM. Social network registration and authentication can be used except Apple. Registration workflows are customizable in the GUI and allow fine-grained consent and sophisticated authorization evaluations. All typical account recovery mechanisms are present. Identity proofing is not built-in but can be configured via the policy framework. OTP, mobile push, and the most common authenticator apps are accepted. Cloudentity provides a mobile SDK with limited device intelligence capabilities. Behavioral biometrics are not utilized but can be considered in authorization policies if they are gathered by 3rd-party products and provided to Cloudentity during the authorization request flow. Credential intelligence from 3rd party providers such as Vericlouds can be easily leveraged in risk decisions. The administrative console is highly functional and intuitive, enabling customers to create detailed authentication and authorization policies using a flow-chart and drag/drop style interface. Rego policy authoring for Open Policy Agent (OPA) is supported. Rego policies can then be embedded in regular policies created in the console.

GraphQL, gRPC, REST, RPC, SOAP, Webhooks, and WebAuthn can be used to extend the solution. No connectors for FRIP services or SaaS apps are present, but customers could code their own connectors to any FRIP or SaaS API using the above methods. Cloudentity performs automated discovery of applications, services, and workloads; automated onboarding of applications; and automated deployment of baseline policies. Cloudentity can control enforcement points within Amazon, Axway, Apigee (Google), Docker, HashiCorp, Istio, Kong, Kubernetes, and Mulesoft (Salesforce). Basic identity analytic reports are available. Logs can be sent to customer SIEMs or analytics programs over CEF or syslog. Connectors are available for ELK, HubSpot, and Salesforce.

Cloudentity presents a consumer dashboard where users can view, edit, and delete personal information and consents in accordance with privacy regulations. Cloudentity has good support for family management use cases, including US COPPA regulations. Moreover, Cloudentity adheres to the Kantara Consent Receipt specification for interoperability with 3rd-party consent management platforms. Cloudentity can leverage OAuth2 Device Flow register and manage consumer IoT devices.

Cloudentity completed ISO 27001 and SOC 2 Type 2 audits in early 2022. Some additional features, such

as support for 3rd-party identity proofing and FRIP services, more authenticator types, and FIDO certification would enhance the offering. Cloudentity is a smaller vendor, but they continue to gain traction in the marketplace, due to their highly innovative features and ability to support advanced authorization and consent management use cases that other vendors have not addressed. Cloudentity's cloud-based service architecture is leading-edge and should scale as needed. Organizations that are looking for CIAM solutions with a modern design or add-ons to CIAM solutions that can support complex authorization and consent management scenarios should take a look at Cloudentity.

Security	●●●●●
Functionality	●●●●●
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●●

CLOUDENTITY

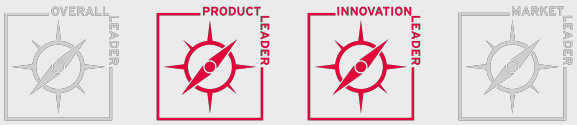
Strengths

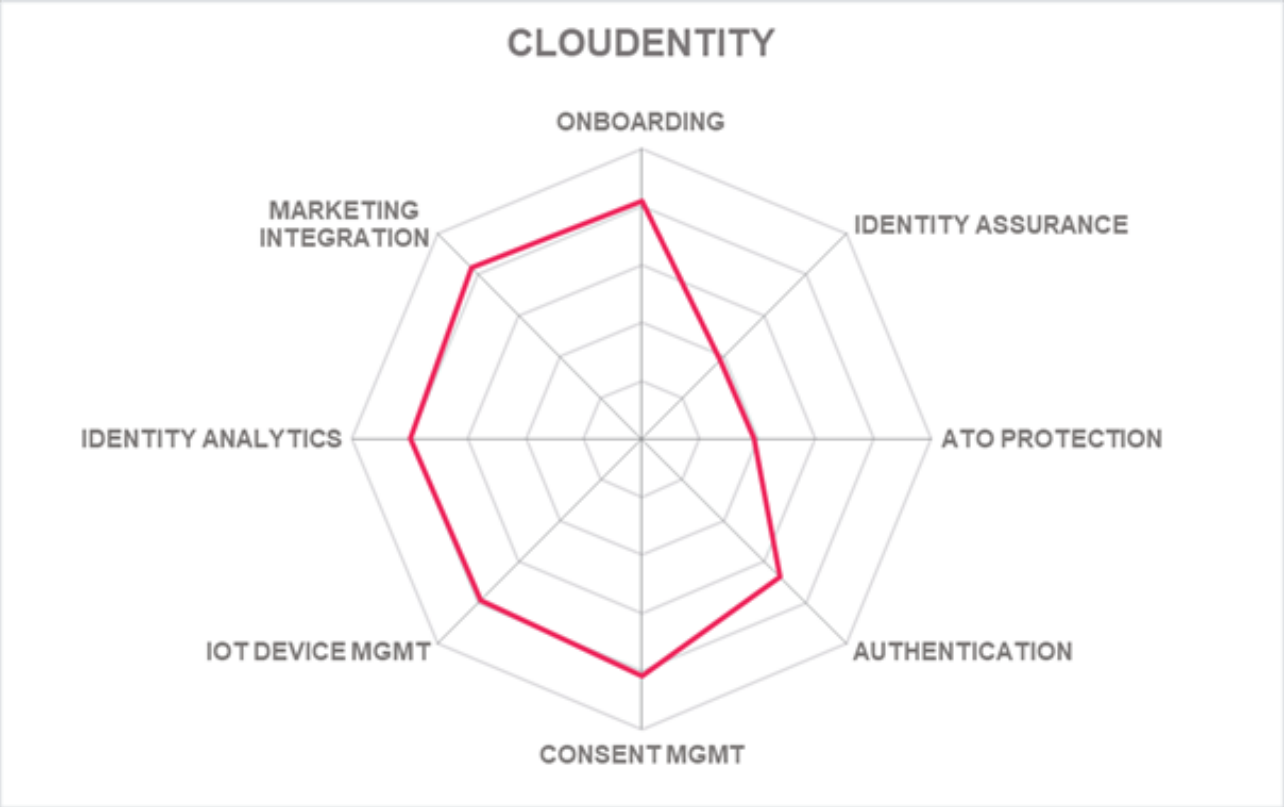
- Highly scalable micro-services architecture
- OPA and Rego policy authoring supported
- Fine-grained authorization and consent management features
- Can work alongside other CIAM and consent management solutions to provide advanced authorization features
- Excellent administrative GUI
- Well-documented APIs with code samples
- Strong consent and family management capabilities

Challenges

- Requires integration with 3rd party vendors for mobile biometric and additional authenticator types
- Not FIDO certified; requires integration with 3rd-party vendors to support FIDO mechanisms
- Limited ATO protection capabilities
- Identity proofing not built-in
- Few pre-built connectors for apps, intel sources, or identity proofing services

Leader in




CLOUDENTITY
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.4 CoffeeBean Technology

Consumers can self-register and CoffeeBean offers Registration-as-a-Service. Registration workflows are customizable to a degree, but not through a BPE or GUI. LDAP and SCIM can be used to import users from other repositories. CoffeeBean does not have identity proofing built-in. A connector for Experian for both identity proofing and FRIP services is available. All major account recovery mechanisms are supported. CoffeeBean accepts the following forms of authentication: Android and iOS biometrics, email/phone/SMS/WhatsApp OTP, many mobile authenticator apps, and FIDO UAF/U2F/2.0. It also supports JWT, OAuth2, OIDC, and SAML tokens. CoffeeBean has an SDK that customers can use to integrate their apps, and it can collect common device attributes. In-network credential intel is analyzed for risk; behavioral biometrics are not used. Risk engine configuration requires manual editing, there is no GUI yet for policy creation and maintenance.

For app connectivity, REST, Webhooks, Websockets, and WebAuthn APIs are supported. Standard identity analytics reports are available, and customers can create additional report types. Connectors are available for CRM, data analytics, and marketing automation including ELK, IBM UBX, PowerBI, Salesforce, and Tableau. Event data can be sent to customer SIEMs over syslog.

CoffeeBean offers a consumer portal for managing consent and personal information. CoffeeBean facilitates compliance with EU GDPR and LGPD (privacy regulation of Brazil). Consents can be recorded in Kantara Consent Receipt format. Family management is not supported. CoffeeBean does not handle IoT device identity association for consumers. CoffeeBean has engagement plug-ins for mobile apps and Wi-Fi captive portal features such as ad and content management. These Wi-Fi captive portal features can be used by retailers and facilities operators to interact with consumers in real-time, both when they are online or are in customer facilities such as shopping malls, airports, and restaurants.

CoffeeBean is focused on retail, hospitality, insurance, healthcare, transportation, and finance industries, bringing social media content to consumer profiles, and developing apps to more actively engage the consumer. They are strong in the South American market and are adding customers in North America and Europe. The solution would benefit from FIDO certification, consumer IoT device identity management, and additional integrations for identity proofing and ATO protection. Companies that are looking for a CIAM solution that is designed for active engagement of consumers in the retail, hospitality, or finance industries should consider CoffeeBean.

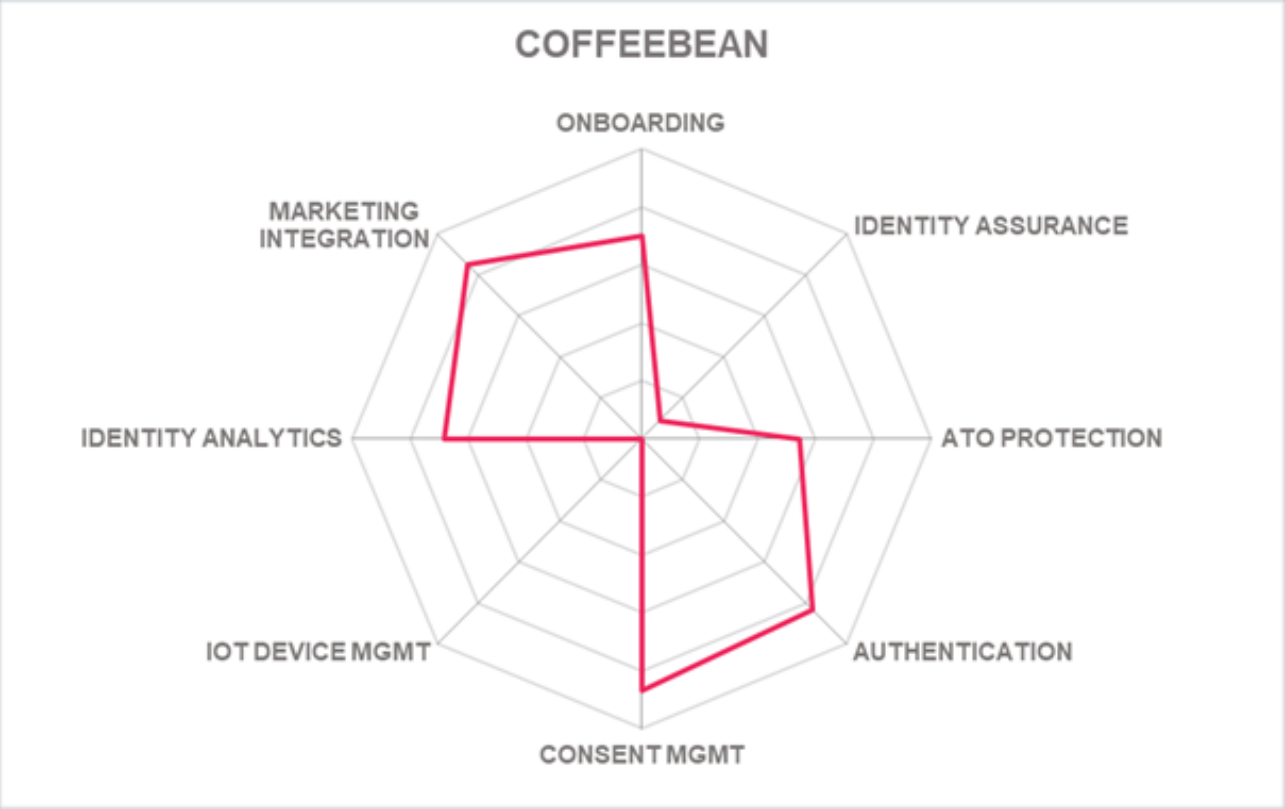
Security	●●●●○
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●○

Strengths

- Wide range of authenticators accepted
- Helps compliance with GDPR, and LGPD privacy regulations
- Wi-Fi captive portal integrations are well-suited for retail, hospitality, and event management use cases
- SDK captures a good range of device attributes for risk analysis
- Connectors for BI, CRM, and other analytics tools are available

Challenges

- FIDO supported but not certified
- GUI for workflow and policy editing not present
- Identity proofing limited to a single service
- Limited ATO protection
- No facilities for consumer IoT device identity management


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

5.5 DruID

DruID was launched in 2020 from the Genetsis Group and is now an independent startup. They are headquartered in Madrid, Spain. CIAM is their sole focus. Identity and Pulse are deployed via Kubernetes, and therefore can run on any OS and/or IaaS instance that supports that. They do not host it as SaaS, although that is planned for 2023. Licensing is primarily by container instance.

DruID accepts user self-registrations, registration from the admin console, and registrations from social networks (except Amazon). Workflows are somewhat configurable but not through a graphical interface. They are mostly targeting retail, fintech, electronics, sport, and leisure industries. A connector to FacePhi is available, which allows remote identity and document verification via their mobile biometric widget which can be used on mobile or desktop. No other identity proofing connectors are present. Account recovery requires the user to contact call center. Authentication methods are limited to email/phone/SMS OTP, biometrics, and the Authy mobile app. Multi-IDE SDK can be used to facilitate customer app development. Detailed device intelligence and behavioral biometrics are not supported. In-network credential intelligence is processed, although the risk engine is not exposed for modifying authentication policies.

Customers can use REST API and ETL methods for migrating users; LDAP and SCIM are not supported yet. Webhooks can be used for limited customization application integration. No connectors for FRIP services are present yet. DruID has integrations for Facebook Custom Audiences and Lead Ads, Google Analytics and Tag Manager, Hubspot, Salesforce, Xeerpa Social Profiling, and Zoho. Basic identity analytics reports, consumer timelines, and activity reports are provided. DruID Pulse is the built-in lead acquisition and marketing analytics component that de-duplicates user information and provides reports and demographic information that can be used for campaigns. Standard protocols for communication with SIEM systems is not present yet.

DruID offers a self-service portal for reviewing, granting, and revoking consent actions as well as editing consumer profile information. Social media accounts, email addresses, and mobile identifiers can be linked or disconnected in the consumer portal. The consumer portal offers a unique timeline view of user activities. DruID Cockpit is the admin interface for handling integration management, user searches, and detailed view of user activities. Family management is not addressed by the solution.

DruID is undergoing ISO 27001 auditing. As a fairly new entrant in the market, DruID needs to add features to get to the baseline of what is common for CIAM. For now, the product has functionality that is targeted at lead generation, marketing, and rewards management: features which are a subset of those found in Customer Data Platform solutions. They have an initial customer base in various consumer-facing industries in Spain and are working toward expanding both their product and geographic coverage.

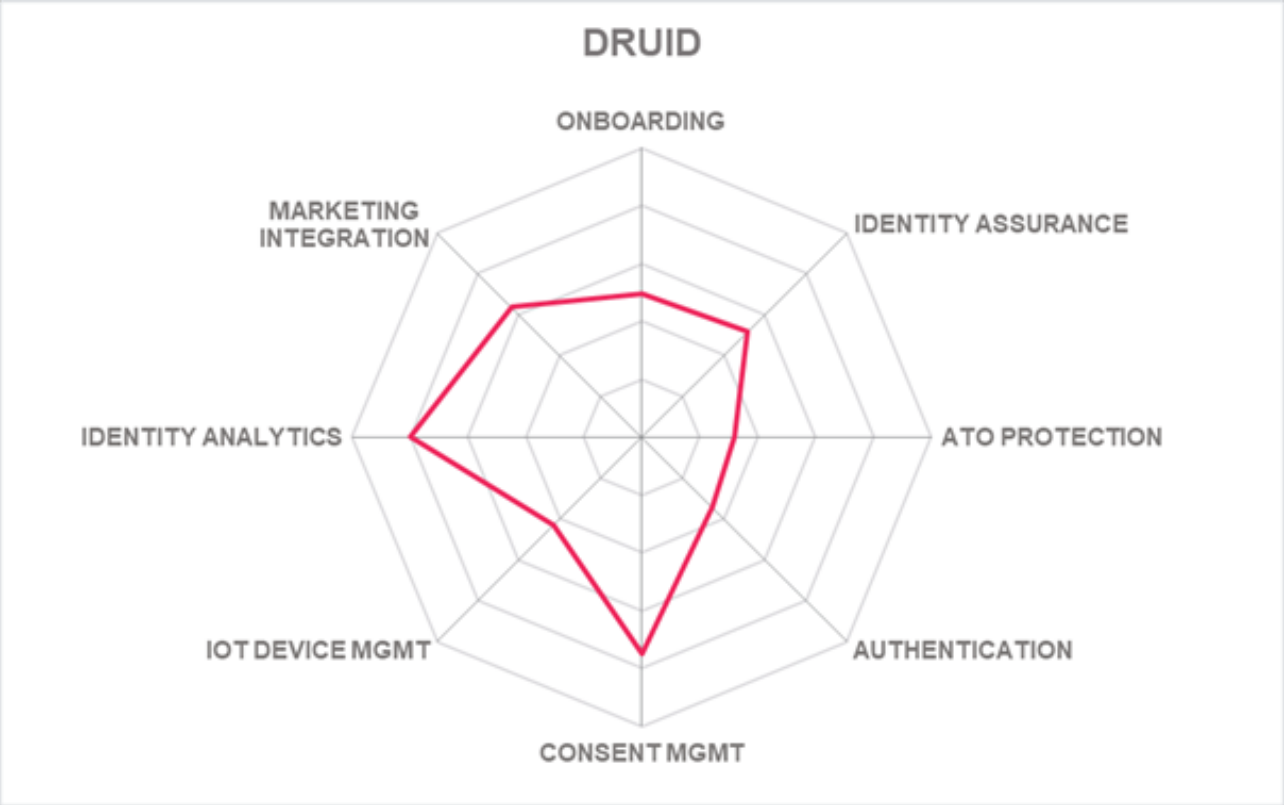
Security	●●●○○
Functionality	●●○○○
Deployment	●●○○○
Interoperability	●●●○○
Usability	●●●○○

Strengths

- Kubernetes-based deployments
- Connectors for common social media platforms
- Pulse component provides some marketing analytics and conversion features, such as lead acquisition, de-duplication, and consumer and IoT real time activity tracking engine.
- Timeline view in user self-service dashboard
- OEM integration with FacePhi for remote identity proofing

Challenges

- New and small startup, mostly active in Spain
- No SaaS options currently
- Manual account recovery only
- Needs more authenticator types
- Lacks device intelligence and risk-adaptive authentication capabilities
- Does not integrate with 3rd-party FRIP services


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

5.6 ForgeRock

ForgeRock was founded in 2010 and became a publicly traded company in 2021. They are headquartered in San Francisco. ForgeRock supports most major IAM standards and is a significant contributor to several international standards organizations. Their Identity Platform is both their CIAM and workforce identity solution. It is part of a full suite of IAM products including Access Management, Autonomous Access and Identity, Directory Services, Identity Cloud, Identity Gateway, Identity Governance, Identity Management, IoT/Edge Security, and Privacy & Consent Management. ForgeRock Identity Platform runs on-premises on most Linux variants, in any IaaS environment, in hybrid environments, or as SaaS hosted in public IaaS across many regions. SaaS instances can be fully isolated to prevent noisy neighbors or even different CIAM functions within a single customer from affecting performance of critical functions. Each SaaS instance comes with full CI/CD pipeline. Licensing/subscription costs are determined by the number of active users per quarter or year.

ForgeRock makes it easy to onboard users, with highly customizable registration workflows that accept any OIDC compliant and/or social network credential. LDAP/REST/SCIM enable migrations from other platforms. All account recovery methods are supported. ForgeRock Identity Platform works with Authentiq, GBG, ID Dataweb, ID.Me, Jumio, LexisNexis, OneSpan, OnFido, Socure, and Veriff for identity proofing. ForgeRock accepts a huge list of authenticators: FIDO UAF/U2F/2.0, OTP mobile push, and most 3rd-party authenticator apps. JWT, OAuth, OIDC, and SAML are supported. They offer secure SDKs that leverage mobile biometrics and collect some device intel attributes. ForgeRock has integrations with Biocatch, Intensity Analytics, Kount, LexisNexis ThreatMetrix, and TypingDNA for passive biometrics. User history and behavioral analysis are also processed by the sophisticated risk engine. The drag & drop / flow-chart admin interface is very intuitive for orchestrating customer journeys and managing policies.

ForgeRock has connectors for many IAM, IDaaS, fraud intelligence sources on their marketplace. Customers can push identity data into 3rd-party analytics solutions. BI and marketing analytics connectors are available for Adobe, Google, HubSpot, Marketo, Salesforce, and SAP. ForgeRock supports the widest range of secure API types and data formats, including OData, REST, RPC, SOAP, WebAuthn, Webhooks, and Websockets, in CSV/JSON/XML. ForgeRock can send event data to customer SIEMs over CEF or syslog.

The ForgeRock Profile and Privacy Management Dashboard presents consumers with the abilities to view, edit, and delete their personal information and grant/revoke consent granularly to facilitate compliance with EU GDPR, CCPA/CRPA, and AU CDR. ForgeRock supports OpenBanking and PSD2 use cases as well. ForgeRock supports advanced consumer IoT use cases with a “Thing SDK” and device registration API. ForgeRock Identity Platform can address many categories of IoT devices, including set top boxes, connected cars, smart speakers, SmartHome, medical devices, and wearables.

ForgeRock has audited, attested, and/or obtained many security certifications including CSA Star Level 1, HIPAA/HITRUST, ISO/IEC 15408, ISO 27001, PCI-DSS, SOC 2 Type 2, and has several OpenID profile certifications. ForgeRock Identity Platform has broad capabilities in CIAM and is flexible enough to support

most any use case. In order to achieve this, The on-premises deployment of ForgeRock Identity Platform requires more expertise and attention than other solutions in this market, but the SaaS version is easier to implement. ForgeRock supports most relevant standards and contributes to standards development organizations. Certifying their components with the FIDO Alliance would be advantageous. ForgeRock offers functional isolation in its SaaS for maximum protection and scalability and is a leading Identity Fabric vendor. ForgeRock remains a top contender in the CIAM market.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

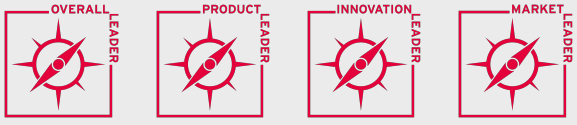
Strengths

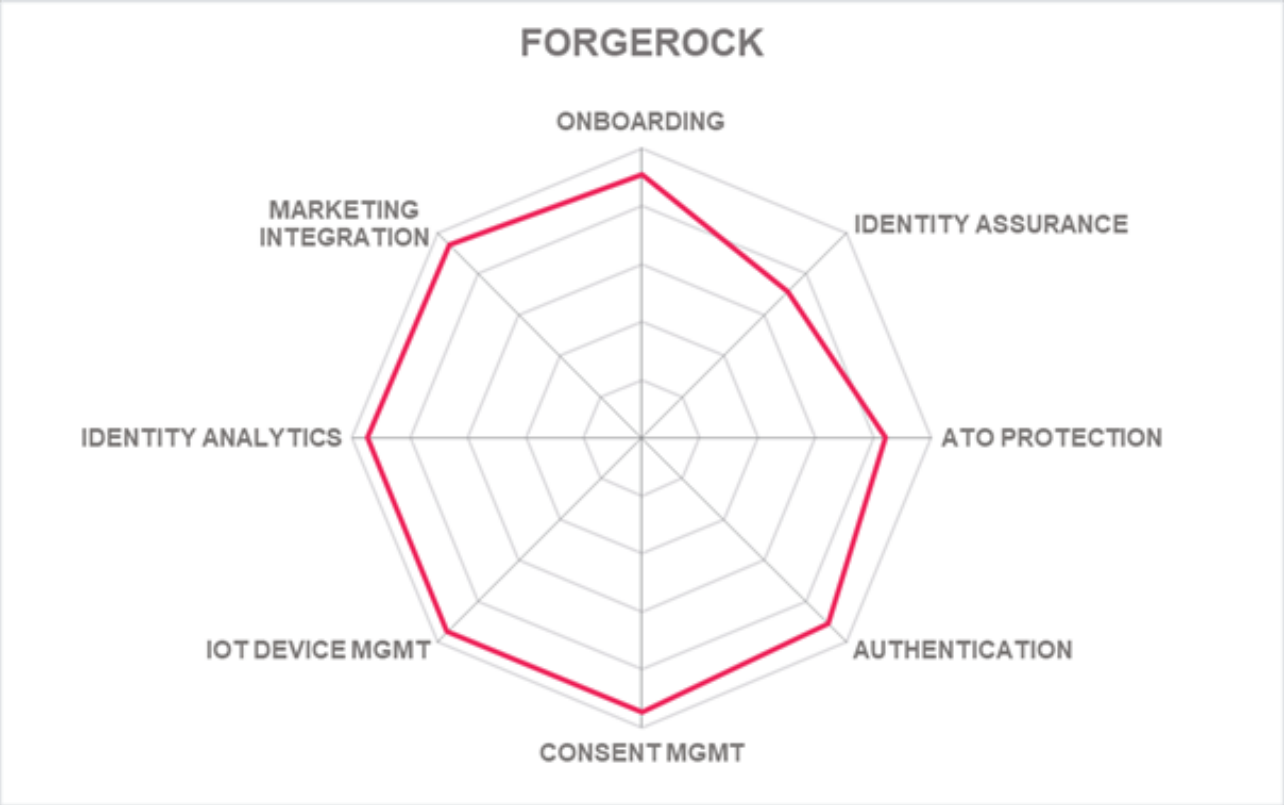
- Excellent admin interface for defining registration workflows and authentication/authorization policies
- Many integrations to extend identity proofing, fraud reduction intelligence, and authenticator support
- Micro-service level isolation for optimum protection, performance, and scalability
- Full CI/CD pipeline for each customer in SaaS
- Many authenticators accepted
- Excellent connectivity to other apps and infrastructure
- Consent management facilitates compliance with GDPR, CCPA, CDR, and more
- FAPI, OpenBanking, and PSD2 support
- Advanced consumer IoT device identity integration

Challenges

- On-prem version is more labor intensive in terms of deployment and maintenance; their SaaS is easier to implement
- FIDO is supported but the solution is not certified
- Marketing analytics require 3rd-party solutions
- Some integrations on the marketplace are unsupported

Leader in




FORGEROCK
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.7 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 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.

Customer users can be imported over LDAP or SCIM, and self-registration workflows can be customized by editing provided templates. In addition to social networks, they support many gaming platforms IdPs. Identity proofing is not offered and there are no connectors to 3rd-party services. Most of the common account recovery methods are supported, and others can be coded with APIs. Accepted authenticators are limited to email/SMS OTP and Google Authenticator. Customers can configure other MFA providers, but development is needed. JWT, OAuth2, OIDC, and SAML can be used for federation. FusionAuth has SDKs that can gather a small subset of device intel attributes. Passive biometrics are not implemented. The risk engine is somewhat configurable; decisions but not risk scores are rendered; and policies are edited using a drop down and action list GUI.

FusionAuth supports REST API, Webhooks, and WebAuthn. Integrations can be built by customers to FRIP services, BI and marketing analytics/automation tools, and SaaS apps, but no connectors are present out-of-the-box. Basic identity analytics and identity threat detection metrics are shown in the dashboard and reports.

Consent collection for privacy management requires some coding and configuration by customers. FusionAuth offers authorization for family management use cases such as granular controls for home entertainment devices. Other consumer IoT use cases can be supported if developed by customers.

FusionAuth is SOC 2 Type 2 certified. The solution lacks some built-in CIAM functions as outlined above, but customers can use their well-documented API platform to develop those additional CIAM capabilities if needed. FusionAuth offers a number of 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.

Security	●●●○○
Functionality	●●●○○
Deployment	●●●●○
Interoperability	●●●○○
Usability	●●●○○

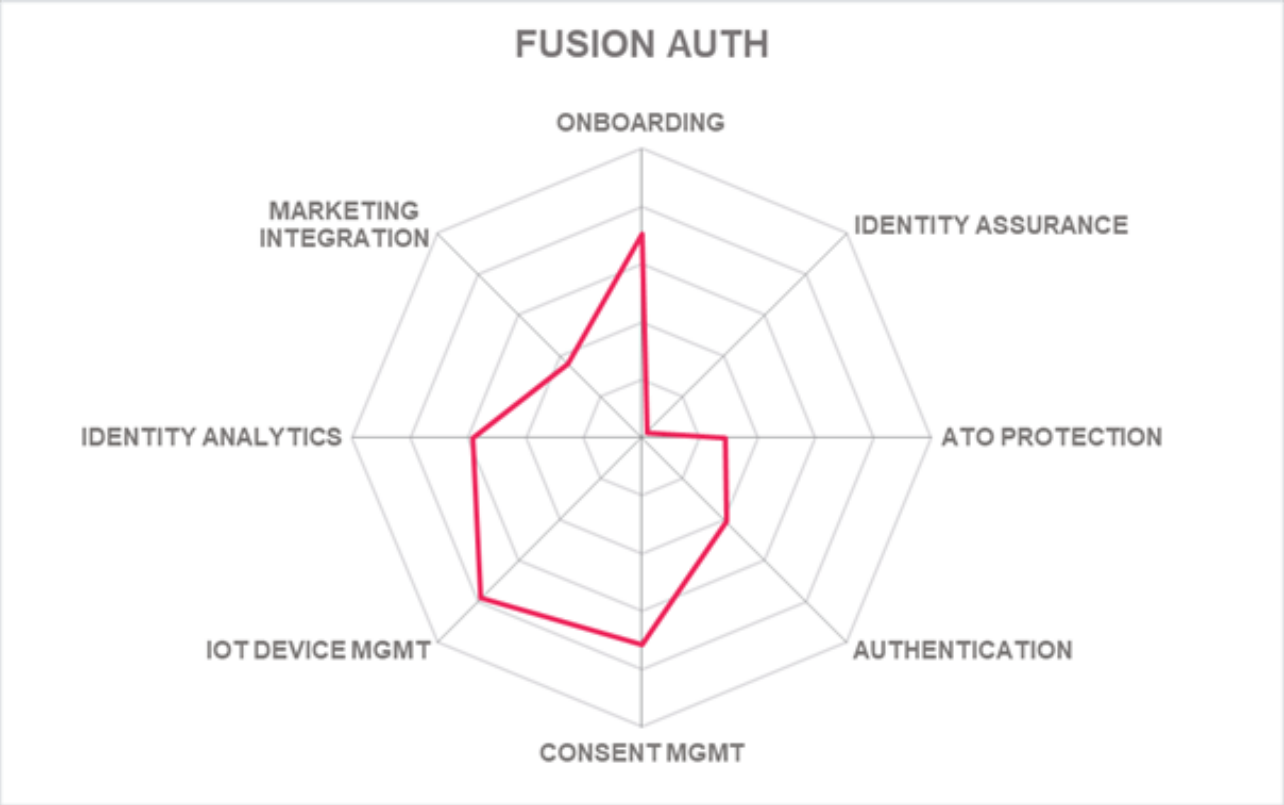
FusionAuth

Strengths

- Container based delivery and architecture
- Customers can create logically separate instances for service and tenant isolation
- Granular authorization for family management and delegated administration
- Templates for EU GDPR, CCPA, and US COPPA compliance
- Enables advanced consumer IoT device management use cases

Challenges

- Lacks identity proofing capabilities
- Needs built-in support for additional strong authenticators
- Limited device intel and no passive biometrics
- Coarse-grained risk engine
- Integrations with common CIAM add-on services must be configured by customers, such as BI, FRIP, and marketing tools
- Consent management requires coding


FUSION AUTH
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.8 IBM

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. Multiple licensing/subscription options are available.

IBM supports LDAP, REST, and SCIM for customer migrations. Self-registration workflows can be customized and orchestrated in the intuitive and modern admin interface. Registration using social network credentials (except Amazon) is possible. All expected account recovery methods are available. Identity proofing is not built-in but can be configured via API if customers desire. Security Verify accepts a wide array of authenticators, including FIDO U2F/2.0, many 3rd-party authenticator apps, Android/iOS biometrics, email/phone/SMS OTP, and social logins. It supports JWT, OIDC, OAuth, SAML, WS-Federation, and WS-Trust. IBM has SDKs that can collect a robust range of device intelligence and behavioral biometrics attributes. The service uses in-network sources for credential intelligence. Risk-based authentication and fraud reduction capabilities are powered by IBM Trusteer, which was an Overall, Product, Innovation, and Market leader in the last edition of the KuppingerCole Leadership Compass on Fraud Reduction Intelligence Platforms.

IBM Security Verify supports REST API, SOAP, Webhooks, Websockets, and WebAuthn. All functions including identity and marketing information are accessible via the API. Security Verify provides comprehensive analytics and reports for identity analytics right out of the box. Marketing analytics and BI functions are available in other IBM products or via a multitude of connectors to 3rd-party apps. Consumer event information can also be sent to SIEMs such as QRadar via syslog.

A self-service portal allows consumers to view/edit/delete information. Kantara Consent Receipt is not supported. Family management is not built-in but could be configured as a delegated administration model. Device identity management is provided, and IBM supports a number of token issuance and complex use cases with OAuth2 Device Flow. Consumer portals for device identity management are not built-in but can be developed by customers or professional services.

IBM Security Verify has achieved FedRAMP Ready, ISO 27001, SOC 2 Type 2, and multiple OIDC profile certifications. The solution is also FIDO 2 Server certified. There are a few gaps in the consent management model that still need to be addressed. IBM Security Verify has a leading-edge, highly scalable architecture. Security Verify can leverage IBM Trusteer for fraud prevention and risk-adaptive authentication. Any organization looking for a high performance and secure CIAM solution should consider IBM Security Verify.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

IBM

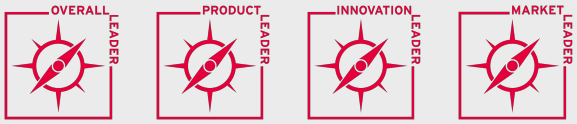
Strengths

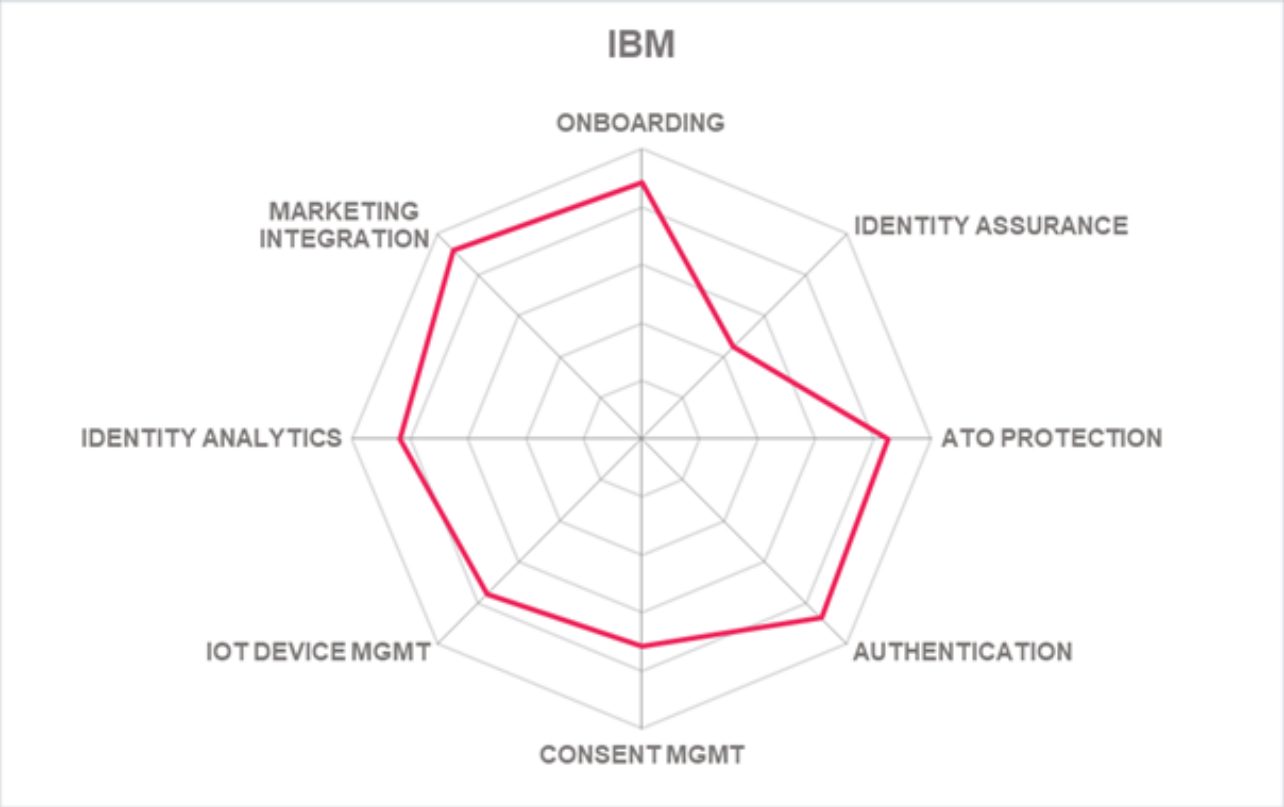
- Highly scalable containerized, multi-cloud architecture
- Offers management of isolated single customer instances in IaaS
- Many security certifications; FIDO 2 Server certified
- Intuitive administrative interface
- Excellent support for many authenticator types
- FIDO 2 Server certified
- Embeds IBM Trusteer for fraud reduction and risk-based authentication
- Many connectors to 3rd-party apps, including marketing analytics/automation
- Wide range of professional services for customization and management

Challenges

- Simplification of licensing schemes could be beneficial for customers
- Identity proofing not built-in, but can be coded in by customers or professional services
- Family management only configurable as delegated administration
- Consumer device management portals not available out-of-the-box, but can be built

Leader in




IBM
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.9 LoginRadius

Founded in 2011, LoginRadius is a VC-backed CIAM vendor based in Vancouver, BC. The company provides CIAM as SaaS via a multi-cloud model hosted in globally distributed data centers. Customers can deploy on-premises on CentOS, RHEL, or Ubuntu; or run it in any of the major IaaS providers. LoginRadius has over one billion consumer identities under management. Subscription costs are based on the number of active users per month, quarter, or year.

LoginRadius allows customers to design onboarding workflows for self-registration graphically. Social network registration is supported. Identity proofing can be configured by customers but requires coding to APIs. All standard account recovery mechanisms are present. LoginRadius works with Android and iOS biometrics; Duo and Yubikey FIDO 2 devices; email/phone/SMS OTP; many major authe apps; and any OIDC based social login. JWT, OAuth, OIDC, and SAML are supported for SSO. FIDO U2F/2.0 are supported but the platform is not certified. Most standard account recovery mechanisms are supported. LoginRadius has a mobile SDK which examines some key device attributes except device hygiene. In-network credential intelligence is also evaluated. The authentication risk engine is somewhat coarse-grained: risk factors cannot be prioritized by clients. Policy creation is constrained to drop-down list selections. Risk scores are used internally but not shared with customer applications directly.

REST API, Webhooks, and WebAuthn are enable interaction with customer apps. Customers can configure connections to FRIP services, but out-of-the-box integrations are not provided. They do have integrations for Age Verification and Trulioo. LoginRadius has a marketplace where customers can get packaged connectors for SaaS apps in advertising, BI, CRM, marketing automation, data management platforms, payment systems, SIEM, and more. LoginRadius' built-in analytics engine provides 50+ OOTB reports, allowing detailed marketing analysis according to a plethora of consumer attributes. Comprehensive identity analytics can be viewed from the dashboard and delivered via reports.

Users may view, edit, export, or delete their stored data at any time. Kantara Consent Receipt is not supported at this time. LoginRadius can automatically notify consumers when privacy terms change. Family management can be handled as a delegated admin model. Consumer IoT devices such as Smart TVs, Smart speakers, gaming consoles, etc. can be easily managed using LoginRadius' APIs and UIs. OAuth2 Device Flow is supported. They do not provide built-in consumer device management portals currently.

LoginRadius is designed as a turnkey CIAM solution. APIs are exposed and the platform is extensible, but it is not a developer-focused platform. There are a few areas for improvement as listed above. LoginRadius has attested and/or certified with CSA Star Level 2, ISO 27001/27018, PCI-DSS, and SOC 2 Type 2. Such efforts demonstrate their commitment to security and reliability. Their multi-cloud, global data center deployment strategy provides excellent availability and scalability. Any organization that is looking for a straightforward, easy-to-maintain CIAM solution should think about LoginRadius.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

loginradius

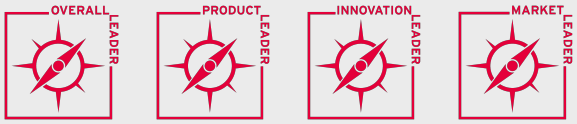
Strengths

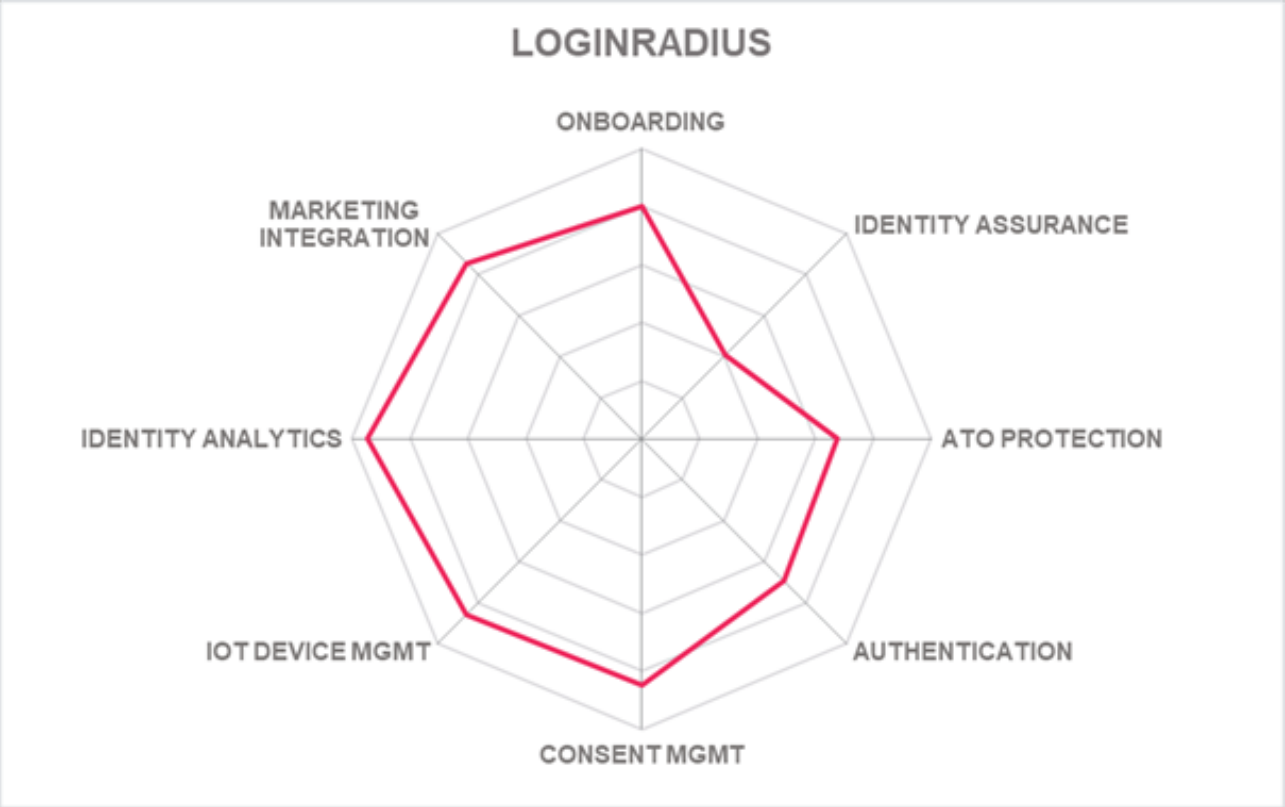
- Easy to operate / turnkey CIAM solution
- Multi-cloud / global data center deployment for high availability and scalability
- Multi-tenant with single instance support options
- Good selection of authenticators accepted
- Many connectors for marketing analytics/automation and other SaaS tools
- Very usable reports and dashboards
- Addresses consumer device management

Challenges

- Identity proofing services must be manually integrated
- LDAP and SCIM not supported
- FIDO supported but not certified
- Coarse-grained authentication risk engine
- Additional OOTB connectors for FRIP services would be helpful
- Mobile SDK could pull more device intelligence for risk analyses

Leader in




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

5.10 Microsoft

Microsoft External Identities is a cloud-based identity and access management service with integrated security to manage and protect external user identities and data and includes the Azure AD B2C service which facilitates business-to-consumer applications. This offering is designed to meet the core CIAM needs of both large and small organizations. It serves hundreds of millions of consumers and B2B users and handles over one billion logins per day. Azure is one of the global leaders in the cloud infrastructure market. It is a tiered subscription model based on number of monthly active users.

Microsoft does not support migrating users by SCIM, but a 3rd-party integration facilitates migration via LDAP. Self-registration and social network registration are available but the ability to edit onboarding processes is limited. Microsoft now provides integration kits for eight identity proofing services. Most account recovery mechanisms are present. Microsoft External Identities accepts OTP, various mobile authenticator apps, and Android/iOS biometrics. FIDO 2 and other passwordless authenticators are usable through partnerships. A partnership with Asignio can enable additional facial recognition and limited behavioral biometrics capabilities. The service also accepts JWT, OAuth, OIDC, and SAML tokens. Their mobile SDK can collect many device intel parameters except for device hygiene and MNO data. Risk-adaptive authentication policy construction is coarse-grained; customers cannot weight risk factors for evaluation. Microsoft's in-network credential intelligence helps prevent ATOs across their customer base.

REST, OData, and Webhooks API types are supported for customer developed integrations. Connectors are available for several FRIP services, including ArkoseLabs, BioCatch, Experian, LexisNexis, and Microsoft Dynamics Fraud Protection. Signals from Microsoft Security Intelligence Graph allow for basic bot detection, and integration with Microsoft Azure Front Door WAF, licensed separately, can provide advanced bot management functions. Microsoft PowerBI can be used for advanced identity and data analytics. Direct integration with Microsoft Dynamics CRM is possible. Admin dashboards and reports covering identity events are present and can be further customized in the Microsoft Graph API and exported to customer SIEMs.

Microsoft External Identities provides the capability for customers to present consent options to consumers, via progressive profiling. User privacy dashboards and data subject access request templates are not available. Family management can be configured as group administration. Kantara Consent Receipt is not supported. Microsoft External Identities can provide authentication capabilities for consumer IoT devices such as Smart TVs, but full device identity management requires additional development.

The Azure platform is CSA Star Level 1 and 2 certified, HIPAA/HITRUST, ISO 27001/27018, PCI-DSS, SOC 2 Type 2 attested and/or certified. Microsoft has the infrastructure to enable massive scalability. Microsoft External Identities has added capabilities since the last iteration of this report, particularly adding FIDO2 and identity proofing support via partnerships. However, it is missing some key features for privacy management and consumer IoT device identity integration. Microsoft is still working toward feature parity between their CIAM and Azure AD platforms. Organizations that need scalability and ease of use that do not require advanced privacy management or consumer device management should review Microsoft External

Identities when selecting CIAM solutions.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●●●
Interoperability	●●●○○
Usability	●●●●○

Microsoft

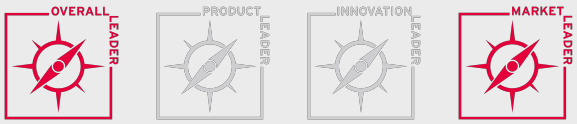
Strengths

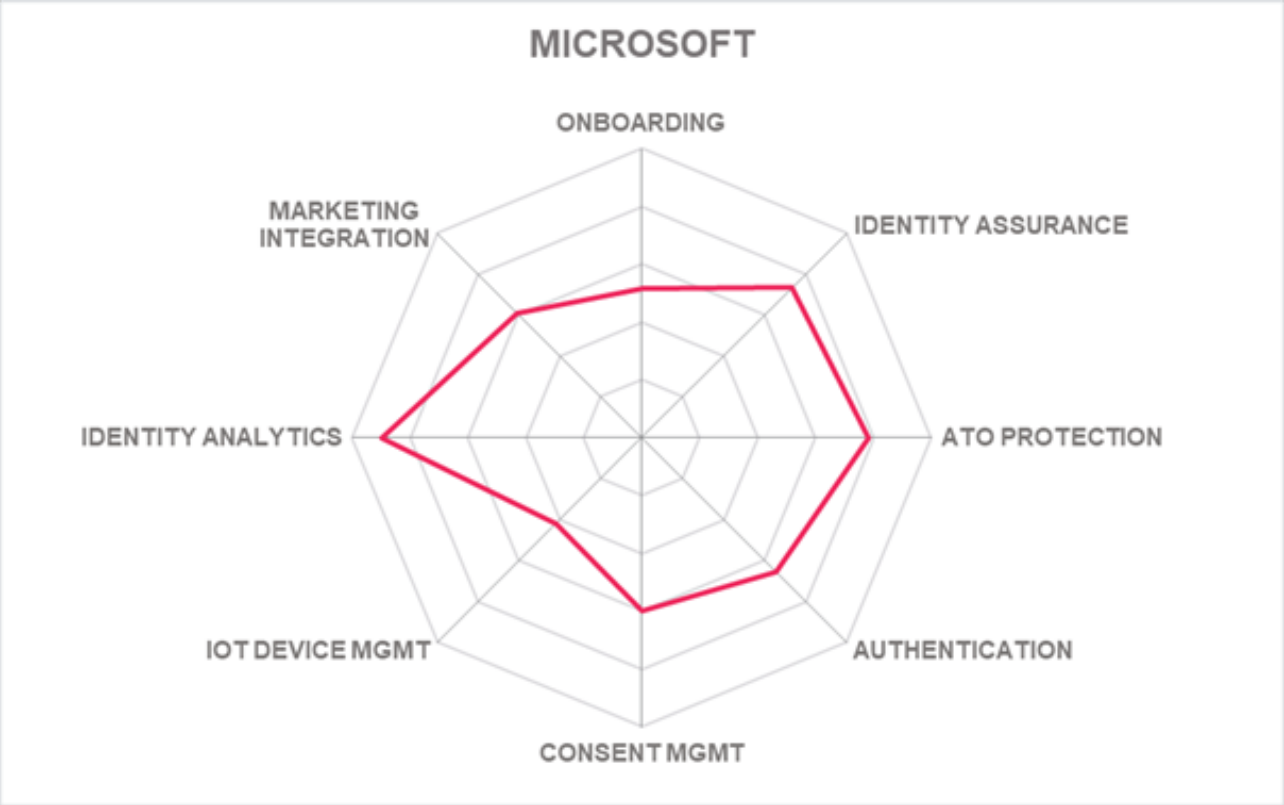
- Massively scalable SaaS
- Excellent in-network credential intel for ATO prevention
- Partnering with multiple identity proofing solution providers for stronger identity assurance
- Supports authentication for input-constrained consumer IoT devices

Challenges

- LDAP/SCIM not supported; onboarding workflow editing is limited
- Advanced device intelligence requires Microsoft Dynamics Fraud Protection
- No consumer privacy dashboards
- Built-in connectors for CRM and data analytics limited to Microsoft Dynamics
- Lacks OOTB full consumer IoT device identity management functions

Leader in




MICROSOFT
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.11 NEVIS Security AG

Nevis was spun out of Adnovum Informatik in 2020. They are a private company headquartered in Zurich. Their product focus is on CIAM. Identity Suite can be installed on Linux on-premises or in any IaaS, though Nevis provides additional support for instances on 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 monthly/quarterly/annual active users or quarterly/annual registered users.

Nevis supports social network registration (except Amazon), self-registration with customizable workflows, and bulk imports over LDAP or SCIM. Nevis has OEM’d PXLVision’s remote identity proofing technology for web and mobile onboarding. Other identity proofing services could be integrated via API. All expected account recovery mechanisms are present, including secure options leveraging the remote onboarding app. Nevis accepts many authenticator types including OTP, most mobile authenticator apps, Android/iOS biometrics, and FIDO UAF (certified) and 2.0. Hardened SDKs are available which can collect and utilize a full range of device intel attributes. Partnership with BehavioSec (now LexisNexis) allows for profiling of consumer typing as the single passive biometrics function. Other passive biometrics are avoided due to GDPR concerns. Credential intelligence is not currently evaluated. The risk engine is customer configurable and extensible through a well-designed admin UI that allows low-code/no-code customization.

Nevis provides built-in FRIP services, augmented by IP2Location and MaxMind IP sources. Arxan integration allows for application protection and threat detection. Basic reports include failed logins, profile and credential changes, applications accessible and permissions. A connector for Splunk is available, and syslog and CEF are supported for connectivity to other SIEMs. Customers can export identity event information for consumption by 3rd-party BI, CRM, and other analytics solutions.

Consumer privacy dashboards are not part of the standard offering, but customers can construct them using APIs. Nevis does not provide the ability to filter attributes from social network registrations; however, Nevis does allow data labeling over API. Kantara Consent Receipt is not supported. Nevis can enable customers to provide IoT device management capabilities to their consumers and B2B customers. OAuth2 Device Flow is available for IoT device identity management.

Nevis has not yet attested to SOC 2 Type 2 or obtained ISO 27001 certification. Nevis scales well for on-premise or IaaS deployments, and its cloud presence is growing and maturing. Nevis emphasizes rapid implementations for customers, with low-code, no-code, and hardened SDK features. An expansion of features for privacy management and marketing analytics and automation would be helpful. Most sales and support are in Switzerland, with a long-established presence in Germany and Singapore, but they are actively moving in other areas. Nevis is strong in the finance industry, and the product suite benefits from the focus on security for that sector. They are also targeting the gaming, gambling, government agencies, and insurance markets. Organizations with requirements for high security and identity proofing will want to review Nevis’ offering for CIAM.

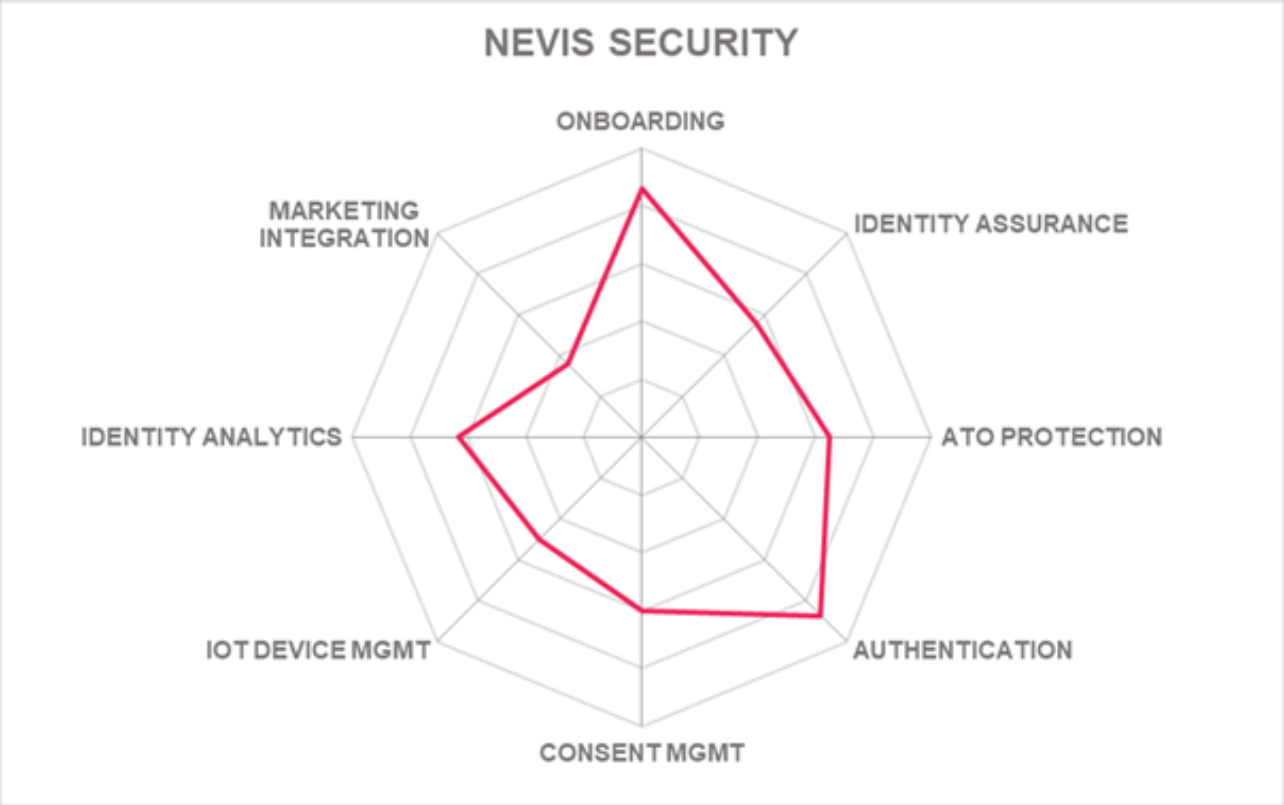
Security	●●●●●
Functionality	●●●○○
Deployment	●●●●○
Interoperability	●●●○○
Usability	●●●○○

Strengths

- Wide variety of authentication methods available; omni-channel authentication approach
- Integrated PXLVision identity proofing; secure account recovery
- Hardened SDK for rapid app building
- Integrated Arxan app shielding and threat detection
- Support for HSMs for financial transaction security
- Leading edge integration with chatbot and conversational AI technologies

Challenges

- Having additional FRIP services available for customers could be advantageous
- FIDO 2 supported but not certified
- Needs out-of-the-box integrations with marketing tools
- Limited consumer device IoT identity management capabilities
- No consumer self-service portal
- Latecomer to cloud hosting
- Most sales and support in Switzerland but actively expanding


NEVIS SECURITY
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.12 NRI Secure Technologies

NRI Secure Technologies was founded in 2000 as a subsidiary of Nomura Research Institute in Japan. NRI Secure also provides security consulting. Uni-ID Libra is their CIAM product, which was first launched in 2008. 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 and/or subscription costs are determined by the number of monthly registered users.

Social network (minus Amazon and LinkedIn) and self-registration options are present for Uni-ID Libra. Customers can edit templates for consumer onboarding workflows, but no graphical editor is available. SCIM can be used for platform migrations. Identity proofing is not offered yet but is on the roadmap. Account recovery options are limited to OTP. Uni-ID accepts OTP, various mobile authentication apps, hardware tokens, Android/iOS biometrics, and all FIDO authenticators. JWT, OAuth, OIDC, and SAML tokens are also accepted. Integrations with Azure AD and Salesforce IdP are available. An SDK is not provided; thus, device intelligence and passive biometrics are not implemented. Uni-ID's risk engine allows weighting of available risk factors, but credential intelligence is not processed. The policy builder interface is drop-down list style.

Uni-ID supports REST API and WebAuthn. Customers can use the API to export identity event data to 3rd-party BI, CRM, or other analytics applications. Pre-packaged connectors for 3rd-party applications are not available. Basic identity analytics reports are present within the console. SIEM integration may require development effort, but integrations with DataDog and Splunk are available.

Uni-ID Libra allows consumers to view, edit, and delete their saved profile data. Kantara Consent Receipt is not supported. Family management is present, which includes relationship management and some access controls. NRI supports consumer IoT device identity association and management. Uni-ID Libra is used by customers for large scale connected car and Set Top Box (STB) use cases.

NRI Uni-ID Libra is ISO 27001 certified. NRI continues to add features to Uni-ID Libra including support for more types of authenticators and excellent consent and family management. Uni-ID Libra's architecture allows for high scalability. Adding an SDK that can harvest device intelligence and passive biometrics and enhancing the risk engine accordingly would be helpful. Identity proofing is on their roadmap. NRI is still focused on the CIAM market in Japan. Any organization in Japan that is considering adding or replacing CIAM should evaluate NRI Uni-ID Libra.

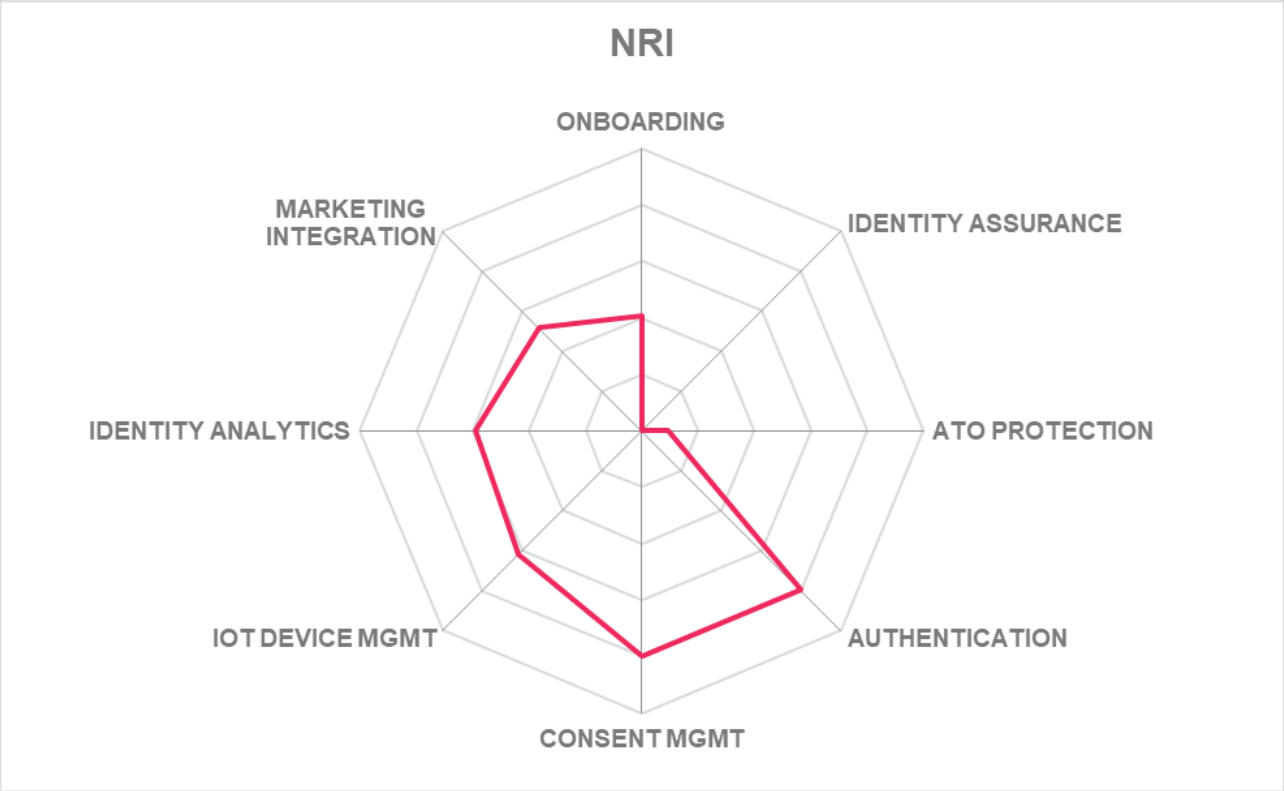
Security	● ● ● ○ ○
Functionality	● ● ● ○ ○
Deployment	● ● ● ○ ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ○ ○

Strengths

- FIDO certified for UAF/U2F and 2.0
- Impressive range of authentication options
- Good implementation of consent and privacy management
- Family management includes relationship definition and access controls
- Consumer IoT device identity management: support for connected cars and other use cases

Challenges

- No GUI for onboarding workflow customization
- Identity proofing not supported
- Additional account recovery methods needed
- SDKs not provided
- No credential or device intelligence or passive biometrics capabilities
- Needs connectors for 3rd-party apps
- Sales and support limited to Japan


NRI
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.13 Okta

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. Pricing is by number of monthly active users.

Self-registration and social network registration are permitted. Onboarding workflows are easily customized if needed via the visual workflow editor and editable templates. LDAP, SCIM, and any other API can be used to migrate users from other platforms. Account recovery mechanisms include KBA (security questions), OTP, mobile push, email, SMS, and voice. Okta accepts many mobile authenticator apps in addition to their own, Android/iOS biometrics, OTP, and FIDO U2F/2.0 authenticators. SDKs are available which can pull a limited set of device intel attributes. Passive biometrics are not implemented. The mobile app and SDK enable some identity proofing features which can be extended with Acuant (now GBG), Evident, Experian, Jumio, and OnFido. Authentication and access control policies can be edited in the intuitive flow-chart style admin interface. Okta ThreatInsight provides credential intelligence and identity protection and is supplemented by external intelligence sources.

Okta supports REST, Webhooks, Websockets, and WebAuthn APIs. Okta/Auth0 have many connectors for BI, CRM, marketing analytics and automation, other IAM systems, and popular SaaS apps. Connectors are sorted by original product platform: connectors for Auth0 and connectors for Okta. Integrations for FRIP services include Arkose Labs, Forter, Kaspersky, PerimeterX, and TransUnion. Rudimentary bot detection via CAPTCHAs is included. Basic identity reports are available out-of-the-box. Identity event data can be sent to 3rd-party solutions using REST and customer SIEMs using CEF or syslog for analysis.

Consumers can edit, export, and delete their profile information. Consents and delegation records are stored within the consumer profiles. Okta/Auth0 supports Kantara Consent Receipt. Family relationships can be defined as a form of delegated administration to allow parents/guardians to govern which content is available to children. Okta/Auth0 supports OAuth2 Device Flow and machine-to-machine authorization. Customers are using their IoT device identity management features for use cases such as connected cars, home automation, smart speakers, etc. This is a focus area for their service roadmap.

The Okta and Auth0 solutions still exist separately and do not appear to be consolidating quickly. Okta/Auth0's services are CSA Star Level 2, ISO 27001, ISO 27018, HIPAA, PCI-DSS, SSAE SOC 2 Type 2, US FedRAMP and FISMA attested and/or certified. The platform has excellent support for a broad range of authentication types. The solution could use additional device intelligence capabilities and behavioral biometrics. WebAuthn is supported, and FIDO Passkey is on their long-term roadmap, but FIDO server certification should be pursued also. Okta/Auth0 delivers extreme scalability for customers, both for public and private deployment options. Okta should be on the shortlist for any organization conducting CIAM RFPs.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

okta

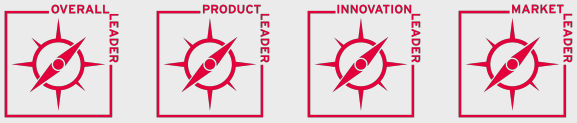
Strengths

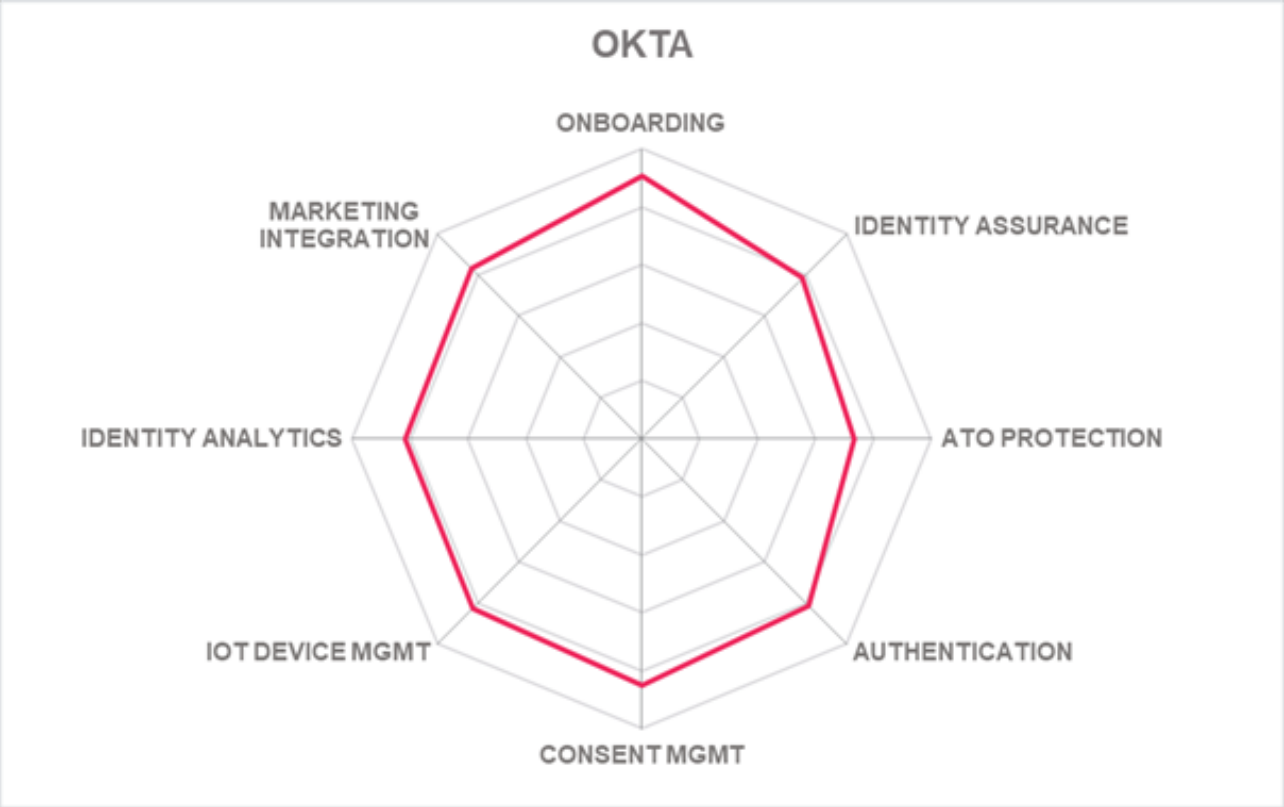
- Flexible consumer onboarding processes
- Many authentication methods supported
- Numerous connectors for SaaS apps, BI, CRM, analytics, and other IAM systems
- Intuitive customer admin interface
- Built-in ATO capabilities which can be extended as needed
- Good consent management features including support for Kantara Consent Receipt
- IoT device identity management available and extensible

Challenges

- FIDO supported but not certified
- Behavioral biometrics are not built-in
- Limited ability to collect device intel via mobile SDK

Leader in




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

5.14 OneWelcome

OneWelcome launched as a new brand in 2021 after iWelcome and Onegini (both founded in 2011) joined together. They are headquartered in the Netherlands. OneWelcome specializes in CIAM and B2B IAM. OneWelcome acquired Scaled Access, a dynamic authorization product, in early 2022. The Thales Group began the process to acquire OneWelcome in summer 2022. The OneWelcome Identity Suite is composed of multiple discrete services: Core, User Journey Orchestration, Consent & Preferences, Delegation & Relationships, and Mobile. The solution is SaaS, hosted in public IaaS providers across multiple data centers in the EU. Multiple subscription options are available.

OneWelcome User Journey Orchestration module allows customization of onboarding processes. The GUI is currently not exposed to customers, however. Any OIDC or social login (except Amazon) can be used for self-registration, and LDAP and SCIM can be used for migrations. All expected account recovery mechanisms are present. For identity proofing, OneWelcome integrates with services such as iProov and ReadID for document and photo verification with liveness detection. Other IdPs and attribute providers supported include BankID, Experian, FranceConnect, ID.me, IDNow, OnFido, Signicat, Verimi, WebID, and Yes. Authenticators accepted include OTP, mobile push, and Android/iOS biometrics. JWT, OAuth2, OIDC, and SAML tokens are accepted. OneWelcome has a mobile app and SDK which can collect device attributes and device health but does not include passive biometrics. Authentication policies are configurable by OneWelcome or support partners. Third-party credential intelligence services are utilized for ATO protection.

REST, Webhooks, and Websockets are supported. No out-of-the-box connectors exist for FRIP, but OneWelcome professional services could build them. OneWelcome can track key user activities per-tenant including registrations, logins, failed logins, etc. in its dashboard as well as via tag-manager integration. OneWelcome has connectors for Adobe Experience Cloud and Tag Manager, Google Analytics, Marketo, Tableau, and Thallium. Customers can also use Native MongoDB connectors for Spotfire, Cognos, MicroStrategy, or SAP Business Objects to develop additional reporting capabilities. Syslog and REST enable communications with BI, CRM, and SIEM systems.

The OneWelcome Consent and Preference Management module provides view/edit/export/delete choices for consumer information, leveraging a metadata per attribute approach. The Consent API exposes all platform functions enabling Just-in-Time consent and deep customer application integration capabilities. Kantara Consent Receipt is supported. This module can run standalone and in conjunction with 3rd-party consumer authentication platforms. Family management is supported in the relationship management module, which allows definitions or roles and access controls over content and the use of managed underage user identity information. The Scaled Access acquisition brings granular dynamic authorization capabilities to the platform to enable handling of sophisticated use cases in consumer subscription management. OAuth2 Device Flow enables management of consumer IoT devices such as SmartHome components, which can be administered by consumers in their individual portals.

OneWelcome is certified/attests to ISAE3000, ISO 27001/27018, SOC 2 Type 1 & 2, EHerkenning, and

FSQS-NL. OneWelcome needs to enhance authentication and risk analysis capabilities and expose orchestration and policy management in the admin interface. FIDO support would be beneficial, but they state that they have not encountered customer demand for it yet. OneWelcome's SaaS is designed for scalability. Consent and privacy management has been a primary focus for OneWelcome since their founding. It continues to be a strong differentiator in the market. OneWelcome's Relationship management module allows definition of complex roles and controls. OneWelcome's dynamic access management features allow it to be layered on top of other CIAM solutions to add fine-grained authorization capabilities. Organizations in the EU, or global organizations that do business with EU consumers, should put OneWelcome near the top of the consideration list when looking for CIAM solutions.

Security	●●●●●
Functionality	●●●●●
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●●

onewelcome

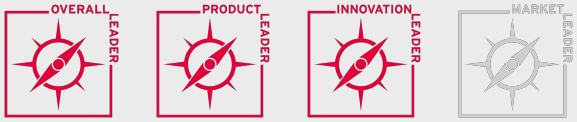
Strengths

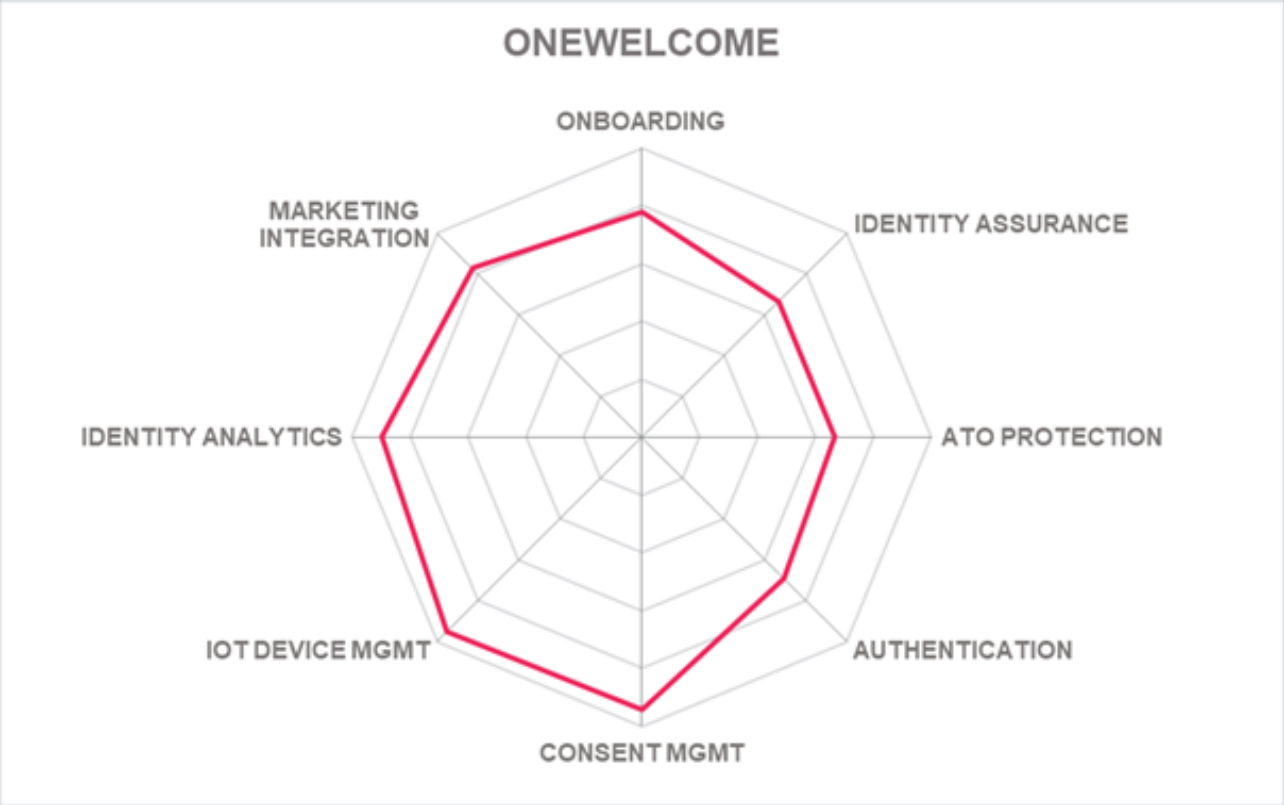
- Many integrations with ID proofing and attribute services
- Strong privacy compliance features for GDPR including EU data localization
- Excellent consent and privacy management capabilities, available as standalone product
- Kantara Consent Receipt format conformance
- Support for SmartHome device identity management
- Fine-grained authorization functions enable complex consumer access control use cases
- Good built-in identity and marketing analytics which can be extended with 3rd-party services

Challenges

- Lacks FIDO support
- No passive biometrics functions or integrations
- No FRIP connectors out-of-the-box, but can be configured
- Sales and support currently centered on EU

Leader in




ONEWELCOME
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.15 Optimal IdM

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. 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. 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 allows onboarding process customization, self-registration, and registration from social networks except Amazon and Apple. LDAP and SCIM enable customer migrations. Most major account recovery options except account linking are present. Optimal Cloud accepts OTP, many authenticator apps, Android facial recognition, and iOS FaceID and TouchID. FIDO authenticators are supported but Optimal Cloud has not certified. JWT, OAuth2, OIDC, and SAML tokens are supported. A mobile SDK is not available; thus, many device intel characteristics are not evaluated. Partnership with TypingDNA enables some behavioral biometrics. Compromised credential intelligence is not processed. Authentication policies are constructed via a drop-down list style interface.

The dashboards provided are informative and intuitive. Reports include operational metrics and identity but not marketing analytics. REST, SOAP, Webhooks, and WebAuthn APIs are supported. Customers can manually configure callouts to FRIP services, but no integrations are present out-of-the-box. Identity event information can be exported to SIEM systems over CEF or syslog. Third-party BI, CRM, and marketing analytics integrations can be manually configured by customers.

Optimal Cloud allows consumers to view/edit/delete information in their self-service portal. Consumers can select which attributes to share from social networks when registering with customer sites. Kantara Consent Receipt format is supported. Family management is possible via role-based and delegated access models. No specific support is provided for managing consumer IoT device identities in conjunction with user accounts.
The Optimal Cloud is ISO 27001 and SOC 2 Type 2 compliant. There are a few areas of basic functionality that need to be added to be a more complete CIAM offering, detailed above. Optimal IdM does have strengths in terms of the admin and consumer interface design and API documentation and protection. Organizations should consider Optimal Cloud for CIAM if their requirements align with the vendor’s strengths.

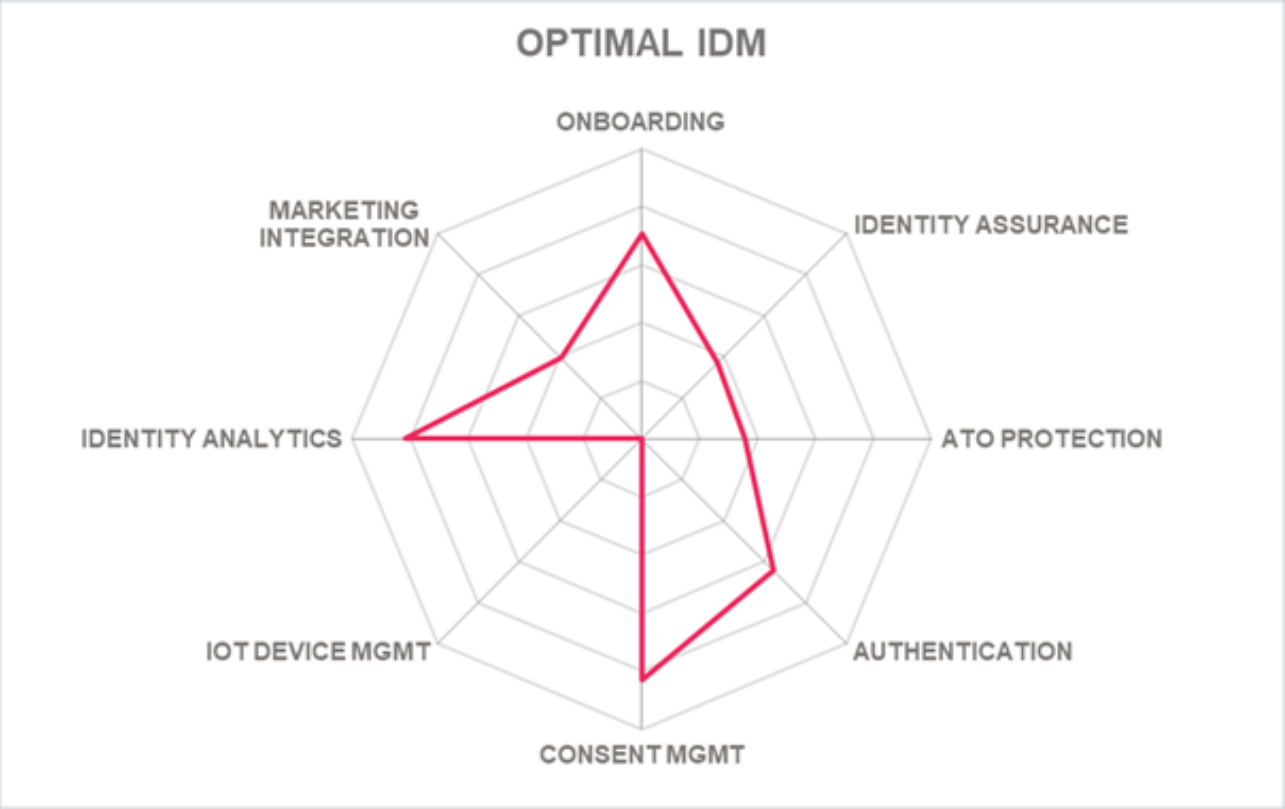
Security	●●●●○
Functionality	●●●○○
Deployment	●●●○○
Interoperability	●●●●○
Usability	●●●○○

Strengths

- Easy-to-use admin interface
- Well-designed dashboards for both customer admins and consumers
- Supports many authentication apps
- ISO 27001 and SOC 2 Type 2 audited
- Well-documented REST APIs with OAuth2/OIDC authentication

Challenges

- FIDO supported but not certified
- No mobile SDK
- Limited device intelligence evaluation
- Out-of-the-box integrations with FRIP, BI, CRM, and marketing analytics/automation systems would be advantageous
- No consumer IoT device management support


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

5.16 Ping Identity

Ping Identity has been a pioneer in identity federation and access management since its founding in Denver in 2002. Ping Identity has grown substantially and went public on the NYSE late in 2019. 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 IaaS is supported. The PingOne Cloud Platform is SaaS-hosted in public IaaS in data centers across the world. Licensing and/or subscription prices are calculated by numbers of active users per month/quarter/year, per-login or session, and per node for on-premises deployments.

PingOne allows for a high degree of customization of consumer onboarding processes through an excellent low-code/no-code GUI. LDAP, SCIM, and REST API support enable bulk imports of user account data; OIDC support permits the use of any compliant social network credential. PingOne Verify performs identity document to selfie matching, biometrics, and NFC reading of passport and eID information. Moreover, many connectors to 3rd-party IdPs and attribute providers can be leveraged. The full gamut of account recovery options is available. OTP, most mobile authenticators, Android/iOS biometrics, social logins, and FIDO U2F and 2.0 (certified) authenticators are accepted. Ping's mobile SDK can harvest most device attributes except MNO and Wi-Fi parameters. Behavioral biometrics are considered for granular risk analysis. The PingOne Fraud module provides alternatives to credential intelligence. Authentication policies can be handily edited in the admin GUI.

Ping exposes all functions through well-documented and secured APIs, including REST, RPC, SOAP, Webhooks, Websockets, and WebAuthn. Any external FRIP service can be integrated and evaluated by the risk engine. Detailed identity analytics are present within the dashboard. For advanced BI, CRM, and marketing analytics and automation, Ping supports integration with Hubspot, MailChimp, Marketo, and Zoho. Identity event information can be sent to any customer SIEM over CEF, REST, or syslog.

Rudimentary permission management for consumers is present in the user portal. More advanced features such as opting out of data collection, automating consumer notifications, and deleting stored user data require customization in the PingOne DaVinci interface. PingOne does not distinguish between identity types, which allows it to manage device identities similarly to user identities. OAuth2 Device Flow support facilitates consumer device identity management.

Ping Identity self-certifies as CSA Star Level 1 and is audited for ISO 27001 and SOC 2 Type 2. Ping Identity components are also OpenID certified Basic OP, FAPI, Implicit OP, Hybrid OP, Config OP, and Form Post OP. More out-of-the-box connectors for marketing apps and ready-made consent management capabilities would be welcomed. Ping supports all relevant identity and security standards. Their SaaS options are designed to be highly scalable. The PingOne Cloud Platform is feature-rich and should be on the short list of any organization searching for CIAM solutions.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

Ping Identity

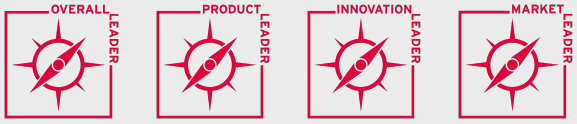
Strengths

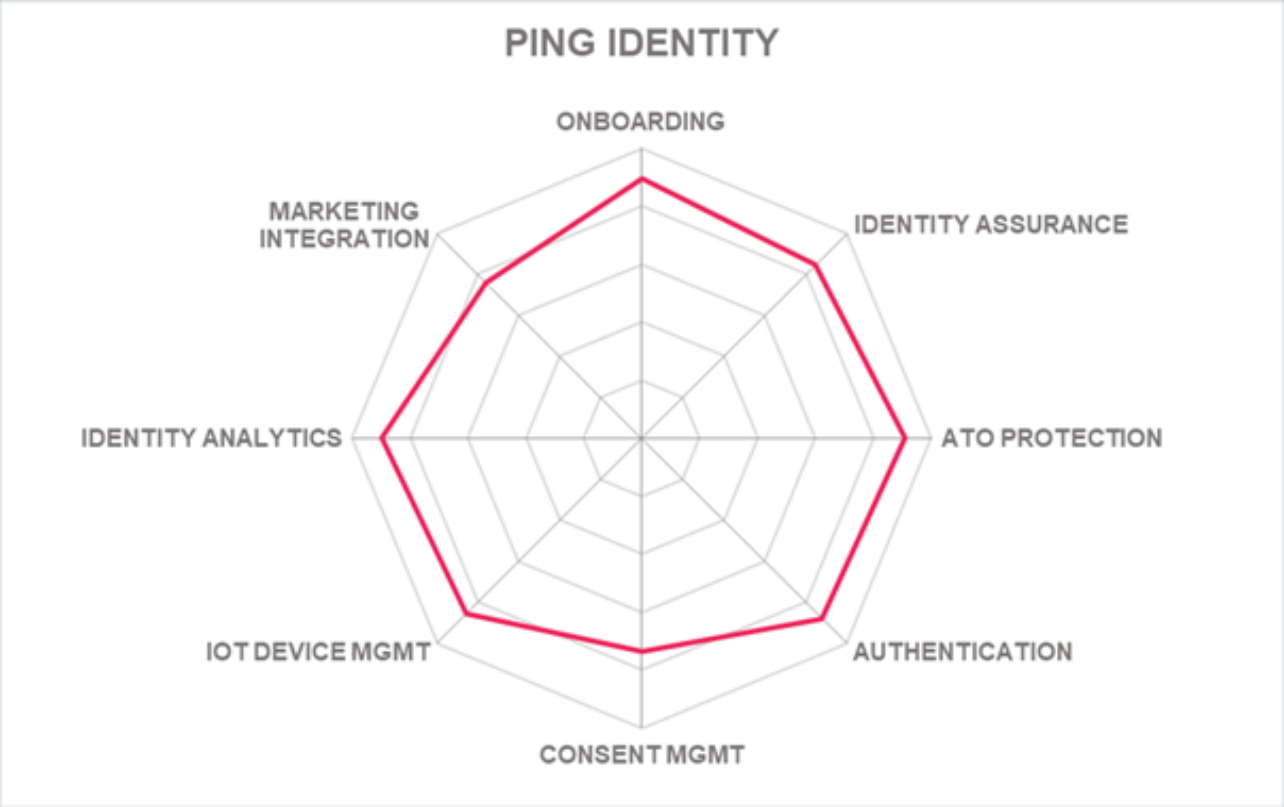
- Highly flexible orchestration that is easily configurable through admin interface
- Wide range of authenticator types accepted
- FIDO 2 certified server
- PingOne Verify adds strong identity proofing functions which can be extended with 3rd-party services
- SDK with excellent device intel and behavioral biometrics
- Good API documentation and security
- PingOne Fraud add-on

Challenges

- Additional out-of-the-box connectors for BI, CRM, and marketing analytics and automation platforms are in work
- Consent handling for privacy regulatory compliance requires additional customization
- Lacks the ability to collect some device attributes
- Connectors to credential intelligence providers are in work

Leader in




PING IDENTITY
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.17 ReachFive

ReachFive is a small, 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, and most customers are in France. The offering is SaaS and is hosted in top tier IaaS providers. Service prices are calculated by the number of active or registered users per quarter or per year.

Customers can migrate users into Reach Five using SCIM. Consumers can register by email or social logins. Onboarding workflows are minimally customizable, and devices are not associated with consumer accounts. There are no in-platform identity proofing features and connectors for 3rd-party services have not been coded yet. Account recovery options include most common methods except mobile push. Authenticators accepted include OTP, Android/iOS biometrics, social logins, and FIDO 2. JWT, OAuth2, and OIDC are supported, but not SAML. ReachFive has a mobile SDK, but it does not pick up most device intelligence signals, nor does it evaluate passive biometrics. Authentication policies are written and administered in the GUI, which uses a standard drop-down attribute and action list approach.

Customers can view consumer identity analytics in pre-configured reports and dashboards. REST, Webhooks, and WebAuthn APIs are supported. Connectors are available for Adobe Campaign, DialogInsight, Google Big Query and Data Studio, Microsoft Dynamics and PowerBI, Salesforce, and Splio. There are no connectors out-of-the-box for FRIP services.

ReachFive allows consumers to view, edit, and delete their personal information. The solution does not support Kantara Consent Receipt, but the ReachFive family management implementation follows the Kantara User Managed Access standard. ReachFive is not yet aligned with OAuth2 Device Flow and does not offer consumer IoT device identity management within their platform.

ReachFive is still growing and adding features. It lacks some key areas of CIAM functionality but could be a contender in the retail market in France and Europe.

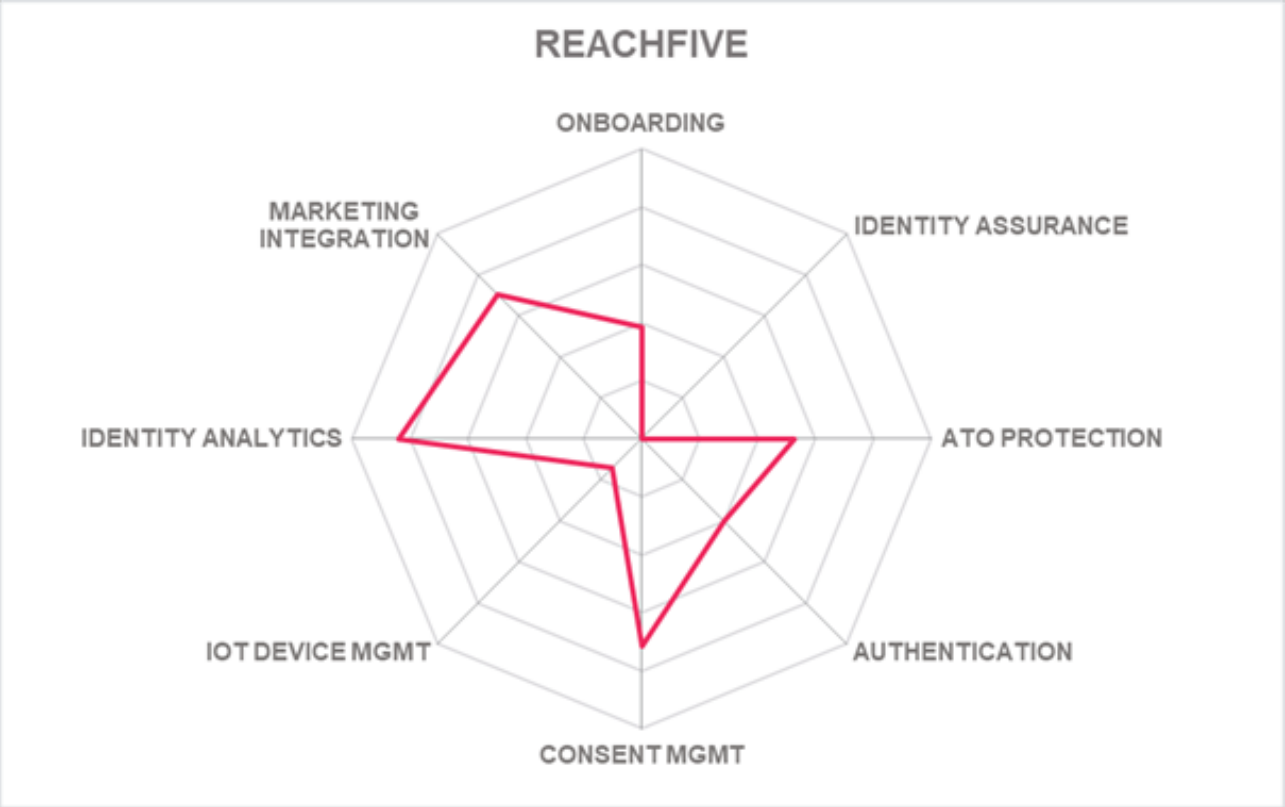
Security	●●●●○
Functionality	●●○○○
Deployment	●●●○○
Interoperability	●●○○○
Usability	●●●○○

Strengths

- Evaluates in-network credential intelligence in authentication risk decisions
- Connectors for some popular BI, CRM, and MarTech vendors
- Family management model follows Kantara UMA

Challenges

- Identity proofing integrations on the roadmap
- Rigid onboarding processes
- Needs to support more types of authenticators and SAML federation
- FIDO supported but not certified
- Few device attributes evaluated
- Still in startup mode, with most clients in France


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

5.18 SAP

SAP was originally founded in Germany in 1972. 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.

SAP allows self-registration and social network registration for onboarding. SAP's Identity Journey enables customers to tailor the onboarding experience through a low-code/no-code interface. SCIM and dedicated migration API and ETL functions facilitate bulk import of user data. Identity proofing connectors are not available yet but are planned. SAP CIAM supports all major account recovery mechanisms. OTP, Google Authenticator, Android/iOS biometrics, and FIDO 2 authenticators are accepted; however, SAP is not FIDO certified. JWT, OAuth2, OIDC, and SAML are supported for federation. SAP provides SDKs for many platforms; the mobile SDKs can collect a useful subset of available device intelligence characteristics but lack behavioral biometrics. In-network credential intel is considered by the risk engine. Authentication policies are managed in a flow-chart style admin interface.

REST, RPC, Webhooks, and WebAuthn APIs are supported. For FRIP services, connectors are available for Arkose Labs and Trans Union. SAP CIAM excels at identity and marketing analytics, providing many pre-defined reports covering most aspects of consumer identity. Identity Query allows customization of reporting based on any defined attribute. The Customer Insights interface offers rich marketing data, covering demographics as well as social interest data. SAP has connectors for 3rd-party BI, CRM, marketing analytics and automation systems such as Adobe Analytics and Experience Manager, CheetahMail, Constant Contact, Crowdriff, Eloqua, Google Analytics, KissMetrics, MailChimp, Marketo, Optimizely, Responsys, Sailthru, Salesforce, SAP Marketing Cloud, WebTrends, Zendesk, and others.

SAP Enterprise Consent and Preference Management allows customers to set up CIAM instances that facilitate compliance with regulations such as CCPA, GDPR, and LGPD. Very granular options can be presented to consumers. The solution is also highly scalable, processing billions of consent actions and having the ability to store consent records for up to 7 years. Full family management is possible by defining family relationships and granting entitlements in the consumer portal. SAP's Global Login feature allows customer admins to localize consumer data to their region, facilitating regulatory compliance. SAP CIAM supports managing consumer IoT devices such as Smart Speakers, wearables, and home automation in conjunction with their digital identities.

SAP self-attests to CSA Star Level 1 and has been audited for ISO 27001 and SOC 2 Type 2. The well-designed multi-cloud service is highly scalable. SAP still needs to add support for more authenticators and achieve FIDO certification. Support for more FRIP services, particularly identity proofing 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 enhancing features.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●●●
Interoperability	●●●●○
Usability	●●●●○

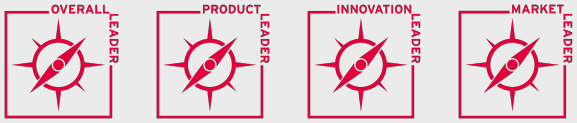
Strengths

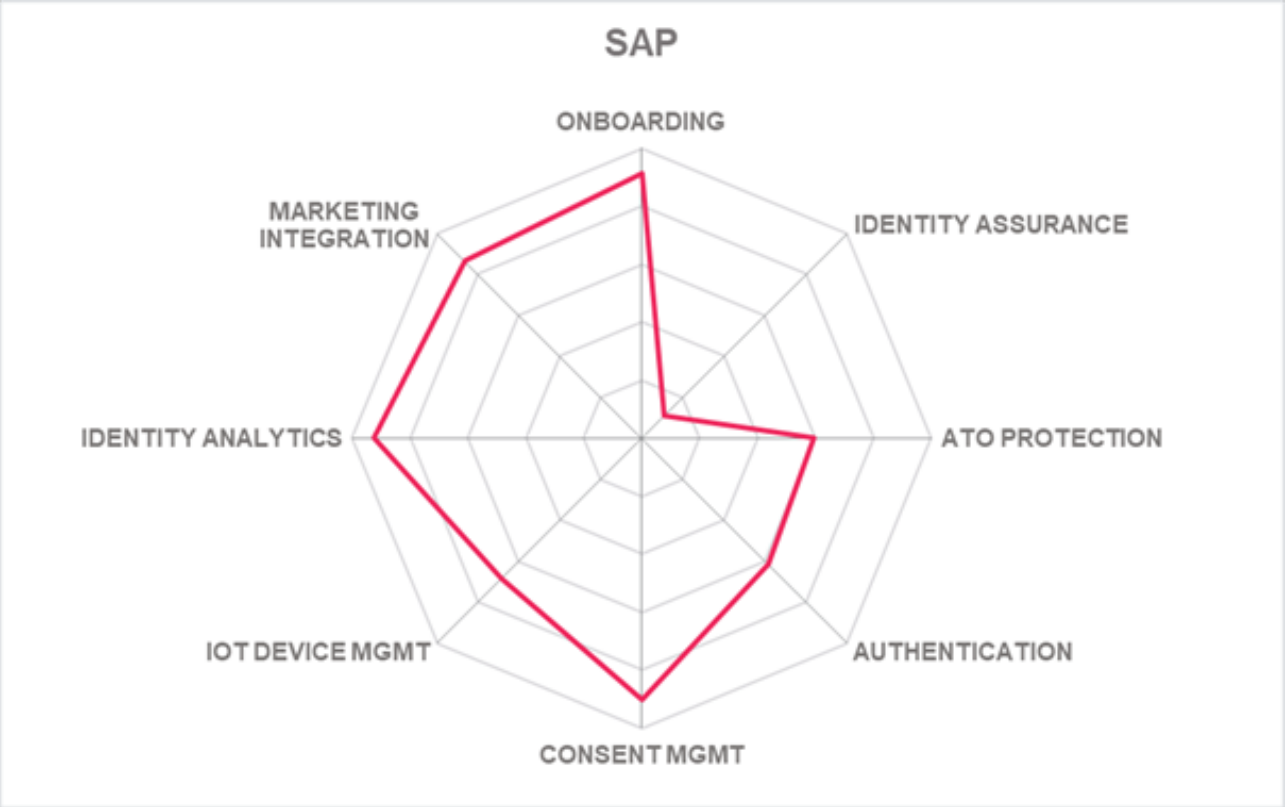
- Highly customizable onboarding workflows
- Offers extensive account recovery options
- Very scalable, cloud-native offering
- Excellent built-in identity and marketing analytics capabilities which can be augmented via integrations with many 3rd-party tools
- SAP Enterprise Consent and Preference Manager support for GDPR, CCPA, and LGPD
- Support for complex consumer IoT device identity management use cases

Challenges

- No identity proofing integrations currently
- FIDO supported but not certified
- Needs support for additional authenticator types
- No behavioral biometrics support
- Orchestration and policy administration interface could be improved
- Additional connectors for fraud reduction services would be beneficial

Leader in




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

5.19 Simeio Solutions

Simeio was founded in 2007 in Alpharetta, GA, US, providing IAM consulting and system integration services. Simeio launched their IDaaS and CIAM services in 2017. Simeio serves both B2C and B2B use cases. Identity Orchestrator is delivered as SaaS, hosted in North American and European data centers in public IaaS platforms. Pricing for the service is according to the numbers of monthly/quarterly/annual active users or by number of registered users per quarter/year.

Simeio allows self-registration and registration from social networks except Amazon. As the product name implies, it allows customization of onboarding workflows, though some of the customization must be performed by Simeio staff. Simeio offers a mobile identity verification app which can be augmented with many 3rd-party identity proofing services. All recommended account recovery options are present. A plethora of authenticators can be used with Simeio, including OTP, most mobile authenticator apps, Android/iOS biometrics, FIDO U2F and 2.0. Third party apps require separate licensing. JWT, OAuth2, OIDC, and SAML are supported for federation. APIs but not SDKs are provided; thus, there is no direct consumption of device intelligence or passive biometrics. Credential intelligence is evaluated by the risk engine. Authentication policies are crafted in intuitive flow-chart style interface.

Simeio supports REST APIs only. Simeio has integrations with multiple FRIP providers including Broadcom, Experian, HID Global, IBM, ID Data Web, IDNow, Kaspersky, LexisNexis, Outseer, Transmit Security, and Trans Union. Simeio's admin dashboards and reports provide basic identity event information and analytics. There are no connectors for BI, CRM, or marketing automation and analytics, but customers or Simeio services teams could configure them if needed. Simeio does have integrations with major IAM and IDaaS solutions.

Identity Orchestrator provides portals so that users can view, edit, and delete their personal information and consents. At present, Kantara Consent Receipt is not supported. Family management is not implemented. OAuth2 Device Flow is present, but the ability to manage consumer IoT device identities has not been further developed.

Simeio's services are CSA Star Level 2, ISO 27001, ISO 27018, and SOC 2 Type 2 attested and/or audited. Simeio has a scalable architecture. Identity Orchestrator has some functional omissions that have not been built as outlined above. Simeio is growing and we expect these will be addressed on their roadmap. Simeio's strengths arise from their history of providing IAM customization and consulting for clients. Organizations that need orchestration capabilities, built-in and supplemental identity proofing requirements, and the ability to pull in fraud reduction intelligence should review Simeio's solutions.

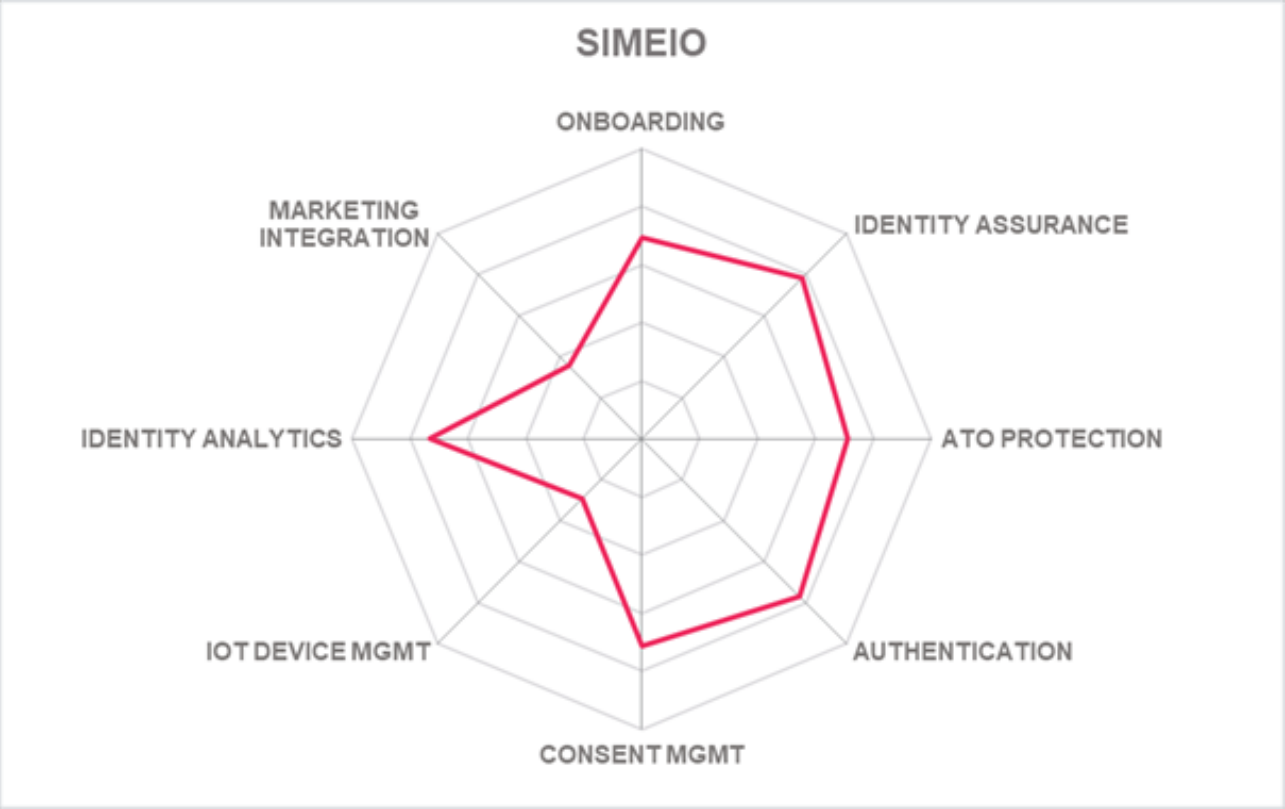
Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●○○
Usability	●●●●○

Strengths

- Integrations for many 3rd-party identity proofing services
- Mobile identity verification app
- Full range of account recovery options supported
- Intuitive admin interface
- Connectors for fraud reduction intelligence services

Challenges

- Some customizations require Simeio support
- FIDO supported but not certified
- No SDKs: no device intelligence or passive biometrics
- Webhooks and WebAuthn support needed
- No out-of-the-box integrations with BI, CRM, or marketing automation/analytics
- Family management is not implemented
- Consumer IoT device management not addressed


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

5.20 Synacor

Synacor was founded in Buffalo, NY in 1998. Synacor was acquired by Center Lane Partners, a private equity company, in April 2021. The Media Division was divested, but they retain Zimbra Cloud Email. 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 media. Synacor hosts Cloud ID as fully multi-tenant SaaS in their own data centers and a public IaaS platform from data centers within the US. Subscription costs are determined by monthly active or registered users.

Migrations from and directory synchronization with other platforms can be achieved using LDAP and ETL. Self-registration and social network registration (except Apple and LinkedIn) are accepted. Many aspects of the consumer onboarding processes can be customized, but such orchestration is generally handled by Synacor for their clients. Identity proofing is neither provided nor directly available via pre-packaged integrations. Synacor enables all relevant forms of account recovery. Authenticators accepted include OTP, mobile push, Authy and Google authenticators, and Android/iOS biometrics. FIDO is not supported but is on their roadmap. JWT, OAuth2, OIDC, and SAML can be used for federation. SDKs have been deprecated in favor of API access but are still supported for those customers who use them. Device intelligence and behavioral biometrics are not considered in risk evaluations but compromised credential intelligence from in-network and 3rd-party sources does inform the risk engine. Authentication policies support levels and actions that are suited to the use cases they are designed to address. The client admin interface is simple and straightforward.

REST, RPC, SOAP, and Webhooks are supported API types. Cloud ID interoperates with NuData Security and Google reCAPTCHA for reducing fraud risks. Cloud ID provides many identity related out-of-the-box reports and they can, at customer request, create more. There are no out-of-the-box connectors to 3rd-party BI, CRM, and marketing analytics platforms, but customers can create real-time data exports using Kafka and Webhooks. Identity event information can also be sent via syslog or REST to customer SIEMs.

Cloud ID allows consumers to view, edit, and delete personal information. Complex family management can be configured by customers, allowing for parent/guardian control over minors' access to content. For example, device management views permit heads of households to configure parental controls and authorize specific apps for dependents. Cloud ID creates and maintains opaque IDs to shield service provider customers from obtaining and storing personal data of their consumers. Cloud ID obtains consent to broker one digital identity for use in other ecosystems. Cloud ID accepts device authentication from Set Top Boxes, Set Back Boxes (used in the hospitality industry), streaming media devices, Smart TVs, Smart Speakers, automotive satellite/internet receivers, and Wi-Fi hotspots.

Cloud ID has been audited for SOC Type 2, and it is PCI-DSS compliant. Cloud ID is missing a few 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. Therefore, Synacor has robust capabilities in that rapidly growing specialty within the CIAM market. Organizations in those industries as well as any organization that may have advanced use cases involving consumer IoT devices will want to closely

evaluate Synacor Cloud ID for CIAM or as an adjunct to existing IAM/IDaaS solutions.

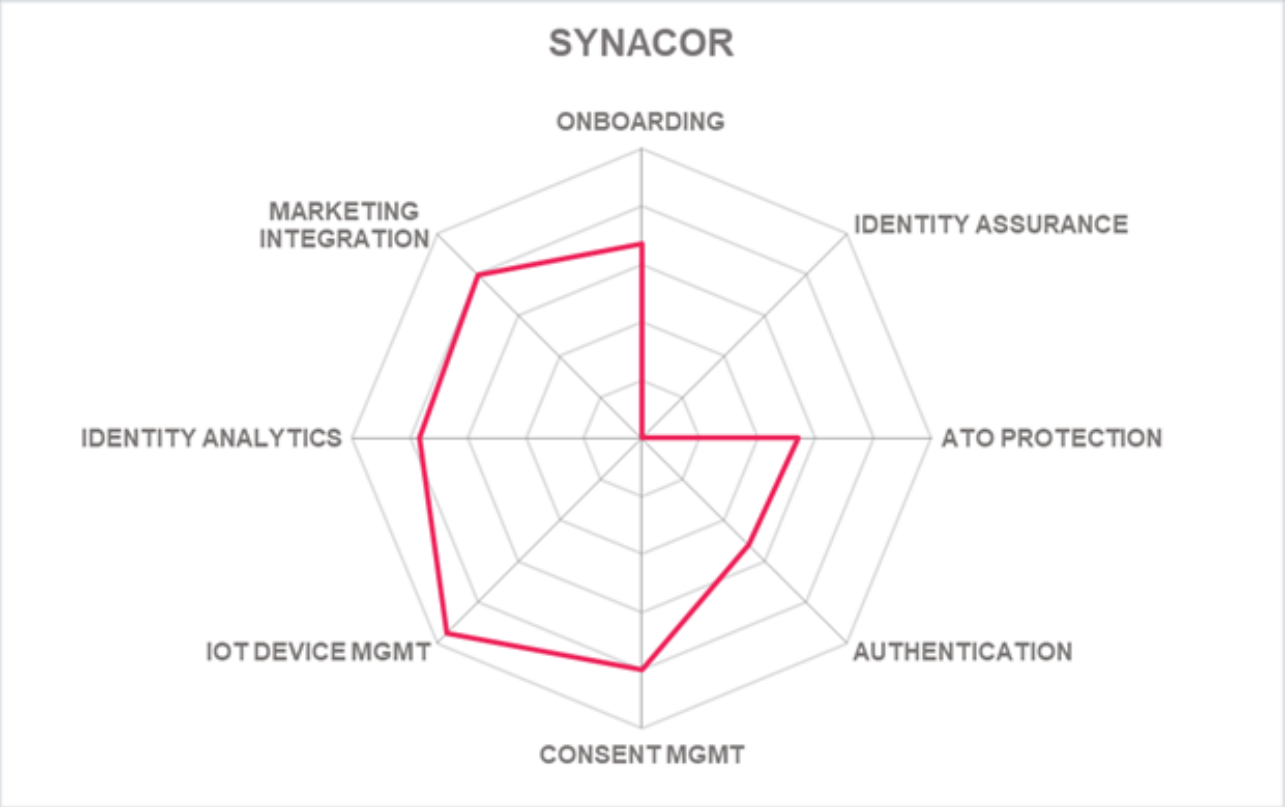
Security	●●●●○
Functionality	●●●○○
Deployment	●●●○○
Interoperability	●●●●○
Usability	●●●●○

Strengths

- Leverages multiple sources of credential intelligence
- Built-in bot detection and management
- OOTB integration with popular consumer IoT products such as Smart TVs, STBs, home automation, home security, and fitness equipment
- Consent management features help with CCPA, COPPA, GDPR, and LGPD compliance
- Flexible family management options include parental controls

Challenges

- No identity proofing capabilities
- FIDO not supported but is on the roadmap
- Does not use device intelligence or behavioral biometrics
- Integration with BI, CRM, or marketing analytics and automation tools may require coding, but deep customization is possible via the Cloud ID Identity Bridge


SYNACOR
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.21 Transmit Security

Transmit Security was founded in 2014 and is headquartered in Tel Aviv and Boston. Its software can run on-premises, but they host SaaS in public IaaS across globally distributed data centers. Transmit Security also competes in the Enterprise Authentication and Fraud Reduction Intelligence Platforms markets. Transmit Security has integrated and rebranded their multiple products in this area to CIAM Platform. Transmit Security CIAM Platform can be installed on-premises or in Amazon, Azure, or GCP. Transmit operates the products for customers as SaaS spanning multiple continents hosted in two public IaaS providers for high availability. Multiple licensing and/or subscription models are offered.

Transmit makes it easy to onboard users: fully customizable workflows for self-registration, registration from social networks or OIDC, and migration over LDAP. All standard account recovery methods are present. Transmit has an API that can perform remote identity proofing including functions such as taking selfies with liveness detection, identity document verification, and email and phone verification. Transmit has connectors to 3rd-party identity proofing services such as Equifax, LexisNexis, Pindrop, and others. Transmit Security allows customers to integrate compromised credential intelligence sources via API calls and consider those results in risk decisions. Transmit accepts FIDO U2F/2.0, OTPs, and mobile push authentication. They offer their own authenticator app and SDK. The authenticator app leverages built-in fingerprint and facial recognition biometrics. The SDK harvests device information and behavioral biometrics. Transmit Security's risk engine is configured through the Journey Editor policy builder. It features an innovative, flowchart style interface. Transmit Security supports call center integration with Genesys, Nuance, and Pindrop, allowing call-to-web session mapping.

External identity and fraud intelligence data sources can be consumed, and risk engine output can be sent over REST APIs that can be secured using JWT, OAuth2, OIDC, and SAML authentication. WebAuthn is supported as well. There are no out-of-the-box connectors for CRM, marketing analytics/automation tools, or other SaaS apps yet. Many identity analytics reports are present. Syslog enables connections to customer SIEMs.

The Transmit Security suite provides consent collection and user self-service profile management capabilities. Family management is not implemented, however. Consumers have limited abilities to manage their IoT devices via the Transmit Security solution, although the OAuth2 Device Flow specification is not supported.

Transmit Security is FIDO certified. The service has been audited for ISO 27001 and SOC 2 Type 2. Transmit Security was an Overall, Product, Innovation, and Market Leader in the last edition of the KuppingerCole Leadership Compass on Fraud Reduction Intelligence Platforms. Their solution was an Overall, Innovation, and Product Leader in the previous KuppingerCole Enterprise Authentication Solutions Leadership Compass. Transmit has recently added remote identity proofing features via an app, and passive biometrics support in their SDK. There are a few features that have yet to be implemented, but Transmit Security has a multi-cloud architecture and integrated fraud prevention capabilities, making it a potentially suitable solution for organizations that have requirements for high scalability and high-volume

transaction analysis.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●●●
Interoperability	●●●●●
Usability	●●●●○

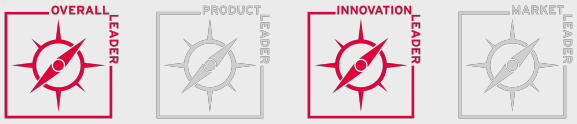
Strengths

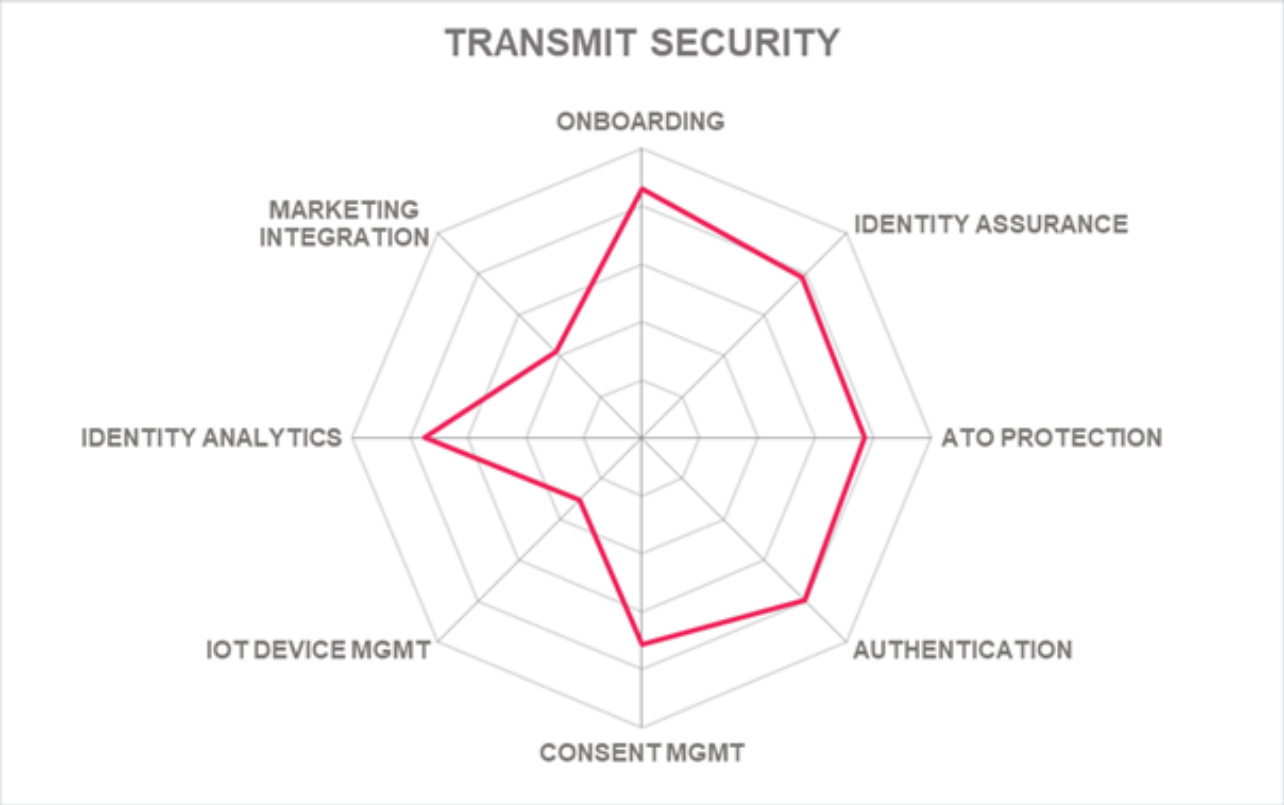
- FIDO UAF & 2.0 server certified
- Scalable, high availability micro-services architecture
- App for remote identity verification, including document verification and liveness testing
- Full-featured FRIP service built-in
- Excellent admin interface
- Call center integration, including call-to-web session mapping

Challenges

- Complex licensing options
- Credential intelligence evaluation is on the roadmap
- Lacks connectors for marketing analytics/automation, but customers can code their own
- Family management is not addressed

Leader in




TRANSMIT SECURITY
ONBOARDING
IDENTITY ASSURANCE
ATO PROTECTION
AUTHENTICATION
CONSENT MGMT
IOT DEVICE MGMT
IDENTITY ANALYTICS
MARKETING INTEGRATION

5.22 WSO2

WSO2 was founded in 2005 in Sri Lanka and is headquartered in Santa Clara, CA. They are an 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. Related products include Enterprise Integrator and API Manager. 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. Identity Server is licensed per node, and Asgardeo is priced by numbers of monthly active users.

WSO2 allows social network and self-registration for consumers. The admin console features a flow-chart interface for configuring orchestration for registration, information collection, consent, authentication types, etc. Devices like mobile phones cannot be associated with consumer profiles. Both LDAP and SCIM can be used to import user accounts in bulk. A connector for EvidentID provides limited identity proofing; integration with additional 3rd-party identity proofing services is planned. Customers can build integrations with other identity assurance providers. Most account recovery mechanisms are present. Email/SMS OTP, many mobile authenticator apps, and FIDO U2F/2.0 are accepted authentication methods. WSO2 has connectors for Veridium Biometrics and Aware Knomi for mobile biometrics, but Android and iOS biometrics are not supported directly. JWT, OAuth2, OIDC, and SAML are supported for federation. A mobile SDK is available, but it does not collect device intelligence attributes. Integration with TypingDNA enables some passive biometrics. There are no out-of-the-box credential intelligence feeds, but customers could create connections through the API. The risk engine is highly configurable through an intuitive natural language style interface.

WSO2 has excellent API coverage: AMQP, MQTT, OData, REST, RPC, SOAP, Webhooks, Websockets, and WebAuthn. Choreo and API Manager (related WSO2 products) enable customers to integrate their own and public APIs into new applications and secure them. Many identity metrics are collected and displayed in the customizable admin dashboards. No FRIP connectors exist out-of-the-box, but those too can be constructed by customers. WSO2 supports integrations with CRM and marketing analytics and automation solutions such as Google Analytics, HubSpot, Mailchimp, Marketo, Microsoft Dynamics, Mixpanel, Pardot, Pipedrive, Salesforce, Sendgrid, and Zoho. Both Asgardeo and Identity Server can use syslog to send identity event data to customers SIEMs. Outbound provisioning connectors are available for popular SaaS applications.

WSO2 allows consumers to view, edit, export, and delete personal information within a self-service portal. Identity Server supports the Kantara Initiative User Managed Access (UMA) and Consent Receipt specifications. Family management is not implemented, however. WSO2 supports OAuth2 Device Flow and enables some consumer IoT device identity management but does not expose the device management features within the consumer self-service portal. WSO2 maintains strong ties with Entgra, which was spun out from WSO2 in 2018; Entgra provides additional advanced endpoint and IoT/OT device management features.

WSO2 is ISO 27001 certified. SOC 2 Type 2 certification is in work. WSO2 was late to the cloud but is rapidly catching up with the Asgardeo offering. The solution is missing a few key features as detailed above. The core strengths of WSO2 solutions are the open-source plus support model, adherence to industry standards, and its API emphasis. These features enable WSO2 to serve the CIAM role and enable its customers to extend the solution as needed to meet their requirements. WSO2 reports a strong upsurge in the use of their product for B2B customer identity use cases. Any organization that has develops its own business applications that needs a highly extensible CIAM solution should consider WSO2.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●●●
Interoperability	●●●●●
Usability	●●●●○

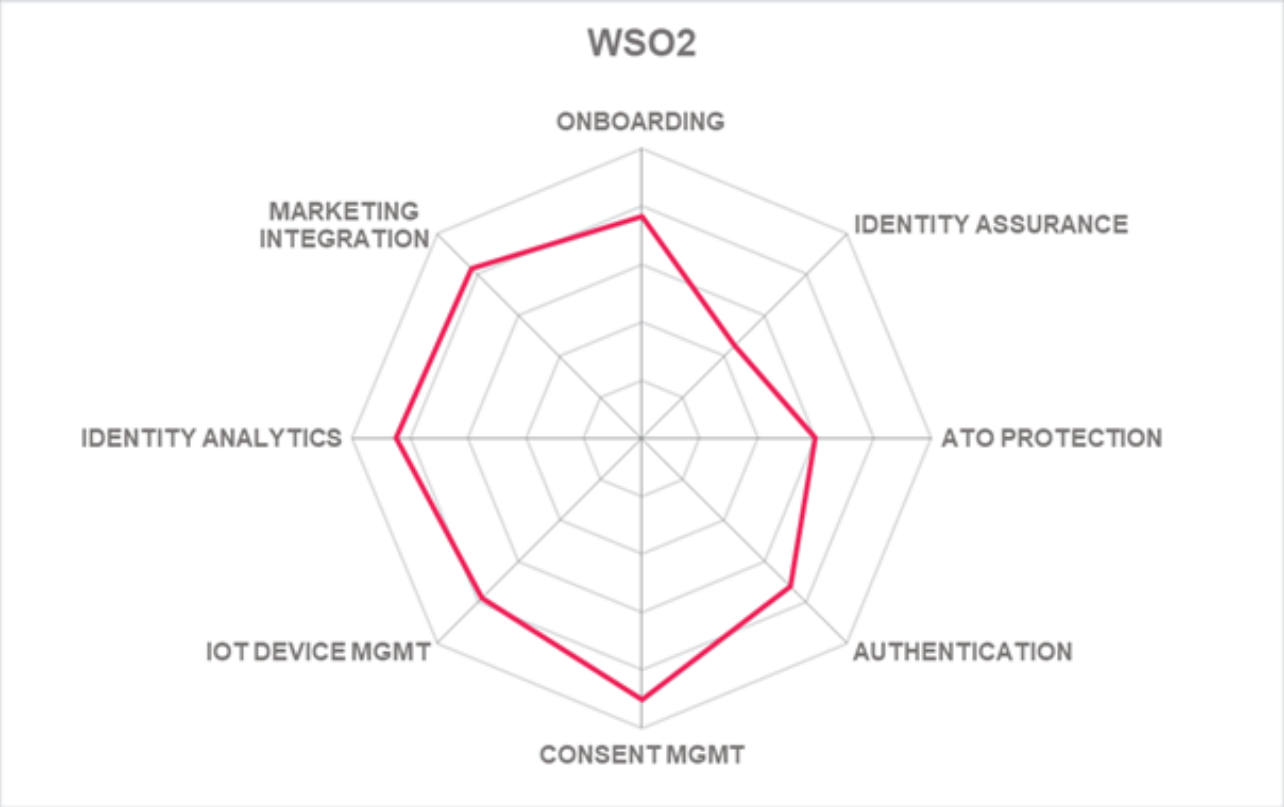
Strengths

- Flow-chart and natural language style admin and developer interfaces
- Highly configurable risk engine
- Connectors for IAM/IDaaS and many SaaS apps
- Broad support for API types and IAM communication standards
- Focus on API documentation, exposure, and security facilitates customer application development
- Good consent management features
- Highly extensible and customizable

Challenges

- FIDO supported but not certified
- Does not support Android facial recognition or iOS biometrics
- Mobile SDK needs enhancement: no device intelligence functions yet
- Identity proofing capabilities need to be expanded
- Lacks family management
- No consumer portal for managing IoT device identities

Leader in


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

5.23 XAYONE Solutions

XAYONE Solutions was founded in 2012 as Oxyliom Solutions. They are headquartered in Luxembourg and have offices in Casablanca and Dubai. 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 in most Tier 1 IaaS platforms. XAYONE Platform is offered as SaaS and operates from a single cloud provider in Luxembourg. Multiple licensing/subscription models are available.

Onboarding workflows can be tailored in the no-code admin GUI. XAYONE Platform allows migration of customers via LDAP, SCIM, or REST API as well as Just-In-Time (JIT) SAML account creation. XAYONE offers a remote identity verification app that can scan any ICAO passport and perform hologram verification, facial recognition, NFC reads against chipped documents, and passive liveness and spoofing checks. Connections to 3rd-party identity proofing services are not provided. Account recovery options include all standard means. XAYONE accepts OTP, mobile push, some authenticator apps, social logins, Android/iOS biometrics, and FIDO U2F/2.0. JWT, OAuth2, OIDC, and SAML are supported for federation. XAYONE's mobile SDK can harvest a subset of key device intelligence parameters. Passive biometrics are not built-in. In-network and 3rd-party sources of credential intelligence are utilized. Customer admins edit policies in a drop-down style interface.

REST, Webhooks, Websockets, and WebAuthn APIs are available. XAYONE has a connector for Broadcom for fraud prevention. A good range of identity activity reports are available through the customer dashboard, including anonymized metrics related to regulatory compliance. Identity event information can also be passed to customer SIEMs over syslog. Marketing automation and analytics are handled by 3rd-party integrations with DemandBase, eMarketer, Marketo, Oracle, Salesforce, webCRM, and Zoho.

XAYONE Platform features user dashboards for self-service consent and privacy management, including the abilities to view/edit/export/delete personal information. Family management can be configured via roles and a delegated admin model. XAYONE has strong support for relevant regulations in the financial industry, including AML, eIDAS, GDPR, KYC, and PSD2. XAYONE Platform offers key management in the platform and works with leading HSMs to provide high levels of data security and consumer privacy. XAYONE adheres to OAuth2 Device Flow for registration and association of consumer IoT device identities with consumer identities. SmartHome and vehicle x.509 certificate association are two types of device management use cases addressed by XAYONE.

XAYONE Platform Trust Platform has not been audited for ISO 27001 or SOC 2 Type 2. The solution is based on microservices which should enable scalability, but the service is run from a single data center. Most sales and support are currently in Africa, the Middle East, and the Benelux region of the EU. Their remote onboarding app that accepts any ICAO passport is a differentiator for Oxlyiom along with their passwordless authentication capabilities. Their marketing focus has been in banking. XAYONE has been adding features in a number of areas since the last iteration of this report. Organizations in the finance industry, particularly those in the regions well-served by XAYONE, should review their capabilities when

searching for CIAM solutions.

Security	●●●●●
Functionality	●●●●○
Deployment	●●●○○
Interoperability	●●●●○
Usability	●●●●○

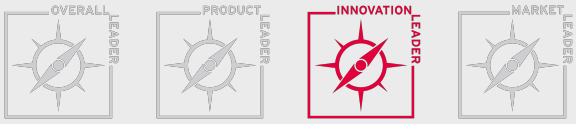
Strengths

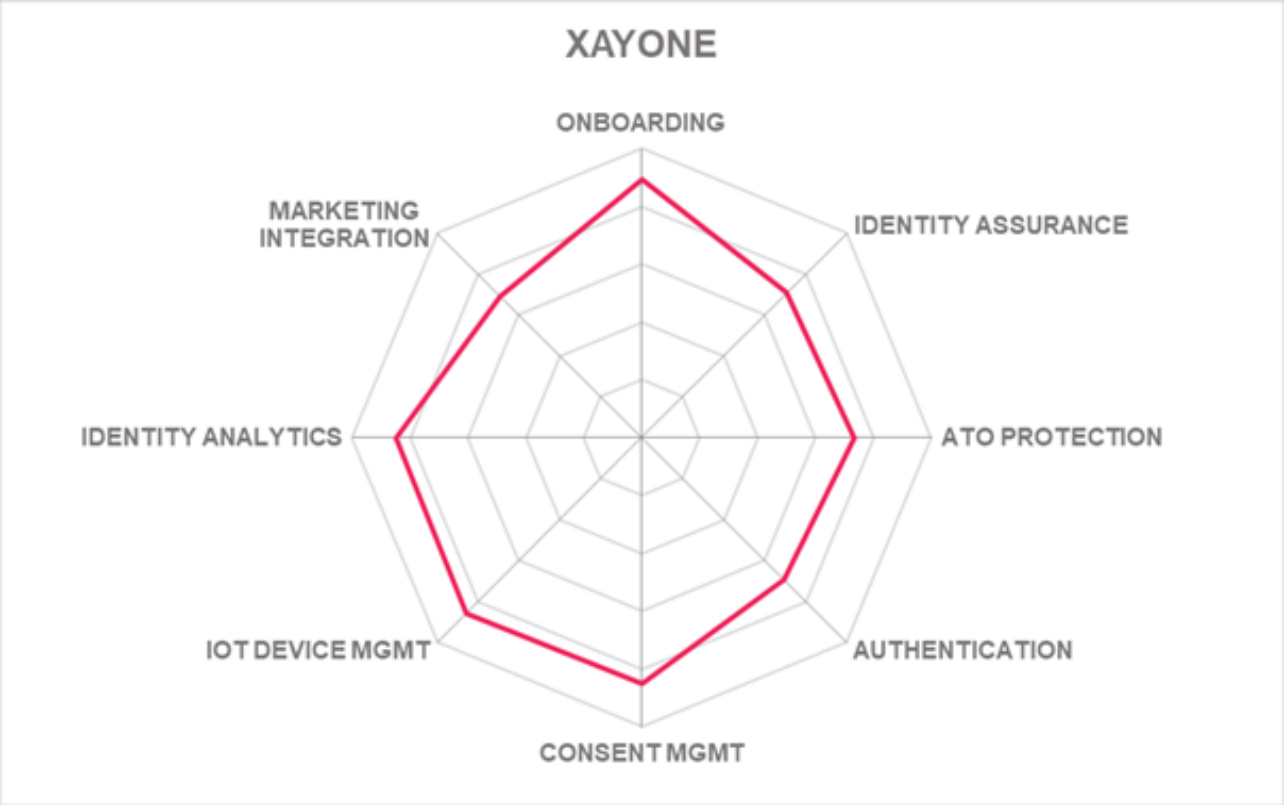
- Highly flexible remote identity verification app for identity proofing
- Good support for AML, eIDAS, e-KYC, GDPR, and PSD2
- ML detection models used for identity proofing fraud prevention
- Above average range of authenticators accepted
- Consumer IoT device identity management

Challenges

- FIDO supported but not certified
- Device intelligence capabilities should be expanded; no passive biometrics
- Needs integration with privileged access controls
- Customer admin console needs updating
- Small vendor but with a growing customer base, mostly in Africa at present

Leader in




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

6 Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment or may be a fast-growing startup that may be a strong competitor in the future.

Amazon Cognito - Amazon offers some CIAM functionality with Cognito. Cognito supports OAuth, OIDC, and SAML for federation, allowing users to sign in using social media credentials. Cognito is built for controlling access to Amazon resources. All services are exposed via APIs, meaning it would be categorized as more of an Identity API Platform than a full CIAM solution. Amazon's computing environment is PCI-DSS, SOC, ISO/EIC 27001, ISO/EIC 27017, ISO/EIC 27018, and ISO 9001 compliant. As the largest IaaS provider in the world, Amazon's identity services will be increasingly used to provide CIAM style experiences. KuppingerCole will follow developments in Amazon Cognito.

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 doesn't 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. 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 2019. They are a well-funded startup headquartered in New York and focused on passwordless authentication. Their solutions address both consumer and workforce use cases. Beyond Identity Secure Customers is a cloud-native solution hosted by a single IaaS platform distributed across US and EMEA data centers. Beyond Identity provides a mobile app that leverages built-in biometrics for authentication. Beyond Identity has been audited and attests to SOC 2 Type 2. KuppingerCole has published research on Beyond Identity, and will continue to track their developments.

Curity – Curity was launched in 2015 and is headquartered in Stockholm. Curity Identity Server can be deployed on-premises, in the cloud, or across multi-cloud architectures. Curity Identity Server is API driven and focused on API security. OAuth and OIDC are supported. Moreover, Curity supports financial grade API (FAPI), Client Initiated Backchannel Authentication (CIBA), and Push Authorization Requests (PAR). Thus, Curity has an emphasis on strong authentication and secure token services. A free community edition is available. KuppingerCole has reported and will continue to publish research on Curity.

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. Admins can also use Google Analytics for identity and marketing analyses. Google is a major SaaS platform with lots of business productivity applications and customers. It would be easy for Google to pivot into offering full-scale CIAM.

Login Alliance Syntlogo Login Master - Login Alliance Syntlogo was founded in 2001 near Stuttgart. They have leveraged their experience in IAM consulting to create Login Master (CIAM) and Secu-Role (IAM role management) solutions. Login Master can run on-premise 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. are strongest in the DACH region of Europe in terms of sales and support. KuppingerCole will continue to monitor Syntlogo and cover them in future reports.

Miracl - Miracl is a London-based startup focused on strong but user-friendly MFA. Their solution is passwordless (but does require a PIN, however it is not stored). It uses cryptographic keys which are split protected by PIN. PIN entry serves a zero-knowledge proof for authentication. Miracl can also be used for document and transaction signing. The solution can run on-premises and in the cloud. Miracl has an open-source SDK upon which clients can build apps. Miracl has unique MFA capabilities that address high security requirements. While it is missing some CIAM functions, it would be a good authentication add-on for companies needing convenient and strong authentication.

Pirean (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. Pirean was a Product and Innovation Leader in the previous version of this report, but they were unable to participate this time.

PRIVO – Privacy Vaults Online, better known as PRIVO, was founded in 2001 and is headquartered in the Washington, DC area. Their emphasis is on providing US COPPA (Children's Online Privacy Protection Act) and GDPR compliant consumer identity solutions and related services with a focus on the unique needs of organizations interaction with minors' data. PRIVO is SaaS-delivered, residing in public IaaS distributed across multiple data centers in the US. The company is a member of the Age Verification Providers Association and US COPPA Safe Harbor. PRIVO serves a specific subset of the CIAM market, and as such does not offer full CIAM features yet. We will continue to monitor and report on their progress.

Secfense – Secfense was founded in Krakow, Poland in 2018. They have MFA and authorization solutions for the B2C space. Their User Access Security Broker solution uses reverse-proxy deployment to front-end customer applications. The User Access Security Broker can work with passwordless 2FA and MFA options such as FIDO2, SMS OTP, RADIUS, facial and fingerprint biometrics, and hardware tokens. Secfense Microauthorizations are resource-driven authentication policies which can interoperate with 3rd-party IdPs

and attributes providers. Secfense Full Site Protection allows customers to extend authorization to resources within the full site or application, not only the login process. Most customers run the software on-premises, but SaaS hosting is available. KuppingerCole will track developments at Secfense as they expand their feature set.

Signicat – a leading regional IDP and e-signature service provider, was founded in 2006 in Norway. In 2019, they were acquired by Nordic Capital; Signicat acquired Connectis and IDFy in the last year. Signicat offers CIAM related services including secure authentication, identity verification, and e-signatures Their services are ISO 27001 and SSAE 18 SOC 2 Type 2 certified. Signicat supports a wide range of strong authentication methods, electronic signatures, and national IDs; therefore, the solution also has good identity verification services integration, which is critical for decreasing fraud and improving consumer experiences.

Strivacity - Strivacity was founded in 2019 as a CIAM specialist service provider. They are headquartered in Virginia. Strivacity Fusion follows the microservices and serverless trends in deployment architecture, which allows for optimum flexibility. Strivacity hosts their SaaS in public IaaS across global data centers. Strivacity Fusion received its SOC 2 Type 2 certification in August 2022. As a relatively young startup in CIAM, Strivacity is rapidly adding features and attempting to capture market share. Their Isolation-by-Design adds layers of data separation for security and privacy. Strivacity Fusion has a large number of identity proofing and fraud reduction intelligence connectors that can be advantageous for customers.

TrustBuilder – TrustBuilder started up in 2016 in Belgium. They are private equity owned and specializing in customer-centric IAM. TrustBuilder has other offices in Netherlands, Germany, the UK, and US. TrustBuilder.io Suite is composed of the eponymous product, TrustBuilder ID Hub, and TrustBuilder Mobile Authenticator. TrustBuilder is delivered as SaaS and runs in a public IaaS platform hosted in Belgium. The solution has connectors for EU IdPs such as Itsme, eHerkenning, and BankID; and identity and attribute providers including Experian, HID Global, ID.me, OneSpan, Signicat, Thales, etc. For authentication, they offer a mobile authenticator app and SDK. The company is adding functionality and we will continue to cover their development and expansion in other reports.

Ubisecure - Ubisecure was founded in 2002 in Finland. Ubisecure is a full-service CIAM and IDaaS provider with additional services. Ubisecure is ISO 27001 compliant. Their Identity Platform provides good basic CIAM functionality, is flexible in deployment, and is designed to facilitate customer compliance with EU regulations such as GDPR and PSD2. The company is actively adding functionality, so we expect to see more features for API integration and consumer IoT device identity integration.

7 Related Research

Leadership Compass CIAM Platforms (2020)
Leadership Compass CIAM Platforms (2018)
Leadership Compass Customer Data Platforms
Leadership Compass Identity Fabrics
Leadership Compass Fraud Reduction Intelligence Platforms
Buyer's Compass CIAM Solutions
Whitepaper Customer Authentication with Zero-Friction Passwordless Authentication
Whitepaper Serving the Customer in the Digital Age
Whitepaper Technical Approaches to Consent Management and Dynamic Access Management: Ping Identity
Executive View Beyond Identity Secure Customers
Executive View NRI Uni-ID Libra v. 2.6
Executive View OneWelcome Customer Identity and B2B Identity
Executive View WSO2 Asgardeo
Executive View cidaas
Executive View Strivacity Fusion
Executive View IBM Security Verify for CIAM
Executive View Synacor Cloud ID
Executive View Cloudentity Control Plane
Executive View Oxyliom Solutions GAiA Advanced Identity Management
Executive View Auth0 Platform
Executive View Curity Identity Server

Methodology

About KuppingerCole's Leadership Compass

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders:** Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders:** Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- **Security
- Functionality
- Deployment
- Interoperability
- Usability**

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position

- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

Strong positive
Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral

Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.

Weak
Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical
Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Declined to participate:** Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- **Lack of information supply:** Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will

provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Content of Figures

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 make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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