KuppingerCole Report

LEADERSHIP COMPASS

by John Tolbert December 2018

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
December 2018

Leadership Compass
CIAM Platforms
By KuppingerCole

Content

Content of Tables

Content of Figures

Related Research

Advisory Note: Identity & Access Management/Governance Blueprint - 70839

Advisory Note: IAM Predictions and Recommendations 2014-2018 - 71120

Advisory Note: Secure your Cloud against Industrial Espionage - 70997

Advisory Note: Cloud IAM: More than just Single Sign-On to Cloud Applications - 71031

Advisory Note: The new ABC for IT: Agile Businesses – Connected - 70998

Advisory Note: Connected Enterprise Step-by-step - 70999

Executive View: Cloud Standards Cross Reference - 71124

Executive View: EU Guidelines for Cloud Service Level Agreements - 71154

Executive View: Executive View Microsoft Azure RMS - 70976

Executive View: PingFederate 7 - 70801

Executive View: Salesforce Platform as a Service – Security and Assurance - 70751

Executive View: Exostar Services for Life Sciences - 70878

Executive View: PingOne® - 70870

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 70960

Leadership Compass: Access Management and Federation - 70790

Leadership Compass: Access Governance - 70735

Product Report: Microsoft Azure Active Directory - 70977

Scenario: Understanding Cloud Security - 70321

Scenario: Understanding Cloud Computing - 70157

Scenario: Understanding Identity and Access Management - 70129

Vendor Report: SecureAuth Corporation - 70260

1 Introduction

Consumer Identity and Access Management (CIAM) is a sub-genre of traditional Identity and Access Management (IAM) that has emerged in the last few years to meet evolving business requirements. 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 goes beyond 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 beginning to be 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. Having IAM systems dedicated to hosting consumer identities and their associated profiles is a good first step toward KYC.

Support for self-registration and social network logins is now nearly 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. We expect to see more changes and 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 this 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 growing, with some 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-consumer (B2C). 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.

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. The major players in the CIAM segment are covered within this KuppingerCole Leadership Compass. This Leadership Compass will examine solutions that are available for both on-premise and cloud-based deployment.

Other 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. KuppingerCole is also producing a Leadership Compass focuses on Identity API platforms.

In this report we consider three major categories of CIAM products and services: the all-in-one turn-key solutions; solutions which need to be installed, configured, and perhaps extended with customization; and those which may require extensive assembly, integration, and some coding.

The three genres of CIAM:

- **Turn-key CIAM:** Organizations deploying CIAM solutions often have markedly different requirements. Some may already be embracing the cloud and mostly utilize SaaS solutions. Generally, these organizations have small IT staffs, preferring the "outsourced" approach. For these kinds of companies, a turn-key SaaS-based CIAM solution would work best. It fits with the existing architecture, whether explicit or not, and it's highly unlikely that a CIO would hire a staff just to manage a CIAM system. Thus, these solutions don't usually require a lot of effort by IT staff to deploy and maintain. Turn-key CIAMs often include lots of marketing analytics capabilities within the platform, which can be accessed and extended by customer marketing teams. Such packaged solutions may offer less flexibility from an IT standpoint, but function well for many organizations.
- **SysAdmin CIAM:** Other organizations have adequate IT staffs and their own data centers. The choice for approach to CIAM can become more difficult in this case. If the organization has a cloud migration strategy, it may make sense to start all new projects, including CIAM as SaaS. However, if they have enterprise IAM, there may already be some mixing of employee and customer data. Some companies decide to add CIAM as a new instance of their enterprise IAM, if their enterprise IAM has sufficient consumer-facing features. Others may have specific requirements, often around authenticator types supported or intelligence-to-risk-engine integration that are best achieved with a more configurable CIAM solution. This style of CIAM solution requires more expertise from system administrators, since these systems generally run on-premises or in IaaS. In many cases, marketing and identity analytics reports may be more basic within the solution, but accessible by 3rd-party analytics tools.
- **Dev-centric CIAM:** Lastly, some organizations may want a completely customizable CIAM solution. Some may have a predilection for open-source and build their own from components. Others only need limited CIAM functionality, such as wrapping a single

consumer-facing application with a CIAM layer. In these cases, SaaS and fully packaged CIAM solutions may not be the best fit. Dev-centric CIAMs allow customers to build a modular solution around existing infrastructure or services, without having to buy more features and functionality than needed. As the name implies, in order to successfully deploy a Dev-centric CIAM system, knowledgeable developers are required and will have the most work to do.

In Chapter 5, the differences in these categories are represented in the spider charts as "DIY". Turn-key solutions have low DIY values, whereas SysAdmin or Dev-centric CIAM products have higher DIY ratings. Each vendor entry in Chapter 5 will have more information about vendor subjects.

1.2 Delivery models

In the CIAM market, solutions are offered as SaaS, PaaS, and for on-premise or in-IaaS deployment. Pure-play SaaS solutions are 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. For managed services or PaaS, the licensing costs can be per instance, or per managed identity. For on-premise deployments, licensing costs can be measured in a variety of ways, such as per-user, per-server, or per transaction.

1.3 Required 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: SmartCards, USB tokens, OTP, mobile biometrics, mobile push apps, etc.
- Risk adaptive authentication: Evaluation of runtime environmental parameters, user behavioral analytics, and fraud/threat intelligence to match the appropriate authentication mechanism to the level of business risk or as required by regulations
- Cyber threat and/or fraud intelligence: Consume internal or external cyber threat or fraud information, such as known bad domains, compromised credentials, accounts suspected of fraud, fraud patterns, botnet behavior, etc., for the purpose of evaluation by the risk engine to choose the right authentication mechanisms and permit/deny access or transaction completion.
- Business intelligence: Transform data about user activities into information for marketers
- Privacy and consent management: Explicit user consent must be received for the use of their information
- Enhanced user experience: White-labeled CIAM solutions allow seamless branding, and self-registration and social 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.

To a degree, CIAM is an outgrowth of yesterday's IAM systems. Many organizations are feeling and responding to the pressure to provide a better user experience and return more on the investment on their online presences and user databases. To do so, they must capture more identity data from users, with their outright consent, and then transform it into meaningful information to increase consumer satisfaction and improve their bottom lines.

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 also considered a series of specific features. These functional areas, which are reflected in the spider charts for each company in Chapter 5 include:

Authentication options	Social logins; multi-factor authentication (MFA), SDKs, etc.
Consent management	Facilities within the UI to allow consumers to unambiguously opt-in to services and 3rd party usage of their data. 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 IoT devices by associating consumer identity with device identity. The use of OAuth2 Device Flow specification is a good means to achieve this
Internal analytics	Transforming information for marketing campaigns, creating special offers, encouraging brand loyalty. Includes identity analytics features, such as the ability to generate and customize reports on user actions, as well as representing aggregated activity on enterprise dashboards in real-time. This measure describes built-in capabilities within the CIAM solution, as contrasted with those products and services which choose to open APIs for tenants/customers to acquire and transform this data outside the CIAM solution.
APIs	APIs are increasingly available in CIAM solutions to provide means for 3rd party application to perform identity analytics, marketing analytics, security integration, provisioning/de-provisioning, consent auditing, and more

Risk Analysis	Evaluation of user attributes, environmental factors, fraud/threat intelligence, and other information to determine authentication and authorization levels required per transaction
SSO	Solutions use standards such as SAML, OpenId, OIDC, and OAuth for identity federation amongst a customer's websites. It can also include proprietary connectors for internally hosted applications and SaaS applications, such as CRM, Marketing Automation, etc.
DIY	(Do-It-Yourself): Some of the solutions considered here are turnkey, meaning customers subscribe to a CIAM SaaS and most administrative details are handled by the vendor. Little or no software development must be done by the customers in these cases. Other solutions require significant amounts of administrative configuration and/or programming to integrate the CIAM solution with existing infrastructure. Some organizations need the ability to customize, while others do not need customization and only want to create a stand-alone CIAM system. This category represents the level of customizability and corresponding effort to deploy the system. For organizations that need lots of customization, a high score in this category is desired. Both SysAdmin and Dev-centric CIAM categories have high DIY scores. Those looking for turnkey solutions with minimal effort to stand up should look for the low scores in this category.

Each of the categories above will be considered in the product evaluations below. 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 new standards such as GSMA Mobile Connect, Kantara Initiative UMA (User Managed Access), 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 and consistent set of REST-based APIs for identity, marketing, and security analytics.
- Advanced support for authentication mechanisms, especially mobile biometrics.
- Mobile app integration capabilities (SDKs).
- Integration with national e-IDs and passports.

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 only based on the comparison provided by 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

This year we find that the Leader section is expanding. Janrain, SAP, and Auth0 lead the pack, showing strong ratings in all Leadership categories. These vendors provide comprehensive CIAM solutions to a large share of the market.

ForgeRock, IBM, Login Radius, Ping Identity, and Salesforce are also Overall Leaders in this survey.

It is important to note that each one of Overall Leaders offers high quality customer identity and engagement solutions. However, their methodologies and delivery methods are quite different. IBM, Janrain, Login Radius, SAP, and Salesforce are cloud-delivered, and are largely turn-key services, and tend to show a lower "DIY" value. Auth0, ForgeRock, and PingIdentity offer highly configurable and customizable CIAM products that require more administration and development from their customers. Accordingly, these vendors have high ratings for "DIY" in the spider charts. Auth0 and Ping Identity allow their customers to choose where and how to deploy their products. That these vendors are very successful even though they have taken different approaches to product/service design and implementation shows that there is adequate room in the market for CIAM solution variety.

In the Challenger segment, iWelcome, Microsoft, and Okta are near the top. Here again we see that each of these companies has taken a different track in developing CIAM solutions. iWelcome has excellent consent management capabilities to help EU customers comply with GDPR. Microsoft leverages their strong IAM base to provide robust, scalable, and secure solutions for their customers. Rounding out the Challenger block is Cloudentity, EmpowerID, Pirean, Widas ID, and WSO2. For the most part, these companies rate highly in the DIY category. EmpowerID has a CIAM offering derived from high security IAM technologies which may make them a good fit for customers with these types of requirements. Cloudentity is a relatively new entrant in CIAM but has a strong debut in the Overall Leader comparison due to their innovative features. Pirean and Widas ID each have some innovative features but are more regionally focused. WSO2 offers a support model for their open source IAM product and all the related open source connectors.

In the Follower segment, we see CoffeeBean and NRI. Each have good solutions for their customers but have somewhat limited functionality and small market share and geographic coverage

Overall Leaders are (in alphabetical order):

- Auth0
- ForgeRock
- IBM
- Janrain
- Login Radius
- Ping Identity
- Salesforce
- SAP

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

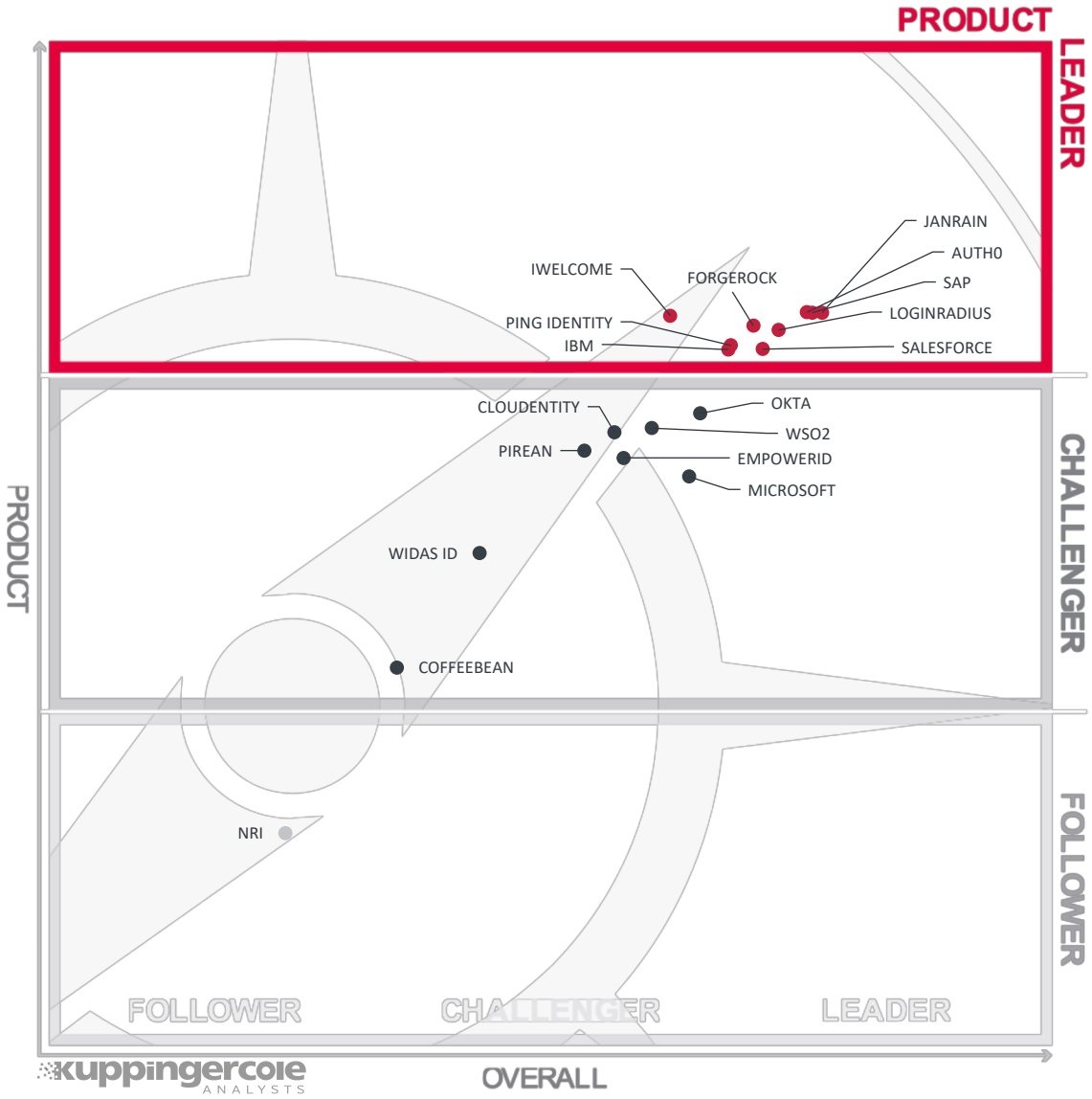


Figure 2: Product Leaders in the CIAM market segment

Product Leadership, or in some cases Service Leadership, is where we examine the functional strength and completeness of products. Auth0, Janrain, and SAP are found at the upper right space, indicating that each has the power to satisfy many business requirements in the CIAM arena. Auth0 offers a full set of CIAM capabilities that can be integrated with customers' existing IT infrastructure, including legacy applications. Auth0 has a high DIY value. Janrain and SAP are Turn-key SaaS solutions, designed for quick and easy initialization and maintenance. All three offer a rich set of CIAM features. Also, at the top, just slightly left, is iWelcome. iWelcome's platform continues to excel in the GDPR era with fine-grained consent options and detailed auditing. ForgeRock, IBM, Login Radius, Ping Identity, and Salesforce are

also found in the Product Leader section. ForgeRock Identity Platform, while not offered as SaaS yet, can be run in IaaS, and offers much flexibility to customers. IBM also has significant functionality in IoT identity integration. Login Radius has offers clients a Turn-key SaaS solution. Ping Identity's CIAM solution suite is available for either on-premise or cloud deployment and offers customers excellent standards-based support to achieve their objectives. Salesforce provides rich marketing functionality via Turn-key SaaS delivery as well as extensive IoT identity integration.

The number of Product Leaders is growing year-over-year, as is the number of entrants into the market.

Many companies are clustered together at the top of the Challenger range: Cloudentity, EmpowerID, Microsoft, Okta, Pirean, and WSO2. Cloudentity's position is due to their microservices architecture and licensing model, as well as the rich feature set available in the product. EmpowerID has enterprise-grade security and easy-to-deploy workflows for customization. IBM and Microsoft have strong built-in threat protection available for the customers' consumers. Okta's strategy of pursuing security certifications is a boon for their customers. Pirean has a good risk engine to help protect their consumers. WSO2's open source approach allows for extensive customization.

Following them, we see Widas ID, whose cidaas product covers a large subset of CIAM product/service capabilities. CoffeeBean is adding functionality to their baseline, which has focused on marketing analytics and mobile authentication.

In the Follower segment, we find NRI Secure with a basic CIAM product, possessing fewer baseline features. NRI is also operating in a region which has less stringent privacy compliance requirements.

Product Leaders (in alphabetical order):

- Auth0
- ForgeRock
- IBM
- iWelcome
- Janrain
- Login Radius
- Ping Identity
- Salesforce
- SAP

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 cutting-edge features, while maintaining compatibility with previous versions.

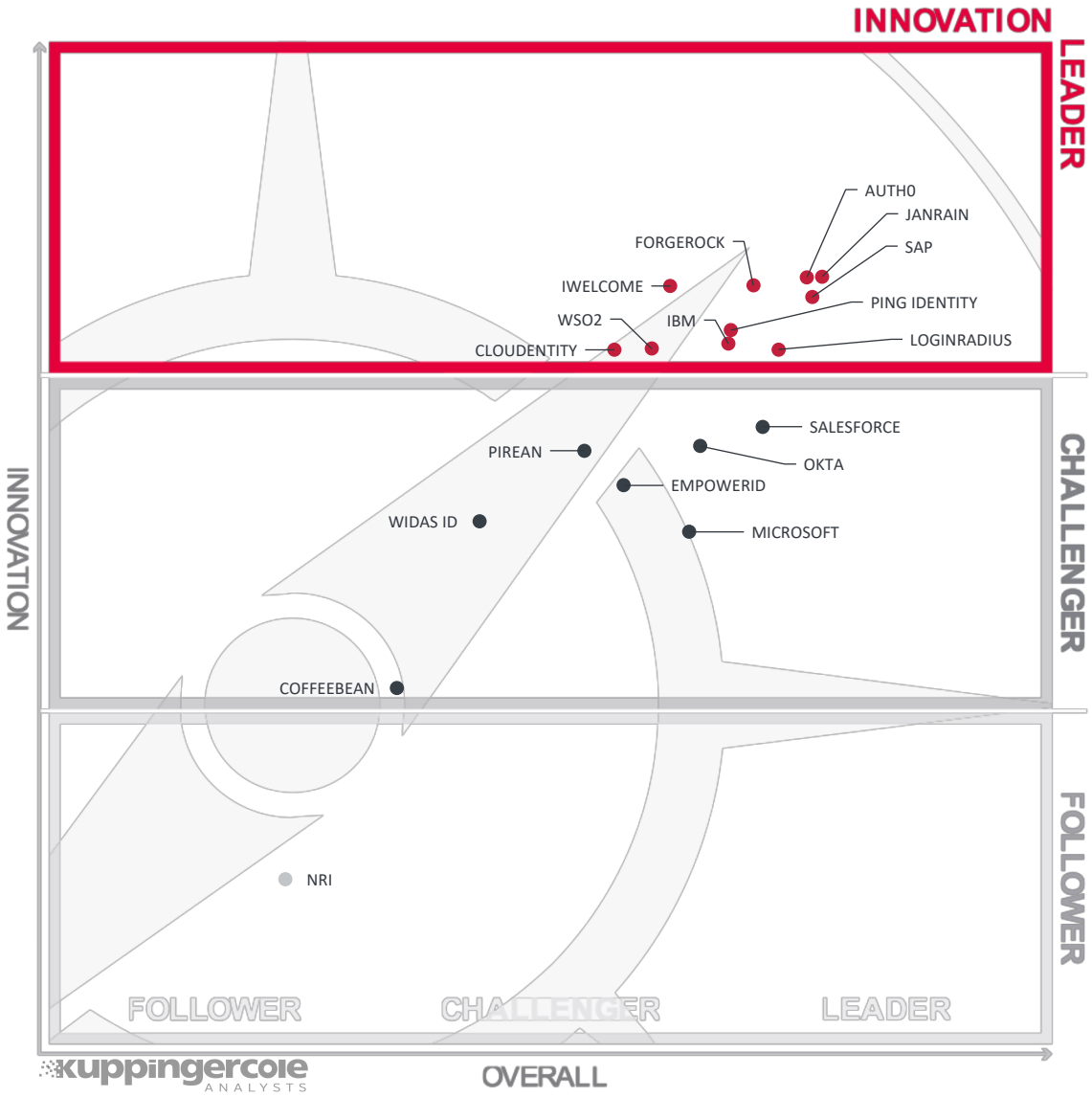


Figure 3: Innovation Leaders in the CIAM market segment

Many companies are in the Innovation Leadership bracket this time. The field is rapidly maturing, and business requirements are driving vendors to come up with new features to meet these requests. In the uppermost strata, we find Auth0, ForgeRock, iWelcome, Janrain, and SAP. Cloudentity, IBM, Login Radius, Ping Identity, and WSO2 are also Innovation Leaders. Again, what is most remarkable in the results is the significant variation in design, deployment models supported, and even the origins of the CIAM strategies

that these vendors have. Thus, each of these companies is rapidly innovating, but the innovations are in some cases manifested as different kinds of features, depending on the target markets the companies are pursuing. The top innovative features include API access, authenticator selections, consent-per-purpose management, consumer account protection service integration, IoT device identity integration, micros-services architecture, and support for standards such as FIDO and Kantara's UMA.

In the top half of the Challenger segment, we see EmpowerID, Microsoft, Okta, Pirean, and Salesforce. Each of these vendors has made significant enhancements to their products that address real business needs. Widas ID is also in the Challenger block. Widas ID is new to the market and are building in more CIAM baseline functionality; thus, we expect them to improve in the months ahead. CoffeeBean has been focused on the marketing analytics component, but has recently passed FIDO certification and offers U2F/UAF/2.0 clients and servers.

NRI Secure appears in the Follower section. NRI has been building for the Japanese market, which has different requirements.

Innovation Leaders (in alphabetical order):

- Auth0
- Cloudentity
- ForgeRock
- IBM
- iWelcome
- Janrain
- Login Radius
- Ping Identity
- 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, 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.

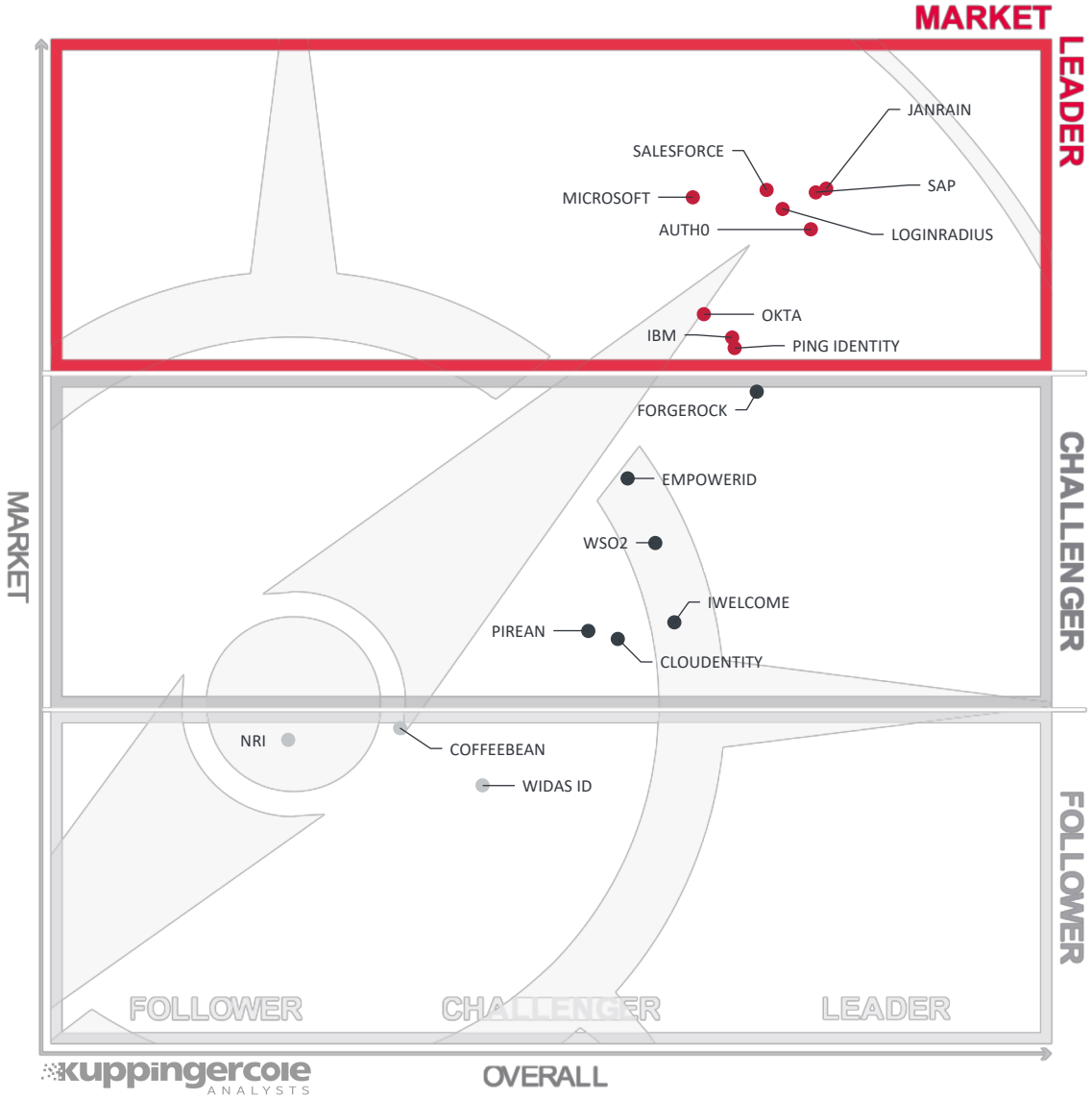


Figure 4: Market Leaders in the CIAM market segment

The CIAM market is growing, and solution providers have been actively acquiring more customers since the last report. In this iteration of the report, we see a cluster of high-performing Market Leaders at the top (in alphabetical order): Auth0, Janrain, Login Radius, Microsoft, Salesforce, and SAP. Notably, five of the six top Market Leaders offer turn-key services, while Auth0 specializes in identity API integration services to the application developer.

IBM, Ping Identity, and Okta are also Market Leaders. Each of these companies is well-established and has a good reputation in traditional IAM and IDaaS, so we are not surprised by their strong position in this market.

We find ForgeRock at the top of the Challenger segment. ForgeRock continues to grow steadily. EmpowerID appears in the mid-range of the Challenger block, with many North American and increasingly some EU customers. Cloudentity, iWelcome, Pirean, and WSO2 make up the rest of the Challenger block. Cloudentity is relatively new to the CIAM game but makes a strong appearance. iWelcome and Pirean are doing well in their geographically localized markets. WSO2 is growing rapidly globally with their open source products plus support model. Pirean's acquisition by Exostar makes for a good debut on the Market Leadership chart.

Finally, we see CoffeeBean, NRI, and Widas ID in the Followers section. CoffeeBean has concentrated on the South American market, particularly Brazil, but is expanding in Germany. Widas ID is young in the CIAM market, and has been somewhat limited to the DACH region. Each of these companies' products fill a niche and are interesting to certain customers.

Market Leaders (in alphabetical order):

- Auth0
- IBM
- Janrain
- Login Radius
- Microsoft
- Okta
- Ping Identity
- Salesforce
- SAP

3 Correlated View

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

3.1 The Market/Product Matrix

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

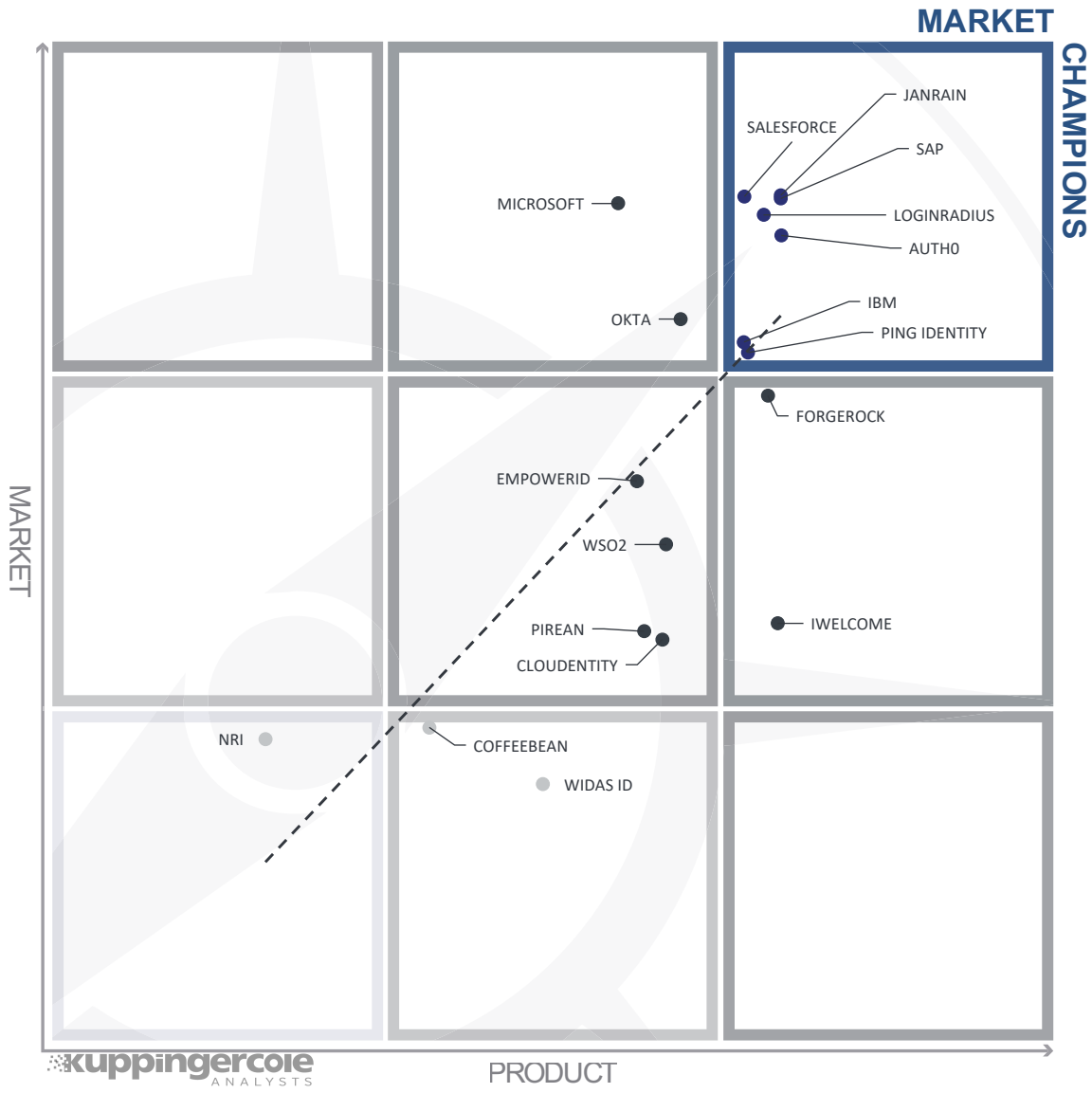


Figure 5: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

In this comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of "overperforming" in the market. It comes as no surprise that these are mainly the very large vendors, while vendors below the line frequently are innovative but focused on specific regions.

The matrix shows a picture that is typical for evolving market segments, with a rather broad distribution of the various players across the quadrants and a weak correlation between Market Leadership and Product Leadership.

In the upper right box, we find Auth0, IBM, Janrain, Login Radius, Ping Identity, Salesforce, and SAP. These vendors are leading in both the product and market ratings.

Below these, we find ForgeRock and iWelcome, which are product leaders but not (yet) in the Market Leader's segment.

On the other hand, in the center top box, we see Microsoft, and Okta, having a significant market share while not being counted amongst the Product Leaders.

In the center of the graphic but below the line, we find Cloudentity, EmpowerID, Pirean, and WSO2. These all have respectable positions in both the Product Leadership and Market Leadership ratings and thus are interesting options to the leading vendors.

CoffeeBean and Widas ID are in the lower center, while NRI is in the lower left. These have smaller market shares and products that may be concentrated on specific feature sets for targeted customers.

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 few exceptions. This distribution and correlation is tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

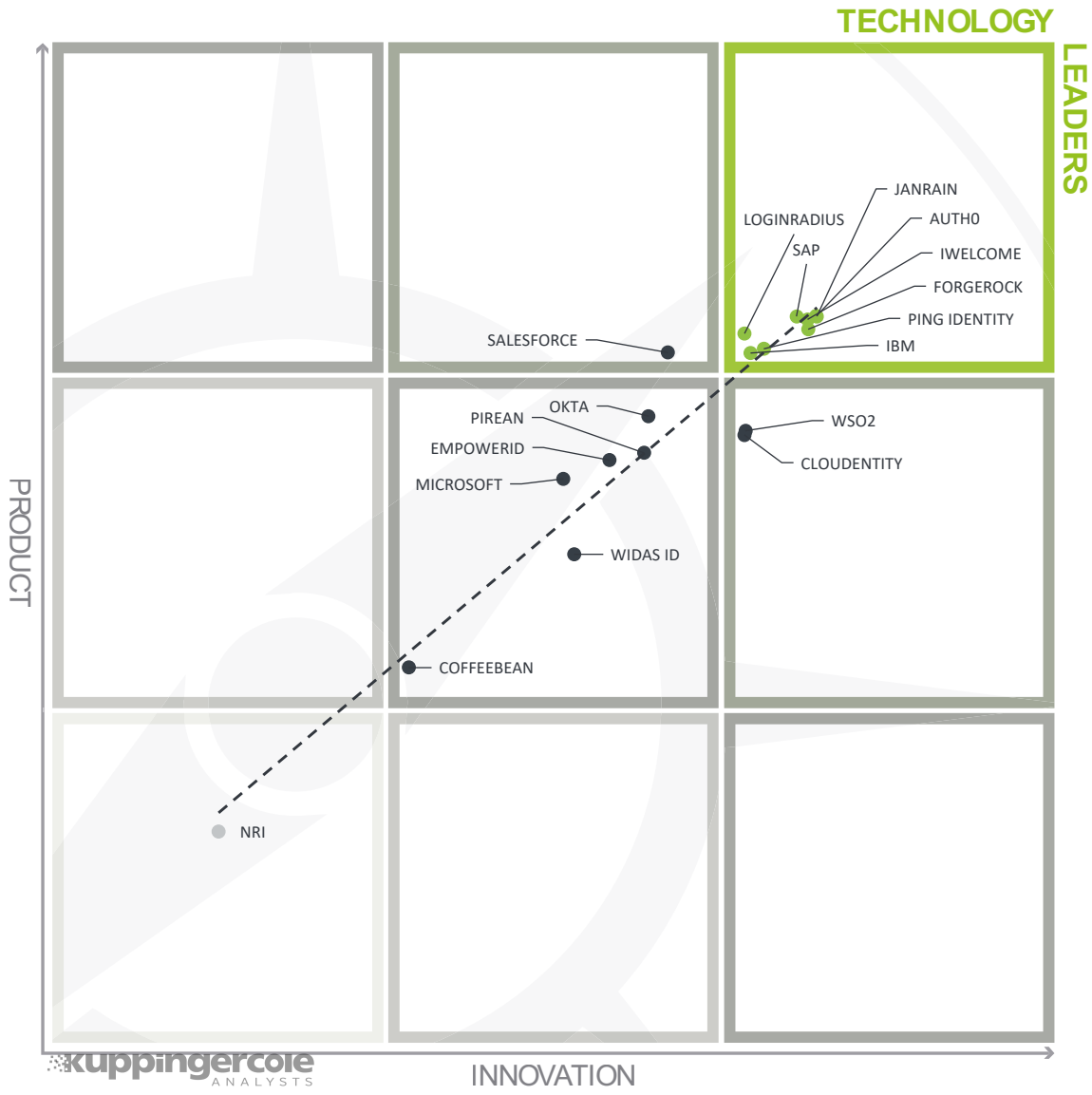


Figure 6: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Like last year, this chart shows a main sequence progression along the line, which means the solutions have a balanced ratio of product capabilities and innovation. Unlike last year, many more vendors are in the top right including Auth0, ForgeRock, IBM, iWelcome, Janrain, Login Radius, Ping Identity, and SAP are the technology leaders, with many advanced features.

Cloudentity and WSO2 are just below the Technology Leaders. In the top center, we find Salesforce, but still close to the median.

Many vendor products reside in the center of the chart: CoffeeBean, EmpowerID, Microsoft, Okta, Pirean, and Widas ID.

In the lower left sector, we find NRI Secure, who will be adding functionality to their product.

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, they might also fail, especially in the case of smaller vendors.

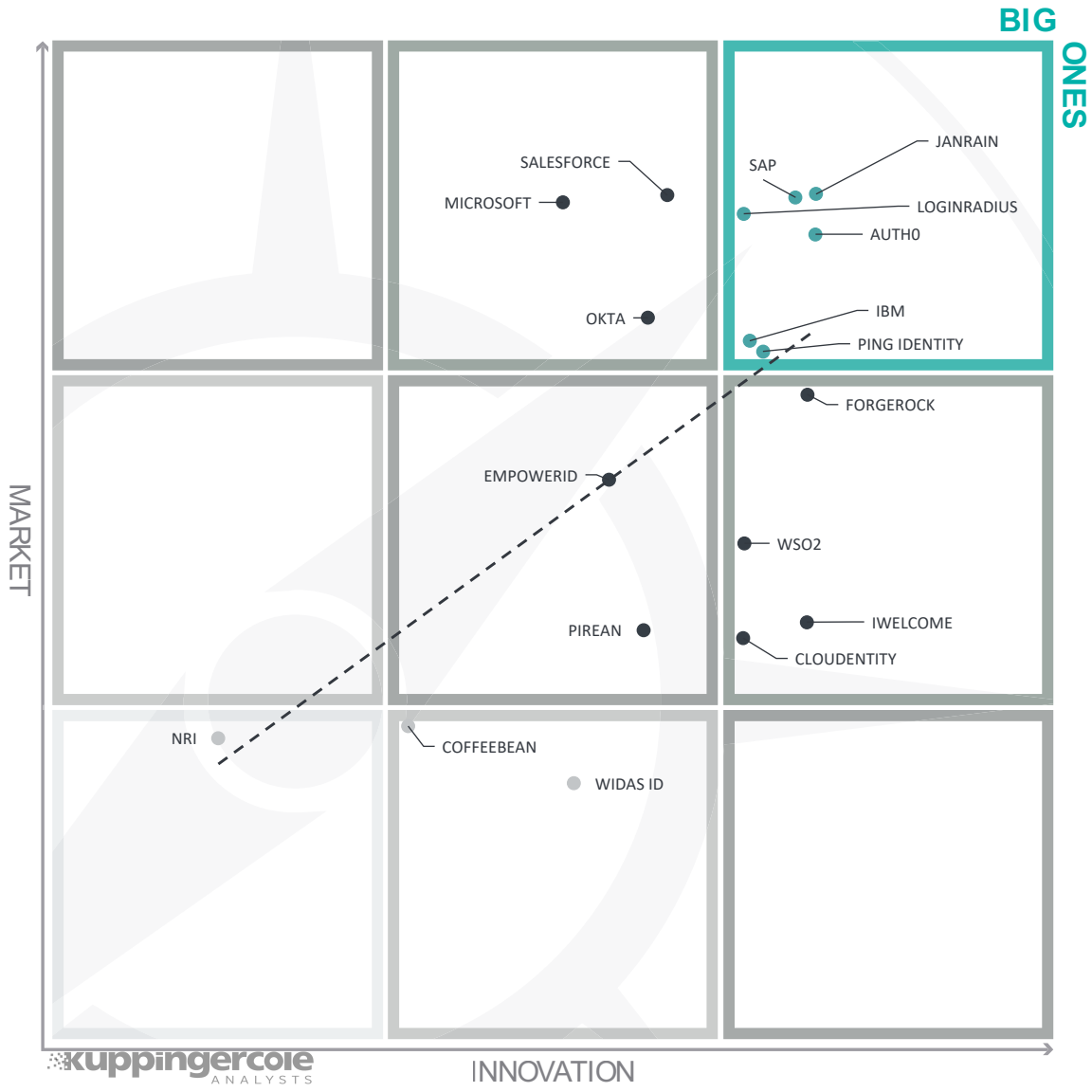


Figure 7: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relatively weak position in the Innovation Leadership rating; while vendors below the line show an ability to innovate, and thus the biggest potential for improving their market position.

Auth0, IBM, Janrain, Login Radius, Ping Identity, and SAP occupy the top right sector, having both an excellent position in the market and presenting innovative capabilities to their customers. Cloudentity, ForgeRock, iWelcome, and WSO2 appear on the leftmost side also, indicating very strong innovation, but having less market share.

Microsoft, Okta, and Salesforce are also on top of the market, and are distributed across the top center box according to their relative innovation.

This time few vendors are found in the center, only EmpowerID and Pirean. Both have more innovativeness than their corresponding position for market share, which indicates excellent room for growth for them.

CoffeeBean and Widas ID are found in the lower center, offering some innovative features but not yet capturing a large share of the market. In the lower left, NRI has the potential for additional product evolution and to capture more market share.

4 Products and Vendors at a glance

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

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	Integration	Interoperability	Usability
Auth0	strong positive	strong positive	strong positive	positive	positive
Cloudentity	strong positive	positive	strong positive	strong positive	positive
Coffeebean	neutral	positive	positive	neutral	neutral
EmpowerID	positive	positive	positive	positive	positive
Forgerock	strong positive	strong positive	positive	strong positive	positive
IBM	strong positive	strong positive	strong positive	strong positive	positive
iWelcome	strong positive	strong positive	positive	strong positive	strong positive
Janrain	strong positive	strong positive	strong positive	positive	strong positive
LoginRadius	positive	strong positive	strong positive	strong positive	positive
Microsoft	positive	neutral	positive	positive	neutral
NRI	neutral	neutral	positive	weak	weak
Okta	strong positive	positive	strong positive	strong positive	positive
Ping Identity	strong positive	positive	strong positive	strong positive	positive
Pirean	strong positive	positive	positive	strong positive	positive
Salesforce	positive	positive	strong positive	strong positive	positive
SAP	positive	strong positive	strong positive	positive	positive
Widas ID	positive	positive	positive	positive	positive
WSO2	positive	positive	positive	strong positive	neutral

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Auth0	strong positive	strong positive	positive	positive
Cloudentity	strong positive	weak	weak	weak
Coffeebean	neutral	weak	weak	weak
EmpowerID	strong positive	positive	positive	neutral
ForgeRock	strong positive	positive	positive	strong positive
IBM	positive	strong positive	strong positive	strong positive
iWelcome	strong positive	neutral	neutral	neutral
Janrain	strong positive	strong positive	positive	strong positive
Login Radius	strong positive	strong positive	positive	positive
Microsoft	positive	strong positive	strong positive	strong positive
NRI	weak	weak	positive	weak
Okta	positive	strong positive	strong positive	strong positive
Ping Identity	strong positive	strong positive	positive	positive
Pirean	positive	neutral	positive	neutral
Salesforce	positive	strong positive	strong positive	strong positive
SAP	strong positive	strong positive	strong positive	strong positive
Widas ID	neutral	weak	weak	weak
WSO2	strong positive	neutral	neutral	positive

Table 2: Comparative overview of the ratings for vendors

Table 2 requires some additional explanation regarding the “critical” rating.

In Innovativeness, this rating is applied if vendors provide none or very few of the more advanced features we have been looking for in that analysis, like support for multi-tenancy, shopping cart approaches for requesting access, and others.

These ratings are applied for Market Position in the case of vendors which have a very limited visibility outside of regional markets like France or Germany or even within these markets. Usually the number of existing customers is also limited in these cases.

In Financial Strength, this rating applies in case of a lack of information about financial strength or for vendors with a very limited customer base, but is also based on some other criteria. This doesn’t imply that the vendor is in a critical financial situation; however, the potential for massive investments for quick growth appears to be limited. On the other hand, it’s also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding Ecosystem applies to vendors which have no or a very limited ecosystem with respect to numbers and regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that growth and successful market entry of companies into a market segment relies on strong partnerships.

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.

5.1 Auth0

Bellevue, WA based Auth0 is a rapidly growing CIAM and B2E IAM solution provider. Since being founded in 2013, they have been pioneering API-driven identity services. Auth0 targets developers 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. Their solutions can run on-premise or in the cloud, and they offer a hosted service. Auth0 licensing is based on active users per month.

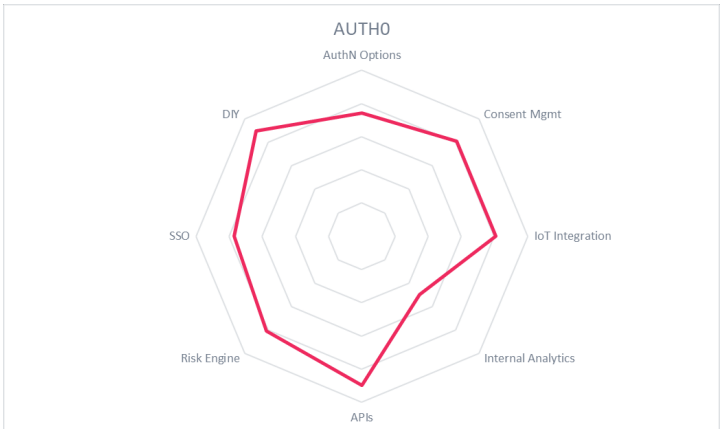
Strengths	Challenges
• API-driven identity services • Code snippets for copy-and-paste CIAM services • Developer-focused • Rapid deployment of CIAM functionality	• Requires some coding expertise • Does not support family management • Mobile apps don't use Global Platform SE/TEE

Table 3: Auth0's major strengths and challenges

Auth0 supports Duo, FIDO U2F, Google Authenticator, mobile apps and push notifications, mobile biometrics, OIDC, OTP, SAML, social logins, and Yubikeys as authentication methods. Customer administrators can use MFA and set up delegated or role-based administration. Users can be provisioned in by LDAP but not SCIM. Brute Force Password protection is an elective service that Auth0 provides to avert brute force password guessing attacks. This mechanism temporarily blocks the offender's IP address after a configurable number of incorrect guesses. Auth0's Breached Password Usage Protection prevents potential credential misuse by blocking users from attempting to resources using known compromised credentials. Auth0 compiles and scrubs compromised credential intelligence.

Some marketing and identity analytics reports are available within the solution. All system generated data can be pulled through APIs analyzed via 3rd-party data analytics tools.

Auth0 offers GDPR-ready consent management and supports both UMA and Consent Receipt. It interoperates with SIEMs, directory services, and many SaaS apps. For IoT devices, Auth0 supports OAuth2 Device Flow.



Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	positive

Table 4: Auth0's rating

Auth0 is a well-funded, high-revenue startup experiencing enormous growth. They identified a previously untapped segment in CIAM: developers. They emphasize providing all CIAM/IAM functionality through well-documented APIs. Auth0's successful business model challenges traditional IAM and CIAM delivery models. Auth0 is a strong contender in the CIAM space, especially for organizations that need quick-to-deploy CIAM solutions and those that have programming expertise alongside major consumer-facing applications should strongly consider Auth0 when doing RFPs.

5.2 Cloudentity

Cloudentity is headquartered in Seattle. In 2014, Cloudentity parlayed their IAM expertise from Syntegrity into a full-featured CIAM and IDaaS solution. Their approach is cloud-first and a defining goal is scalability; thus, their offering is based on micro-services. 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 or in the cloud, and they offer a hosted service. Cloudentity has licensing options based on the number of micro-services used, rather than per-user.

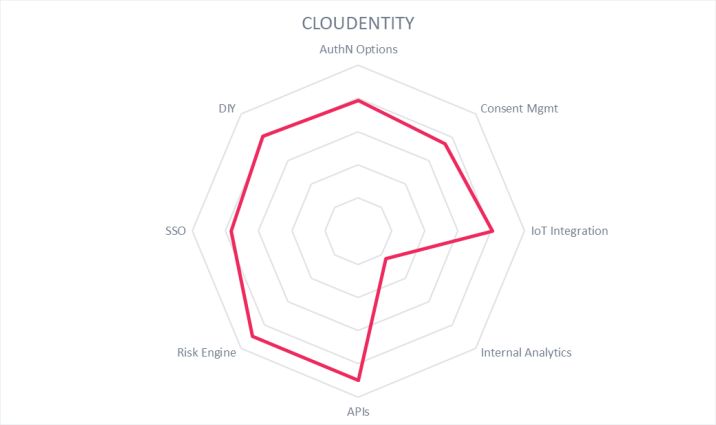
Strengths	Challenges
• Micro-services architecture • Rapid deployments • API-driven CIAM platform • Integrated API gateway can share policies	• Small but growing customer base and support ecosystem • Consumer profiles stored separately • Admin UI and documentation needs improvement

Table 5: Cloudentity's major strengths and challenges

For authentication and federation, Cloudentity supports Google Authenticator, JWT claims, mobile apps, OIDC and social logins, OAuth, TOTP, and SAML. Support for FIDO 2.0 and W3C WebAuthN is planned. Cloudentity offers an SDK for mobile app development. 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, Imperva, RSA and Secureworks. LDAP and SCIM interfaces are available for provisioning. The product integrates with SIEM via Kafka, REST, or syslog, and with GRC and SRM systems via APIs.

Marketing analytics is not a current focus for Cloudentity's customers. But Cloudentity does allow for integration with 3rd-party big-data, identity, and marketing analytics via REST APIs. Cloudentity is delivering innovative identity and IoT integration for healthcare customers by capturing data-level consent and RFID technology through their CIAM micro-services.

User dashboards facilitate consent collection and editing. Cloudentity supports user data export/deletion and UMA. Delegated administration and family management are partially supported.



Security	strong positive
Functionality	positive
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 6: Cloudentity's rating

Cloudentity represents the newest approach to CIAM and IAM; that is, by making all services available via APIs. Cloudentity's 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.

5.3 CoffeeBean Technology for CIAM

CoffeeBean started up in 2008 in California with a focus on increasing ROI in marketing solutions. They began developing their consumer identity and marketing solution in 2010. They are still privately held, but now 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 user. CoffeeBean hosts their solution as a SaaS for customers.

Strengths	Challenges
• FIDO U2F/UAF/2.0 clients and servers • WiFi captive portal and engagement plug-ins facilitate deep connections with consumers • One of few vendors actively pursuing CIAM market in South America	• Startup with small customer base • Strong marketing features may hinder privacy compliance • Missing SIEM and fraud intelligence integration

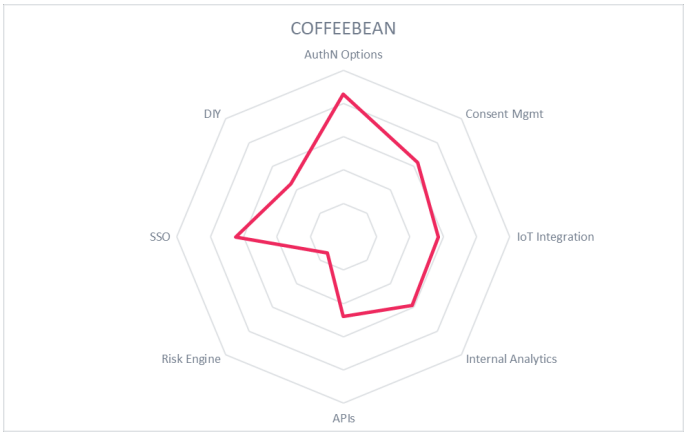
Table 7: CoffeeBean's major strengths and challenges

CoffeeBean's authentication options include Duo mobile, email/phone/SMS OTP, FIDO U2F/UAF/2.0, Google Authetnicator, LastPass, and mobile apps and biometrics; social logins including Facebook, Google, LinkedIn, and Twitter. It is compatible with OAuth, OIDC, OpenID and SAML standards. CoffeeBean produces an SDK that customers can use for building mobile apps. It does not yet support LDAP or SCIM for provisioning. CoffeeBean offers many built-in marketing analytics reports. Reports contain detailed data about consumers' social media profiles as well as from mobile device interactions. It can also work with IBM Watson Campaign Automation.

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. However, tenants must be diligent to ensure that the marketing features do not jeopardize GDPR compliance.

Security	neutral
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	neutral

Table 8: CoffeeBean's rating



CoffeeBean is strongly focused on retail, hospitality, and finance industries, bringing social media content to consumer profiles, and developing apps to more actively engage the consumer. Integration with 3rd-party fraud and threat intelligence is on the roadmap. The service possesses the capabilities to aid tenant compliance with GDPR and other regulations, but the onus is on the tenant customer to implement the service in a compliant way. Their presence in South America, both in terms of development center and sales target, is a plus for that region and for their own growth potential. Companies that are looking for a CIAM solution that is tilted toward retail, hospitality, or finance, and who want to actively engage with consumers in shops should give CoffeeBean a look.

5.4 EmpowerID IAM Suite

EmpowerID provides a CIAM solution derived from enterprise IAM. EmpowerID is strongly focused on workflow. Workflow is useful for organizations that need to customize CIAM functions but do not want to write and maintain lots of custom code. EmpowerID ships with more than 800 ready-to-use workflows with covering user provisioning, entitlement management, SaaS integration, and identity federation. The product is available as on-premise virtual appliance.

Strengths	Challenges
• Visual workflows obviate the need for coding • Many authentication options • IoT device tracking via asset management console; OAuth2 Device Flow support • Fine-grained consent management	• Currently on-premise, Windows only solution, SaaS options in development • No user dashboard by default, but customers can build them using workflows

Table 9: EmpowerID's major strengths and challenges

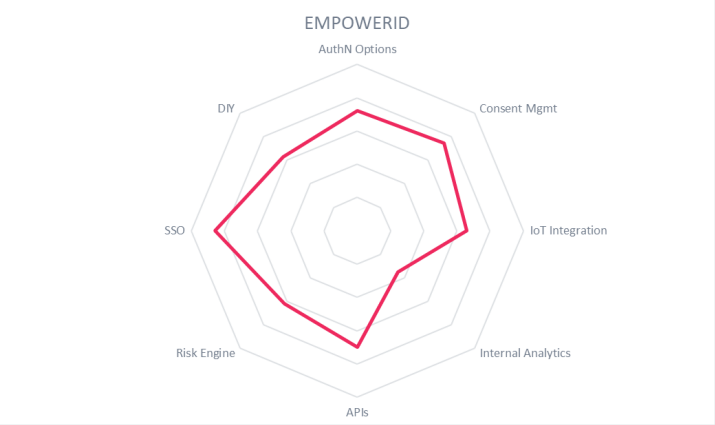
EmpowerID's authentication options include chatbots, email/phone/SMS OTP, FIDO U2F, Duo Security Push, mobile push, RADIUS, social logins, x.509, and Yubikeys. It also contains a risk engine capable of processing geo-location, geo-velocity, internal risk, device user-agent, encrypted cookies, user attributes, and user history while evaluating against static policies. They will be adding Azure services for IP reputation analysis. EmpowerID also features SaaS integration to Google Apps, Office365, Salesforce, Amazon, and Box. The product is moving to a micro-services architecture.

EmpowerID has many OOTB reports, but they are geared mostly toward enterprise IAM. The product does provide for integration with 3rd-party Big Data, identity, and marketing analytics via REST APIs.

The workflow engine supports obtaining consent from users for the use of their PII during registration and when terms of service change. Consent collection and editing can be configured per policy or regulation. EmpowerID supports user data export and deletion requests, as well as family management. Parents can control children's access to content.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 10: EmpowerID's rating



EmpowerID is a privately owned IAM company that is rapidly expanding its CIAM business. The product has many authentication options and good consent management features that will help customers comply with GDPR. It lacks some capabilities in terms of marketing analytics but makes up for it with API access. These features plus the customizable workflow engine make it an appealing choice for some environments.

5.5 ForgeRock Identity Platform

ForgeRock is a leading, venture-backed IAM vendor, headquartered in the US but with many offices around the world. ForgeRock was founded in 2010 by former Sun Microsystems employees. 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. ForgeRock provides the tools that their clients can use to build robust CIAM deployments either on their own premises or in IaaS.

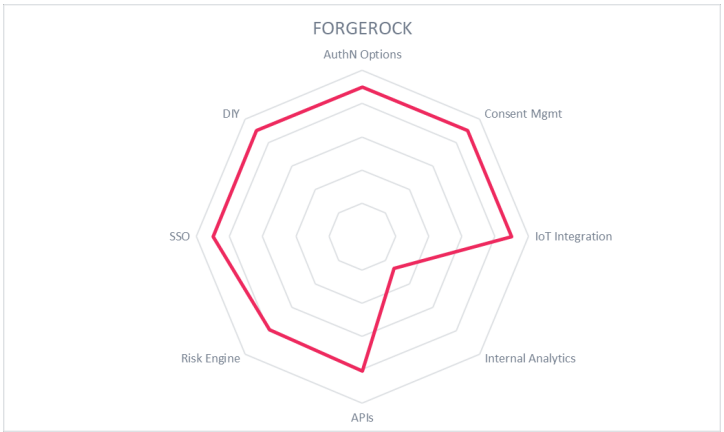
Strengths	Challenges
• Large scale CIAM deployments • Wide array of authentication methods • Intelligent Authentication / AuthN Trees • IoT integration via OAuth2 Device Flow, microservices, and mobile push authorization • API-first development strategy	• Not available as SaaS yet • No OOTB Business Intelligence functionality, but APIs allow access for 3rd-party analytics

Table 11: ForgeRock's major strengths and challenges

ForgeRock Identity Platform provides numerous choices for how customers can authenticate. Users may login from social networks or use OpenIDs, SMS OTP, FIDO-enabled devices, and mobile applications. It features an intuitive, flow-chart-based policy authoring tool called Intelligent Authentication. Authentication Trees allow customer admins to create policies in the GUI that meet the levels of assurance needed for sophisticated use cases. The details of designing complex, risk-adaptive authentication and authorization rules are abstracted by the interface.

Though Identity Platform does not have built-in identity and marketing analytics, the extensible nature of the product allows it to export data in many formats which can be consumed by other vendors' specialty solutions, such as Splunk, ArcSight, Marketo, etc., using REST APIs and Open ICF. Identity Platform's risk engine can be configured to consume 3rd-party threat intelligence.

Identity Platform supports obtaining consent from users for the use of their PII during registration and when terms of service change. These features are configurable and can be governed by policy. Organizations who deploy ForgeRock Identity Platform can build GDPR-compliant CIAM solutions including right-to-be-forgotten, but the onus is on the administrators to create consent management practices and processes to do so.



Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	positive

Table 12: ForgeRock's rating

ForgeRock has a global partner ecosystem. Identity Platform serves hundreds of customers with a total user count above 1.2 billion. With its many innovative features and flexible architecture, ForgeRock Identity Platform should be on the short list for organizations considering deploying CIAM solutions.

5.6 IBM Cloud Identity

Cloud Identity is IBM's multi-tenant cloud-based IDaaS. In addition to hosting enterprise identities, and serving B2B use cases, CI is also used by many clients across a variety of industries to provide consumer identity services. IBM hosts customer profile data for clients as well. The solution is based on a micro-services architecture. With customers and partners across the globe, IBM is a major player in the market.

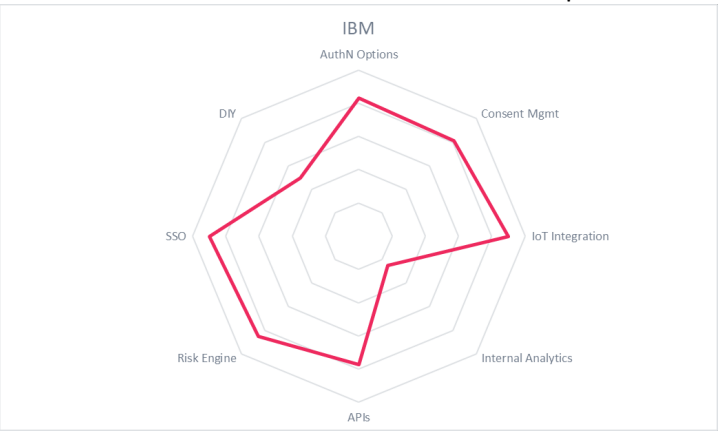
Strengths	Challenges
• Excellent administrative security • Large number of authentication options • Multi-purpose IoT integration; OAuth2 Device Flow support • Thorough Swagger-based API documentation • Trusteer for built-in fraud reduction • FIDO 2.0 certification	• Obtaining threat and fraud intelligence outside of Trusteer requires customization

Table 13: IBM's major strengths and challenges

IBM provides self-registration and profile management features, and accepts a wide array of authenticators, including FIDO U2F and 2.0, mobile apps, mobile biometrics, OTP, social logins, and 3rd-party mechanisms via IBM Security App Exchange. It supports OIDC, OAuth, SAML, WS-Federation, and WS-Trust. For provisioning, LDAP and SCIM interfaces are available.

CI and SAM (Security Access Manager) integrate well with other IBM solutions in the Identity Governance, Security, and enterprise business application space. For example, CI and SAM integrate with SIEM tools such as QRadar. CI has a risk engine that processes device fingerprint, IP reputation, geolocation for step-up authentication decisions. CI includes IBM Trusteer for real-time threat feeds. CI and SAM interoperate with Salesforce, and various Big Data analytics platforms for enhanced marketing analyses, but provides identity analytics natively. IBM has made great strides in IoT integration, and now supports OAuth2 Device Flow as well as use cases across multiple industries. IBM is investing heavily in blockchain/DLT.

For consent management, CI does allow users to choose which attributes they want to pass at registration time. Users can edit, export, and delete information afterward. Kantara UMA and Consent Receipt are not supported. Family management can be achieved through customization.



Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 14: IBM's rating

IBM CI and SAM are strong in terms of IAM features: administrative security, authentication options, and interoperability with 3rd-party products. IBM is Privacy Shield certified. They have made significant improvements with IoT use case support this year. IBM joined the Sovrin Foundation, and is actively experimenting with blockchain identity solutions for CIAM. IBM is a strong contender in CIAM, and organizations performing RFPs should fully evaluate their extensive list of capabilities.

5.7 iWelcome

iWelcome is a VC-backed IDaaS vendor based in the Netherlands. The CIAM functionality is a core feature of their overall IDaaS program. iWelcome's customers and support ecosystem are initially located within Europe, with initiatives started in the US. iWelcome uses some market leading open-source components for broad standards support including OAuth2 Device flow for IoT, UMA, and XACML, in its microservices-based core. It hosts customer profiles as well as identities. Licensing is per named user.

Strengths	Challenges
• Very granular consent model • Excellent support for GDPR compliance • Support for flexible registration processes in the BPMN 2.0 workflow engine • Strong admin and private tenant security	• Small but growing partner ecosystem • Heavily centered on EU currently but with near term global expansion plans

Table 15: iWelcome's major strengths and challenges

For authentication, iWelcome accepts FIDO U2F/UAF, mobile biometrics, RADIUS, SMS OTP, social logins and their own mobile push app. The risk engine processes location, device ID, and IP address information and can trigger step-up events. For provisioning, LDAP, SCIM, and Consent APIs are supported.

For security analytics, iWelcome utilizes the ELK stack plus Grafana, as well as provides syslog forwarding. For identity and marketing analytics, iWelcome offers ETL tooling to securely export both profile and event data to customers' data lakes as well as in-tenant Tableau Server reporting and analytics.

As an EU-based company, iWelcome provides the strongest GDPR compliance features and integrates with various in-country trusted identity providers. They have 15 data centers within the EU and 5 elsewhere. Consumers can granularly select which attributes to share from social networks at registration. At any point after registration, users may edit their choices. iWelcome supports Just-in-Time consent requests. The solution supports GDPR compliant export and deletion of data upon request. iWelcome makes its functionality available via API's for developers and has adopted the OpenAPI 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.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 16: iWelcome' rating

iWelcome is well-known for delivering CIAM solutions that foster GDPR compliance for the EU market by providing industry-leading consent management mechanisms. Third-party data analytics can easily extend the usefulness of consumer data due to iWelcome's use of Open APIs. Organizations in the EU that need flexibility and strong consent management in their consumer identity systems should always include iWelcome in RFPs.

5.8 Janrain Identity Cloud

Janrain is a private equity backed CIAM SaaS provider, based in Portland, Oregon. The company was launched in 2002 to provide user management and login capabilities for the social media market. Today the company has many large enterprise clients around the world serving 1.5 billion consumers across many sectors, including retail, entertainment, health, pharmaceutical, and finance. The Janrain suite of solutions is offered as a cloud-native multi-tenant service, and they host customer profile data. Licensing is annual per managed user.

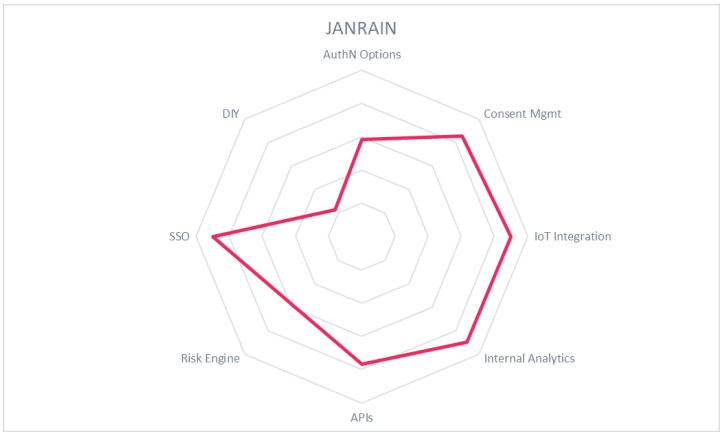
Strengths	Challenges
• Very large enterprise customer base • Fine-grained consent management • Excellent integration with social networks • IoT integration via OAuth2 Device Flow • Privacy Shield certified	• FIDO U2F/UAF support planned

Table 17: Janrain's major strengths and challenges

Janrain was the pioneer in social network integration. Besides any OIDC-based social logins, Janrain also accepts authenticators and federation standards: mobile apps, mobile biometrics, mobile push, OAuth, SAML, and SMS OTP authentication. Janrain supports LDAP and SCIM for bulk import. Janrain uses both internal network intelligence and partners with major IdPs for more comprehensive compromised credential intelligence to protect consumer accounts from fraud and identity theft.

Identity and marketing analytics are Janrain's forte. Examples of built-in reports include demographics such as gender, age, location, nationality; segmentation analysis such as generation, age range, income bracket; events including logins, registrations, social providers used; "likes" such as favorite TV shows, sports teams, books; and social engagement including top commenters and time spent on site. Janrain also permits API access to integrate with a wide range of 3rd party marketing analysis tools as well.

Consumers can edit, export, or delete their information at any time in accordance with GDPR. Janrain 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. Kantara UMA is supported but Consent Receipt is not currently supported.



Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 18: Janrain's rating

Janrain is a leader in the CIAM market. The solution focuses on high availability and harvesting user data for marketing analysis. It provides almost every feature expected in an advanced CIAM solution. Since 2017 the company has shifted much of its R&D to security, which should show up in the roadmap, such as including more strong authentication options. Janrain is mature and highly scalable and should be seriously considered by organizations that need HA, GDPR compliant consent management, and comprehensive marketing analytics features.

5.9 LoginRadius cIAM Platform

Established in 2011, LoginRadius is a VC-backed CIAM vendor based in Vancouver, Canada. The company provides CIAM as SaaS and customer profile hosting for enterprises around the world, and has hundreds of millions of identities under management. LoginRadius has a strong European presence, with multiple data centers within the EU for regulatory compliance. Multiple licensing models are available.

Strengths	Challenges
• Strong social login/Graph API support • Large customer base • Broad support by 3rd party marketing, e-commerce, and CRM solutions • IoT identity association by REST API and OAuth2 Device Flow	• Focused on low-risk, high volume customers and use cases • No automatic notification of privacy settings changes • FIDO and SCIM are not supported

Table 19: LoginRadius' major strengths and challenges

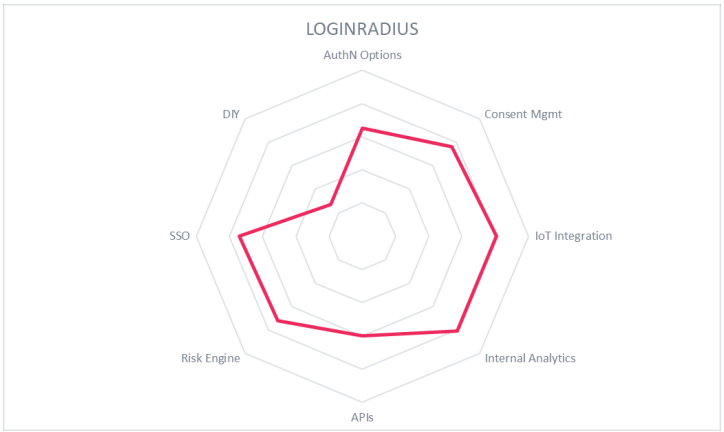
LoginRadius supports OIDC and thus allows social logins from any conformant provider. Other authentication mechanisms supported include Google Authenticator, mobile apps, mobile biometrics, mobile push, and SMS OTP. The risk engine can process external fraud and threat intelligence. Users can be provisioned using LDAP and proprietary APIs but not SCIM. LoginRadius features IoT device linking through a REST API, which allows user-to-device permission mapping. The service also supports OAuth2 Device Flow.

LoginRadius' built-in analytics engine provides 50 OOTB reports, allowing segmentation analysis according to date range, geography, age, gender, etc. Identity analytics can be viewed from the dashboard and delivered via reports. These identity activity reports can include registrations, logins, logouts, and password changes. All CIAM data is accessible via API. LoginRadius has obtained certification for ISO 27001/2, FISMA, HIPAA, and PCI DSS L1.

Users may edit, export, or delete their stored data at any time. It supports Kantara UMA but not Consent Receipt. LoginRadius does not automatically notify consumers when privacy terms change. Family management can be handled with customization.

Security	positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 20: LoginRadius' rating



LoginRadius' target customers are in industries with low authentication assurance requirements. Supporting additional authentication methods would make the service stronger. LoginRadius' service is highly scalable. Overall, the LoginRadius offering is up-and-coming in the CIAM market and deserves evaluation in CIAM RFPs, particularly for those organizations without high security requirements, such as apparel, fashion, retail, and media.

5.10 Microsoft Azure Active Directory B2C

Microsoft Azure Active Directory B2C is a cloud-based identity and access management service focused on facilitating business to consumer applications. Built upon Microsoft Azure AD, the B2C offering is architected to scale and perform well with hundreds of millions of users and over one billion logins per day. Azure is one of the global leaders in the cloud infrastructure market, second only to Amazon's AWS. It is licensed by number of stored users and authentications. Charges are slightly higher for MFA.

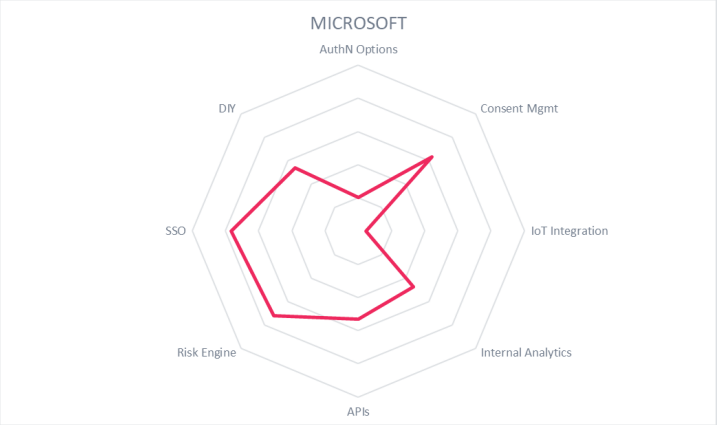
Strengths	Challenges
• API access for reporting and marketing analytics • Adaptive risk engine evaluates 100+ factors • Strong attack detection through robust cyber threat intelligence network • Resilient against cyber attacks	• Limited support for 3rd party SaaS app integration • Needs stronger fine-grained administrative capabilities for application & policy management • Consent management improving • No UMA support • Consumer data not encrypted by default

Table 21: Microsoft's major strengths and challenges

Microsoft Azure AD B2C accepts password-based, FIDO UAF, mobile app, SMS OTP, and social login authentication. Additional MFA options are available through partners. Azure AD B2C also accepts OAuth, OIDC, and SAML. Azure AD B2C does not support LDAP and SCIM for provisioning. Microsoft customers benefit from the rich and comprehensive threat intelligence and account protection services that are built-in to the Azure AD B2C offering.

Microsoft Azure AD B2C features a RESTful API, through which integration with systems such as SIEM, CRM, and big data analytics is achieved. Thus, it provides the infrastructure to collect and store large volumes of user data, but it requires Microsoft's PowerBI platform or similar analytic tool to transform the data into business intelligence.

Microsoft Azure AD B2C has coarse-grained functionality that allows user data to be stored within the region of each individual user. Customer admins can write policies allowing consumers to view, edit, export, and delete their data.



Security	neutral
Functionality	neutral
Integration	strong positive
Interoperability	strong positive
Usability	neutral

Table 22: Microsoft's rating

Microsoft Azure AD B2C has the scalability and performance to meet business requirements but lacks some CIAM functionality that are found in other solutions. Given Microsoft's commitment to cloud services, we expect it to mature in time.

5.11 NRI Secure Uni-ID Libra

NRI Secure Technologies was founded in 2000 as a subsidiary of Nomura Research Institute. With headquarters in Tokyo, NRI Secure provides security consulting and solutions. Uni-ID is their CIAM product, first developed in 2008 and rebranded and relaunched as Uni-ID Libra in mid-2017. The product is licensed per named user and can be deployed on-premises or in IaaS. NRI also offers it as a hosted service in single-tenant mode.

Strengths	Challenges
• Large-scale deployments in leading Japanese telecom, finance, and hospitality companies • Good IAM standards support • FIDO UAF certified	• Incomplete English language documentation and limited English tech support • No sales or support presence outside of Japan • No built-in or API access for marketing analytics • Delegated administration not available • Cannot require MFA for admins

Table 23: NRI's major strengths and challenges

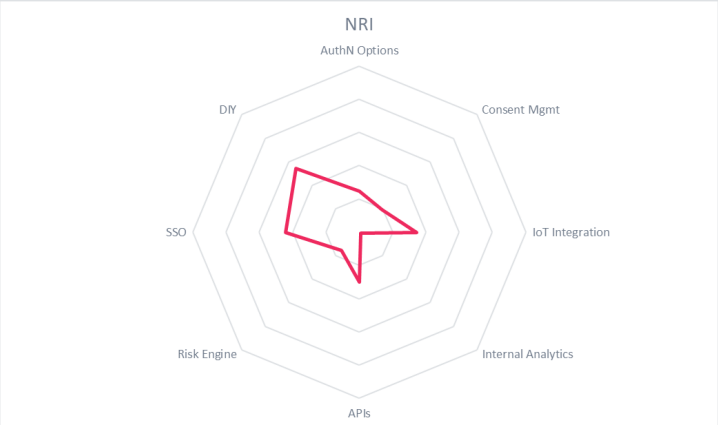
Uni-ID Libra accepts username/password, FIDO UAF, SMS OTP, and social logins such as Facebook and Google. It supports OIDC and SAML. Consumers can self-register and can be provisioned from other systems using SCIM. LDAP is not supported currently.

Uni-ID Libra can interoperate with security tools such as Splunk and the ELK stack. The solution contains basic risk-adaptive authentication capabilities, which include the evaluation of IP address, device fingerprints, geo-location, and user behavioral analysis. The risk engine cannot be augmented with 3rd-party fraud or threat intelligence.

Users can view and edit their own data per relying party. Users cannot opt-out of certain data collection procedures, nor can they export or delete their data. Family management is not supported, nor are Kantara Consent Receipt or UMA specifications.

Security	neutral
Functionality	neutral
Integration	positive
Interoperability	weak
Usability	weak

Table 24: NRI's rating



NRI Uni-ID Libra provides good basic CIAM functionality with flexible and scalable deployment options. They are almost exclusively focused on the Japanese market, but have some very large customers and installations there. Accordingly, the consent management features are somewhat lacking compared to others in the space. NRI is enhancing their product offering at customer request, as evidenced by the recent achievement of FIDO UAF certification. Adding MFA options, especially for customer administrators, as well as consent management features and A PI access would strengthen the product. Organizations in Japan with CIAM needs should consider NRI Uni-ID Libra.

5.12 Okta Identity Cloud

Okta, founded in 2009, offers Identity Cloud as its CIAM solution, originally derived from their enterprise IAM IDaaS solution. It is fully multi-tenant and hosts customer profiles. Okta has a focus on security, with HIPAA, ISO 27001, SOC 2 Type 2, ISO27018, and CSA Star Level 2 certifications. The service is licensed by monthly active users.

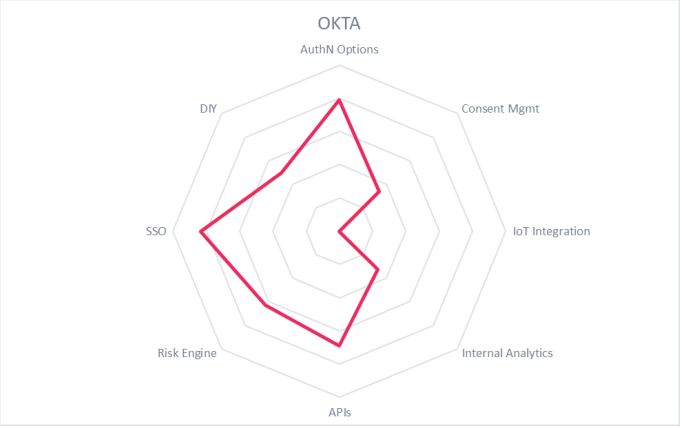
Strengths	Challenges
• Large user base	• Heavily centered on North American market
• Strong security model	• Limited consent management options
• Adaptive MFA	• No IoT identity integration
• Multiple security certifications	

Table 25: Okta's major strengths and challenges

Okta Identity Cloud accepts email/voice/ SMS OTP, FIDO U2F, Google Authenticator, Okta's Verify/push, social logins, and Yubikeys. It supports OAuth, OIDC, and SAML protocols. Okta's flexibility allows interopability with Microsoft AD and allows Okta to integrate with many SaaS apps or any database. Okta's policy framework can evaluate user, group membership, device ID, location, and IP address. Okta draws upon its own large network for threat intelligence, and its risk engine can process 3rd-party intelligence about IP reputation, breached credentials, other cyber threats, and can then be configured to require step-up authentication as needed. Okta allows LDAP, SCIM and SAML Just-in-Time provisioning.

The Okta System Log collects comprehensive data on user actions, which gives system administrators a real-time view into user activities across all applications. Examples of reports available from System Log include producing a timeline of all user authentications and provisioning activities; reporting with location, endpoint, and user agent data; map visualization; and debugging data to help developers and administrators troubleshoot issues. Okta also provides an API so that System Log data can be mined by 3rd party analytics tools for both real-time security intelligence as well as for marketing research.

Okta Identity Cloud allows users to export and delete their customer data but not view or edit their data through the default UI. However, Okta customers can build a "view profile" page with Okta's Users API, which allows users to view/edit their stored attributes. Some data collection procedures cannot be changed by consumers.



Security	strong positive
Functionality	positive
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 26: Okta's rating

Okta is leveraging their enterprise IDaaS strength in the CIAM world. Opening up access via APIs makes it more competitive as well. The solution needs additional consent and privacy management features OOTB as they currently require custom development. However, Okta does focus on security and performance, making it good CIAM candidate where strict GDPR compliance is not a must.

5.13 PingIdentity Platform

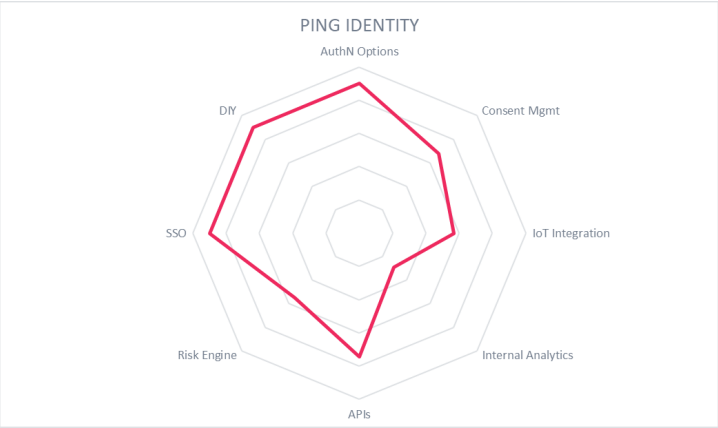
PingIdentity has been a pioneer in identity federation and access management since its inception. PingIdentity was among the first of the enterprise IAM vendors to adapt to consumer-facing requirements. The services are available for both on-premise and cloud deployment, and the PingOne IDaaS platform can host customer profiles in the cloud, amongst other capabilities. The solution is licensed by annual subscriptions based on the total number of managed identities.

Strengths	Challenges
• Lots of authentication options • Many OOTB connectors to SaaS / IDaaS • IoT integration via OAuth2 Device Flow • Cyber Threat Intelligence integration • Secure API access to internals	• Limited identity analytics • Main presence in North America as of now, but growing in other regions • Risk engine needs enhancement

Table 27: Ping Identity's major strengths and challenges

Ping CIAM users can login with email/phone/SMS OTP, FIDO U2F/UAF, RECAPTCHA, or native mobile apps. Ping provides an SDK to embed multi-factor authentication features into any mobile app. This includes transaction approvals for purchases, password changes, or other transactions, as well as the ability for customers to self-manage multiple trusted mobile devices. Social logins are accepted as well. It also supports all standards for identity federation. Bulk provisioning and bi-directional synchronization is possible via LDAP and SCIM. This solution can serve as an identity bridge to IDaaS, SaaS, and on-premise AD, IAM, and SSO implementations. Ping provides on-premises and cloud directory options with the ability to support structured and unstructured data. Reports show basic identity analytics. More advanced identity and marketing analytics require 3rd party applications, for which APIs are provided. IoT identity integration is achieved via OAuth2 Device Flow.

Ping has made significant GDPR-related enhancements to its consent management and enforcement features. Users can view, edit, export, and delete profile information. Family management can be implemented as delegated administration.



Security	strong positive
Functionality	positive
Integration	strong positive
Interoperability	strong positive
Usability	neutral

Table 28: Ping Identity's rating

Ping offers a full-service CIAM solution in flexible deployment models, with a wide range of authentication methods, and new-and-improved consent management capabilities for supporting EU customers with GDPR. Ping provides access via APIs for 3rd-party access for identity and marketing analytics. The recent acquisition of Elastic Beam, an API security startup which utilizes machine learning techniques, will likely lead to further enhancements and even more secure integration with their CIAM solution. Companies looking for CIAM solutions should consider Ping Identity's products and services.

5.14 Pirean Access: One

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 and Defense and Life Sciences. Pirean provides a Consumer and Workforce IDaaS platform called Access: One. The product can be deployed either on-premises or in IaaS, and Pirean hosts it as a managed service. Pirean can also host consumer profiles in the cloud for their customers. It is licensed by a measure of managed users, either monthly or annually.

Strengths	Challenges
• Large number of authenticators accepted • Strong audit and behavioral analytics • Strong risk controls for high assurance environments • Well-designed REST API framework	• IoT identity integration can be achieved through customization • Currently small but expanding partner ecosystem • Limited visibility outside of UK, but Exostar acquisition will likely increase visibility

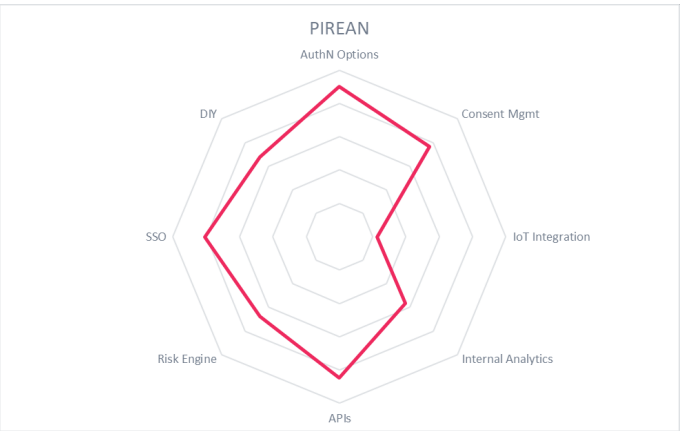
Table 29: Pirean's major strengths and challenges

Pirean supports FIDO U2F/UAF, mobile apps, native biometrics for Android and iOS, OATH TOTP, OneSpan DigiPass, RSA SecurID, and SMS OTP for authentication. Access: One can be configured to query external services such as IBM Trusteer and Experian Hunter for real-time threat intelligence. Policies can be written to use mobile apps via push notification as second factor authentication/authorization for access to SaaS apps. The risk engine is robust and can evaluate historical user behavior and user device details. It supports OAuth, OIDC, and SAML for federated authentication and authorization, and LDAP and SCIM for provisioning. API access is via JWT. Customers can send data to SIEMs over syslog or through OOTB connectors.

Built-in reports are complemented by the ability to connect over APIs to BI platforms. Consumers can view, edit, export, and delete their shared information through a dashboard. Family management, consent management, and delegation are configurable within the UI.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	strong positive
Usability	positive

Table 30: Pirean's rating



Pirean's Access: One is designed to function equally well for B2E and B2C use cases. The solution has a lot of advanced functionality in the mobile authentication and risk engine areas, developed in response to customer needs. Pirean has made most functions available through APIs. Basic IoT integration is possible due to support of OAuth2 Device Flow. Additional IoT integration can be customized on a case-by-case basis. The acquisition by Exostar adds strength in terms of customer base, geography, and ecosystem. The on-premise product or cloud-delivered service is an interesting and usable alternative and is worth a look when considering CIAM solutions.

5.15 Salesforce Identity

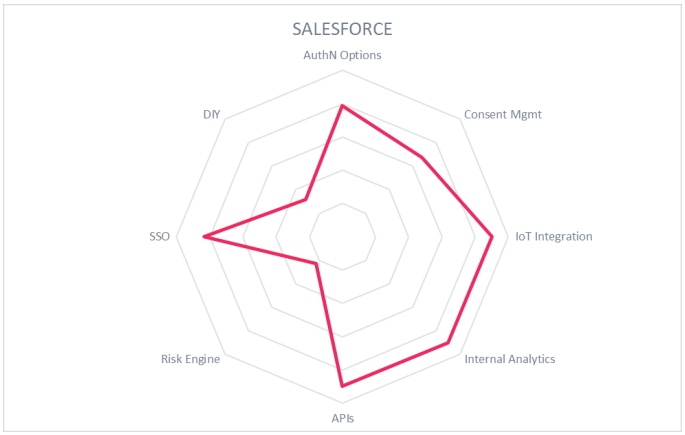
Salesforce is a cloud pioneer with their flagship CRM solution. Their identity platform has grown from servicing their own CRM to be a multi-purpose identity provider for customers. Salesforce Identity is designed to be omni-channel, offering the same features and consistent feel across web, mobile, and IoT devices. The cloud-based system is fully multi-tenant and can store complex data structures in customer profiles. The service is licensed by monthly active user counts.

Strengths	Challenges
• Very large customer base with many large-scale deployments • Very good built-in identity and marketing analytics • Customers can use many 3rd-party tools to access data via APIs • IoT identity with OAuth2 Device Flow	• Extra licensing fee to connect to on-premise AD • CIAM functionality focused on serving Salesforce.com ecosystem

Table 31: Salesforce's major strengths and challenges

Salesforce Identity accepts FIDO U2F, OATH TOTP, OIDC, SAML, and social logins. Salesforce Authenticator is the out-of-band push-based contextual strong authentication offering. They provide a Mobile SDK which can be leveraged by developers to create mobile and IoT integration apps. The platform defines standard and high assurance authentication levels, and the GUI allows administrators to define workflows for triggering high assurance logins. Salesforce Identity also allows customers to associate IoT devices with user identities. Salesforce supports OAuth2 Device Flow for IoT device registration. Many analytics features and reports are available within Salesforce Identity. Marketing Cloud, an add-on, can further deliver details such as detailed audience segmentation, user journey management, and marketing campaign effectiveness. Salesforce makes the raw data available to 3rd party analytics applications via REST APIs. Consumers can be provisioned in from LDAP or SCIM.

Salesforce uses in-network credential and threat intelligence, and customer administrators can configure feeds of 3rd party risk intelligence into login flows and can require higher assurance authentication if any defined criteria fail. Consumers can view, edit, export, and delete their data. Family management can be configured using roles.



Security	positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	positive

Table 32: Salesforce's rating

Salesforce Identity is a robust and scalable CIAM solution that provides much flexibility for customers. Additional consent management APIs are on the horizon. For existing Salesforce customers, Salesforce Identity may be the natural choice for B2C.

5.16 SAP Customer Data Cloud (formerly Gigya Identity Enterprise)

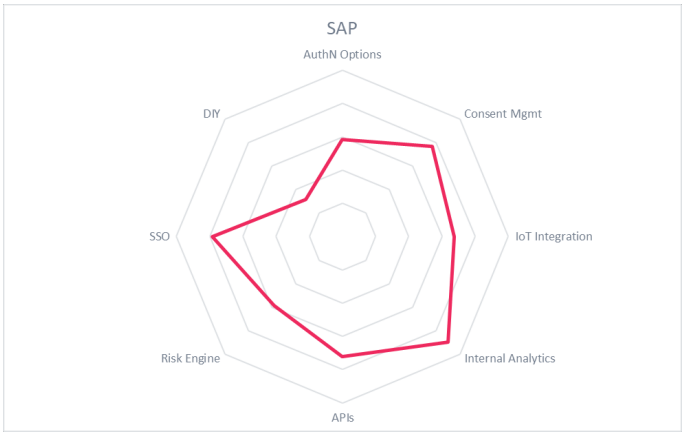
Gigya was acquired by SAP. Identity Enterprise is now known as SAP Customer Data Cloud and is becoming tightly integrated within the SAP platform. Their product accommodates most all social logins and integrates with many SaaS vendors. The service itself is entirely cloud-based, and it hosts customer profile data as well. Annual subscription licenses are based on the total number of contacts, which includes all unique records of customers, prospects, employees, and business partners.

Strengths	Challenges
• Large customer base and ecosystem • High performance • Detailed Marketing Analytics and Reporting • Many connectors to 3rd-party analytics as well as well-documented APIs • Excellent consent management features in SAP Customer Consent module	• Strong authentication options needed • No support for FIDO or UMA • Sales/marketing focused on the SAP customer base • Licensing is by total number of contacts rather than active users

Table 33: SAP's major strengths and challenges

SAP supports OAuth, OpenID, OIDC, and SAML. Consumers can authenticate with email/SMS OTP and Android/iOS biometrics. SAP has OOTB integrations with Socure, Trulioo, and LexisNexis for identity verification. Network Protected Identity provides real-time analysis and alerting on in-network credential compromises. It also has some risk analytics capabilities, evaluating device IDs, IP addresses, locations, and blacklisted locations. Customer admins can configure 3rd-party threat intelligence consumption via APIs. FIDO and other MFA options are not present yet.

SAP's IDX Partner Program offers more than 50 OOTB connectors to major apps and SaaS. SAP Customer Consent provides good consent management, allowing consumers to view, edit, export, and delete their data. Family management is a designed-in option. SAP has added more support for IoT use cases, including OAuth2 Device Flow. Customers can connect SAP Customer Data Cloud to external SIEMs using CEF or LEEF.



Security	positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	positive

Table 34: SAP's rating

SAP's acquisition of Gigya gained them a dominant position in the CIAM market. SAP has been focused on integrating Gigya into their toolset, and deploying it at existing SAP customers. SAP's consent management and marketing analytics capabilities are excellent. They have global reach and the platform is highly scalable. The solution does need stronger MFA options, particularly for mobile devices. The licensing scheme may need to be reconsidered. Organizations looking for SaaS-delivered CIAM solutions should definitely evaluate SAP Customer Data Cloud.

5.17 Widas ID cidaas

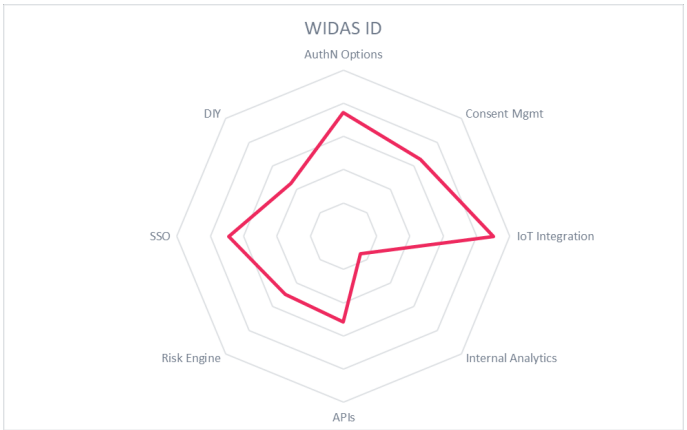
ID was founded in Germany in 1997. They do custom development for Big Data and IoT applications as well as consulting for many large organizations in Germany. The genesis for cidaas, their CIAM offering, evolved from some of the work they were doing to help clients integrate IoT devices with their consumer-facing businesses. The solution is mainly intended for cloud delivery, though some clients run it on-premises. It is licensed by the number of features used.

Strengths	Challenges
• Easy to integrate with common SaaS applications • Good consent collection capabilities • Micro-service architecture allows for dynamic scaling and continuous deployment of service enhancements • Forward-looking support for CIAM and physical access use cases • Beacons, NFC, OAuth2 Device Flow for IoT control	• Small customer base and geographic presence • Third-party threat intelligence processing requires customization using webhooks

Table 35: cidaas' major strengths and challenges

cidaas 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. Consumers can be in-provisioned via LDAP but not SCIM. Threat and compromised credential intelligence can be integrated via APIs and/or webhooks.

Consumers have the ability to view, edit, export, and delete their profile data. Family management is possible within the UI. cidaas supports OAuth2 Device Flow and has retail clients using IoT beacons and other devices for direct interaction with consumers on customer sites.



Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 36: cidaas' rating

cidaas is an established company making an entry into the CIAM field. They are localized to mainly Germany at present, but they have plans to expand. The solution covers the basics well and has some innovative features in the IoT integration area. Additional authenticators and more complex risk engine would enhance the product. cidaas is off to a good start and may be worth looking at, especially for retail-focused companies in their areas of operation.

5.18 WSO2 Identity Server

WSO2 was founded in 2005. They are an open source IAM/CIAM solution provider. Their emphasis is on providing Identity APIs and components for their customers to use for API integration scenarios as needed. The solution can be run on-premises, in IaaS, and they also offer a managed service capability. The product is licensed under the Apache 2.0 License and is supported under an annual subscription.

Strengths	Challenges
• Many pre-defined connectors for SaaS, attribute providers, and security services • Integrated adaptive risk engine • Comprehensive support for most every IAM standard including UMA and Consent Receipt	• Lacks family management • Does not support OAuth2 Device Flow for IoT integration

Table 37: WSO2's major strengths and challenges

WSO2 Identity Server accepts email/SMS OTP, FIDO U2F, Google Authenticator, JWTs, Microsoft Authenticator, Mobile Connect, RSA SecurID, social logins, and x.509 certificates. They have connectors for Veridium Biometrics and Aware Knomi for mobile biometrics, and others are in work. The solution does not have a mobile app or SDK. 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 intelligence can be imported, but there are no pre-built connectors. WSO2 has good support for IAM standards, including OAuth, OpenID, OIDC, SAML, and WS-Fed. They support standards-based and just-in-time provisioning using LDAP and SCIM.

WSO2 Identity Analytics server, which is built-in but runs as a separate process, can be used to generate identity and marketing analytics. Additionally, most all functions are exposed through APIs, allowing customer admins to build connectors and data feeds as necessary.

Consumers have the ability to view, edit, export, and delete their profile data. WSO2 supports Kantara UMA 2.0 and Consent Receipt. Family management is not configurable. For IoT device identity integration, WSO2 supports OAuth and OIDC, but not the OAuth2 Device Flow specification.

Security	positive
Functionality	positive
Integration	positive
Interoperability	strong positive
Usability	neutral

Table 38: WSO2's rating

WSO2 is an established open source IAM integrator. Recently they have built more functionality for consumer-facing use cases, and as a result are rapidly gaining customers for their CIAM capabilities. Organizations that prefer open source integration solutions should consider WSO2 for their CIAM and Identity API integration needs.

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 a DIY CIAM solution as defined earlier in this report. 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.

6.2 Avatier

California-based Avatier is an enterprise IAM vendor moving into CIAM. 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.

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 blockchain piece 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. Trust Platform accepts username/password, SMS OTP, and social logins from Facebook, Twitter, Microsoft, LinkedIn, and Google. 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.

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. Trust Platform does support UMA. Family management can be achieved via delegated administration model.

The AvocoSecure Trust Platform is an interesting offering considering its consent management and identity verification service provider integration. KuppingerCole will continue to monitor AvocoSecure and will include them in future publications.

6.4 Bitium

Bitium, based in California, is a provider of IAM solutions for mid-market to enterprise companies. Bitium was recently acquired by Google. They provide enterprise to SaaS integration solutions. Their services include synchronizing, provisioning/de-provisioning, and hosting customer identities. They offer SSO, via identity federation, to many commonly used applications, such as AWS, Box, Dropbox, Office 365, and Google Apps. KuppingerCole will track Bitium's integration into Google.

6.5 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.

6.6 Inversoft Passport

Best known for CleanSpeak, a web service for profanity filtering and site moderation, Inversoft also has a freemium CIAM solution. Passport offers mobile and web MFA options, brute force password attack detection, APIs and Webhooks, customizable consumer data storage, admin UI for managing users, and some reporting capabilities. The product is available for either on-premises or cloud hosting. If cloud-hosted it runs in single tenant mode.

6.7 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. KuppingerCole may evaluate Privo's family management SaaS offering in more detail in future reports.

6.8 Safelayer

Founded in 1999 in Spain, Safelayer has built a reputation for providing strong, PKI-based authentication and identity management systems for government and commercial use. Safelayer provides some CIAM functionality, such as SMS OTP, mobile apps and biometrics for MFA, social registration and login, and SSO multiple web domains via SAML, OAuth, and OIDC.

Furthermore, Safelayer provides EU eIDAS qualified signatures via its Mobile ID app that allows document signing using additional key-pairs protected by cryptographic devices such as cloud HSM. Safelayer's solution is positioned to support transaction confirmation for the EU PSD2 thanks to out-of-band mechanisms, 2FA and remote signature.

Safelayer's products are CC EAL4+ and NATO secret certified for high security assurance. Their associated KeyOne product issues and manages x.509 certificates for certain IoT devices and applications for machine-to-machine communication. KuppingerCole will review Safelayer's solutions in more detail in future reports.

6.9 Ubisecure Identity Server

Based in Finland, Ubisecure offers an integrated product solution that delivers CIAM functionality. Most customers run Ubisecure on-premise on RHEL or Windows servers, but a few run it in the cloud and they have a Canadian MSSP partner.

Ubisecure customers can authenticate with passwords, Mobile Connect, ETSI MSS, TUPAS, NemID, SMS OTP, OTP TAN, MeonTrust MePIN smartphone biometrics authenticator app, and all the major social logins plus VKontakte, Amazon, and GitHub. Ubisecure also supports Legal Entity Identifier (LEI). LEI is a global identifier for companies, specified by the EU eIDAS regulation, and endorsed by the G20. LEI is a new standard to aid in compliance for Anti-Money Laundering (AML) and Know Your Customer (KYC) initiatives. LEI is a 20-digit alphanumeric code. Ubisecure supports federation with SAML, OIDC, WS-Federation, and OAuth. It supports LDAP and REST for bulk provisioning. Ubisecure currently only looks at a small number of risk factors. It does not have the ability to utilize external cyber threat intelligence feeds.

The product sends data to SIEMs using syslog. Ubisecure does not have built-in reporting capabilities for identity and marketing analytics, but they do ship with Pentaho Data Integration. Their CIAM solution does allow consumers to granularly consent to attribute usage via the self-registration portal, and to edit them afterward. It allows users to de-register and delete their stored profile information. Family management can be implemented in the data model, and parent/children relationships can be modeled as service contracts.

6.10 UXP Systems

Toronto, Canada based UXP Systems offers Consumer IAM features in their User Lifecycle Management (ULM) | Identity and Access Management module. ULM can act as a federation hub providing access to multiple domains from a single digital ID. They support SAML, OAuth, and OIDC, and can access user attribute information in both LDAP and SQL databases. For mobile authentication, they support Mobile Connect. The platform also allows registration and authentication via social networks such as Facebook and Twitter. UXP Systems is focused on helping the telecommunications industry with digital transformation. KuppingerCole will monitor UXP Systems and possibly include them in reports in the future.

7 Methodology

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

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

7.1 Types of Leadership

We look at four types of leaders:

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

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

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

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

7.2 Product rating

KuppingerCole as an analyst company regularly does 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 on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management[1]). 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. Unresolved security vulnerabilities and hacks are also understood as weaknesses. This rating is based on the severity of such issues and the way a vendor deals with them.

Functionality is a measure of three factors. One is what the vendor promises to deliver. The second is the state of the art in industry. The third factor is what KuppingerCole expects vendors 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 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 in which products within each vendor's portfolio interoperate with each other. 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. 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 credential can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability can have several elements. 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

[1] http://www.kuppingercole.com/report/mksecnario_understandingiam06102011

standards that are important outside of the product family. Extensibility is related to interoperability, and is 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 to insure its importance is understood by both the vendor and the customer. As we move forward, simly 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. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

Usability 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 good documentation can facilitate adequate accessibility. However, we have strong expectations that user interfaces will be logically and intuitively designed. Moreover, we expect a high degree of consistency across user interfaces of a product or different products of a vendor. We also believe that vendors should 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 highest potential for breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will 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 increase costs, but inevitably lead 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 is of highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns, and will result in weak infrastructure.

[2] http://www.kuppingercole.com/report/cb_apieconomy16122011

7.3 Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

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

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

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

7.4 Rating scale for products and vendors

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

Strong positive	Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.
Positive	Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.
Neutral	Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.
Weak	Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.
Critical	Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

7.5 Spider graphs

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

Authentication options	Social logins; multi-factor authentication (MFA), SDKs, etc.
Consent management	Facilities within the UI to allow consumers to unambiguously opt-in to services and 3rd party usage of their data. 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 IoT devices by associating consumer identity with device identity. The use of OAuth2 Device Flow specification is a good means to achieve this
Internal analytics	Transforming information for marketing campaigns, creating special offers, encouraging brand loyalty. Includes identity analytics features, such as the ability to generate and customize reports on user actions, as well as representing aggregated activity on enterprise dashboards in real-time. This measure describes built-in capabilities within the CIAM solution, as contrasted with those products and services which choose to open APIs for tenants/customers to acquire and transform this data outside the CIAM solution.
APIs	APIs are increasingly available in CIAM solutions to provide means for 3rd party application to perform identity analytics, marketing analytics, security integration, provisioning/de-provisioning, consent auditing, and more
Risk Analysis	Evaluation of user attributes, environmental factors, fraud/threat intelligence, and other information to determine authentication and authorization levels required per transaction
SSO	Solutions use standards such as SAML, OpenId, OIDC, and OAuth for identity federation amongst a customer's websites. It can also include proprietary connectors for internally hosted applications and SaaS applications, such as CRM, Marketing Automation, etc.
DIY	Some of the solutions considered here are turnkey, meaning customers subscribe to a CIAM SaaS and most administrative details are handled by the vendor. Little or no software development must be done by the customers in these cases. Other solutions require significant amounts of administrative configuration and/or programming to integrate the CIAM solution with existing infrastructure. Some organizations need the ability to customize, while others do not need customization and only want to create a stand-alone CIAM system. This category represents the level of

customizability and corresponding effort to deploy the system. For organizations that need lots of customization, a high score in this category is desired. Both SysAdmin and Dev-centric CIAM categories have high DIY scores. Those looking for turnkey solutions with minimal effort to stand up should look for the low scores in this category.

The spider graphs provide comparative information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas, while being strong in other areas. These might 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 decisions on CIAM.

7.6 Inclusion and exclusion of vendors

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

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

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

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

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

8 Copyright

The Future of Information Security – Today

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

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com