

KuppingerCole Report

LEADERSHIP COMPASS

By **John Tolbert**
November 20, 2020

CIAM Platforms

This report provides an overview of the market for Consumer Identity and Access Management and provides you with a compass to help you to find the Consumer Identity and Access Management product 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	4
1.1 Market Segment	5
1.2 Delivery models	7
1.3 Required and Optional Capabilities	7
2 Leadership	10
3 Correlated View	18
3.1 The Market/Product Matrix	18
3.2 The Product/Innovation Matrix	20
3.3 The Innovation/Market Matrix	22
4 Products and Vendors at a glance	25
4.1 Ratings at a glance	25
5 Product/service evaluation	28
5.1 1Kosmos	30
5.2 Akamai	33
5.3 Auth0	36
5.4 Cloudentity	39
5.5 CoffeeBean Technology	42
5.6 ForgeRock	45
5.7 IBM	48
5.8 iWelcome	51
5.9 LoginRadius	54
5.10 Microsoft	57
5.11 NRI Secure Technologies	60
5.12 Oxyliom Solutions	63
5.13 Ping Identity	66
5.14 Pirean	69
5.15 ReachFive	72
5.16 SAP	75

5.17 Synacor	79
5.18 Ubisecure	82
5.19 WSO2	85
6 Vendors and Market Segments to watch	88
6.1 Amazon Cognito	88
6.2 Avatier	88
6.3 AvocoSecure Trust Platform	89
6.4 cidaas	89
6.5 Fusion Auth	90
6.6 Genetsis Group Dru-ID	90
6.7 Google Firebase	90
6.8 Login Alliance Syntlogo Login Master	91
6.9 Miracl	91
6.10 Onegini	91
6.11 Privo ID	92
6.12 Signicat Digital Identity Platform	92
7 Related Research	94
Methodology	95
Content of Figures	101
Copyright	102

1 Introduction

Consumer Identity and Access Management (CIAM) is a parallel to traditional Identity and Access Management (IAM) that has become a substantial market of its own. CIAM solutions are designed to meet evolving technical requirements for businesses and other organizations that deal directly with consumers and citizens. Many businesses and public sector organizations are finding that they must provide better digital experiences for and gather more information about the consumers who are using their services. Enterprises want to collect, store, and analyze data on consumers in order to create additional sales opportunities and increase brand loyalty. Know Your Customer (KYC) initiatives, particularly in the financial sector, are another example of the business driver motivating exploration and adoption of CIAM.

CIAM has diverged from traditional IAM in supporting some baseline features for analyzing customer behavior, as well as collecting consent for user data usage, and integration into CRM, connected devices, and marketing automation systems.

CIAM at first glance seems very much like Customer Relationship Management (CRM) software. However, it differs from CRM in that, with CRM systems, sales and marketing professionals are counted upon to enter the data about the contacts, prospects, and track the sales cycle. The focus of CRM is managing all processes around the customer relationship, while CIAM focuses on the connectivity with the customer when accessing all customer-facing systems, from registration and throughout the relationship. With CIAM, similar kinds of information as in CRM systems can be collected, but the consumers themselves provide and maintain this information. In this sense, CIAM solutions are self-managed CRM systems for consumer-facing organizations, particularly in the retail, media, finance, and health care industries. CIAM solutions are also being used by governments for government-to-consumer (G2C) use cases.

Traditional IAM systems are designed to provision, authenticate, authorize, and store information about employee users. User accounts are defined; users are assigned to groups; users receive role or attribute information from an authoritative source. They are generally deployed in an inward-facing way to serve a single enterprise. Over the last decade, many enterprises have found it necessary to also store information about business partners, suppliers, and customers in their own enterprise IAM systems, as collaborative development and e-commerce needs have dictated. Many organizations have built extensive identity federations to allow users from other domains to get authenticated and authorized to external resources. Traditional IAM scales well in environments of hundreds of thousands of users.

Consumer IAM systems are designed to provision, authenticate, authorize, collect and store information about consumers from across many domains. Unlike regular IAM systems though, information about these consumers often arrives from many unauthoritative sources. Some solutions in this space provide connections to various identity proofing services to strengthen the veracity of the consumer attributes. CIAM systems generally feature weak password-based authentication, but also support social logins and other stronger authentication methods. Information collected about consumers can be used for many different

purposes, such as authorization to resources, or for analysis to support marketing campaigns, or Anti-Money Laundering (AML) initiatives. Moreover, CIAM systems must be able to manage many millions of identities, and process potentially billions of logins and other transactions per day.

In order to reduce money laundering, cyber-crime, terrorist financing, and fraud, regulators are requiring banks and financial service providers to put into place mechanisms for “Knowing Your Customer”. Government regulators expect banks to utilize analytics to develop baseline patterns for all their customers, and to be able to spot deviations from individuals’ normal parameters. Suspicious transactions must be flagged for investigation, specifically to prevent the aforementioned criminal activities. CIAM solutions have become a standard architectural component to help with financial KYC.

Support for self-registration and social network logins is ubiquitous among vendors; and the key differentiators have become the use of new technologies to:

- comply with privacy regulations
- step up the user’s authentication assurance level
- collect and analyze information for fraud prevention
- collect and analyze information for marketing purposes
- connect consumer identities to IoT device identities, e.g. Smart Home devices and apps

The entire market segment is still evolving and growing. We expect to see more entrants within the next few years. This year we are reviewing a number of new product and service entries in this report.

IT departments should welcome CIAM initiatives, as they provide an opportunity for IT, usually considered a “cost center”, to closely team with Marketing, a revenue producing center.

This KuppingerCole Leadership Compass provides an overview of the leading vendors in the CIAM market segment. Picking solutions always requires a thorough analysis of customer requirements and a comparison with product features. Leadership does not always mean that a product is the best fit for a customer and his requirements. However, this Leadership Compass will help identify those vendors that customers should look at more closely.

1.1 Market Segment

The CIAM market is still growing, 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). We often see support for national e-IDs, x.509 certificates, and higher assurance authentication mechanisms in these vendors' products compared to the rest.

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. CIAM vendors that are primarily pursuing retail and media companies as clients tend to not have the customer-driven pressure to support high assurance 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 requirements and capabilities of a country or small 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 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 has grown, 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-premise and cloud-based deployment.

Several noteworthy trends have appeared in the CIAM market, outlined below:

- Many vendors are taking an “API-first” approach to CIAM, which allows organizations with in-house expertise to extend their existing IAM infrastructure to accommodate consumer use cases better. The API-first approach also permits in-house developers to easily “bolt-on” CIAM features to existing or legacy Line of Business applications, without necessarily investing in a full-size CIAM solution. Identity API platforms are not always completely assembled products and services. Rather, these platforms are collections of tools, code, and templates. Identity API platforms may contain many open source elements, and generally leverage well-known standards. In some regards, these granular identity services allow customers to “build (or rent) their own IDaaS”. Deploying CIAM functionality using Identity APIs aligns with the notion of Identity Fabrics. KuppingerCole also has a Leadership Compass that focuses on Identity API platforms and an upcoming Leadership Compass on Identity Fabrics.
- Some startup CIAM vendors are now combining basic CIAM functionality with identity proofing to increase identity assurance and reduce the risk of fraud. Other larger or more established CIAM vendors are partnering with specialty identity proofing services for the same reason.

- Some of the larger vendors, particularly those with cloud-only delivery models, offer a wide range of services covering basic to advanced authentication methods, consent management, and integrated identity and marketing analytics/automation. They aim to provide their customers with most all the features needed not only for CIAM but also for CRM and managing marketing operations.

1.2 Delivery models

In the CIAM market, solutions are offered as SaaS, PaaS, and for on-premise deployment. Pure-play SaaS solutions are often multi-tenant by design. On the other side, Managed Service offerings are run independently per tenant. For SaaS offerings, the licensing 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-premise deployments, licensing costs can be measured in a couple of different ways, such as per-user, per-server.

1.3 Required and Optional Capabilities

Various technologies support all the different requirements customers are facing today. The requirements are

- Deployment options: On-premise, cloud, or hybrid options.
- Social logins: Allow users to login via Facebook, LinkedIn, Twitter, Google, Amazon, etc.
- Multi-factor authentication: Email/phone/SMS OTP, mobile biometrics, behavioral biometrics, mobile push apps, FIDO, risk-adaptive and continuous authentication, etc.
- Risk adaptive authentication: Evaluation of runtime environmental parameters, user behavioral analytics, and fraud/threat/compromised credential intelligence to match the appropriate authentication mechanism to the level of business risk or as required by regulations.
- 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 Knowledge-Based Authentication (KBA; but it is recommended to avoid this method as it is usually even less secure than password authentication), email/phone/SMS OTP, mobile push notifications, and account linking.

- Inclusion of 3rd-party fraud and compromised credential 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 transaction level.
- Identity analytics: Dashboards and reports on common identity attribute activities including failed logins, consumer profile changes, credential changes, registration tracking, etc.
- Business intelligence for marketing: Transformation of data about user activities into information for marketers.
- 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. Compliance with EU GDPR, Canada's PIPEDA, and California's CCPA are notable drivers.
- Enhanced user experience: White-labeled CIAM solutions allow seamless branding, and self-registration and social registration/logins increase successful consumer interaction with websites.
- IoT device identity information: 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 and private use of smart home, wearables, medical, and even industrial devices.

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.

- Support for standards such as Kantara Initiative Consent Receipt, FIDO Alliance, and Global Platform Secure Element and Trusted Execution Environment standards.
- Advanced cloud provisioning capabilities, such as Graph API and SCIM standard support.
- A comprehensive, secure, and well-documented set of REST-based APIs, Webhooks, and/or WebAuthn to allow access to data by 3rd-party identity, marketing, and security analytic tools.
- Advanced support for authentication mechanisms, especially FIDO, mobile, and behavioral biometrics and mobile SDKs.
- Interoperability with Fraud Reduction Intelligence Platforms (FRIP) and identity proofing services.
- Ability to utilize national e-IDs, bank IDs, and passports.
- Advanced support for IoT, SmartHome, connected cars, and wearables use cases.

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 be based only on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

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

- Product Leadership
- Innovation Leadership
- Market Leadership



Figure 1: The Overall Leadership rating for the CIAM market segment

ForgeRock, Ping Identity, SAP, and IBM appear at the top of the Overall Leader chart. Each of these vendors are well-established and have excellent reputations for CIAM. Akamai, Auth0, LoginRadius, and WSO2 are also in the Overall Leader field.

The top CIAM Challengers are Microsoft, iWelcome, Pirean, and Cloudentity. Cloudentity and iWelcome are CIAM focused startups, whereas Microsoft and Pirean also offer B2E IAM solutions. The second half of the

challenger field is composed of CoffeeBean, 1Kosmos, Oxyliom Solutions, Synacor, ReachFive, NRI, and Ubisecure. These challengers are mostly focused on segments of the CIAM market. Details of the specialties can be found in their chapter 5 entries below.

Overall Leaders are (in alphabetical order):

- Akamai
- Auth0
- ForgeRock
- IBM
- LoginRadius
- Ping Identity
- SAP
- WSO2

Product Leadership is the first specific category examined below. This view is based on the analysis of their product and/or service features.



Figure 2: Product Leaders in the CIAM market segment

Product (or Service) Leadership is where we examine the functional strength and completeness of products and services.

In this iteration of the report, we have a growing number of Product Leaders. ForgeRock, Ping Identity, IBM, iWelcome, Auth0, SAP, Akamai, LoginRadius, Pirean, Cloudentity, and WSO2 all have strong products which collectively meet the requirements of thousands of companies and billions of consumer identities. Though their approaches in delivering functionality may differ, all exceed the criteria we have set forth for measurement of CIAM.

Microsoft appears at the top of the Challenger section along with CoffeeBean, which are then followed by

1Kosmos, Microsoft, Oxylion Solutions, Synacor, ReachFive, NRI, and Ubisecure. The challengers in CIAM may be top contenders in customer RFPs, however, as they have specialized focus areas in which they excel.

Product Leaders (in alphabetical order):

- Akamai
- Auth0
- Cloudentity
- ForgeRock
- IBM
- iWelcome
- Login Radius
- Ping Identity
- Pirean
- SAP
- WSO2

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.

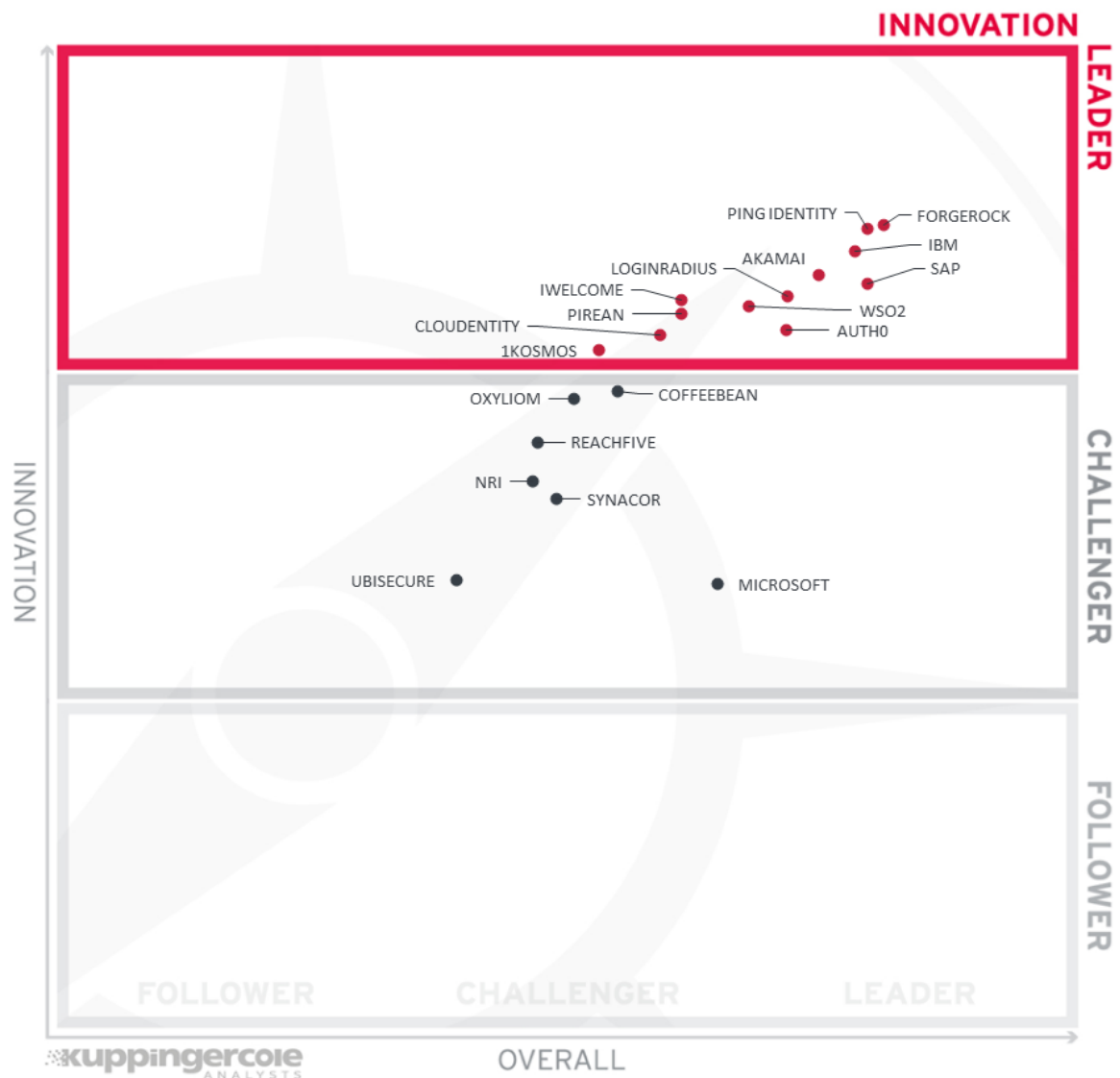


Figure 3: Innovation Leaders in the CIAM market segment

The Innovation Leaders are ForgeRock, Ping Identity, IBM, Akamai, SAP, LoginRadius, iWelcome, WSO2, Pirean, Auth0, Cloudentity, and 1Kosmos. The leaders are an interesting mix of IT heavyweights, venerable IAM/CIAM brands, and startups in various phases. Several of the leading solutions are cloud native, and the others are at different stages of embracing the cloud. This reflects the growing popularity of cloud-first strategies, especially for CIAM.

At the top half of the Challenger section in Innovation we see CoffeeBean, Oxyliom Solutions, ReachFive, NRI, and Synacor. Each of these companies has specific technical innovations leading to their positioning here. Microsoft and Ubisecure are in the second half of the Challenger area.

The leaders in innovation are indeed bringing much needed improvements to the CIAM space. Some vendors seem to be struggling to deliver on their roadmap items when compared to the previous edition of this report.

For a more detailed look at each vendor's innovations, please see their respective chapter 5 sections.

Innovation Leaders (in alphabetical order):

- 1Kosmos
- Akamai
- Auth0
- Cloudentity
- ForgeRock
- IBM
- iWelcome
- LoginRadius
- Ping Identity
- Pirean
- SAP
- WSO2

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of managed identities, 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.

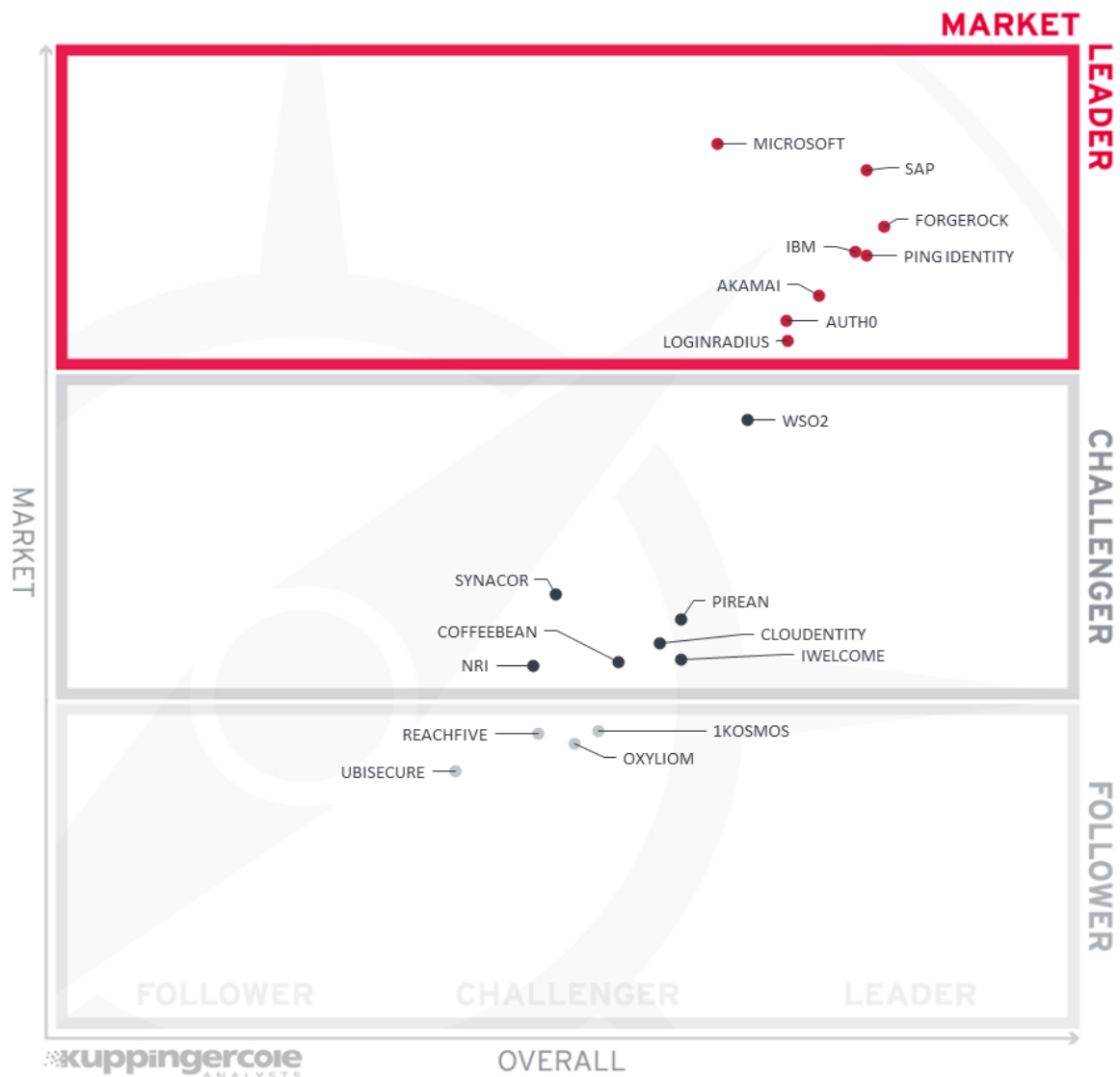


Figure 4: Market Leaders in the CIAM market segment

For CIAM, Market Leadership is determined by a number of factors, including number of reported customers, managed identities (which may include device identities for IoT), geographic distribution of customers and partners, as well as company financial strength and size of ecosystem.

The CIAM Market Leaders are Microsoft, SAP, ForgeRock, IBM, Ping Identity, Akamai, Auth0, and LoginRadius. Most of the market leaders are either large publicly traded IT vendors or are well-funded private IAM/CIAM focused companies.

WSO2 occupies the top challenger spot in the CIAM market. They have global reach, including not only North America, Europe, and Asia Pacific, but are also doing business in areas of the world where other

vendors are not active. Next up we see Synacor, Pirean, Cloudentity, iWelcome, CoffeeBean, and NRI. Most of these companies are regionally focused but may be in the process of expanding globally.

The Leadership Compass on CIAM is much larger this year, and most of the new entrants are Followers in the CIAM market. 1Kosmos, ReachFive, Oxyliom Solutions, and Ubisecure all debut at the top of the Follower area.

The CIAM market is still growing and there will be plenty of opportunities for the Challengers and Followers to gain market share.

Market Leaders (in alphabetical order):

- Akamai
- Auth0
- ForgeRock
- IBM
- LoginRadius
- Microsoft
- 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 improving, 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. 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.

3.1 The Market/Product Matrix

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

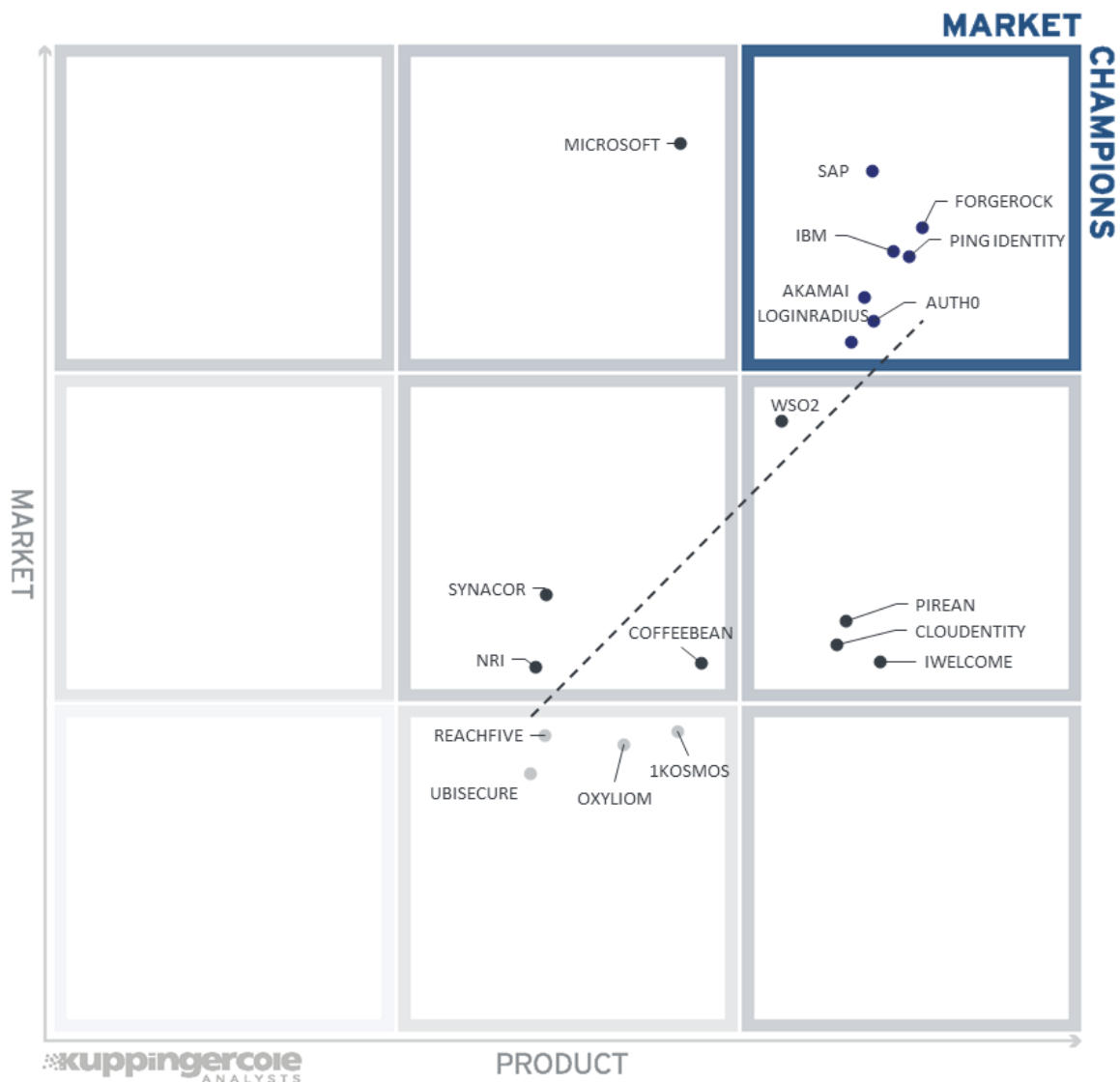


Figure 5: The Market/Product Matrix.

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.

The Market Champions in this version of the report are SAP, ForgeRock, IBM, Ping Identity, Akamai, Auth0, and LoginRadius. All appear above the line, indicating they are doing well in terms of both product strength and market position.

Microsoft appears in the top center box, with a commanding position in the market.

WSO2 is in the right center box above the line, showing room to grow and a good offering. Pirean,

Cloudentity, and iWelcome are also in the right center but below the line.

Synacor and NRI are above the divider in the center box, while CoffeeBean is under.

In the lower center we find the new entrants ReachFive, 1Kosmos, Oxyliom Solutions, and Ubisecure.

All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

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.

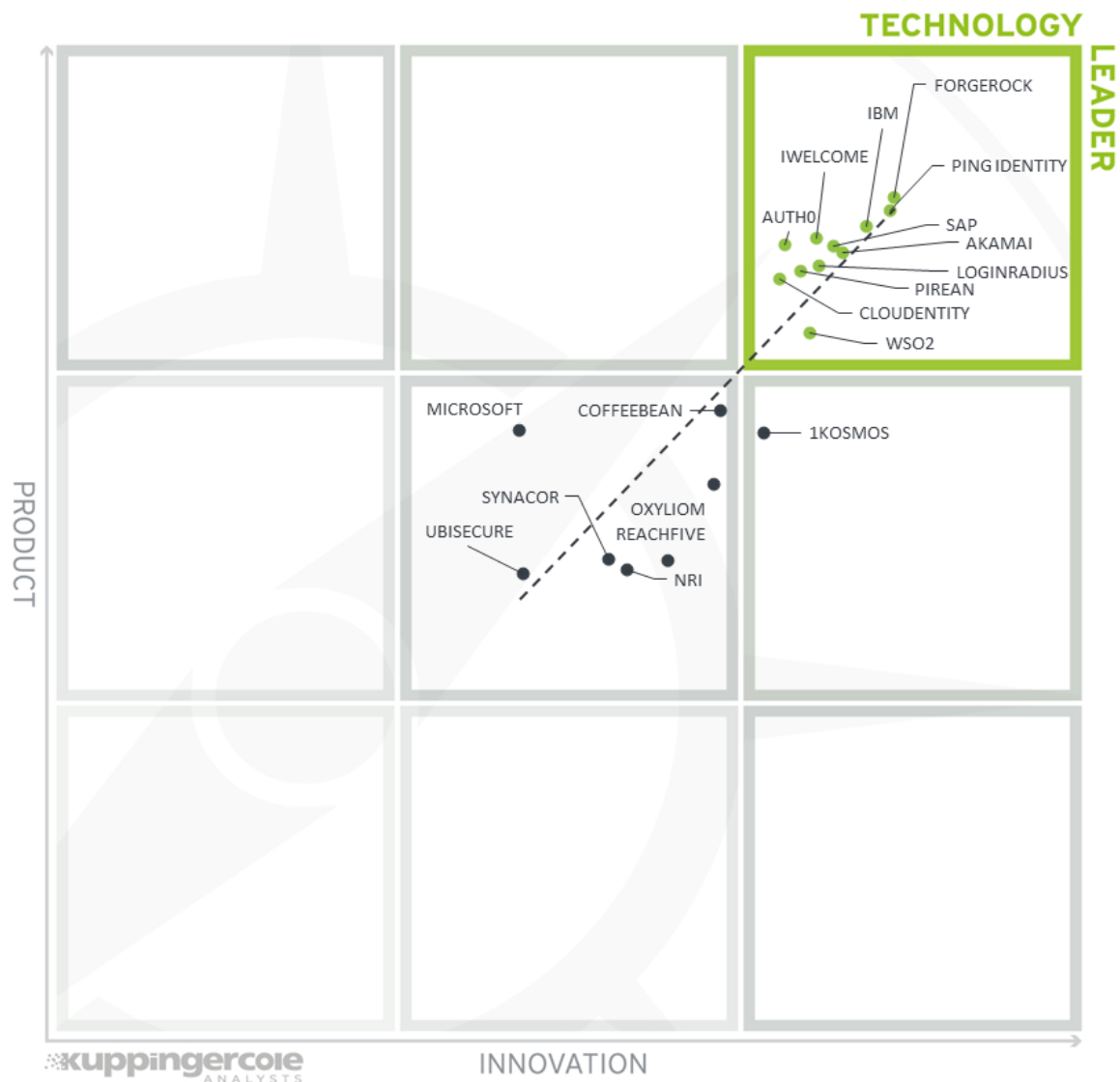


Figure 6: The Product/Innovation Matrix.

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

The Technology Leader box has a large clustering of companies: ForgeRock, Ping Identity, IBM, iWelcome, SAP, Auth0, Akamai, LoginRadius, Pirean, Cloudentity, and WSO2. Almost all are tightly constrained to the line and above it.

1Kosmos is in the right center section below the line.

In the center we find Microsoft and Ubisecure above the line, while CoffeeBean, Oxyliom Solutions, Synacor, ReachFive, and NRI are below the line.

All other squares are blank, indicating the alignment between product strength and constant innovation.

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.

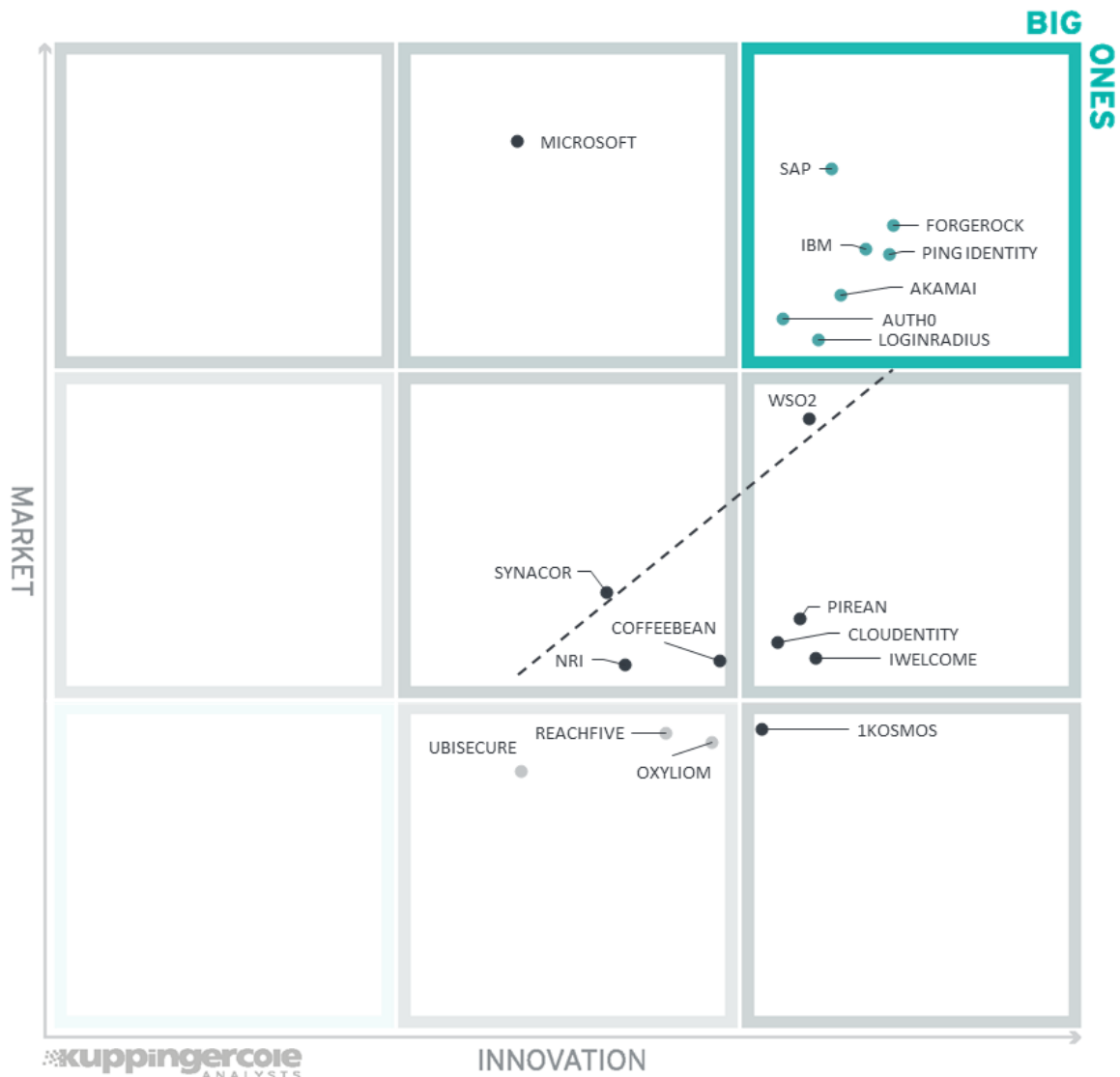


Figure 7: The Innovation/Market Matrix

In our final comparison chart, we identify the Big Ones in CIAM. In the top right, SAP, ForgeRock, IBM, Ping Identity, Akamai, Auth0, and LoginRadius can be seen. The distribution here confirms that the rate of innovation correlates well with market position.

Microsoft is in the top center with an overall lead in market share.

In the right center WSO2 is above the line, while Pirean, Cloudentity, and iWelcome are below. As strong innovators, we expect them to gain market position in the years ahead.

Synacor is in the center above the line, while CoffeeBean and NRI reside below the line. Each has special areas of focus, both technically and geographically that should allow them to expand.

The new entrants to this report are in the lower stratum: 1Kosmos on the right, while ReachFive, Oxylion Solutions, and Ubisecure are in the lower center block.

4 Products and Vendors at a glance

This section provides an overview of the various products/services we have analyzed within this KuppingerCole Leadership Compass on CIAM. This overview goes into detail on the various aspects we include in our ratings, such as security, overall functionality, etc. It provides a more granular perspective, beyond the Leadership ratings such as Product Leadership, and allows identifying in which areas vendors and their offerings score stronger or weaker. Details on the rating categories and scale are listed in chapter 7.2 to 7.4.

4.1 Ratings at a glance

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	Interoperability	Usability	Deployment
1Kosmos BlockID Customer and BlockID Verify	●	●	●	●	●
Akamai Identity Cloud	●	●	●	●	●
Auth0	●	●	●	●	●
CoffeeBean Technology for CIAM	●	●	●	●	●
ForgeRock Identity Platform	●	●	●	●	●
IBM Security Verify	●	●	●	●	●
iWelcome CIAM	●	●	●	●	●
LoginRadius CIAM Platform	●	●	●	●	●
Microsoft Azure Active Directory External Identities	●	●	●	●	●
NRI Secure Uni-ID Libra	●	●	●	●	●
Oxyliom Solutions GAiA Trust Platform	●	●	●	●	●
Ping Intelligent Identity Platform	●	●	●	●	●
Pirean Access: One	●	●	●	●	●
ReachFive	●	●	●	●	●
SAP Customer Data Cloud	●	●	●	●	●
Synacor Cloud ID	●	●	●	●	●
Ubisecure Identity Platform	●	●	●	●	●
WSO2 Identity Server	●	●	●	●	●
Legend	● critical ● weak ● neutral ● positive ● strong positive				

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	●	●	●	●
Akamai	●	●	●	●
Auth0	●	●	●	●
Cloudentity	●	●	●	●
CoffeeBean Technology	●	●	●	●
ForgeRock	●	●	●	●
IBM	●	●	●	●
iWelcome	●	●	●	●
LoginRadius	●	●	●	●
Microsoft	●	●	●	●
NRI Secure Technologies	●	●	●	●
Oxylion Solutions	●	●	●	●
Ping Identity	●	●	●	●
Pirean	●	●	●	●
ReachFive	●	●	●	●
SAP	●	●	●	●
Synacor	●	●	●	●
Ubisecure	●	●	●	●
WSO2	●	●	●	●
Legend	● critical	● weak	● neutral	● positive
			● positive	● strong positive

5 Product/service 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 this LC CIAM Platforms, we look at the following seven categories:

- **Authentication options**
Support for risk-adaptive MFA and mobile SDKs.
- **Consent management**
Facilities within the UI to allow consumers to unambiguously opt-in/out of services and 3rd-party usage of their data. Often constructed as consumer privacy dashboard. Ability to view, export, and delete consumer profiles as requested. Family management.
- **IoT integration**
Extensions to the CIAM platform to allow consumers to register, activate, and monitor usage of home automation and wearable IoT devices 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. This measure describes capabilities within the CIAM solution, as contrasted with information made available over APIs for 3rd-party applications to process.
- **APIs**
APIs for sharing information and even controls are nearly ubiquitous in CIAM solutions. APIs provide the means for 3rd-party applications to perform marketing analytics, security integration, provisioning/de-provisioning, consent auditing, and more. Measures support for REST APIs, Webhooks, Websockets, WebAuthn; JSON and XML formats; and LDAP and SCIM for provisioning.
- **Account Recovery**
This metric shows how flexible the solution in terms of number and type of account recovery mechanisms available. The most common options are email/phone/SMS OTP, mobile push notifications, account linking, etc.

- ATO Protection

Account Take Over (ATO) protection is increasingly an important feature that CIAM solutions offer. Many CIAM solutions incorporate various forms of intelligence to help reduce the risk that their customers and their customers' consumers face from fraud. These sources may cover compromised credential intelligence, device intelligence, user behavioral analysis, and other fraud risk signals. Some CIAM solutions leverage the collective intelligence across all their internal customer base. Some CIAM services subscribe to 3rd-party sources and make it available to their customers as part of their standard offering. Other CIAM solutions allow individual customers to connect to various fraud reduction intelligence feeds and configure risk mitigation policies and techniques themselves. Some of the solution providers in this space offer integration with various state and national government ID issuers for higher identity assurance. Others have sophisticated mobile apps that allow selfie to verified document matching as a precursor for registration. This metric represents the availability of various types of intelligence and identity vetting capabilities within each solution that may serve to promote a safer consumer experience.

Each of the categories above will be considered in the product evaluations below. The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some vendor services may have gaps in certain areas, while are strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations of CIAM technologies.

5.1 1Kosmos

1Kosmos was founded in 2018 and is headquartered in New Jersey. The company is small but self-funded and profitable. They address the consumer and workforce identity management markets with blockchain ID solutions. BlockID Customer is their CIAM offering, and BlockID Verify handles identity vetting and KYC. Beyond providing consumer authentication, 1Kosmos is a decentralized identity (DID) and distributed identity attribute aggregator. 1Kosmos' solutions are hosted as SaaS in AWS and GCP, distributed across APAC, EU, and NA regions. It is multi-tenant, and customers can create sub-tenants under their control. Licensing models include monthly active users, registered users, and per-session or per-login options.

BlockID Customer works with Android and iOS biometrics, email/phone/SMS OTP, FIDO UAF/U2F/2.0, mobile apps and push notifications, OneSpan and SafeNet Authenticators, and social logins. BlockID's Live ID authenticator is a mobile biometric mechanism with built-in liveness detection designed to meet requirements of eIDAS and US NIST 800-63-3 AAL3. Customer admins can also use OneSpan DigiPass or RSA SecurID for authentication to the console. 1Kosmos supports JWT, OAuth, OIDC, and SAML. They offer an SDK which can collect a range of device intel attributes and can use GP SE/TEE for Android. Customers can use the SDK to build their own apps. BlockID Verify can assist with identity vetting by comparing selfies to consumers' government issued ID docs, designed with regard to eIDAS and US NIST 800-63-3 IAL3. Mobile account recovery mechanisms are emphasized, and KBA is not supported, which is a plus. Self-registration and provisioning over LDAP, SCIM, and cloud APIs are possible.

1Kosmos currently provides some identity analytics reports to customers, and more reporting options are in work. Limited internal data can be made available to 3rd-party apps for marketing analytics. JSON, REST API, SOAP, WebAuthn, Websockets, and XML formats and protocols are supported for interoperability. Webhooks are on the roadmap. Connectors are available for Informatica, Oracle BI Publisher, SAP, and Tableau.

BlockID allows customers to view, granularly select attributes, and edit profile information in the mobile app (no web portal). Each user can create multiple personas, which can be deleted within the app. Kantara Consent Receipt is not supported. Family management is not currently possible but is on the roadmap. Consumer IoT device identity integration is possible though largely unexplored. There are no specific facilities within the app for managing device identities.

As a relatively new cloud-based startup, 1Kosmos has a lot of interesting features. BlockID Verify adds innovative mobile app-based identity verification to the solution, for increased identity assurance levels. However, they have not yet gotten CSA Star, ISO 27001, or SASE18 SOC 2 audits or certification. These are reported to be in work, along with US FedRAMP and FISMA. Moreover, their scalability has yet to be tested. 1Kosmos is pushing CIAM frontiers and is suitable for organizations that need these kinds of features, and that are comfortable with early stage startups.

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



Strengths

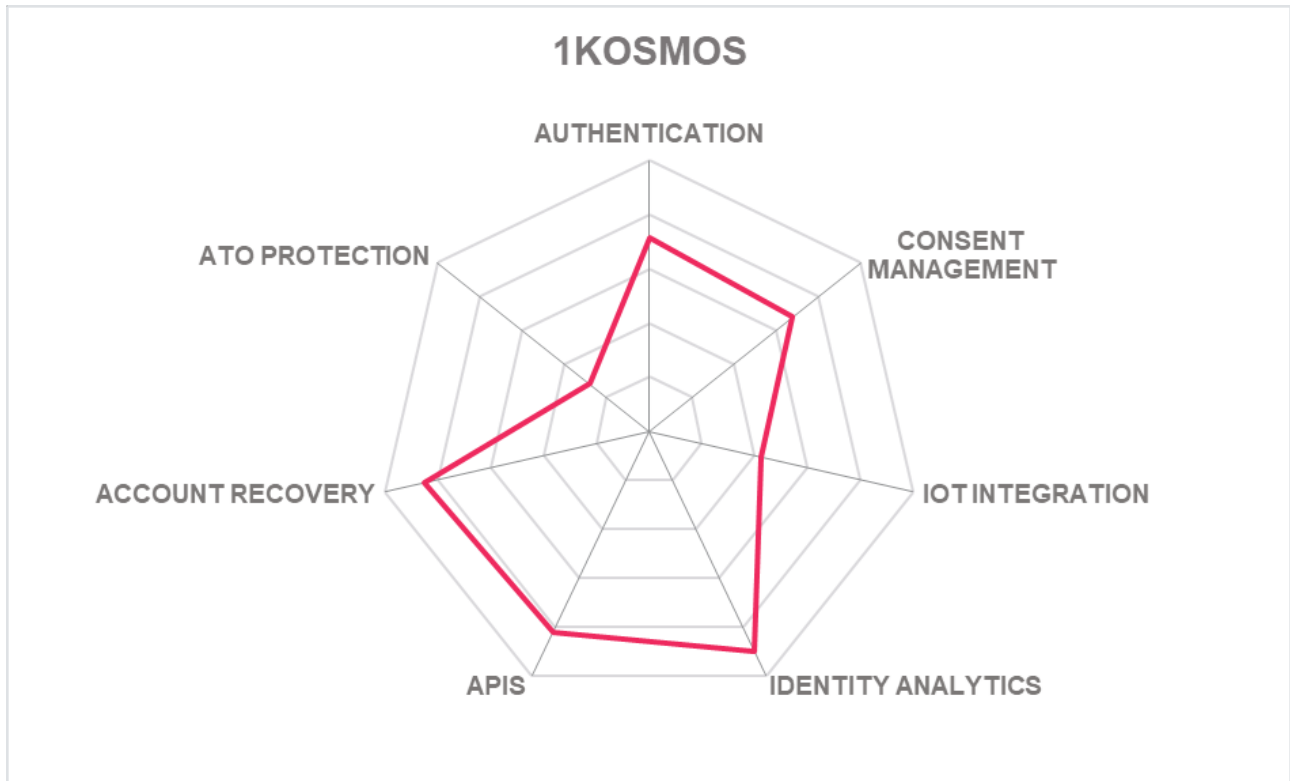
- Secure mobile SDK
- Mobile biometric authenticators
- Mobile app for consent management
- FIDO 2.0 certified server
- Block ID Verify allows for identity verification at enrollment and KYC

Challenges

- Small vendor with regionalized customer and partner base
- No family management or consent receipt
- IoT device management not a focus
- No integration with 3rd party device or compromised credential intelligence

Leader in





5.2 Akamai

Janrain was launched in 2002 to provide user management and login capabilities for the social media market. Akamai acquired Janrain in early 2019. Akamai has integrated Identity Cloud into its suite of enterprise solutions and extended the reach considerably. Akamai's Edge security services, such as Kona Site Defender, Site Shield, and Bot Manager can make the Akamai solution a compelling choice for consumer-facing businesses. Akamai Identity Cloud is offered as a highly scalable multi-tenant SaaS which hosts consumers' profile data. Licensing options include monthly active users, login/session, and registered users.

Akamai accepts any OIDC-based social logins and the following authenticators and federation standards: Android/iOS biometrics, OAuth, SAML, and SMS OTP authentication. Customers can use their mobile SDK, which can collect basic device intel, to embed authentication into apps. Many forms of MFA are supported for customer admins. Fraud and compromised credential intelligence are not built-in but can be configured by customers as desired. Identity Cloud includes a bundled Akamai API Gateway entitlement which allows for tokens issued by Identity Cloud to be used as part of application and API protection. Akamai supports LDAP, SCIM, and other SaaS APIs for bulk import.

Identity and marketing analytics are Akamai's forte. A full range of identity analytics reports are available. Marketing analytics capabilities are robust, in that, not only are all stored attributes available for reporting, but also event-derived intelligence as well. Akamai also permits REST API access and Webhooks v3 to integrate with a wide range of 3rd-party marketing analysis tools as well. Moreover, Akamai has partnered with SnapLogic, which has 500+ pre-built connectors for various data sources.

Consumers can edit, export, or delete their information at any time in accordance with GDPR. Akamai Identity Cloud can help customers comply with CCPA. Akamai provides the capabilities for their tenants to automatically notify users and have them re-consent after privacy policies change. Family relationships can be defined to allow parents to govern the access rights of children. Consumer IoT device identities can be managed and integrated with their CIAM solution via OAuth2 Device Flow.

Akamai's services are CSA Star Level 2, SOC 2 Type 2, ISO 27001, ISO 27018, and HIPAA attested and/or certified. Akamai supports most of the relevant standards to promote interoperability. Akamai has a highly scalable solution and should be seriously considered by organizations that need HA, GDPR compliant consent management, CCPA compliance, and comprehensive marketing analytics features.

Security
Functionality
Interoperability
Usability
Deployment



Strengths

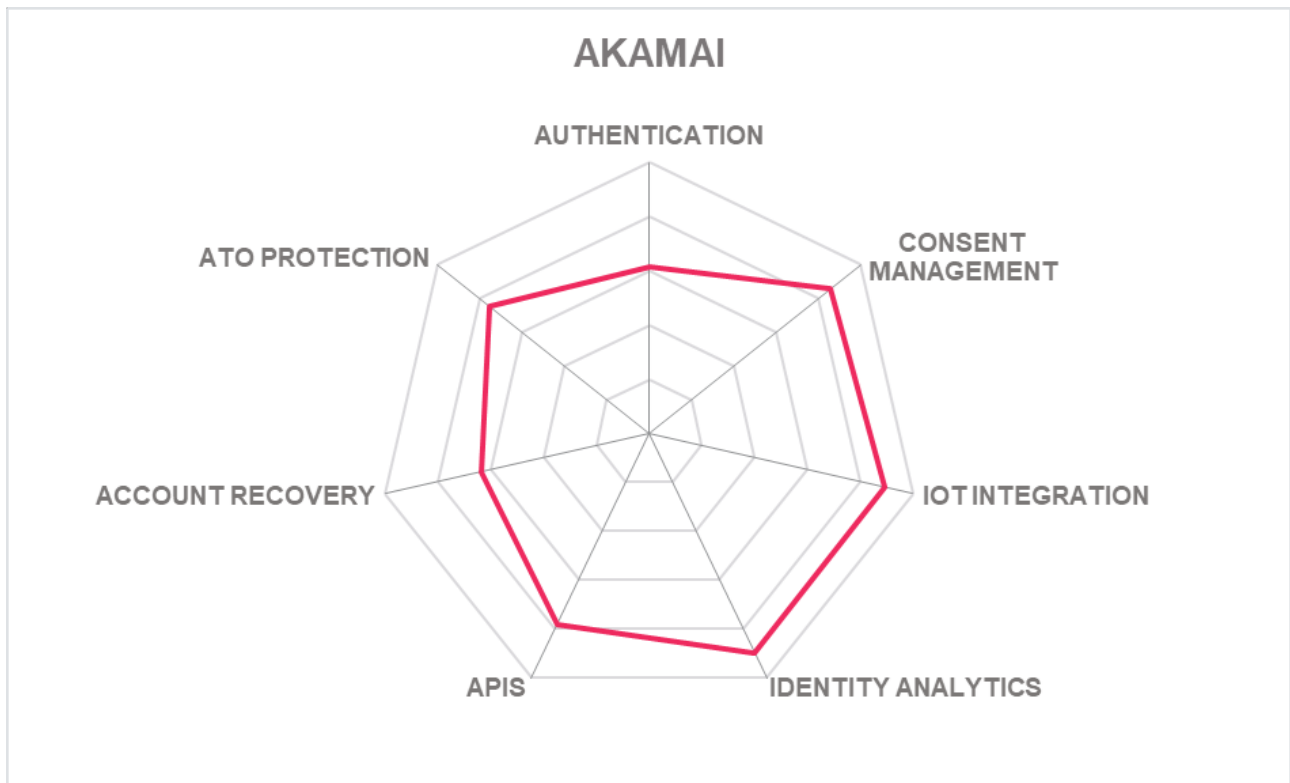
- Highly scalable cloud native service
- Facilitates CCPA and GDPR compliance
- Comprehensive identity and marketing analytics reports
- IoT device identity management
- Can be paired with other Akamai Edge Security solutions

Challenges

- FIDO not supported
- Risk-adaptive authentication features in limited availability for general release later
- Compromised credential intelligence is not built-in but configurable

Leader in





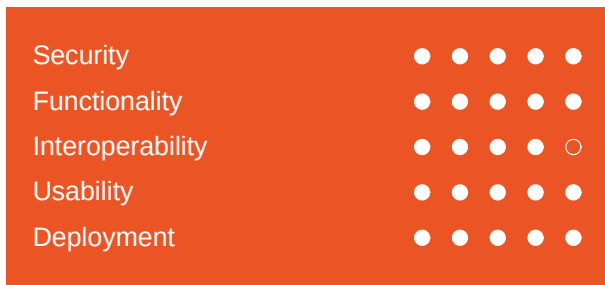
5.3 Auth0

Bellevue, WA based Auth0 is a rapidly growing CIAM and B2B/B2E IAM solution provider. Founded in 2013, they pioneered API-driven identity services. Auth0 targets enterprises and provides code samples for developers to use in order to quickly build CIAM solutions, or to connect identity services to existing customer/consumer-facing applications. Auth0's services are hosted in AWS, and private AWS options are available. Auth0 licensing is based on active users per month/quarter.

Auth0 accepts any OIDC-based social logins and the following authenticators: email/phone/SMS OTP, Aegis/Authy/DeepNet/Duo/Google/LastPass/Microsoft/Okta/OneSpan/SaaS Pass/SafeNet Authenticators, FIDO U2F, mobile app and push notifications. FIDO 2.0 support is planned for later in 2020. Customers can use their mobile SDK to embed authentication into their apps, though device intelligence is largely missing. Auth0 supports JWT, OAuth, OIDC, and SAML federation. Auth0 uses its internal compromised credential intelligence, including brute force and breached password detection. Auth0 supports LDAP and SCIM for bulk import. All standard account recovery mechanisms are present. Auth0 offers pre-built identity analytics reports only. Auth0 permits REST API access, Webhooks, and Websockets to integrate with 3rd-party marketing analytics and automation packages such as Adobe Campaign, Alterian, Constant Contact, Google Analytics, Hubspot, MailChimp, Marketo, Microsoft Dynamics CRM, Oracle CX, Sailthru, Salesforce, Watson Campaign, or ZenDesk. Customer admins configure such data pushes in the Auth0 rules engine and choose connectors in the newly launched Auth0 Marketplace.

Consumers can edit, correct, export, and delete their information in accordance with GDPR. Consents and delegation records are stored within the consumer profiles. Auth0 supports Kantara Consent Receipt. Auth0 does not provide the capabilities for their tenants to automatically notify users and have them re-consent after privacy policies change. Family relationships can be defined as a form of delegated administration to allow parents/guardians to govern which content is available to children. Consumer IoT device identities can be managed within the platform: Auth0 supports a variety of use cases including smart home and speaker automation as well as connected cars, although no separate device identity management console is present. Auth0 supports OAuth2 Device Flow.

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. Auth0 has excellent support for a broad range of authentication types. Auth0 delivers extreme scalability for customers, both for public and private deployment options. Given Auth0's focus on facilitating DIY CIAM solutions and adding modern IAM capabilities to web-facing apps, Auth0 should be on the RFP list for any organization with in-house development expertise that is looking for CIAM quick wins.



Auth0

Strengths

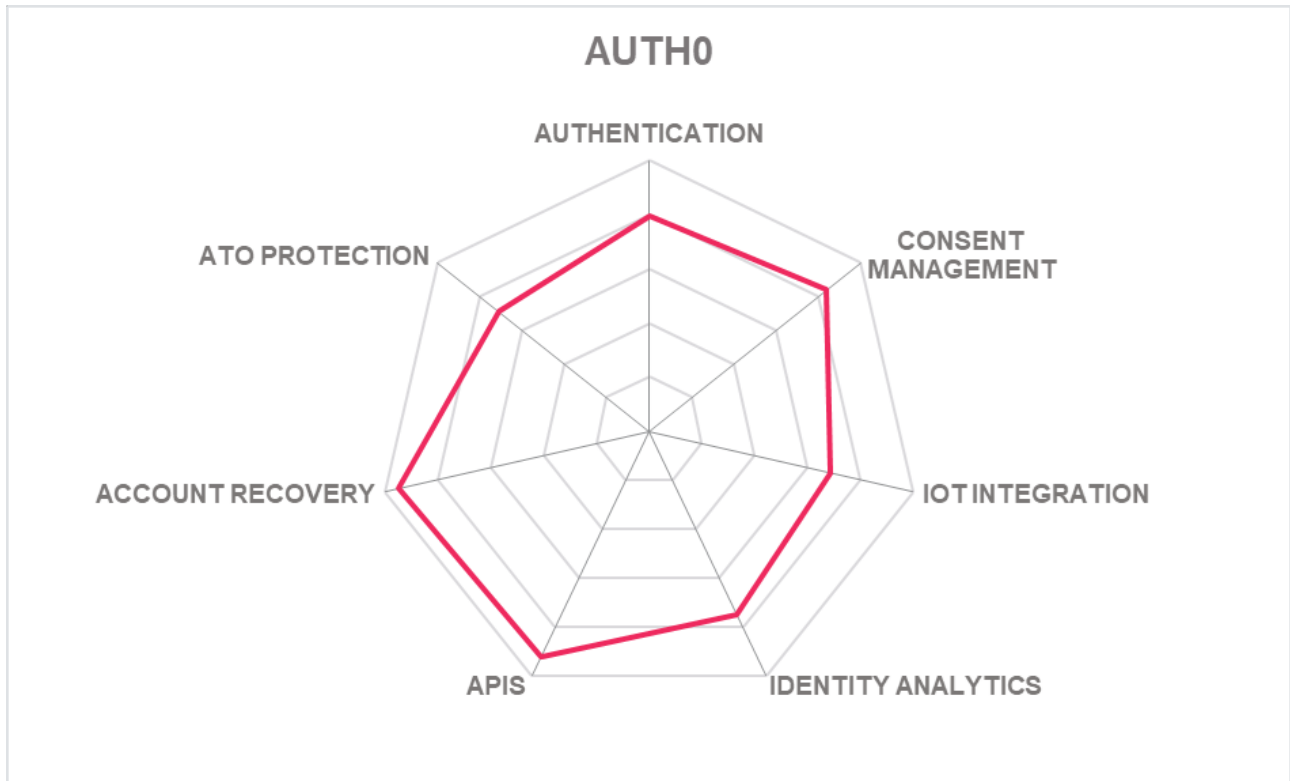
- Highly scalable cloud native service
- API focused, developer-driven solution
- Facilitates adding modern CIAM capabilities to consumer-facing apps
- Many authentication options

Challenges

- Multi-cloud support not yet present
- FIDO 2.0 support planned for near term
- Device intel should be collected by SDK and used for risk-adaptive scenarios

Leader in





5.4 Cloudentity

Cloudentity was founded in 2017 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, Istio, and Pivotal, to deliver their services. Their solution can run on-premise on CentOS, RHEL, SUSE, or Ubuntu; or in Alibaba, AWS, Azure, or GCP. They also offer their solution as SaaS. Cloudentity has licensing options based on the number of monthly active users or micro-services used.

For authentication and federation, Cloudentity supports Android fingerprint biometrics, email/SMS OTP; Authy/Duo/Google/Okta Authenticators; mobile apps and push notifications; JWT claims, OIDC and social logins, OAuth, and SAML. Cloudentity provides a developer portal for APIs and an SDK for secure mobile app development, which can collect device intelligence signals. Cloudentity is addressing more complex consumer authorization use cases with dynamic scopes in OAuth, PKCE, and Kantara Consent Receipts. A wide range of account recovery options are available. Cloudentity has a risk adaptive micro-service that provides comprehensive policy management ranging from micro-segmentation to API security. It can process external intelligence from Cylance, CrowdStrike, Exabeam, Imperva, RSA, Signal Science, and SecureWorks. LDAP and SCIM interfaces can be used for provisioning as well as social logins and self-service. The product integrates with security tools and other 3rd-party applications via REST APIs, RPC, SOAP, Webhooks, and Websockets.

Cloudentity provides reports with separate views for business, security, and B2B2C management in customer dashboards. For marketing analytics, customers can push information into 3rd-party marketing solutions. They have connectors for Elasticsearch, Salesforce, WorkDay, and various IDPs.

Common consent management options are available for GDPR, OpenBanking, and CCPA, including granular selection of attributes, profile editing, export/deletion of consumer data upon request. Customers can offer consumers privacy checkup dashboards. Family management and granting permissions align with US COPPA. Consumer IoT device identity management is possible using OAuth2 Device Flow.

Cloudentity is an API-driven CIAM and IDaaS provider. Cloudentity's cutting-edge micro-services architecture allows surge scalability across hybrid environments, and SecDevOps for secure CIAM. Their customer base and support ecosystem are small but growing. Organizations that have a need to deploy and manage rapidly evolving consumer-facing infrastructures, or those that need controllable scalability should consider Cloudentity when shopping for CIAM solutions.

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

CLOUDENTITY™
CUSTOMER IDENTITY AT CLOUD SPEED

Strengths

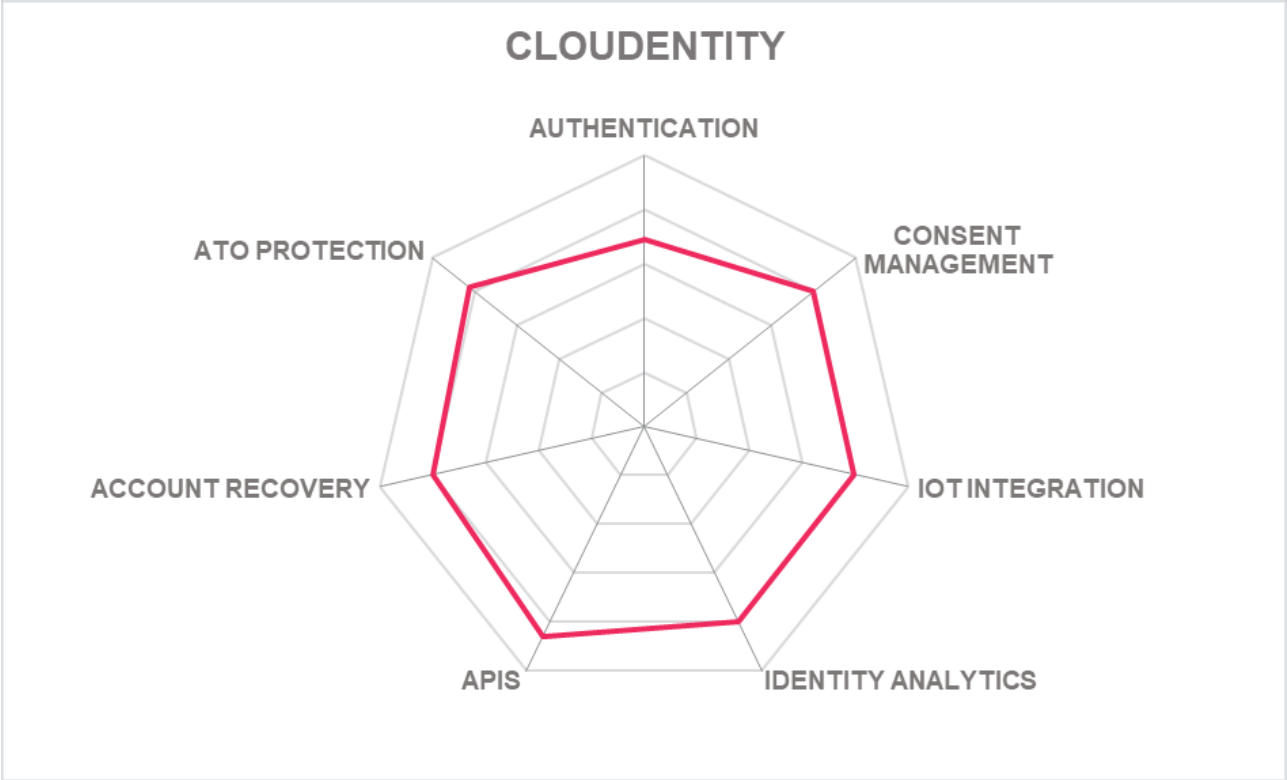
- Excellent support for modern standards
- Capable of handling complex authorization use cases
- FAPI certified, Open Banking ready
- Microservices architecture for high scalability
- Evaluation of multiple sources of external intelligence
-

Challenges

- Smaller but growing vendor
- No cloud security certifications yet but working on SSAE SOC 2
- Additional FIDO support planned

Leader in





5.5 CoffeeBean Technology

CoffeeBean Technology was founded in 2008 in the Bay area of California. They focus on increasing ROI via marketing integrations and improving consumer identity security for customers. They began developing their consumer identity and marketing solution in 2010. They are privately held but have operations in Germany and a large development center in Brazil. CoffeeBean has a number of IT partners in various locations, but mostly in Brazil, for system integration and support for digital marketing. Licensing is per registered monthly user. CoffeeBean hosts their solution as a SaaS in AWS for customers and provides on-premise and self-hosted IaaS options (CentOS or RHEL, AWS or Azure) for those that prefer that model.

CoffeeBean accepts the following forms of authentication: Android and iOS native biometrics, email/phone/SMS OTP, Google and Microsoft Authenticators, and FIDO UAF/U2F/2.0. It also supports tokens including JWT, OAuth2, OIDC, and SAML. They have a mobile app SDK that captures basic device intel for customer development. In addition to email/phone/SMS OTP and KBA, CoffeeBean can use WhatsApp for account recovery. Compromised credential checks via haveibeenpwned are included in the base service, and the processing of fraud risk intelligence services such as Aware behavioral biometrics, IDWall, and Kaspersky Fraud Prevention can be tailored by CoffeeBean for clients. Self- and social network registration is supported, as are LDAP and SCIM for bulk provisioning.

CoffeeBean has engagement plug-ins for mobile apps and Wi-Fi captive portal features that can be used by retailers to interact with consumers in real-time, both when they are shopping online or are in tenant facilities. CoffeeBean can be configured by tenants to allow viewing, editing, exporting, and deleting of personal information for privacy regulation compliance. CoffeeBean also works with 3rd-party marketing tools via REST APIs, Elasticsearch/Kibana, and IBM UBX and Salesforce connectors.

Consumers can choose what to share with customers, as well as view and edit their profile data via a self-service portal. CoffeeBean provides customers with the means to honor consumer data deletion requests, but each customer must decide to implement it. Thus, the ability to comply with regulations such as CCPA and GDPR is built-in, and CoffeeBean helps tenants customize their implementations as needed. CoffeeBean supports Kantara Consent Receipt. Family management and consumer IoT device identity schemes are not supported.

CoffeeBean has been focused on retail, hospitality, and finance industries, bringing social media content to consumer profiles, and developing apps to more actively engage the consumer. These advantages in marketing come at the expense of additional work to make it compliant with privacy regulations. CoffeeBean has made many enhancements to their offering since the last edition of this report: adding FIDO support, the ability to consume fraud and threat intel, and numerous security improvements. They are strong in the South American market and are adding customers in North America and Europe. 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	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ○ ○
Deployment	● ● ● ○ ○

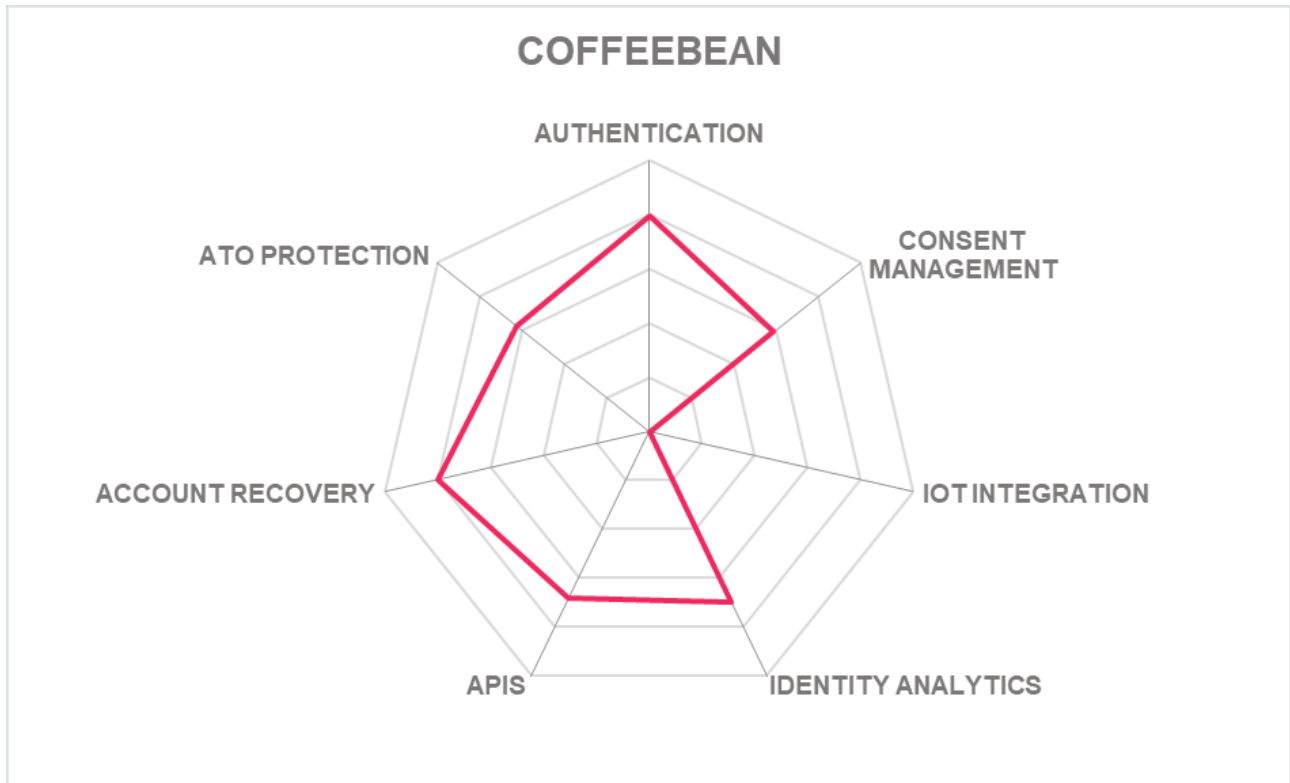


Strengths

- Good selection of authentication mechanisms
- FIDO support
- Unique consumer engagement models well-suited for retail and hospitality industries
- Strong CIAM offering in LatAm

Challenges

- Smaller but growing vendor
- No family management or IoT device identity integration
- Additional efforts needed by customers for CCPA and GDPR compliance



5.6 ForgeRock

ForgeRock is a leading venture-backed IAM vendor, headquartered in the US but with many offices around the world. ForgeRock supports most major IAM standards and is a significant contributor to several international standards organizations. Their Identity Platform serves both B2E and B2C markets. It is part of a full suite of IAM products including Access Management, Directory Services, Identity Management, IoT/Edge Security, Identity Gateway, Identity Governance, and Privacy & Consent Management. ForgeRock Identity Platform runs on-premise on most Linux variants, in any IaaS environment, in hybrid environments, or as SaaS in AWS, Azure, and GCP in the 20 regions. Licensing is quarterly/annually enrolled or registered users.

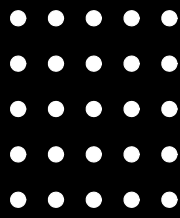
ForgeRock sports an impressive list of authenticators: Android/iOS biometrics, email/phone/SMS OTP, Authy/DeepNet/Duo/Entrust/Google/LastPass/Microsoft/OneSpan/SaaS Pass/SafeNet Authenticators, FIDO UAF/U2F/2.0, mobile app and push notifications, and social logins. Integrations with Daon, Entrust Datacard, HYPR, Nok Nok Labs, OneSpan, Trusona, and Veridium allow more MFA options. ForgeRock has a secure mobile SDK that uses Global Platform SE & TEE for Android and Secure Enclave for iOS. It can collect and evaluate key attributes for device intel. ForgeRock Identity Platform works with Id.Me, Jumio, ID Dataweb, OnFido, Socure, Thales for identity proofing; Behaviosec, BioCatch, Exabeam, Iovation/TransUnion, Kount, Microsoft, and ThreatMetrix/LexisNexis for fraud, risk, and threat intelligence sources. All account recovery methods are available. JWT, OAuth, OIDC, and SAML are supported. Flexible provisioning includes self-registration, LDAP, and SCIM.

Customers can pull and analyze all relevant identity analytics data from Identity Platform. BI and marketing analytics connectors are available for Adobe, Google, HubSpot, Marketo, Salesforce, and SAP. ForgeRock supports the widest range of API types and data formats, including OData, REST, RPC, SOAP, WebAuthn, Webhooks, and Websockets, in CSV/JSON/XML. These options provide full programmatic control over any or all of ForgeRock's products.

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. ForgeRock supports advanced consumer IoT use cases with a special Thing SDK, registration API, authentication nodes, and more. ForgeRock Identity Platform can address many categories of IoT devices, including set top boxes, connected cars, smart speakers, medical devices, and wearables.

ForgeRock is certified and/or attested with CSA Star Level 1, ISO 27001, and OpenID. ForgeRock Identity Platform allows customers to implement high, medium, and low security models as needed. The ability to add in identity proofing and fraud and threat intelligence is a plus for advanced CIAM use cases, as is the depth of support for consumer IoT device identity. ForgeRock's SaaS presence is smaller than some, but we expect it to ramp up quickly, thereby providing the same flexibility for customers who may not have the in-house resources to run the on-premise, hybrid, or IaaS versions. ForgeRock Identity Platform is well-suited to tackle most any set of CIAM requirements and should be near the top of RFP shortlists.

Security
Functionality
Interoperability
Usability
Deployment



FORGEROCK®

Strengths

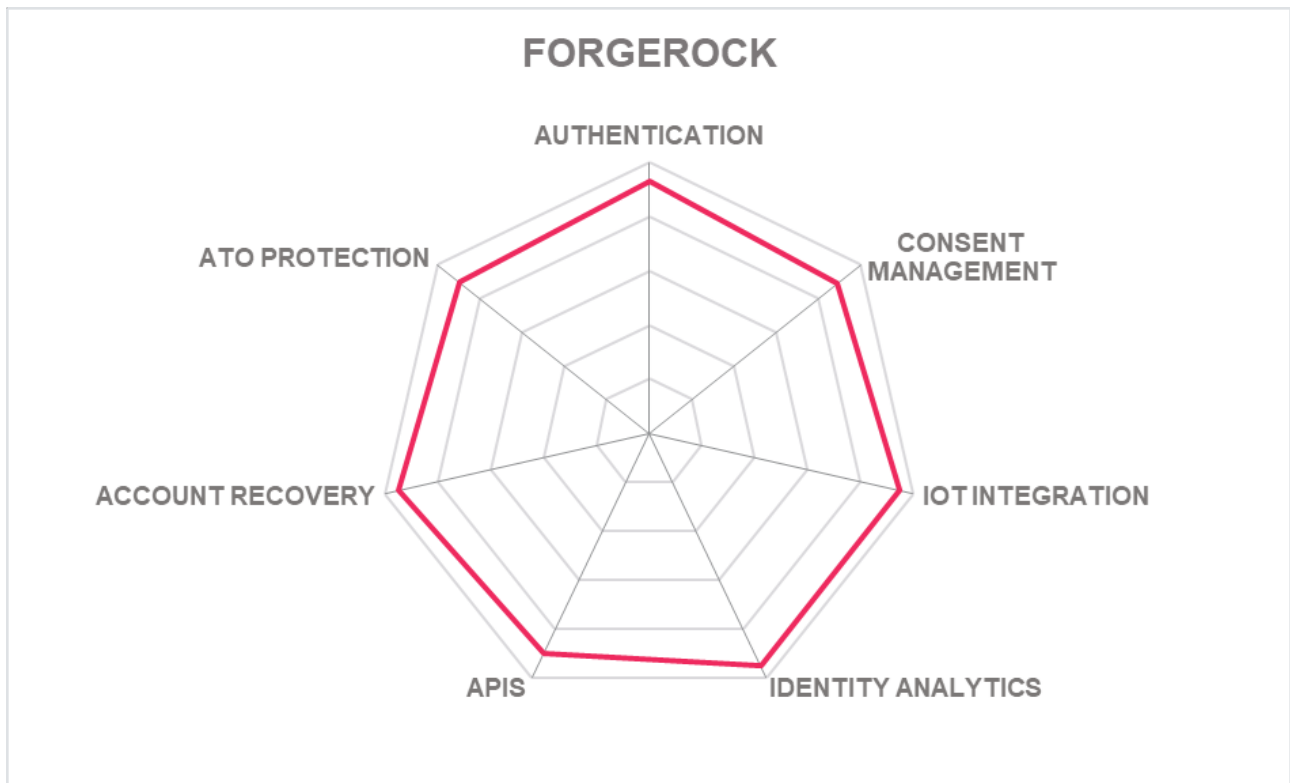
- Vast list of authentication mechanisms
- Leading contributor to IAM standards
- Easy-to-use GUI-driven flow-chart style policy authoring tools
- Many connectors for ID proofing and compromised credential intelligence
- Support for advanced IoT device <-> consumer identity use cases
- Highly extensible and scalable platform enables it to perform well in almost every CIAM scenario

Challenges

- Latecomer to SaaS deployment model; smaller footprint compared to cloud-native vendors
- Very flexible but requires more expertise to implement and manage on-prem and IaaS instances
- 3rd-party tools needed for identity and marketing analytics

Leader in





5.7 IBM

IBM has renamed and branded their CIAM and IDaaS solution to Security Verify from Cloud Identity. It can be used for B2B and B2C use cases. The SaaS version is fully multi-tenant and highly scalable; it is also offered as on-premise, running on most Linux types, and can be installed in IaaS. IBM hosts customer profile data for clients as well. The solution is based on a micro-services architecture. Licensing models include monthly/quarterly/annual active or recognized users as well as per-session and per-node options. With customers and partners across the globe, IBM is a major player in the market.

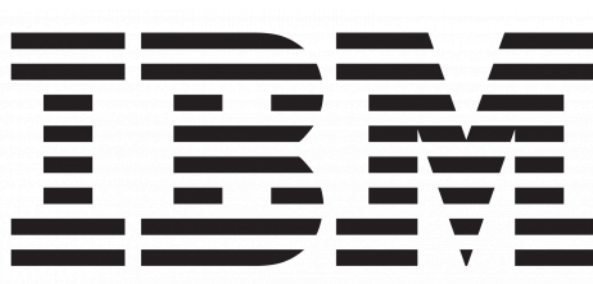
Security Verify accepts a wide array of authenticators, including FIDO U2F and 2.0, Aegis/Authy/Duo/Google/LastPass/Microsoft/Okta/SaaS Pass apps, mobile biometrics, email/phone/SMS OTP, social logins, and 3rd-party mechanisms via IBM Security App Exchange. It supports JWT, OIDC, OAuth, SAML, WS-Federation, and WS-Trust. IBM provides adaptive authentication based on risk determined by contextual information that is evaluated by machine learning. IBM has a mobile app SDK which collects the full spectrum of device intel attributes. Account recovery options span from KBA to account linking to various OTP types. For provisioning, IBM provides self-registration and profile management features, and LDAP and SCIM interfaces are available. Up to 150 custom attributes can be defined. Within the same platform, IBM provides governance capabilities such as access request workflows, recertification campaigns, and account reconciliation.

Security Verify provides good 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 applications. All functions including identity and marketing analytics are exposed via APIs (REST, SOAP, Websockets, but not Webhooks).

Consumers are presented with a self-care UI that allows them to view/edit/delete information. However, opting out of data collection after registration requires account deletion. The solution does not automatically notify users when terms of service change. Kantara consent receipt is not supported. Family management is not built-in but could be configured with customized delegation. Device identity management is provided, and IBM supports a number of complex use cases with OAuth2 Device Flow, but consumer portals for device identity management are not built-in.

IBM Security Verify is designed for scalability. It is ISO 27001/27018 certified, PCI-DSS Level 1, and SSAE 18 SOC 2 Type 2 attested. Fraud reduction capabilities are available within the IBM Trusteer suite of products. There are some omissions in the consent management model that may make it more difficult to achieve privacy compliance with some newer regulations. IBM plans on addressing those gaps in the near-term. Organizations that are looking for mature, highly scalable, and secure CIAM solutions built on a contemporary micro-services architecture should put IBM on the RFP list.

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



Strengths

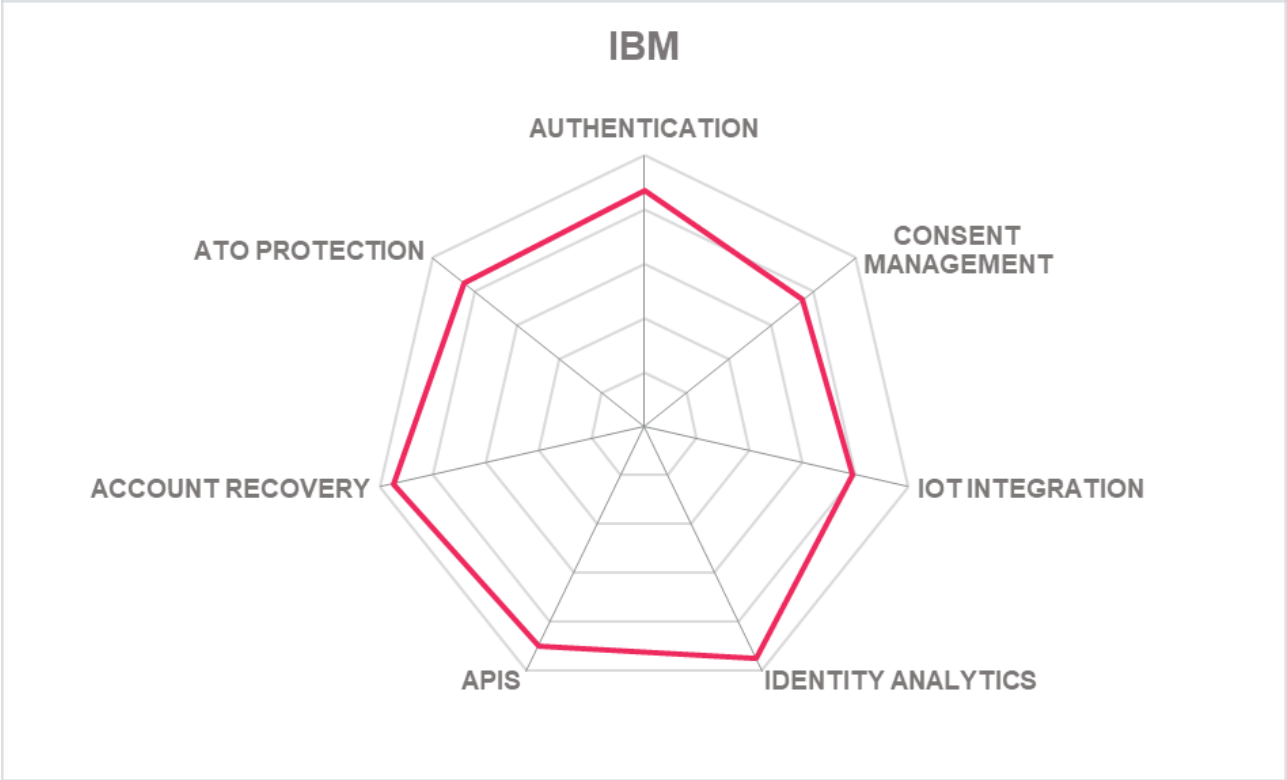
- Impressive selection of authentication mechanisms supported
- Highly scalable micro-services architecture
- Excellent and well-documented APIs for maximum extensibility
- High quality device intel capabilities
- FIDO and OpenID (multiple profiles) certified

Challenges

- Mobile SDK doesn't use TEE on Android
- Does not allow users to opt-out of data collection after registration
- Family management is not directly available

Leader in





5.8 iWelcome

iWelcome, founded in 2011, is a VC-backed IDaaS vendor based in the Netherlands. The CIAM functionality is a core feature of their overall IDaaS program. iWelcome's feature set is geared toward satisfying the business requirements of B2C/B2B2C customers in Europe. iWelcome's CIAM is SaaS, hosted in multiple AWS data centers around the EU. The list of related products above are constitutive of their full CIAM solution. It hosts customer profiles as well as identities. Licensing is per active or registered user per time period.

For authentication, iWelcome accepts mobile biometrics and push notifications, email/phone/SMS OTP, Google and Microsoft Authenticators, and social logins. JWT, OIDC, and SAML tokens can also be consumed. iWelcome also offers a mobile SDK which utilizes security features such as Global Platform SE and TEE; apps built with the mobile SDK can harvest rich device intel including location, device fingerprint/health/ID, and IP address information and can trigger step-up events. iWelcome does not have built-in sources of compromised credential intelligence, but such feeds can be configured by customers. iWelcome has connectors for identity proofing service providers including BelgianID, eHerkenning, Entersekt, FranceConnect, iDIN, iProov, ItsMe, ReadID, Signicat, Verimi, and WebID. All standard account recovery options are available. For provisioning, LDAP, SCIM, and social/self-registration methods are supported.

For real-time analysis of user behavior, iWelcome integrates with Google Analytics and Adobe Tag manager. Captured events can be shared via syslog with Google Analytics or other solutions. REST APIs, Webhooks, and Websockets can be used to facilitate connections to 3rd-party marketing analytics and automation tools. iWelcome offers a pre-built connector for Tableau.

As an EU-based company, iWelcome excels at facilitating GDPR compliance for customers. Consumers can provide consent on documents and on their data for multiple processing purposes. At any point after registration, users may edit their choices in the privacy portal. iWelcome supports Just-in-Time consent requests and GDPR compliant export/deletion of data upon request. iWelcome is active contributor to Kantara Consent Receipt specification. iWelcome offers traveling consent, whereby metadata is attached to data files. By combining data, metadata, and events in ETL exports, it offers an innovative enhancement to customers' big data analytics strategy. The RITM component (relationship manager) allows true family management within the platform for consumer use cases and is also used for B2B2C delegation. iWelcome supports consumer IoT device management via OAuth2 Device Flow.

iWelcome's approach to CIAM emphasizes privacy compliance (specifically GDPR, but other regulations too) but not at the expense of thwarting insights that increase value to marketers. iWelcome has cutting edge features in consent and family management and has strong security in private cloud deployments, with ISO 27001 and ISAE3000 attestations. Organizations in the EU, or global organizations that do business with EU citizen consumers, should put iWelcome near the top of the consideration list when looking for CIAM solutions.



Strengths

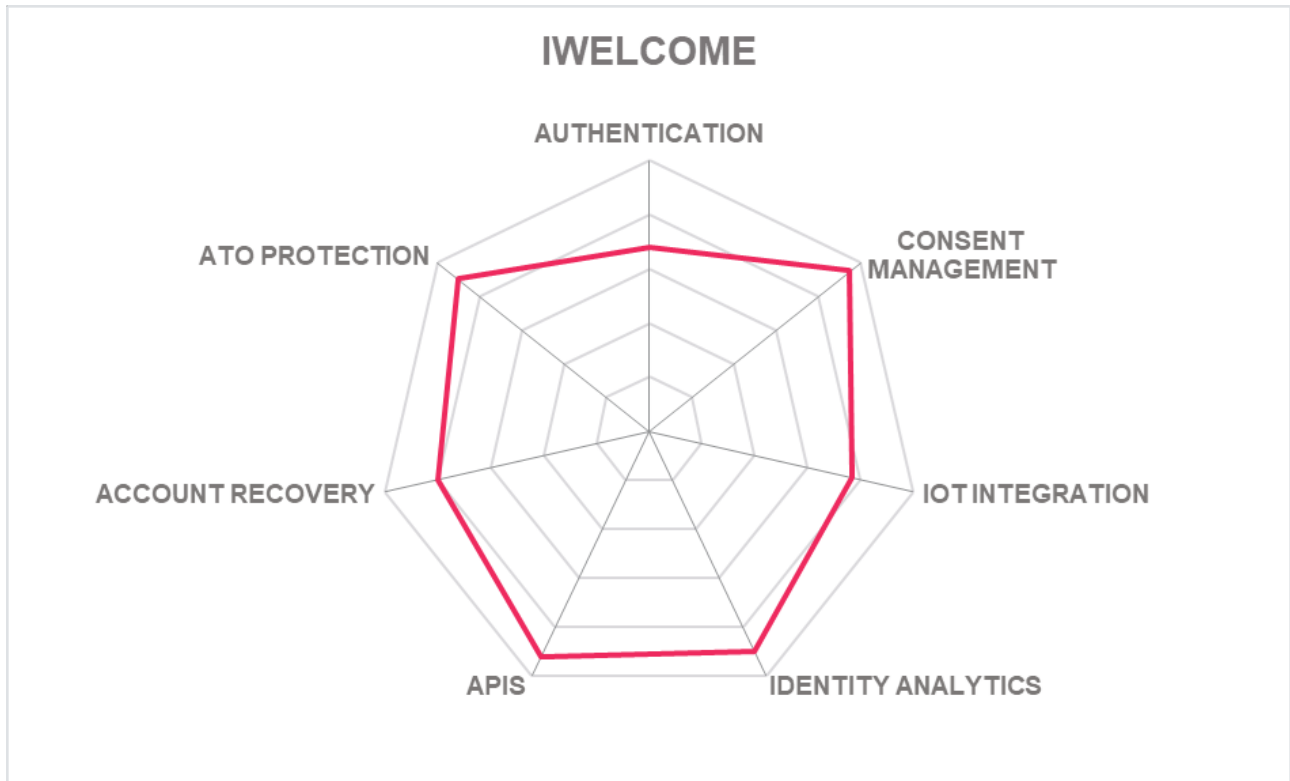
- Multiple data centers in the EU used for effective data localization
- eIDAS ready solution
- Connectors for many ID proofing services
- Excellent consent and family management
- Secure mobile SDK with transaction signing and secure messaging

Challenges

- FIDO not supported but on roadmap
- Sales and marketing centered on EU, no global reach yet
- Entry level pricing is not attractive for start-ups

Leader in





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/region deployment and customer profile hosting for enterprises around the world and has over one billion consumer identities under management. On-premise options are available, running on CentOS, RHEL, or Ubuntu; and customers can run it in any of the major IaaS providers. LoginRadius has a strong European presence, with multiple data centers within the EU for regulatory compliance. Licensing options include monthly active users or quarter/annual registered users for SaaS clients, or per-server from on-premise deployments.

LoginRadius works with Android and iOS biometrics; Duo and Yubikey FIDO 2 devices; email/phone/SMS OTP; Aegis/DeepNet/Duo/Google/LastPass/Microsoft Authenticators; and any OIDC based social login. JWT, OAuth, OIDC, and SAML are supported for SSO. Most standard account recovery mechanisms are supported. LoginRadius offers a flexible mobile SDK which can collect a limited amount of device intelligence. LoginRadius' integrations with Spycloud and Trulioo can cut the risk of fraud. Self- and social registration is possible but LDAP and SCIM bulk provisioning are not.

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. Customers can choose to export data to Chartio, Hubspot, MailChimp, Microsoft Dynamics and PowerBI, Salesforce, and **many other analytics programs**. All CIAM data is accessible via REST API and Webhooks are supported.

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.

LoginRadius has a full-featured CIAM offering that is attested and/or certified with CSA Star Level 2, ISO 27001/27018, PCI-DSS, and SSAE SOC 2 Type 2. Such efforts demonstrate their commitment to security and reliability. Their multi-cloud, multi-region deployment strategy provides excellent scalability. LoginRadius has added many capabilities to their platform over the last few years and has become a strong player in the CIAM market; thus, LoginRadius should be considered by organizations looking for easy-to-deploy, highly scalable CIAM solutions.

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

loginradius

Strengths

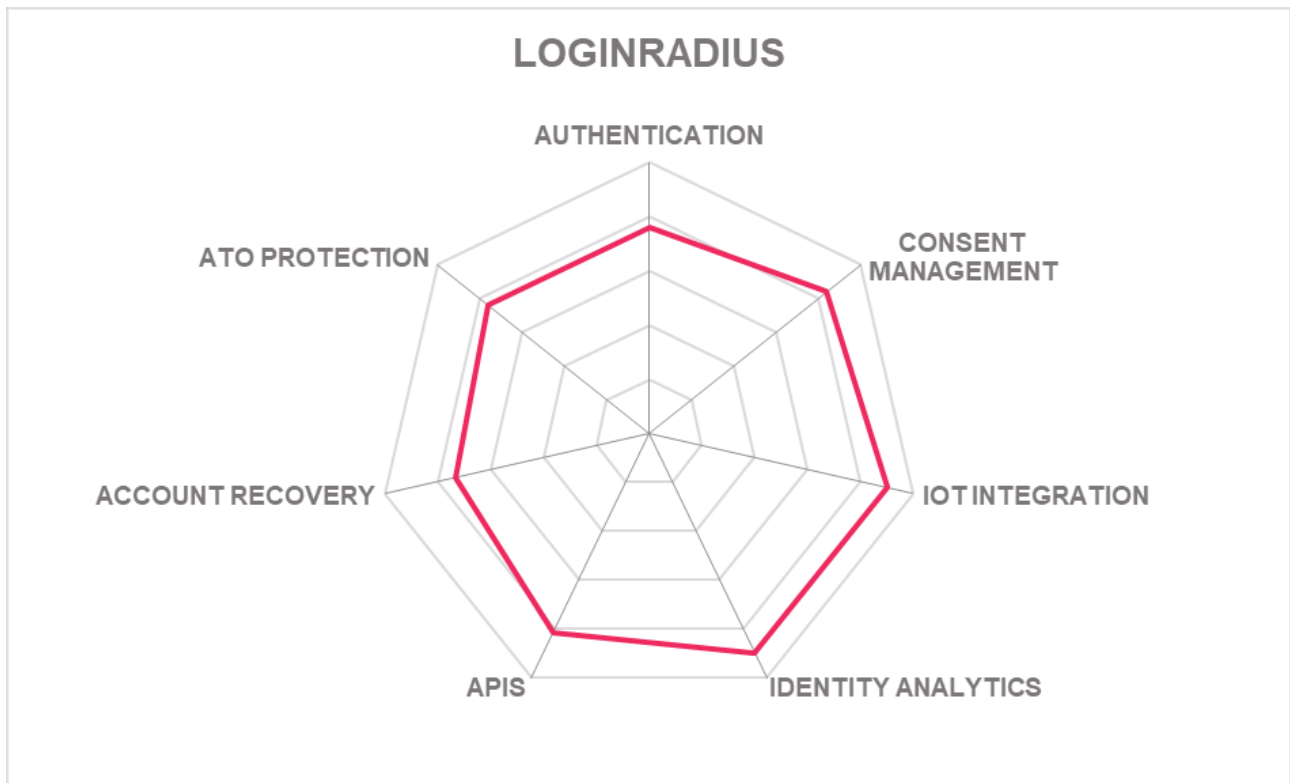
- Good choices for authentication options
- Built-in access to credential and fraud risk intelligence
- Excellent analytics reports as well as interoperability with 3rd-party tools
- Innovative integration with consumer IoT devices

Challenges

- SDK could collect more mobile device intel
- Support for LDAP and SCIM would be useful for some customers

Leader in





5.10 Microsoft

Microsoft Azure Active Directory 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 licensed by number of monthly active users. Charges are slightly higher for a tier of Premium P2 features, such as Azure AD Identity Protection.

Microsoft Azure AD B2C accepts username/password, Authy/LastPass/Microsoft Authenticator, SMS OTP, and self-registration and authentication through social logins including Facebook and Google accounts. Additional MFA options are available through partners. The service also accepts JWT, OAuth, OIDC, and SAML tokens. The standard range of account recovery options are available. Microsoft customers do benefit from the rich in-network credential intelligence and account protection services that can be utilized within the offering. Microsoft is partnering with a variety of fraud reduction intelligence providers to offer those services to customers of External Identities. Device intel capabilities are not natively present. Consumers can self-register and use Facebook and Google accounts.

Microsoft Azure AD B2C features a RESTful API and Webhooks so that customers can send data to SIEM, CRM, and big data analytics solutions. All consumer data can be hosted, and basic identity analytics can be viewed within the console, but Microsoft PowerBI or similar data analytics tools are needed to transform the marketing data.

The Azure AD B2C platform provides the capability for customers to present consent options to consumers, typically in a progressive profiling manner. No central user privacy dashboard is available. Customer admins can configure GDPR compliant CIAM solutions with Azure AD B2C. Family management can be configured as delegated administration. Kantara Consent Receipt is not supported. There are no provisions for IoT device identity management.

The Azure platform is CSA Star Level 1 and 2 certified, HIPAA/HITRUST, ISO 27001/27018, PCI-DSS, SSAE SOC 2 Type 2 attested and/or certified. It also supports a variety of national cybersecurity and some privacy regulations. Microsoft has the power and infrastructure to enable massive scalability. It does lag the competition on a number of key features in the areas of authentication, SDK, modern standards support, privacy management, and IoT integration.

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



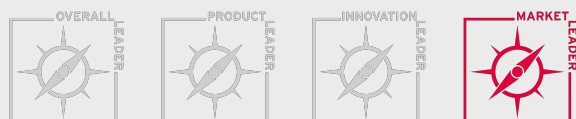
Strengths

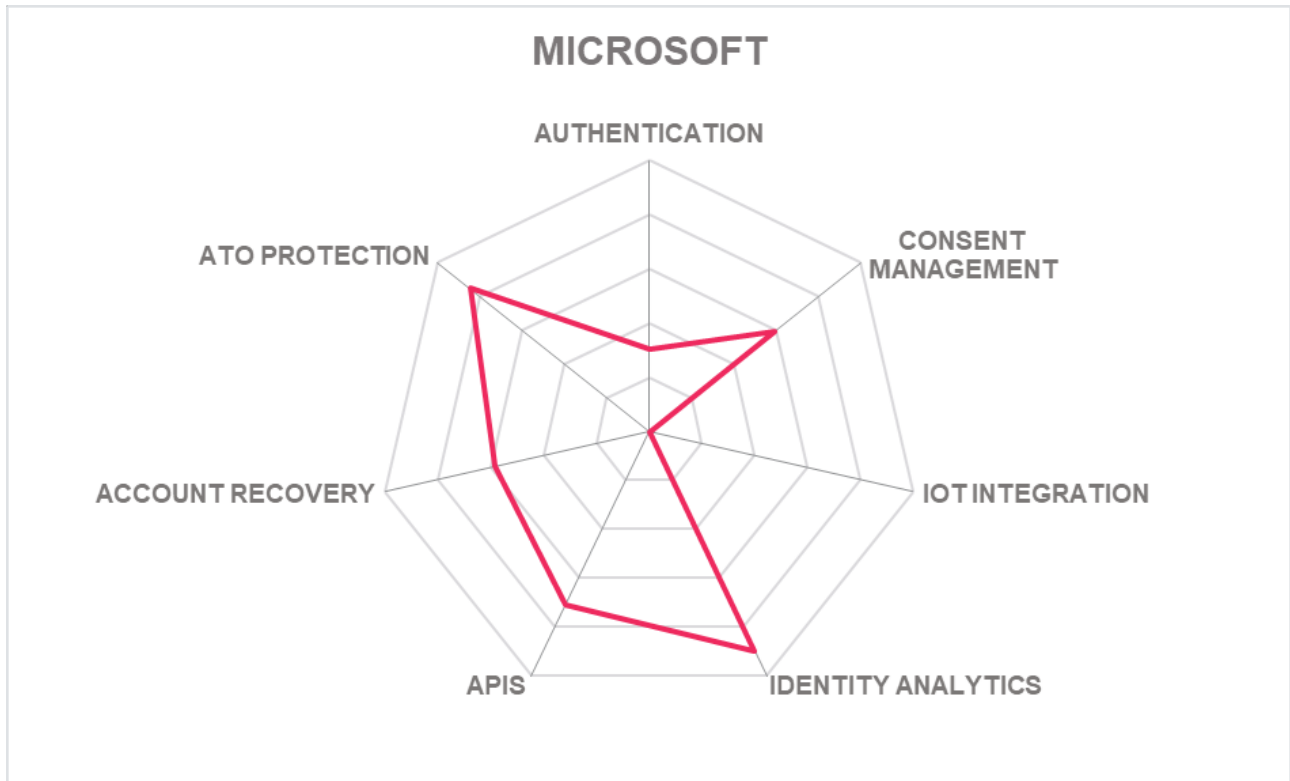
- Massive scalability
- Strong account takeover protection
- Working toward merging control over Microsoft Azure AD and CIAM into a single portal

Challenges

- Insufficient MFA options
- FIDO not supported for CIAM use cases
- Mobile SDK does not collect and process device intel
- Azure AD B2C does not have feature parity with Azure AD B2B collaboration solution

Leader in





5.11 NRI Secure Technologies

NRI Secure Technologies was founded in 2000 as a subsidiary of Nomura Research Institute. NRI Secure also provides security consulting. Uni-ID Libra is their CIAM product, which was first launched in 2008. The product is licensed per monthly active or registered user and can be deployed on-premises on CentOS or RHEL; or in AWS, Azure, or GCP IaaS environments. NRI also offers it as a multi-tenant hosted service in AWS.

Uni-ID Libra accepts Android biometrics, email/phone/SMS OTP, Authy/Google/Microsoft Authenticators, FIDO UAF/U2F/2.0 authenticators, and social logins. It supports JWT, OAuth2, OIDC, and SAML. It does not have a mobile SDK. External sources of credential and threat intelligence can be consumed with customization. Consumers can self-register and can be provisioned from other systems using SCIM. LDAP is not supported currently. Only OTP options are available for account recovery.

NRI supports REST APIs and WebAuthn but is missing Webhooks and Websockets. Identity analytics reports are quite limited. Uni-ID Libra can interoperate with security tools such as Splunk and the ELK stack. Marketing analytics are not directly available.

Uni-ID Libra allows consumers to view, edit, and delete their saved profile data. Kantara Consent Receipt is not supported. Family management can be configured, but it is coarse-grained (no direct parental/guardian control over child accounts). NRI supports IoT device identity management, OAuth2 Device Flow, and specifically connected cars use cases.

NRI's SaaS instance is ISO 27001 compliant. Additional security certifications and controls would be beneficial. NRI has significantly enhanced Uni-ID Libra over the last few years, adding MFA types for consumers and more consumer consent options. FIDO Universal Server support gives them a competitive advantage in the region. Language support is limited to Japanese and English. NRI excels in the Japanese market. Organizations within Japan that are looking for CIAM solutions should put NRI Uni-ID near the top of their RFP list given their experience and feature set.

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

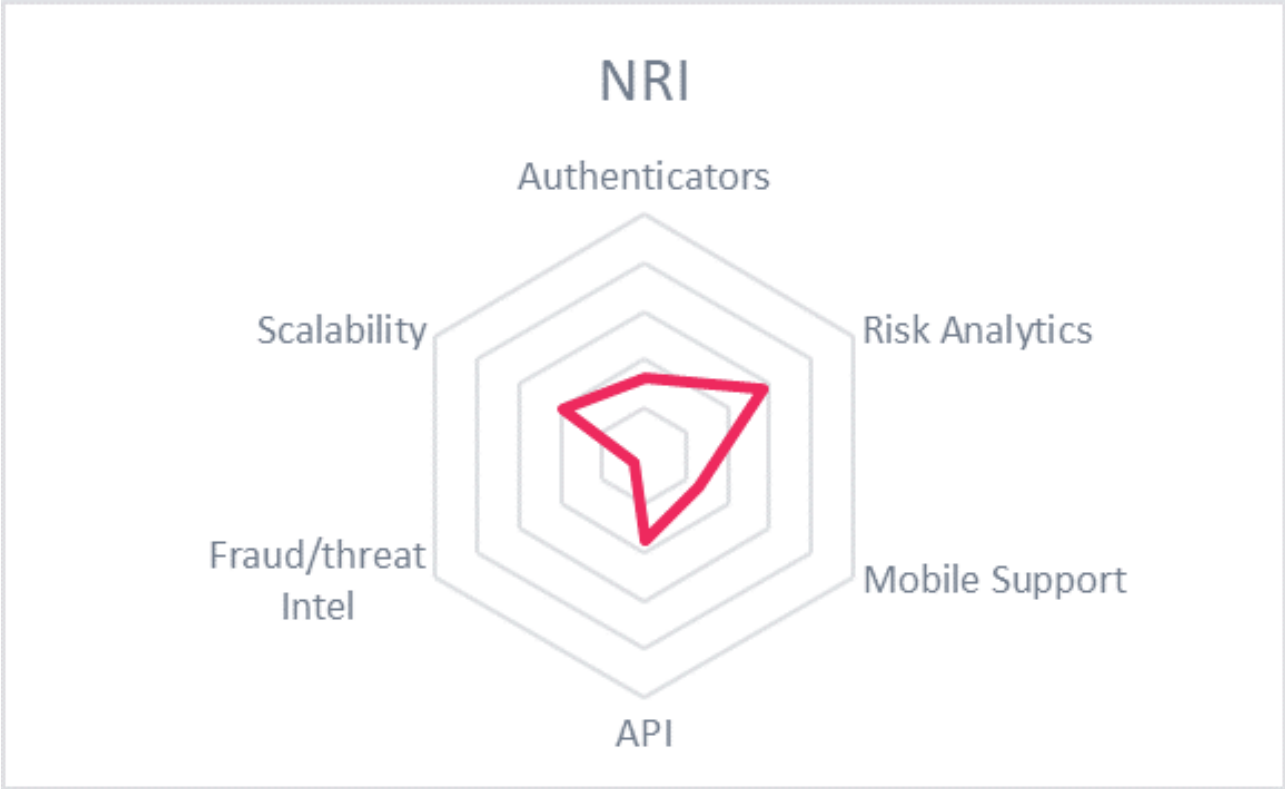


Strengths

- Large-scale deployments in leading Japanese auto, aviation, telecom, finance, and hospitality companies
- Excellent IAM standards support
- FIDO 2 Universal Server certified

Challenges

- No sales or support presence outside of Japan
- Mobile app SDK would benefit customers
- Does not consume 3rd-party fraud or threat intelligence
- Weak account recovery methods



5.12 Oxyliom Solutions

Oxyliom Solutions was founded in 2012. They are headquartered in Luxembourg and also have offices in Casablanca and Dubai. In addition to CIAM services, GAIa has B2E IAM, Data Governance, and Trust Management including electronic signatures and key management features. GAIa is primarily an on-premise solution running on Docker, RedHat Linux, or Windows Server 2008R2+. It can also run in Alibaba, AWS, and Azure IaaS. It has multiple licensing schemes, ranging from monthly/quarterly active and/or registered users and per-login or session metrics.

For authentication methods, GAIa accepts any OIDC-based social logins, Android fingerprint, iOS FaceID and TouchID, email/phone/SMS OTP, Duo/Google/LastPass/Microsoft/Okta Authenticators, FIDO U2F/2.0 hardware tokens such as Feitian and Yubikey, mobile app and push notifications. Oxyliom offers a mobile SDK with limited device intelligence signal collection capabilities. The mobile SDK allows for remote ID proofing and registration and supports e-KYC for banking customers. GAIa supports JWT, OAuth, OIDC, and SAML federation. GAIa does not consume 3rd-party compromised credential intelligence by default but customers can configure this. GAIa supports LDAP and SCIM and other cloud APIs for bulk import. All major account recovery techniques are present.

Oxyliom Solutions has strong support for relevant regulations in the financial industry, including AML, eIDAS, GDPR, KYC, and PSD2. Customers can view basic identity analytics dashboard and reports within the GAIa platform. GAIa has REST API access and WebAuthn support, but there are no connectors for 3rd-party marketing analytics and automation tools.

Consumers can opt-in/out of data collection, as well as view/edit consents and delete accounts via user self-service interface. Kantara Consent Receipt specification is supported. GAIa can allow tenants to automatically notify users and have them re-consent after privacy policies change. Family management is possible if configured as dependent identities. GAIa offers key management in the platform and works with leading HSMs to provide high levels of data security and consumer privacy. Oxyliom implements OAuth2 Device Flow to support registration and association of consumer IoT device identities with consumer identities.

Oxyliom claims FIPS 140-2 and NIST 800-57 adherence with their products. Oxyliom has a good presence in Africa and is expanding throughout EMEA. GAIa Advanced Identity Management integrates key elements of CIAM required for regulatory compliance and a modern digital experience, and the integrated Trust Platform with electronic signature capabilities makes it a product to consider, particularly for companies in their regions of expertise and in the finance industry.

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

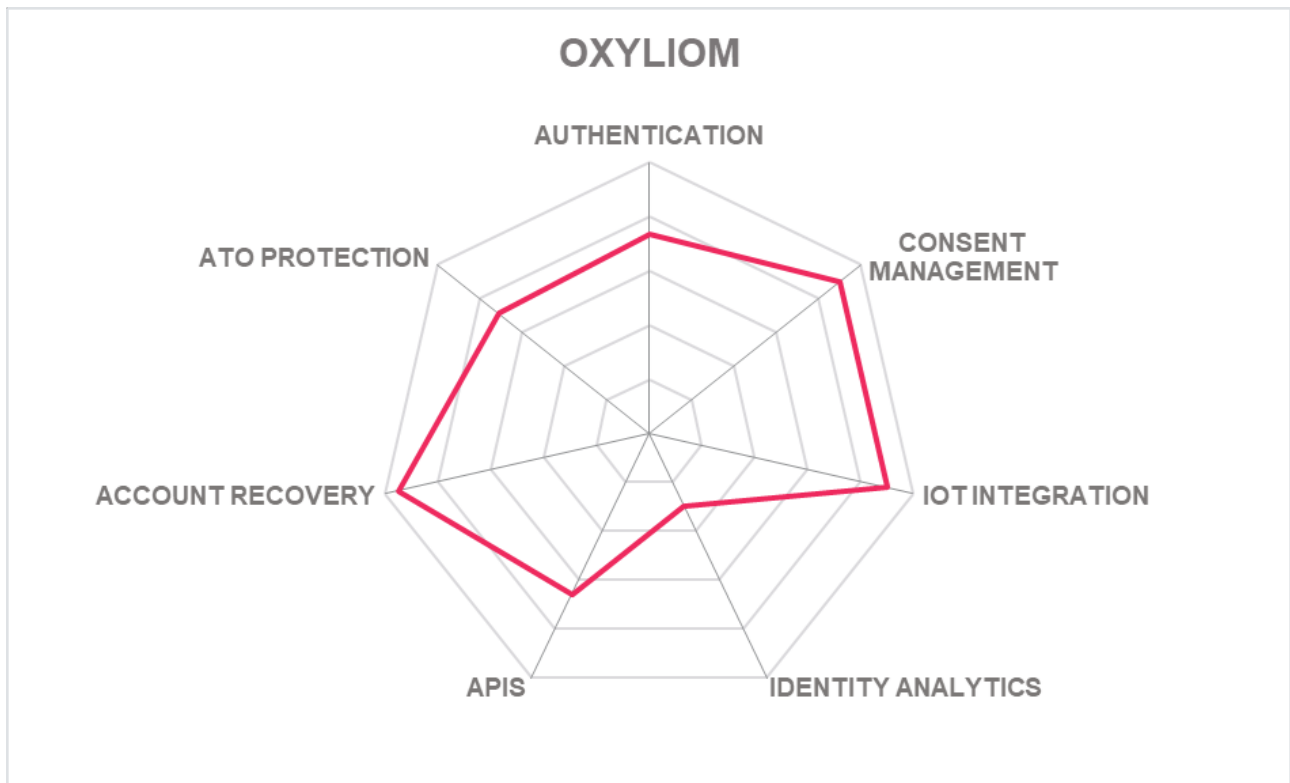


Strengths

- ML-based fraud detection and API security monitoring built-in
- Mobile SDK supports remote identity proofing, registration, and e-KYC
- Integrated Trust Management
- Modern, microservices-based architecture
- REST API-driven CIAM platform
- Good selection of authenticators available

Challenges

- Late to market with SaaS offering
- REST APIs supported but no connectors for marketing analytics and automation tools
- SDK should collect more device intel
- 3rd-party compromised credential intel configurable but not built-in
- Startup with small but growing customer base, support ecosystem, and technology partners



5.13 Ping Identity

Ping Identity has been a pioneer in identity federation and access management since its founding in 2002. Ping Identity has grown substantially and went public on NYSE late in 2019. Ping Identity was among the first of the enterprise IAM vendors to offer CIAM. The services are available for both on-premise and cloud deployment, and the Ping Intelligent Identity Platform can host customer profiles in the cloud, amongst other capabilities. In addition, Ping has a full suite of IAM and API security products for workforce and B2B use cases. Their solutions can run on-premise on RHEL, SUSE, or Ubuntu; in any IaaS environment, with support for Docker and Kubernetes; and they run it as a fully multi-tenant SaaS using multiple regions of AWS. The solution is licensed by the total number of managed identities.

Ping Intelligent Identity users can authenticate with Android/iOS native biometrics, Aegis/Authy/DeepNet/Duo/Google/LastPass/Microsoft/OneSpan/SaaS Pass/SafeNet Authenticators, email/phone/SMS OTP, FIDO U2F/2.0, mobile apps and push notifications, and social logins. JWT, OAuth, OIDC, and SAML are supported. Ping provides an SDK to embed MFA features into any mobile app, collecting a full set of device intel attributes, and utilizing high security features such as SE and TEE for Android. Ping has integrations with ID Data Web, Intersect, Iovation, and ThreatMetrix for additional intelligence. All salient forms of account recovery and linking are supported. Bulk provisioning and bi-directional synchronization are possible via LDAP and SCIM, and self-registration and data management is possible for consumers. This solution can serve as an identity bridge to IDaaS, SaaS, and on-premise AD, IAM, and SSO implementations.

The solution provides a complete range of identity analytics reports, including the ability to apply User Behavioral Analysis to detect and deter fraud and other attacks. Ping Intelligent Identity allows API access for pulling information useful to marketing tools. Ping Intelligent Identity has robust API features to support interoperability, including support for REST, SOAP, WebAuthn, Webhooks, and Websockets using CSV, JSON, or XML. PingIntelligence for APIs is a separately sold product for monitoring and protecting APIs, and PingDataGovernance (also separately licensed) can be used for fine-grained, dynamic authorization to APIs, including the ability to enforce customer data-sharing consent. Ping has 1,400+ connectors for various SaaS and other services.

Ping provides facilities for customers to give consumers the full ability to view, edit, control, and delete their profile information; however, they do not offer specific privacy regulatory compliance guidance or assurance. Family management can be configured as a special case of delegated administration. For IoT device identity management, Ping supports OAuth2 Device Flow Grant and Dynamic Client Registration. Ping Intelligent Identity platform addresses use cases for wearables, mobiles, and connected cars.

Ping Identity self-certified with CSA and certifies/attests with ISO 27001 and SSAE SOC 2 Type 2. Their CIAM SaaS solution is highly scalable and offers maximum flexibility to customers in terms of support for standards as well as innovation for cutting edge use cases. Any type of organization that is in need of CIAM services should consider Ping Intelligent Identity as a potential solution.

Security
Functionality
Interoperability
Usability
Deployment



Ping
Identity.

Strengths

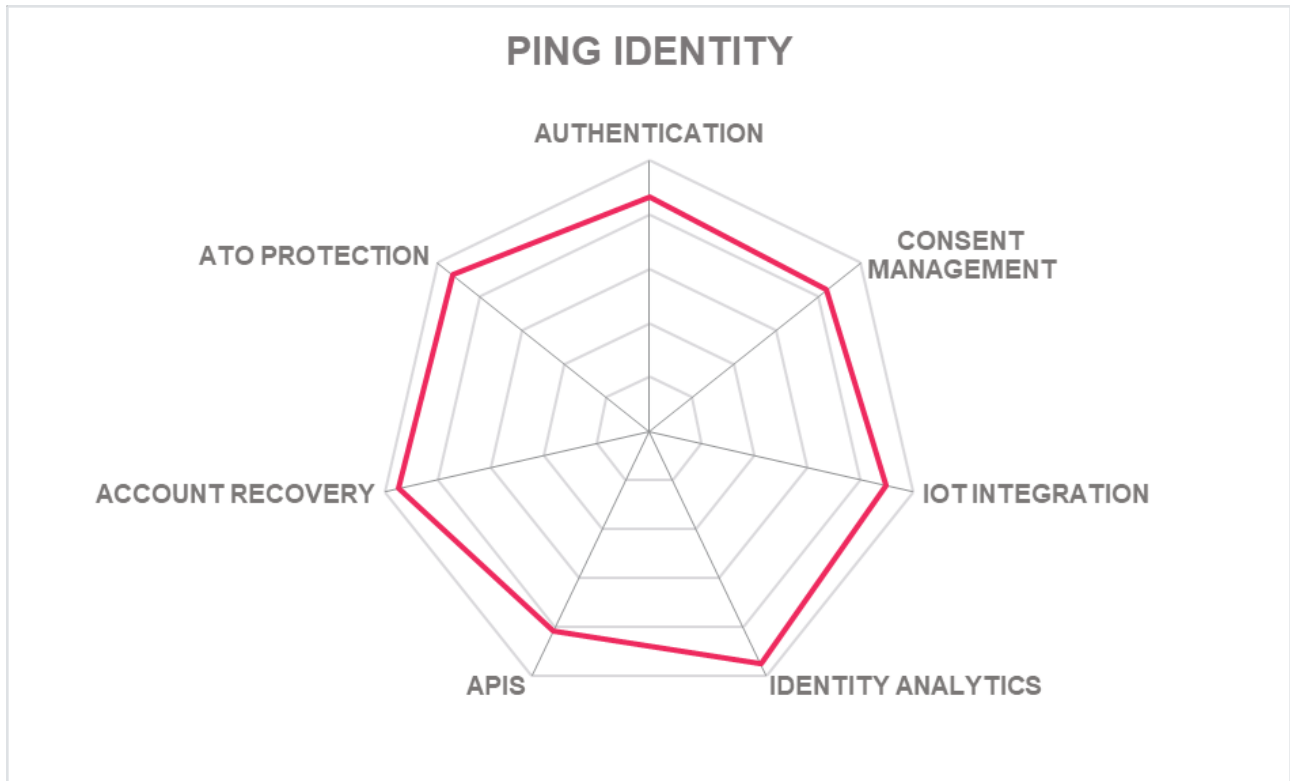
- Vast selection of authentication mechanisms
- Secure mobile SDK with excellent device intel features
- Built-in and extensible threat intelligence
- Support for nearly all relevant standards
- Secure API access for all functions
- Innovative consumer IoT use cases

Challenges

- No connectors to business analytics systems yet, but in work
- Licensing by active user counts should be an option
- Kantara Consent Receipt not supported

Leader in





5.14 Pirean

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. The product can be deployed either on-premises on CentOS, Debian / Dockers, RHEL, Suse, or Ubuntu; or in IaaS on AWS, Azure, GCP, or IBM; and Pirean hosts it as a managed service in AWS and IBM in multiple regions. Pirean can also host consumer profiles in the cloud for their customers. It is licensed according to monthly active users.

Pirean supports Authy/Duo/Google/Microsoft Authenticators, email/phone/SMS OTP, FIDO U2F/UAF/2.0, mobile apps and push notifications, native biometrics for Android and iOS, OATH TOTP, and social logins for authentication. Pirean also has a secure mobile SDK which customers can use to build to their own apps, and it can harvest device intelligence from consumer devices. Additional hardware 2FA devices can be mandated for use by customer admins. Access: One can be configured to query external services such as Experian Hunter, IBM Trusteer, and Threatmark for fraud and threat intelligence. The risk engine is granular and can evaluate a large set of attributes against policies. Policies can be written for step-up authentication/authorization. It supports JWT, OAuth, OIDC, and SAML for federated authentication and authorization (including API access); and self-registration, LDAP and SCIM for provisioning. All standard account recovery mechanisms are present. Customers can send data to SIEMs over syslog or through OOTB connectors.

Customers can get a wide range of identity analytics from Access: One, including reports for KYC initiatives. Data from Access: One can be securely shared with 3rd-party BI, CRM, and marketing analytics tools, including Adobe Campaign, Hubspot, IBM Cognos, Microsoft Dynamics, Microstrategy, NetSuite, and Salesforce, Tableau, and TIBCO. Access: One supports REST APIs, SOAP, WebAuthn, Webhooks, and Websockets; and CSV, JSON, and XML data exchange formats.

Consumers can view, edit, export, and delete their personal information through a user dashboard. Full consent and family management facilities are available within the consumer dashboard. Pirean can produce Kantara Consent Receipts. Access: One also supports OAuth2 Device Flow for consumer IoT registration, focusing on smart watch and mobile phone integration. Consumers can manage their devices within their portals.

Pirean's strong feature set is dictated by its history in heavily regulated industries that require strict security. Pirean has attestations/certifications for AU IRAP, UK Cyber Essentials Plus and G-Cloud. Access: One also is aligned with ISO 27001 and attests to SSAE 18 SOC 2 Type 1 and 2. Given their growth and backing, we expect Pirean to increase its market share. Organizations with the need for strong security for their customers and consumers should be sure to evaluate Pirean Access: One.

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



Access: One

Strengths

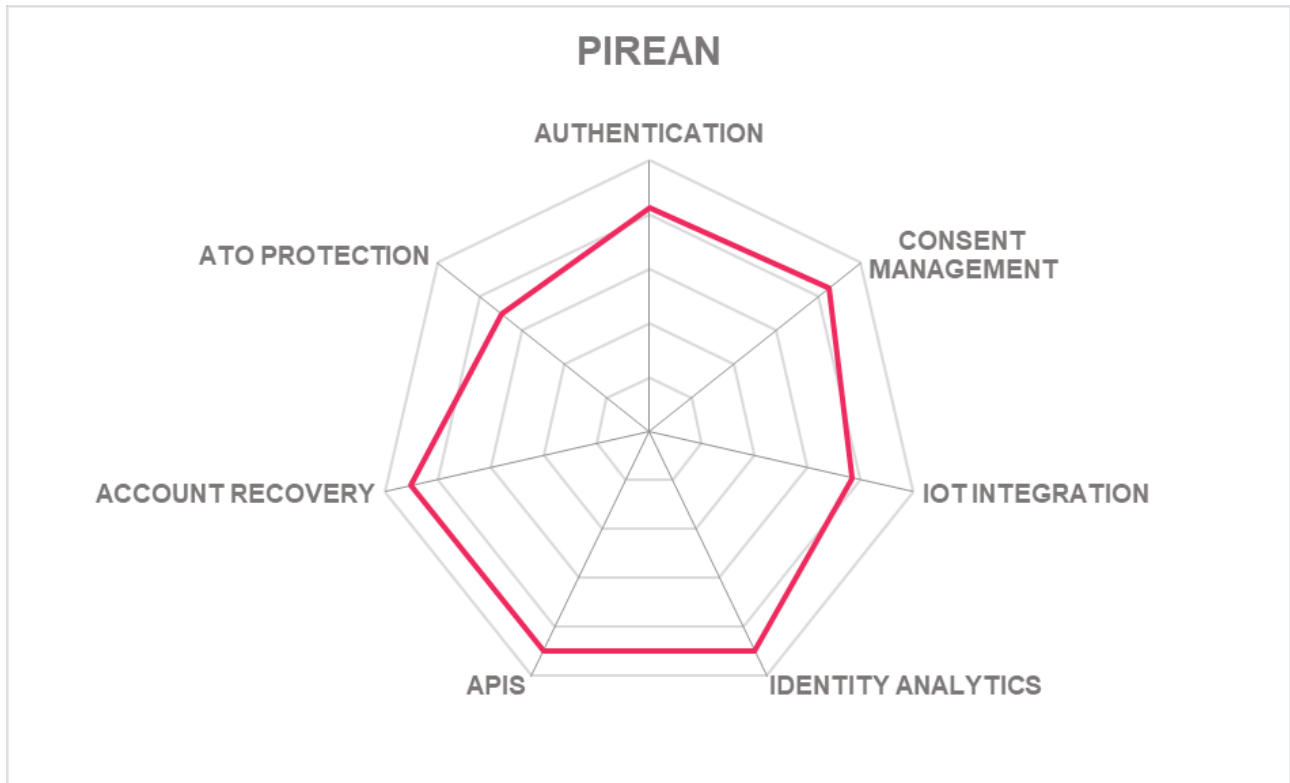
- Good selection of authenticators
- Built-in compromised credential intelligence
- Some high security certifications
- Secure mobile SDK
- IoT device identity management within consumer portal

Challenges

- Small but growing vendor, quite well geographically distributed
- Partner ecosystem needs to expand
- FIDO and OpenID certifications in work

Leader in





5.15 ReachFive

ReachFive is a small, venture-backed CIAM company that was founded in 2014 in France. CIAM is their sole focus. Their solution is SaaS only, running in Alibaba, AWS, Azure, and GCP. Most customers are in the retail market in France, although they support other industries and are looking to expand. Cost models are based on platform utilization.

The ReachFive platform accepts Android and iOS biometrics, email/SMS OTP, FIDO 2 authenticators, and social logins. JWT, OAuth, and OIDC can be used for federated authentication and authorization, but not SAML. No additional authentication or federation types are supported for customer administrators. ReachFive provides a mobile SDK which can collect some device intel signals. ReachFive checks have been pwned for compromised credential intelligence. Account recovery selections include email/SMS OTP and account linking. Self-registration is possible, including using social network credentials, but bulk provisioning over LDAP and SCIM are not.

Customers can view consumer identity analytics in built-in reports and dashboards. ReachFive is addressable via APIs, and supports REST, WebAuthn, and Webhooks, as well as CSV and JSON format. Connectors are available for Adobe Campaign, DialogInsight, Google Big Query and Data Studio, Microsoft Dynamics and PowerBI, Salesforce CRM, and Splio.

As an EU headquartered company, ReachFive is attentive to GDPR, providing the customers with the ability to offer privacy and consent management through their interface. Thus, consumers can view, edit, and delete their personal information. The solution does not support auto notifications for changes in terms of service, nor does it support Kantara Consent Receipt. Basic family management capabilities are present. ReachFive has some limited functions for associating consumer IoT device identity with consumer identities, but it is not aligned with OAuth2 Device Flow.

ReachFive has attested to or certified with CSA Star Level 2, ISO 27001, SSAE SOC 2 Type 2; and facilitates compliance with a variety of EU privacy and security regulations such as GDPR, BSI C5, UK Cyber Essentials Plus and G-Cloud, and the Swiss Federal Act on Data Protection. Their market share is small but they have a growing feature set. Organizations, particularly those in the retail industry in the EU, may want to consider ReachFive as a CIAM solution.

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

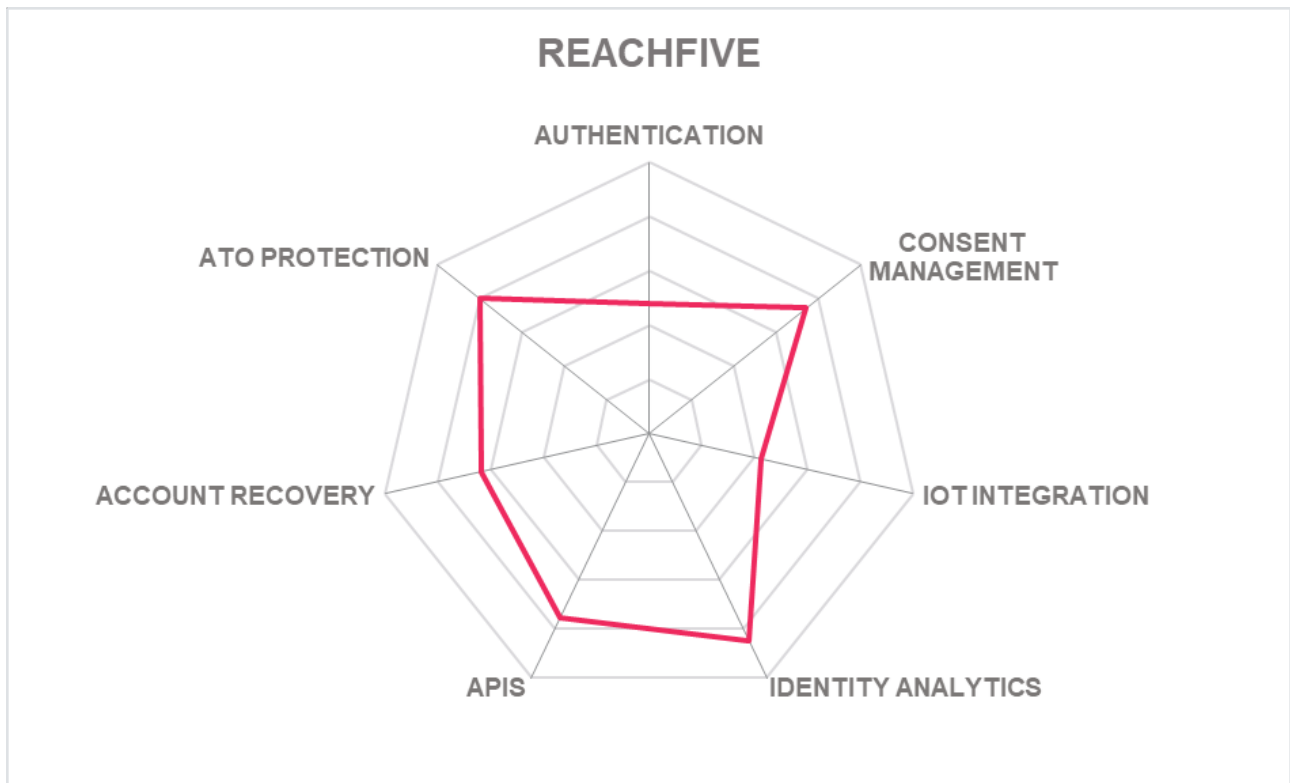


Strengths

- Mobile SDK with some device intel features
- Compromised credential checks performed
- Multi-cloud deployment options
- Utilization based licensing costs

Challenges

- Needs additional authentication and federation options
- OAuth2 Device Flow not supported
- Bulk provisioning is not supported
- More connectors for marketing analytics and automation would be useful for some customers
- Not much market presence outside France



5.16 SAP

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 Customer Data Cloud (CDC) is a fully cloud-native, highly scalable CIAM delivered as SaaS, operated from regionally distributed data centers in SAP's own facilities as well as Alibaba and AWS. Licensing is priced by monthly registered users.

SAP CDC supports Android/iOS biometrics, email/phone/SMS OTP, FIDO U2F/2.0, Aegis/Authy/DeepNet/Duo/Google/LastPass/Microsoft/Okta/OneSpan/SaaS Pass/SafeNet Authenticators, mobile push notifications, social logins, and any TOTP methods. JWT, OAuth, OIDC, and SAML are available for federated authentication and authorization. SAP offers a mobile SDK which can collect IP address and location information. SAP CDC has integrations with LexisNexis, Socure, and Trulioo for identity verification. Credential intelligence protects SAP CDC customers from compromised credential abuse and fraud and includes external sources haveibeenpwned and Telesign. All standard account recovery mechanism except mobile push notifications are present. Consumers can use social logins or self-register, and LDAP can be used for bulk provisioning. SCIM is not supported.

SAP CDC excels at identity and marketing analytics, providing many pre-defined reports covering all 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: Adobe Analytics, CheetahMail, Constant Contact, Eloqua, Google Analytics, KissMetrics, MailChimp, Marketo, Responsys, Sailthru Salesforce, SAP Marketing Cloud, WebTrends, Zendesk, and others. SAP CDC has REST APIs and a wide range of extensibility options including Webhooks, server-side extensions and JavaScript parameters to customize consumer interactions. CSV, JSON, and XML data formats are supported; and WebAuthn is on the roadmap for late 2020.

SAP Enterprise Consent and Preference Management allows customers to set up CIAM instances that facilitate compliance with regulations such as CCPA, GDPR, and more. 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 without having to define relationships as variations of delegated administration. SAP CDC's Global Login feature allows customer admins to localize consumer data to their region, facilitating regulatory compliance. SAP CDC supports complex use cases involving consumer IoT device identity management and linking with managed consumer identities. Some examples of device types include connected cars, home automation, set top boxes, smart speakers, and wearables. OAuth2 Device Flow is supported, and customization over APIs is possible too.

SAP Customer Data Cloud is highly scalable and feature rich. SAP attests/certifies with CSA Star Level 1, ISO 27001/27018, and SSAE SOC 2 Type 2. It now offers many authentication options to cover most popular forms, including stronger MFA. Identity and marketing analytics are readily available. SAP

Enterprise Consent and Preference Management helps customers comply with stringent privacy regulations. SAP Customer Data Cloud should be on the RFP shortlist for any organization seeking SaaS delivered CIAM.

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



Strengths

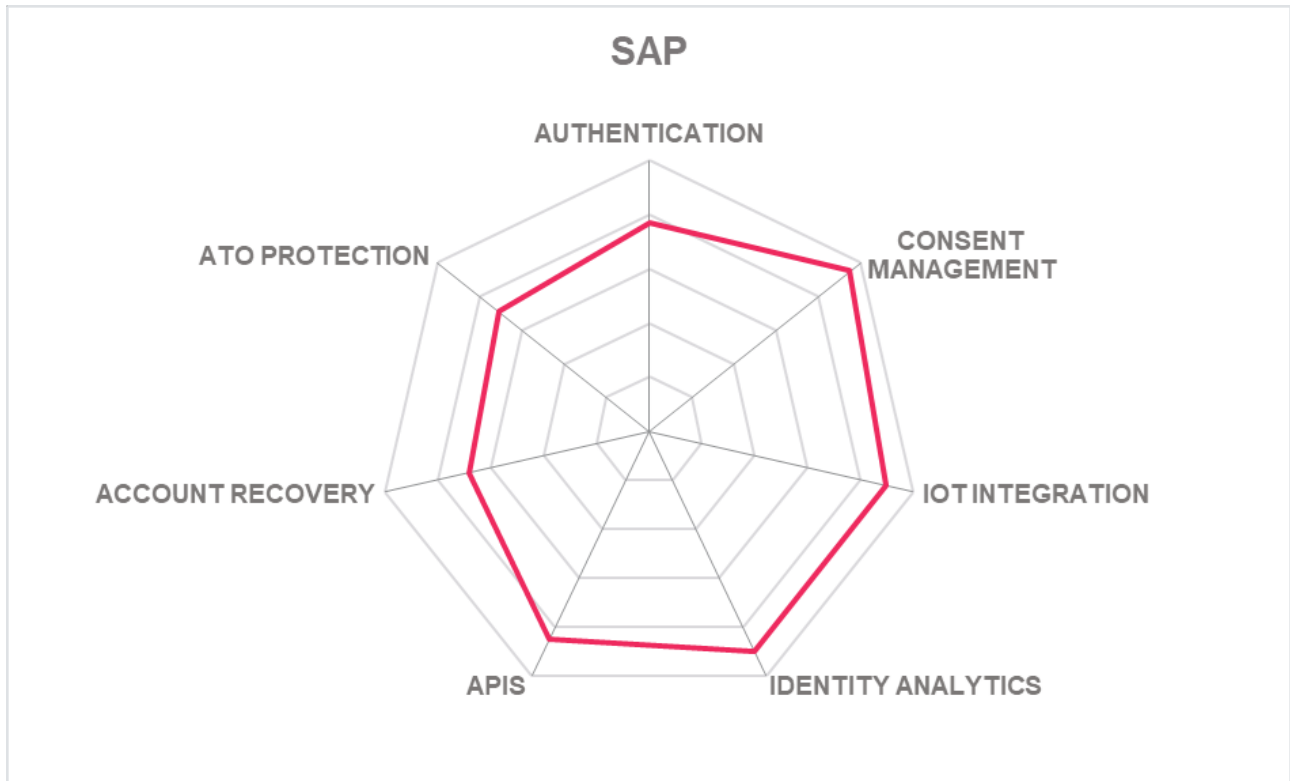
- Many authenticator types supported
- Massive scalability
- Detailed identity and marketing analytics built-in plus many connectors for 3rd-party systems
- Granular consent management and data localization for regulatory compliance
- Full implementation of family management
- Comprehensive support for consumer IoT device identities

Challenges

- Mobile SDK should collect extended device intel attributes
- FIDO2/WebAuthn on the roadmap

Leader in





5.17 Synacor

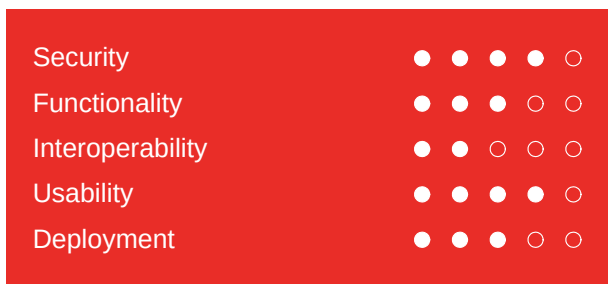
Synacor was founded in Buffalo, NY in 1998. They offer email and cloud hosting/services in addition to their Cloud ID service. Cloud ID's main focus is consumer IAM integration with IoT devices, particularly set top boxes (STBs), smart TVs, and home alarm systems. Synacor hosts Cloud ID as fully multi-tenant SaaS in their own data centers, Amazon, and Oracle Cloud. Licensing is either by monthly active or registered users.

Cloud ID supports Android and iOS biometrics, email/phone/SMS OTP, Authy and Google Authenticators, and social logins. JWT, OAuth, OIDC, and SAML can be used for federation. In-network compromised credential intelligence, NuData, Google RECAPTCHA are used for reducing fraud risks, and additional sources can be configured via APIs. Synacor does not offer a mobile SDK for customers. All account recovery mechanisms except mobile push notifications are available. Customers can bulk provision using LDAP, and consumers can self-register.

Cloud ID can provide identity analytics to customers, but marketing analytics capabilities depend on exporting raw data and configuring 3rd-party tools. Kafka can be used but there are no OOTB connectors. For application connectivity, REST, RPC, SOAP, WebAuthn, and Webhooks communications and CSV/JSON/XML formats are supported. Output to SIEM is not directly available.

Cloud ID's forte is consumer IoT device integration: STBs, smart speakers, smart TVs, and home alarms. It also supports OAuth2 Device Flow. Cloud ID covers basic consent management practices, including the ability for consumers to view, edit, and delete information. However, granular social media attribute selection is not possible. Complex family management is built-in, allowing for parent/guardian control over minors' access to content. Cloud ID helps customers comply with regulations such as COPPA and GDPR. Cloud ID creates opaque IDs to shield customers from obtaining and storing personal data of their consumers.

Cloud ID is SSAE 18 SOC Type 1 and 2 attested. Synacor may be one of the larger CIAM solution providers that many in the industry have not heard about; however, they support 150M users. The solution is scalable and is fine-tuned for TV, telecom, and content provider type customers. Synacor aims to provide tools that allow consumers to manage access appropriately in an efficient way. Support for advanced use cases in family management and home automation/entertainment devices make Synacor's Cloud ID a top contender in CIAM for organizations in those industries.

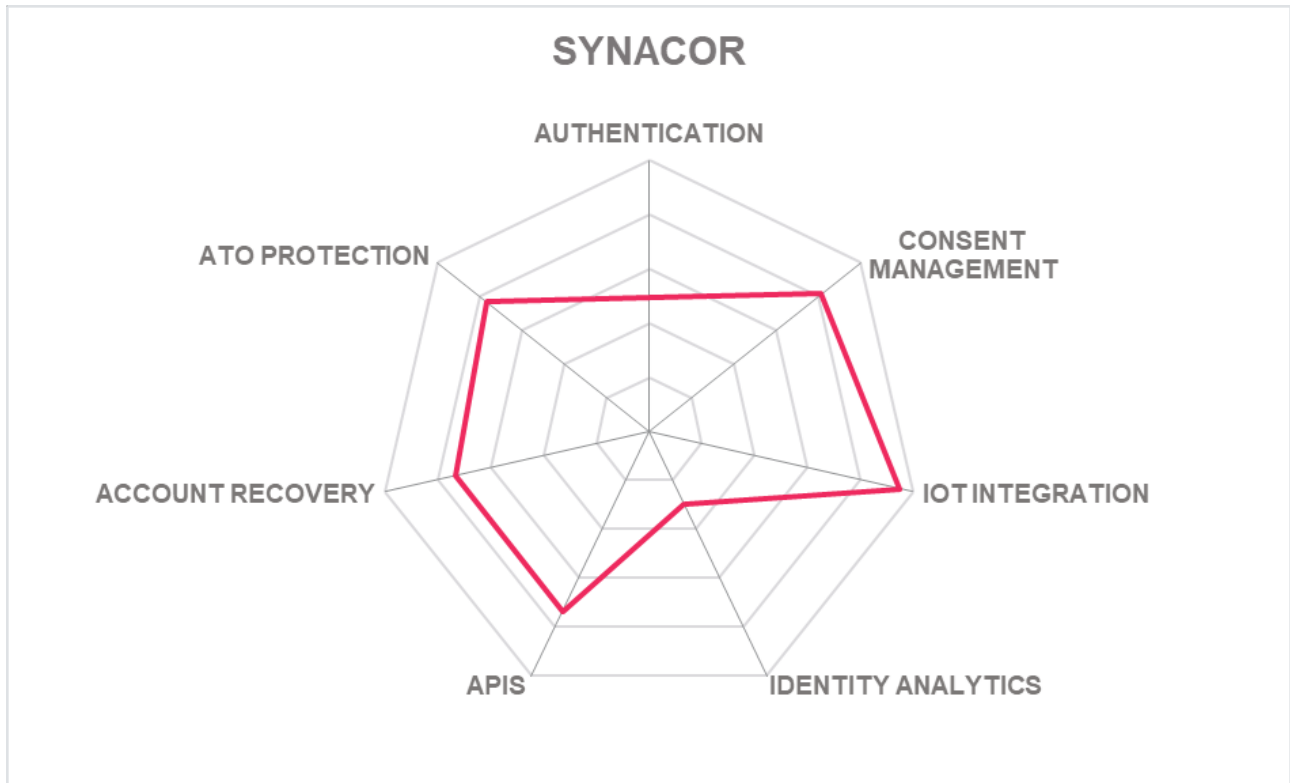


Strengths

- Deep integration with popular consumer IoT products such as smart TV and STBs
- Complex family management capabilities for content control
- Tight mapping of functionality to business requirements of target market provides good value for their customers
- Integration with fraud reduction intelligence services for ATO protection

Challenges

- Data center hosting limited to North America
- No mobile SDK
- FIDO authenticators not supported
- No SIEM connectors



5.18 Ubisecure

Ubisecure was founded in 2002 in Finland. Ubisecure is a full-service CIAM and IDaaS provider with additional services. Their Identity Platform can be run on-premises on CentOS, RHEL, or Windows; hosted by customers in IaaS; or consumed as SaaS hosted by Ubisecure in AWS and Azure. Licensing options include monthly/quarterly/annual active or registered users as well as per-login/session.

Ubisecure accepts email/SMS OTP, ETSI MSS, Google Authenticator, GSMA Mobile Connect, NemID, S-Group, social logins, and support Telia's Identity Broker Service (Finnish Trust Network) which has replaced TUPAS. A CIBA based Authentication Adapter microservice exists within the platform for quick addition of other standards-based authentication methods and Identity Providers. Ubisecure has partnerships for additional authenticators. At this time, external sources of compromised credential intelligence cannot be evaluated. JWT, OAuth, OIDC, SAML, and WS-Federation are available for federation. Email/SMS links, OTP and other strong authentication methods can be used for account recovery. Bulk registration can be done by data import over API, and consumers can self-register and manage their accounts.

Ubisecure provides an average range of identity analytics. There are no OOTB integrations for BI, CRM, or marketing automation and analytics. All functions are exposed via REST API using CSV/JSON/XML. Other connectivity protocols such as OData and Webhooks are not supported.

Ubisecure Identity Platform includes Self-Service Registration and Management, which allows consumers to view, edit, and delete their personal information on customer sites. Kantara Consent Receipt can be set up as needed. Family management is supported. Consumer IoT device identity integration is not directly supported at this time. Ubisecure was accredited to issue LEIs in June 2018. Ubisecure's RapidLEI solution can provide assignment and maintenance of Legal Entity Identifiers (LEIs). LEI is a global identifier for companies, specified by the EU eIDAS regulation, designed to aid in compliance for Anti-Money Laundering (AML) and Know Your Customer (KYC) initiatives.

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 in the months ahead. Support for regional bank and government IDs make Ubisecure a good choice for many organizations in the Nordic region.

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

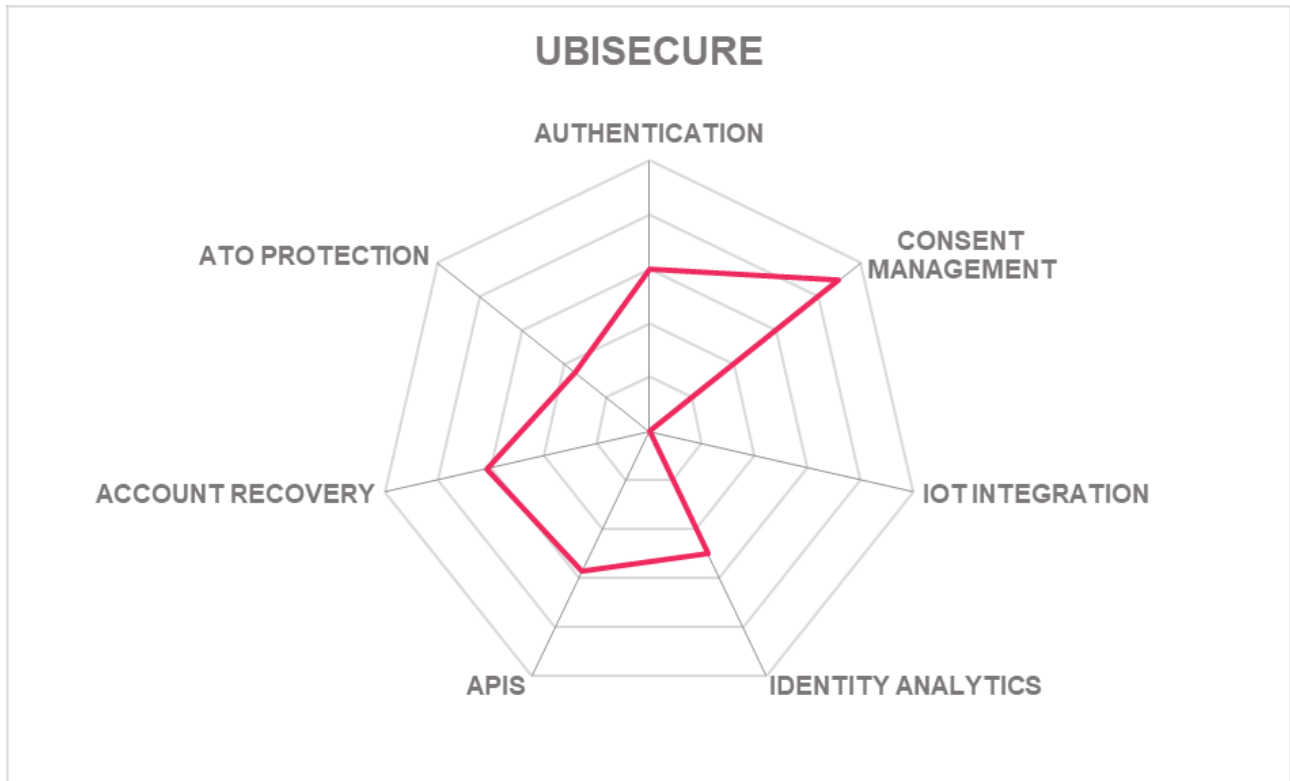


Strengths

- Good selection of authenticators supported, including Mobile Connect
- Accepts Nordic banks and some other regional IDs
- Family management functions built-in
- Contributor to open standards groups

Challenges

- Lacking BI, CRM, and marketing integrations
- Limited API capabilities
- No processing of compromised credential intel
- No IoT device integration
- Smaller vendor mostly focused on Nordic region



5.19 WSO2

WSO2 was founded in 2005. 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. The solution can be run on-premises, in IaaS, and they also offer a managed service capability. They are launching a cloud service later this year. The product is licensed per-server under the Apache 2.0 License and is supported through annual subscriptions.

WSO2 Identity Server accepts the following types of authentication methods: email/SMS OTP, Aegis/Authy/Duo/Google/LastPass/Microsoft/SaaS Pass Authenticators, FIDO U2F, Mobile Connect, social logins, and x.509 certificates. They have connectors for Veridium Biometrics and Aware Knomi for mobile biometrics, but Android and iOS native biometrics are not supported. Mobile push notifications are possible via integration with Duo, InWebo, and MePin. The solution does not have a mobile app SDK yet, though it is in development. Identity Server also has a risk engine that can process device fingerprints and history, geo-location, geo-velocity, user attributes and behavioral analysis. Third-party credential intelligence can be imported, but there are no pre-built connectors. WSO2 has excellent support for IAM standards, including JWT, OAuth, OpenID, OIDC, SAML, and WS-Fed/Trust. They support standards-based and just-in-time provisioning using LDAP and SCIM as well self-registration and management. Standard account recovery mechanisms are supported.

Identity Server dashboard and reports provide detailed identity analytics information, which can also be pushed into SIEMs. WSO2 supports OData, REST, RPC, SOAP, WebAuthn, Webhooks, and Websockets, in CSV, JSON, or XML. Customers can use the extensive API support for exporting data to BI, CRM, and other marketing tools. Connectors are available for Google Analytics, Hubspot, MailChimp, Microsoft Dynamics, Mixpanel, Salesforce, and more. Admin interface allows for easy construction of policies which are also editable as code within the same window.

For customers using WSO2 Identity Server, their consumers have the ability to view, edit, export, and delete their profile data in a self-care app. WSO2 supports Kantara UMA 2.0 and Consent Receipt. Family management is not configurable but is on the roadmap. For IoT device identity integration, WSO2 supports OIDC and OAuth2 Device Flow Grant specifications but does not provide an explicit user interface for managing those identities.

WSO2's crypto functions use FIPS 140-2 components; Identity Server is ISO/IEC 15408 EAL2+ certified. Strong/MFA can be used by customer admins. WSO2 has a good reputation in IAM and is quickly expanding in the CIAM market as they add features. Areas where they have some missing functionality, such as mobile SDK and family management, are due to be addressed in the months ahead. WSO2 is a global company with an extensive support and partner network. Organizations that prefer open source integration solutions should consider WSO2 for their CIAM and Identity API security needs.

Security
Functionality
Interoperability
Usability
Deployment



Strengths

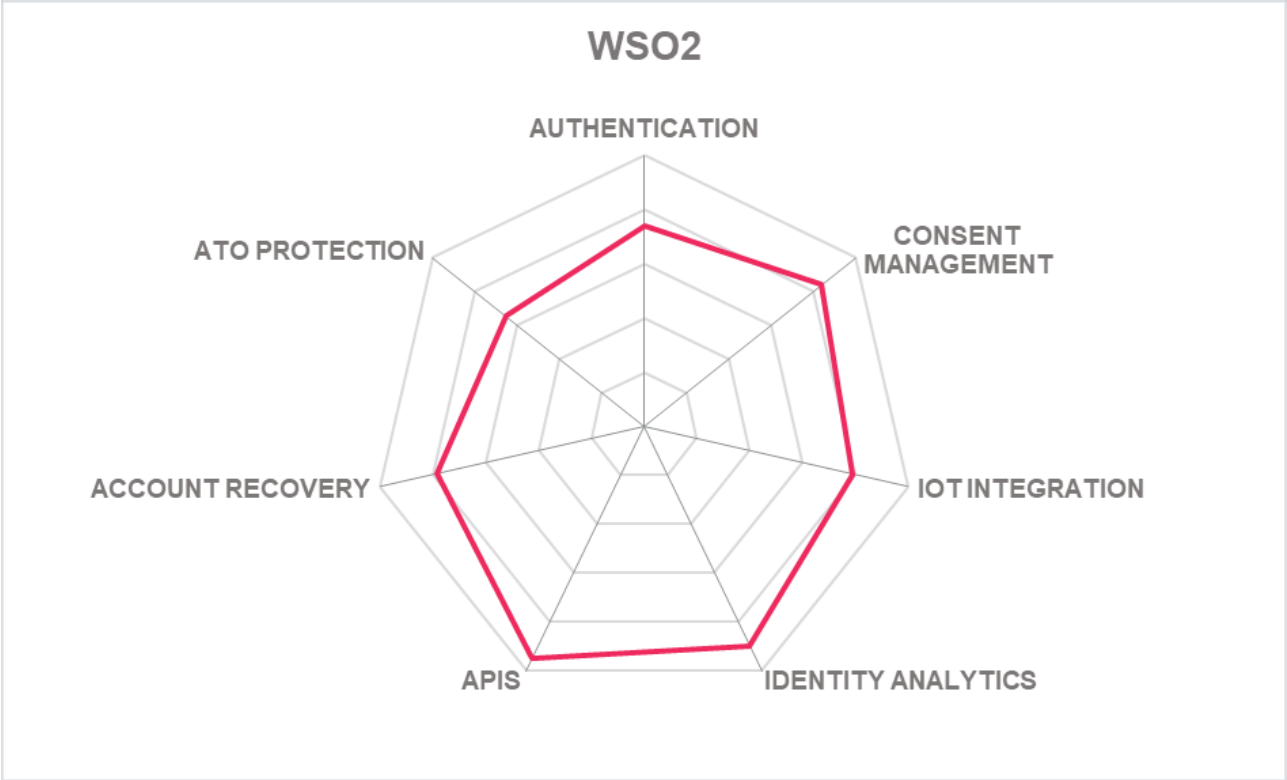
- Great support for IAM standards
- API first strategy facilitates integration with other IAM and security systems
- Good selection of authenticators
- High scalability
- Extensive global partner network

Challenges

- No built-in compromised credential intelligence but can be configured
- Mobile SDK in work
- No family management functions
- Late entrant to SaaS deployment model

Leader in





6 Vendors and Market Segments to watch

Aside from the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors but do not fully fit into the market segment of CIAM or are not yet mature enough to be considered in this evaluation. We provide short abstracts below on these vendors.

6.1 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. KuppingerCole will follow developments in Amazon Cognito.

Why worth watching: As the largest IaaS provider in the world, Amazon's identity services will be increasingly used to provide CIAM style experiences.

6.2 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-premise 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 can accept social logins including Facebook, Microsoft, LinkedIn, Twitter, etc. SAML and OAuth are supported for federation. Users can self-register or be provisioned via LDAP or SCIM. Risk factor evaluation and adaptive authentication are not possible within the product today.

Avatier provides API access for ITSM and SIEM integration. The product does federate with Salesforce and NetSuite SaaS. Detailed identity and marketing analytics are unavailable in this solution. Users can select

which attributes are shared from social logins at registration time but cannot indicate consent to additional usages. Moreover, users cannot delete their accounts and profiles. The product does not support family management. KuppingerCole monitors Avatier and information about their other IAM products is available in other reports.

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

6.3 AvocoSecure Trust Platform

AvocoSecure is a privately-owned UK company offering Cloud and CIAM services. The Avoco Trust Platform API is a toolkit providing extended ecosystem functionality to deliver multiple components, including IDPs, hubs, brokers, verification, and, blockchain. The solution is blockchain-agnostic and privacy enhanced. Trust Platform is not derived from traditional IAM, but rather was built to UK government security standards for high assurance verification of consumer identities. AvocoSecure partners offer customer profile storage in cloud or hybrid installations. Any of the components generated using the Avoco Trust Platform API are available either as a cloud-based service or can be directly integrated into customer's on-premise environments. It has a number of second factors available OOTB and also integrates to third party credential management services that offer biometrics. Risk-based authentication is managed using dynamic rules. It accepts federated login via SAML, OIDC, and OAuth. Avoco also now supports OpenID CIBA.

The Trust Platform can feed data to SIEM systems and Splunk. At present, there are no interfaces to external CRM, marketing, or Big Data style analytics programs. However, Splunk can be used for rudimentary identity and marketing analysis.

AvocoSecure provides privacy consent management functionality. Consumers must approve attributes for use from other networks, and they are prompted to re-accept when terms or conditions change. Consent and personal data/credentials can be managed using a consent interface as part of an account manager/life management platform/eWallet. Family management can be achieved via delegated administration model.

Why worth watching: The AvocoSecure Trust Platform is an interesting offering considering its consent management and identity verification service provider integration. As noted earlier in this report, identity proofing is a key component to fraud reduction and more CIAM solutions are adding such functionality.

6.4 cidaas

Widas ID was founded in Germany in 1997. They do custom development for Big Data and IoT applications as well as consulting for many large organizations in Germany. Widas has developed a flexible consumer authentication solution that supports email/phone/SMS OTP. cidaas has mobile apps and an SDK for

authentication and can do mobile push notifications. cidaas supports JWE, JWT, OAuth, OIDC, and SAML, and thus can accept social logins. cidaas interoperates with 3rd party authenticators, including Google Authenticator, and others which allow for utilization of built-in biometrics such as Android Fingerprint, iOS FaceID/Touch ID, and FIDO U2F. Voice recognition authentication is also possible.

Why worth watching: cidaas has a photo-based identity validation feature that identity providers can use to increase the identity assurance of consumers, business customers, and B2B customers at the time of registration. Having support for identity proofing in a consumer authentication solution solves increasingly complex business requirements and thus increases the value of the solution.

6.5 Fusion Auth

FusionAuth is single-tenant CIAM solution that can be deployed on-premises or in a private cloud. Its self-hosted option is free for unlimited users and offers mobile and web MFA, social login connections, brute force password attack detection, APIs and Webhooks, customizable consumer data storage, admin UI for managing users, and detailed user search and reporting capabilities. Managed cloud hosting, technical support, and custom development options are available.

Why worth watching: Fusion Auth has many core CIAM capabilities, particularly for authentication, and is likely to grow into a full-fledged CIAM offering.

6.6 Genetsis Group Dru-ID

Dru-ID is the CIAM offering from Genetsis Group, which is headquartered in Madrid. Their product, Dru-ID, is focused on identity relationship management for retail clients in the region. It features social media registration/logins/integration, identity and marketing analytics, and SSO to various applications.

Why worth watching: Few of the major CIAM vendors have made significant inroads in the Iberian Peninsula, which is a large market. There could be good opportunities for Dru-ID to grow and address the under-served Spanish language market.

6.7 Google Firebase

Firebase is a mobile app development platform that has a few CIAM features. Firebase allows app developers to manage users and groups, store user data, and provides some authentication options including Google login as well as other social logins. Admins can also use Google Analytics for identity and

marketing analyses.

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

6.8 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.

6.9 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.

Why worth watching: Miracl has a unique MFA capability that addresses 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.

6.10 Onegini

Netherlands-based Onegini supports a plethora of account types for initial registration, including: OpenID, Facebook, Google, Twitter, LinkedIn, Amazon, PayPal, Microsoft, Bank ID Norway and Sweden, IDIN Netherlands, DigID Netherlands, Ideal Netherlands, Buypass Norway, ID-Porten Norway, Commfides Norway, DNile Spain, Tupas, NemID Denmark, Telia Sweden, itsme Belgium, ReadID (NFC), ScanID, IBM Directory, Tivoli Directory, Ping Identity, Salesforce Identity, and SailPoint. For web authentication Onegini

Connect accepts username/password; social logins via Facebook, Google, LinkedIn, Twitter, etc.; iDIN, BankID, and DigID; Onegini Push mobile application; and federation over SAML and OAuth.

Why worth watching: Like several others, Onegini offers remote identity proofing options provided by integration with KYC providers IDNow, Mitek ID checker, Vermini, webID, and Yes solutions. This enables clients to perform stronger validation of official documents, such as passports, through the Onegini Connect service.

6.11 Privo ID

Privo offers a family consent-oriented consumer identity management solution. Privo, headquartered in the US, has focused on providing fine-grained parental consent for children's online activities, identity proofing service integration, and age and relationship verification. Identity profiling can be achieved by analysis of Credit Card Transactions, Partial SSNs, Driver's License Numbers, Employer IDs, Voice over Internet Protocol and Mobile Connect, Toll Free Customer Service, and In Person vetting. Privo supports many family relationship roles, including Child, Teen, Student, Adult, Parent, and Teacher.

They provide the technical means for clients to comply with US COPPA as well as EU GDPR. Their customer base includes companies in the gaming, education, and toy spaces. Mobile apps and an SDK for Android and iOS are in development. Their solution is cloud-based, and supports SSO via OAuth, OIDC, and SAML. Privo is a certified OIX provider and a member of the Minors Trust Framework.

Why worth watching: Privo pioneered support for family management use cases for US COPPA and thus has experience with advanced consent management scenarios.

6.12 Signicat Digital Identity Platform

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. Signicat's services are SaaS, hosted in their own facilities, AWS, and Azure. They employ a per-login/session/transaction cost model. Their services are ISO 27001 and SSAE 18 SOC 2 Type 2 certified.

Signicat accepts Android and iOS biometrics, email/phone/SMS OTP, FIDO 2, and Aegis/Authy/DeepNet/Duo/Google/LastPass/Microsoft/Okta/OneSpan/SaaS/Pass/SafeNet Authenticators using a generic TOTP client. Signicat can also work with 30 different eIDAS compliant national IDs. JWT, OAuth, OIDC, and SAML are available for federation. All expected methods for account recovery are present.

Why worth watching: 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.

7 Related Research

[Advisory Note: Identity & Access Management/Governance Blueprint - 70839](#)
[Advisory Note: Secure your Cloud against Industrial Espionage - 70997](#)
[Buyer's Compass: Consumer Identity and Access Management Solutions - 80111](#)
[Executive View: Auth0 Platform - 80329](#)
[Executive View: iWelcome IDaaS and CIAM - 80328](#)
[Executive View: NRI Secure Technologies: Uni-ID Libra 2.4 - 80161](#)
[Executive View: Onegini Connect - 80168](#)
[Executive View: Pirean Consumer IAM Platform - 70223](#)
[Executive View: Salesforce Identity - 70813](#)
[Executive View: Ubisecure Identity Platform - 79072](#)
[Leadership Brief: 5 Steps to Consumer Identity and Access Management - 72549](#)
[Leadership Compass: CIAM Platforms - 79059](#)
[Leadership Compass: Consumer Authentication – 80061](#)
[Leadership Compass: Identity API Platforms - 79012](#)
[Whitepaper: ForgeRock Identity Platform Capabilities for Authentication - 79080](#)
[Whitepaper: Ping Identity Solutions for Customer Identity and Access Management - 70289](#)

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 in that market segment. It is the compass which assists you in identifying the vendors and products/services in a market segment 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

As part of our evaluation of products in this Leadership Compass, we look at four leadership types:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market segment. These products deliver to a large extent what 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 become an Overall Leader by being above average in all areas.

For every leadership type, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular 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 products which lag behind 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 the 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 a given 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, as well as other sources.

Product rating

KuppingerCole as an analyst company regularly conducts evaluations of 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 of 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**
- **Integration**
- **Interoperability**
- **Usability**

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole Analysts IT Model. Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are

understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

Functionality – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets, they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

Integration – integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability – interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs.

Usability – accessibility refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, we have strong expectations overall regarding well-integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

We focus on security, functionality, integration, 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 potential breakdown for any IT endeavor.

- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product security, functionality, integration, interoperability, and usability which the vendor has provided are of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

Vendor rating

For vendors, additional ratings are used as part of the vendor evaluation. The specific areas we rate for vendors are:

- **Innovativeness**
- **Market position**
- **Financial strength**
- **Ecosystem**

Innovativeness – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the market segment(s) the vendor is in. 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. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. 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 overall markets in which a vendor is active, e.g. 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 become an acquisition target, with massive risks for the execution of the vendor's roadmap.

Ecosystem – this dimension looks at the ecosystem of the vendor. 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 – beyond the Leadership rating in the various categories – a separate rating with five different levels. These levels are

Strong positive

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

Positive

Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. 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. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., 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.
- **Denial of participation:** Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular 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 of 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

Figure 1: The Overall Leadership rating for the CIAM market segment

Figure 2: Product Leaders in the CIAM market segment

Figure 3: Innovation Leaders in the CIAM market segment

Figure 4: Market Leaders in the CIAM market segment

Figure 5: The Market/Product Matrix.

Figure 6: The Product/Innovation Matrix.

Figure 7: The Innovation/Market Matrix

Copyright

©2020 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks[™] or registered[®] trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

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 back 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.