KuppingerCole Report

LEADERSHIP COMPASS

by John Tolbert | November 2016

CIAM Platforms

Leaders in innovation, product features, and market reach for Consumer Identity and Access Management Platforms. Your compass for finding the right path in the market.

by **John Tolbert**
jt@kuppingercole.com
November 2016

Leadership Compass
CIAM Platforms
By KuppingerCole

KuppingerCole Leadership Compass
CIAM Platforms
Report No.: **71171**

Content

Content Tables

Table of Figures

Related Research

Advisory Note: Consumer Identity and Access Management for "Know Your Customer"
Leadership Brief: Your customer identities: How to do them right - 72006
Consumer Identity Summit

1 Management Summary

Consumer Identity and Access Management (CIAM) is on one hand 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 analyse 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.

On the other hand, CIAM goes beyond traditional IAM in commonly supporting some baseline features for analyzing customer behaviour, but also integrations into CRM 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 any type of systems, on premises and in the Cloud, from registration to tracking. With CIAM, to some extent similar kinds of information as in CRM systems can be collected, but the consumers themselves provide and maintain this information.

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. CIAM systems generally feature weak password-based authentication, but also support social logins and other 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 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.

The CIAM market is still emerging, however with some vendors offering rather mature solutions providing standard and deluxe features to support millions of users across almost every industrial sector. IT departments should welcome CIAM initiatives, as they provide an opportunity for IT, usually considered a "cost centre", to closely team with Marketing, a revenue producing centre.

There are a number of vendors in the CIAM market. Many of them are built from the ground up as 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.

Overall, this customer focused market is growing rapidly. 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.

The entire market segment is somewhat young compared to traditional IAM and still evolving. We expect to see more changes and perhaps more entrants within the next few years. Businesses must gain actionable intelligence on consumers to better "Know Your Customers" (KYC).

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 identifying those vendors that customers should look at more closely.

1.1 Overall Leadership

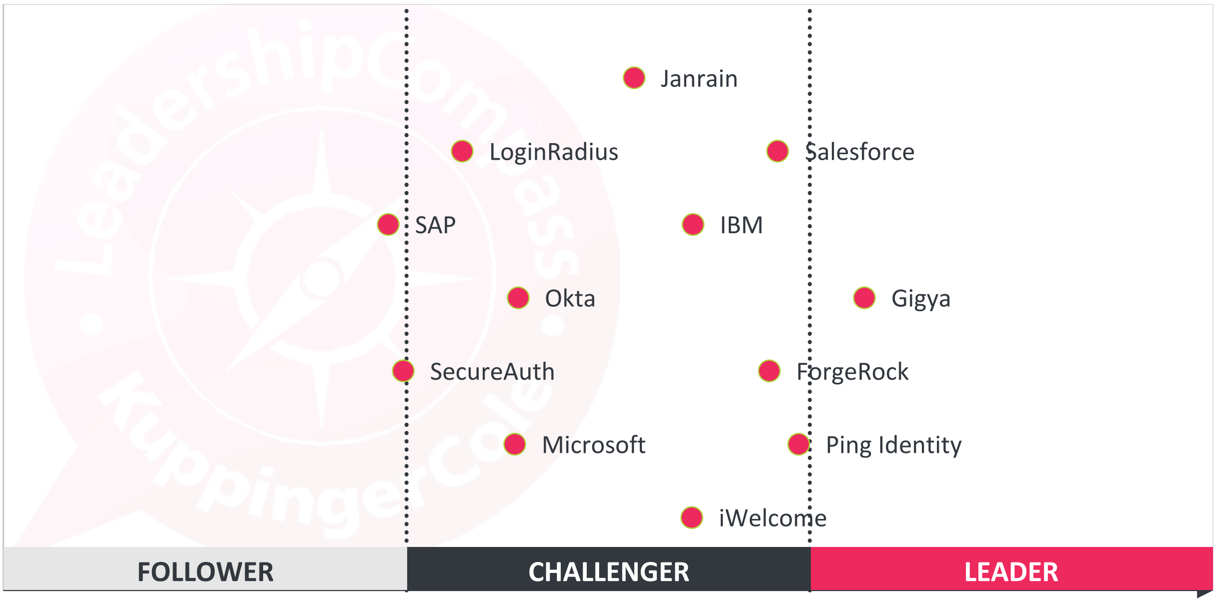


Fig. 1: Overall Leaders in the CIAM segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

Overall Leadership is the combined view on the three Leadership categories, i.e. Product Leadership, Innovation Leadership, and Market Leadership. This combined view provides an overall impression of our rating of the vendor's offerings in the particular market segment. Notably, some vendors with a strong market presence may fall slightly behind in other areas such as innovation, while others may show their strength in the Product Leadership and Innovation Leadership, even though they have a relatively low market share or lack a global presence. Thus, we strongly recommend looking at all Leadership categories and the individual analysis of the vendors and their products for gaining a comprehensive understanding of the players in that market segment.

In the market for CIAM, we currently see one company in the Leaders segment for Overall Leadership. Gigya is the dominant player with the strongest offerings.

The Challenger segment is very crowded, with most vendors being placed in that segment. Here we find a variety of players, including large and established vendors such as ForgeRock, Salesforce, Microsoft, IBM, and PingIdentity, which provide mature offerings, however they are not always as feature-rich and innovative as the companies in the Leaders segment. We also find a number of CIAM specialist companies such as Okta, Janrain, LoginRadius, and iWelcome.

Finally, we have two vendors in the Followers section: SecureAuth focusing on multi-factor authentication, and SAP working primarily with existing customers. These products deliver baseline capabilities, but do not have the breadth of functional coverage as other products in the market. However, they are on their way towards becoming challengers to the more established players in the market and might be a good choice for certain specific use cases and customer requirements.

Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping to the features provided by the vendor's products is mandatory.

1.2 Product Leadership

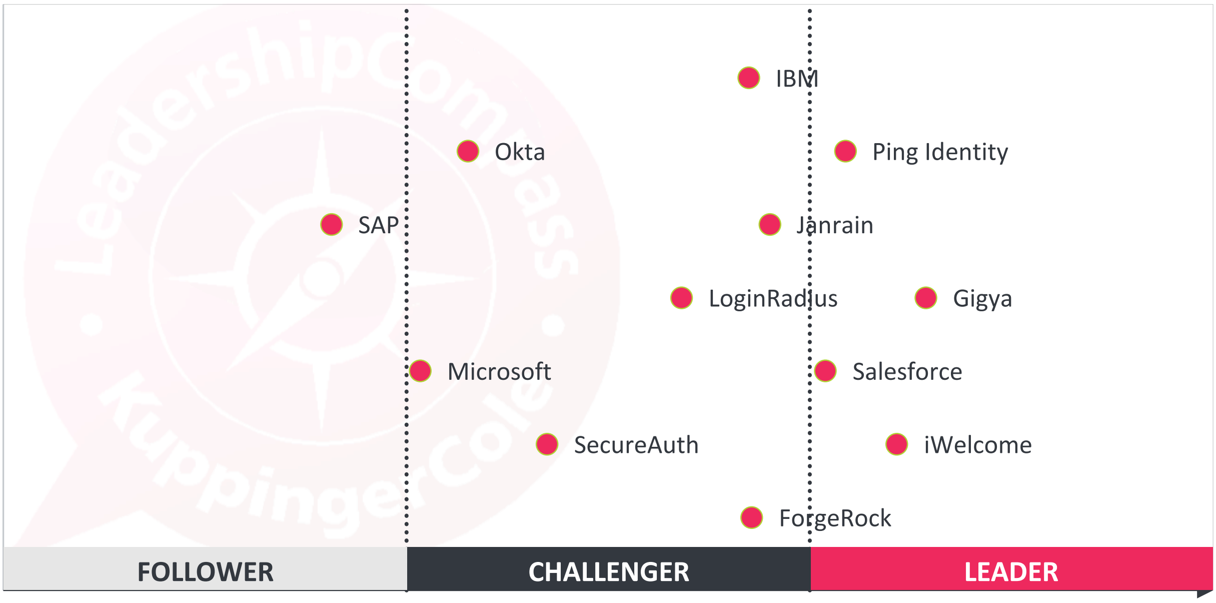


Fig. 2: Product Leaders in the CIAM segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

The second view we provide is about Product Leadership. That view is mainly based on the analysis of product features and the overall capabilities of the various products.

Here we see four companies being placed in the Leaders segment. The Overall Leaders in this segment are Gigya, iWelcome, PingIdentity, and Salesforce (in alphabetical order). All of them have mature product offerings. PingIdentity benefits from their recent acquisition of UnboundID, which brings in a broad set of additional features particularly in the CIAM space, in addition to PingIdentity's strength in Identity Federation.

ForgeRock, IBM, Janrain, and LoginRadius are about to enter the Leaders segment, with strong feature sets and large customer bases. IBM is a strong contender in most IAM market segments. ForgeRock's innovation and standards leadership have pushed it to the threshold of being a leader. Janrain and LoginRadius are both consumer oriented from the beginning, and therefore have a strong focus on marketing. Microsoft, due to the relative newness of their offering, rounds out the Challenger section, along with Okta and SecureAuth.

In the Followers section, we find SAP. The product is somewhat specialized for markets in which it operates: the SAP ecosystem.

Again, to select a product it is important to look at the specific features and map them to the customer requirements. There are sufficient examples where products that weren't "feature leaders" still were the better fit for specific customer scenarios.

1.3 Market Leadership

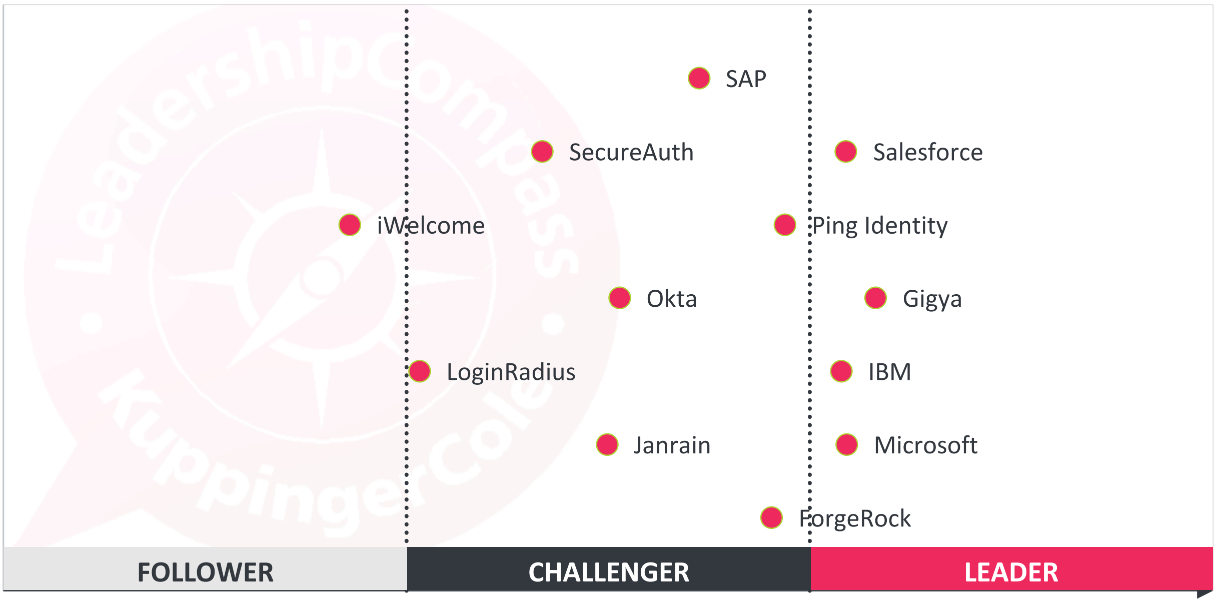


Fig. 3: Market Leaders in the CIAM segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

We expect Market Leaders to be leaders on a global basis. Companies which are strong in a specific geographic region but sell little or nothing to other regions are not considered Market Leaders. The same holds true for the vendor's partner ecosystem – without global scale in the partner ecosystem, we don't rate vendors as Market Leaders.

Market Leadership is an indicator of the ability of vendors to execute on projects. However, this depends on other factors as well. Small vendors might well be able to execute in their "home base".

Small vendors are sometimes more directly involved in projects, which can be positive or negative. The success of projects depends on many other factors, including the quality of the system integrator – so even large vendors with good ecosystems might sometimes fail in projects.

It comes to no surprise that the large and established software vendors dominate the Leaders segment. IBM, Microsoft, and Salesforce made it into the Leaders segment. Gigya, with their growth in the recent past, also made it into that segment, and as such is considered a CIAM market leader.

Near the border between Challenger and Leader we find ForgeRock and PingIdentity. Both command a large market share and have products that work very well for their customers. Other vendors in the Challenger area include Okta, Janrain, LoginRadius, SAP, and SecureAuth.

iWelcome is found in the Followers area, due to small customer base and focus on EU customers.

It must be noted that this Market Leadership rating doesn't allow any conclusion about whether the products of the different vendors fit the customer requirements.

1.4 Innovation Leadership

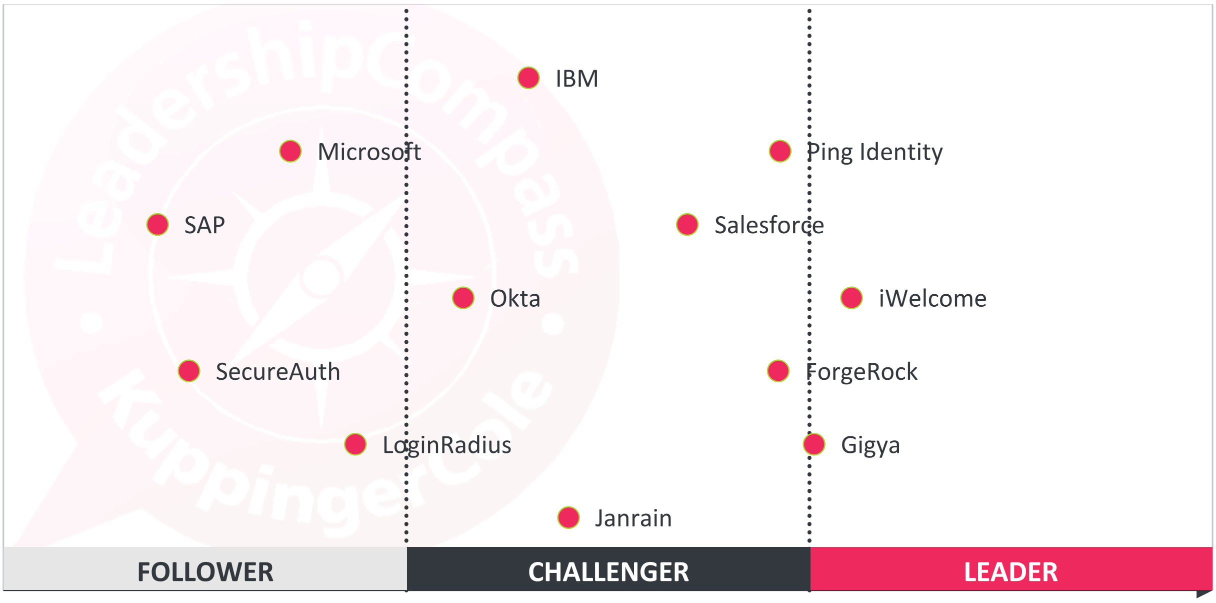


Fig. 4: Innovation Leaders in the CIAM segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

The third angle we take when evaluating products is about innovation. Innovation is, from our perspective, a key distinction in IT market segments. Innovation is what customers require in new releases that meet emerging business needs and use cases. Thus, a look at Innovation Leaders is also important, beyond analyzing product features.

Here we see iWelcome and Gigya in front. Both of them showed significant innovation and strong support of the list of features we consider as innovative in the CIAM market, starting with broad support of multiple authentication methods.   Gigya offers a wealth of marketing analytics, and iWelcome provides GDPR compliant fine-grained consent features.

ForgeRock, PingIdentity, and Salesforce are leading the Challenger segment, all being close to entering the Leaders segment. The other vendors, such as IBM, Janrain, and Okta are also well placed in the Challenger segment, indicating that they show significant innovation in this market.

LoginRadius, Microsoft, SAP, and SecureAuth make up the Followers section. They have some innovative features, however due to the still relatively small feature set they lack support for some of the innovative features we'd like to see.

Again, in some cases, products that appear more to the left in that figure do not necessarily fail in innovation, but are focused on specific requirements.

Some vendors are innovative with respect to new features such as providing new authentication methods or new identity context analytics capabilities. Overall, this view reflects the fact that there is still a lot of innovation happening in the CIAM market, with significant room for some of the vendors to enhance their offerings.

2 Methodology

KuppingerCole's Leadership Compass is a tool that provides an overview of a particular IT market segment and identifies the leaders in that market segment. It is the compass that assists you in identifying the vendors and products in a particular market segment which you should consider for product decisions.

It should be noted that it is inadequate to pick vendors based only on the information provided within this report. Customers must always define their specific requirements and analyze in greater detail what they need. This report does not 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.

We look at four types of leaders:

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

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

- Leaders: This identifies the leaders as defined above. Leaders have products which are exceptionally strong in some areas, and are strong in most other areas.
- Challengers: This level identifies products which are not yet leaders but have specific strengths which might make them leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains products which lag in some areas, such as 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.

In addition, we have defined a series of matrixes which:

- Compare ratings, for example the rating for innovation against the one for the overall product capabilities, thus identifying highly innovative vendors which are taking a slightly different path than established vendors, but also established vendors which no longer lead in innovation. These additional matrixes provide additional viewpoints on the vendors and should be considered when selecting vendors for RFIs (Request for Information) in the vendor/product selection process.
- Add different views by comparing the product rating to other feature areas. This is important because not all customers need the same product features, depending on their current situation and specific requirements. Based on these additional matrixes, customers can evaluate which vendor best fits their current needs, but is also promising regarding its overall capabilities. The latter is important given that a product typically not only should address a pressing challenge but become a sustainable solution. Chosen solutions should address both immediate business needs as well as being good enough for the next steps and future requirements.

Thus, the KuppingerCole Leadership Compass provides a multi-dimensional view on vendors and their products.

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

3 Product Rating

KuppingerCole, as an analyst company, regularly does evaluations of products and vendors. The results are, amongst other types of publications and services, published in the KuppingerCole Leadership Compass Reports, 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 – 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). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings, such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

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

Integration — integration is measured by the degree in which the vendor has integrated the individual technologies or products in the portfolio. Thus, when we use the term integration, we are referring to the extent in which products interoperate with other products from the same vendor. 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 usernames and passwords for every person involved, it is not well integrated. Or, 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 user account can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability—interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to insure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy) for more information about the nature and state of extensibility and interoperability.

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

We focus on security, functionality, integration, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of both cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly 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 of these areas will lead to inevitable identity and security breakdowns and weak infrastructure.

4 Vendor Rating

KuppingerCole includes ratings which may be considered outside the technical realm, but are important to understand when selecting products for RFIs. The specific areas we rate for vendors are

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the market segment(s) the vendor is in. Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. Driving innovation without standardization frequently leads to vendor lock-in scenarios. Thus, active participation in international standards organizations 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, e.g. being weak in one segment doesn't necessarily lead to a very low overall rating. This factor considers the vendor's presence in major markets. The rating in market position is specific to the market segment analyzed in this KuppingerCole Leadership Compass, not related solutions. Thus, a very large vendor might not be a market leader in the market segment we are analyzing.

Financial strength – even while KuppingerCole doesn't consider size to be a value in itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to become an acquisition target, with potential risks to customers of not fulfilling the stated roadmap.

Ecosystem – this dimension looks at the ecosystem of the vendor for the particular product covered in this Leadership Compass document. 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.

5 Vendor Coverage

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, the US, or the APAC region.

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.
- Decline 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 as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular market segment.
- Lack of information supply: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only a 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.

For this Leadership Compass document, almost all major vendors we approached responded to the questionnaire.

Furthermore, there are a few point offerings in the market that have a limited market visibility and were not included in the leadership analysis for this KuppingerCole Leadership Compass. Some of these vendors are listed in the final section of this document and might become part of the next edition of this document, depending on how they evolve.

6 Market Segment

CIAM is a somewhat new market, simultaneously arising from the traditional IAM market while merging and absorbing functionality from CRM and Marketing Automation. Some full stack IAM vendors provide CIAM capabilities, built into their suites, or available as separate products. These products and services will be examined below. Also, there are specialty products focused on CIAM, which were expressly developed to meet the different needs of managing consumer identities. These products may have more in common with CRM and marketing tools than traditional IAM suites.   On the other end of the spectrum, we see CRM companies such as Salesforce offering IDaaS as a mechanism to enable CIAM on their web properties and others. Each of these types of cases will be included in this Leadership Compass.

Various factors have led to this situation. At the core is the need for agility in a complex competitive landscape. Business models have to adapt more rapidly than ever before. Enterprises need to know their customers in more detailed ways to deliver tailored products and services, increase brand loyalty, reduce fraud, comply with regulations, and increase revenues. KYC is a true competitive advantage, which can be facilitated with CIAM solutions.

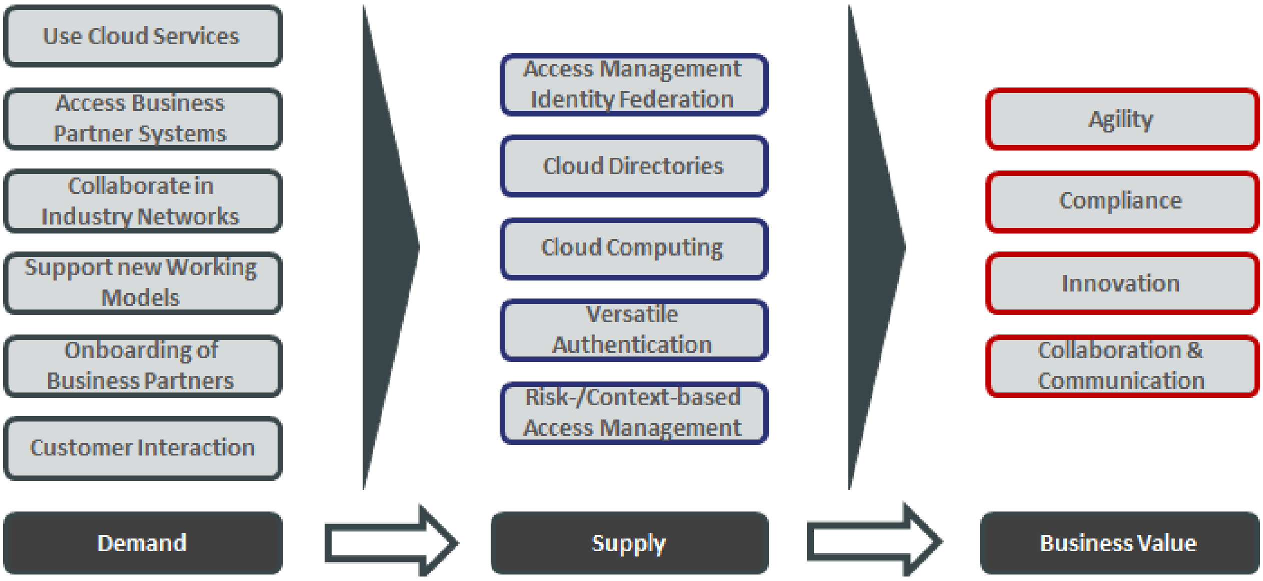

Use Cloud Services
Access Business Partner Systems
Collaborate in Industry Networks
Support new Working Models
Onboarding of Business Partners
Customer Interaction
Access Management Identity Federation
Cloud Directories
Cloud Computing
Versatile Authentication
Risk-/Context-based Access Management
Agility
Compliance
Innovation
Collaboration & Communication
Demand
Supply
Business Value

Fig. 5: Supporting the Extended Enterprise helps organizations addressing major business challenges.

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

- Deployment options: On-premise, cloud, or hybrid options.
- Social logins: Using Facebook, LinkedIn, Twitter, Google, and more
- Multi-factor authentication support: SmartCards, OTP, Biometrics, OOB mobile confirmation apps
- 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

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, ultimately, 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.

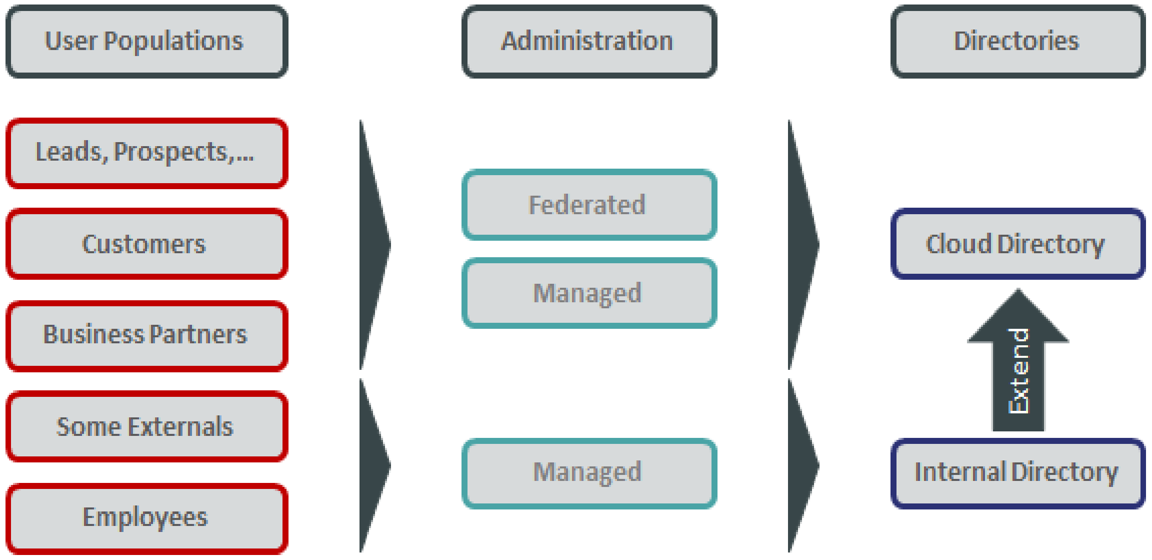


Fig. 6: Dealing with all types of user populations will require both federation and locally managed user accounts.

Based on our view on the market and the current demand, we opted for looking at both on-premise deployment as well as cloud-based deployment features in this Leadership Compass document. Some vendors offer both options, as well as hybrids. The overwhelming majority offer CIAM as SaaS.

7 Specific features analyzed

When evaluating the products, besides looking at the aspects of

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- platform support

we also considered several specific features. These include:

Authentication technologies	Social logins, mobile support, multi-factor authentication
SSO support	SAML 2.0, OAuth 2.0, OIDC, etc., for a seamless browsing experience across all related web properties
User experience	Self-registration, self-maintenance of attributes, consistent branding
Privacy management	User consent options, privacy notifications, GDPR compliance, and family management
Deployment models	On-premise, cloud, or hybrid
User identity analytics	Ability to pull standard and customized reports on user behaviors and preference, as well as enterprise dashboards showing real-time aggregate activities
Marketing	Once consent is given, transforming information for marketing campaigns, creating special offers, encouraging brand loyalty

The support for these functions is included with the evaluation of the products. 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.

8 Market Leaders

Based on our evaluation of the products, we've identified (as mentioned above) different types of leaders in the CIAM market segment. The Market Leaders are shown in figure 9.

We expect Market Leaders to be leaders on a global basis. Companies which are strong in a specific geographic region but sell little or nothing to other regions of the world are not considered Market Leaders. The same holds true for the vendor's partner ecosystem – without global scale in the partner ecosystem, we don't rate vendors as Market Leaders.

Market Leadership is an indicator of the ability of vendors to execute on projects. However, this depends on other factors as well. Small vendors might well be able to execute in their "home base".

Small vendors are sometimes more directly involved in projects, which can be positive or negative. The success of projects depends on many other factors, including the quality of the system integrator – so even large vendors with a good ecosystem might fail in projects.

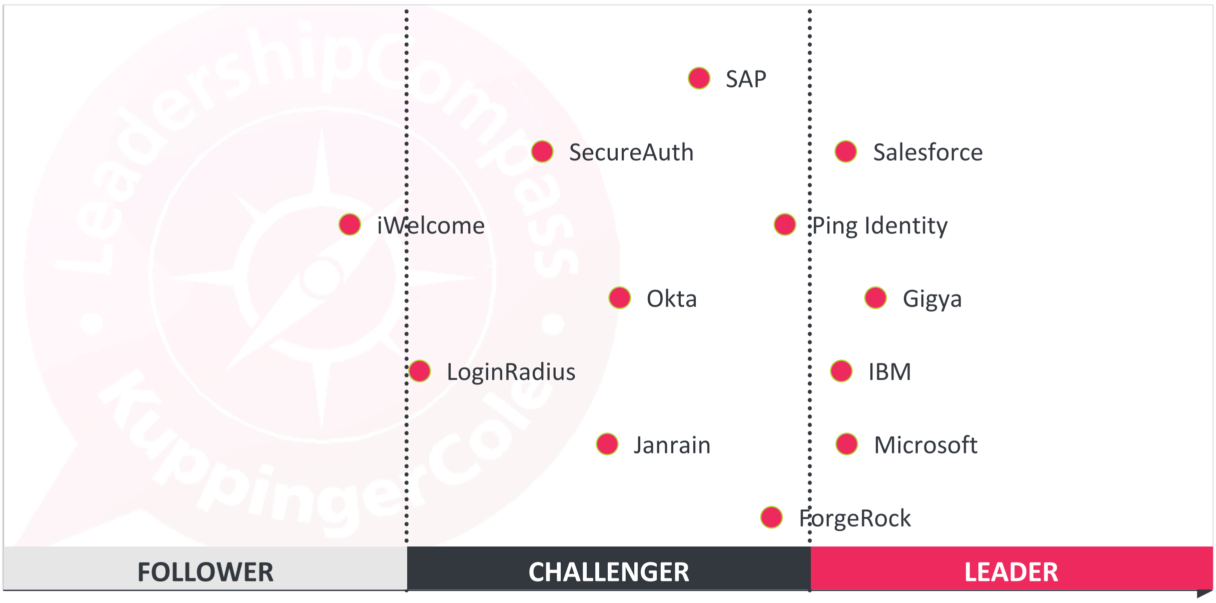


Fig. 7: Market Leaders in the CIAM market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

It comes to no surprise that the large and established software vendors dominate the Leaders segment. IBM, Microsoft, and Salesforce made it into the Leaders segment. Gigya, with their growth in the recent past, also made it into that segment, and as such is considered a CIAM market leader.

Near the border between Challenger and Leader we find ForgeRock and PingIdentity. Both command a large market share and have great products that work well for their customers. Other vendors in the Challenger area include Janrain, LoginRadius, Okta, SAP, and SecureAuth.

iWelcome is found in the Followers section in this analysis, due to their focus on EU customers and relatively small market share.

It must be noted that this Market Leadership rating doesn't allow any conclusion about whether the products of the different vendors fit the customer requirements.

Market Leaders (in alphabetical order):

- Gigya
- IBM
- Microsoft
- Salesforce

9 Product Leaders

The second view we provide is about Product Leadership. That view is mainly based on the analysis of product features and the overall capabilities of the various products.

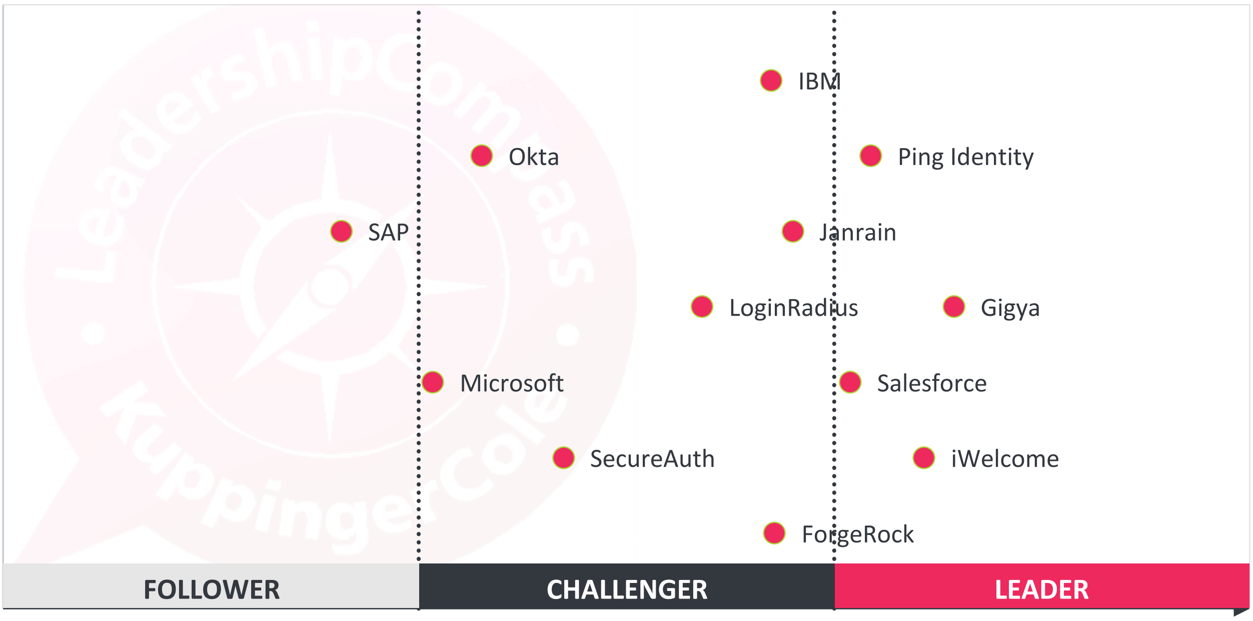


Fig. 8: Product Leaders in the CIAM market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

Here we see four companies being placed in the Leaders segment. Again, the Overall Leaders in that segment are Gigya, iWelcome, PingIdentity, and Salesforce (in alphabetical order). All of them have mature product offerings.

ForgeRock, IBM, Janrain, and LoginRadius are about to enter the Leaders segment, with strong feature sets and large customer bases. IBM is a strong contender in most IAM market segments. ForgeRock's increasing customer base and innovation have positioned it near the threshold of being a product leader. Janrain and LoginRadius are both consumer oriented from the beginning, and therefore have a strong focus on marketing. Microsoft, due to the relative newness of their offering, rounds out the Challenger section, along with Okta and SecureAuth.

In the Followers section, we see SAP. The product is somewhat specialized for the markets in which it operates: the SAP ecosystem.

Again, to select a product it is important to look at the specific features and map them to the customer requirements. There are sufficient examples where products that weren't "feature leaders" still were the better fit for specific customer scenarios.

Product Leaders (in alphabetical order):

- Gigya
- iWelcome
- PingIdentity
- Salesforce

10 Innovation Leaders

The third angle we took when evaluating products was about innovation. Innovation is, from our perspective, a key distinction in IT market segments. Innovation is what customers require to receive new features that meet new requirements.

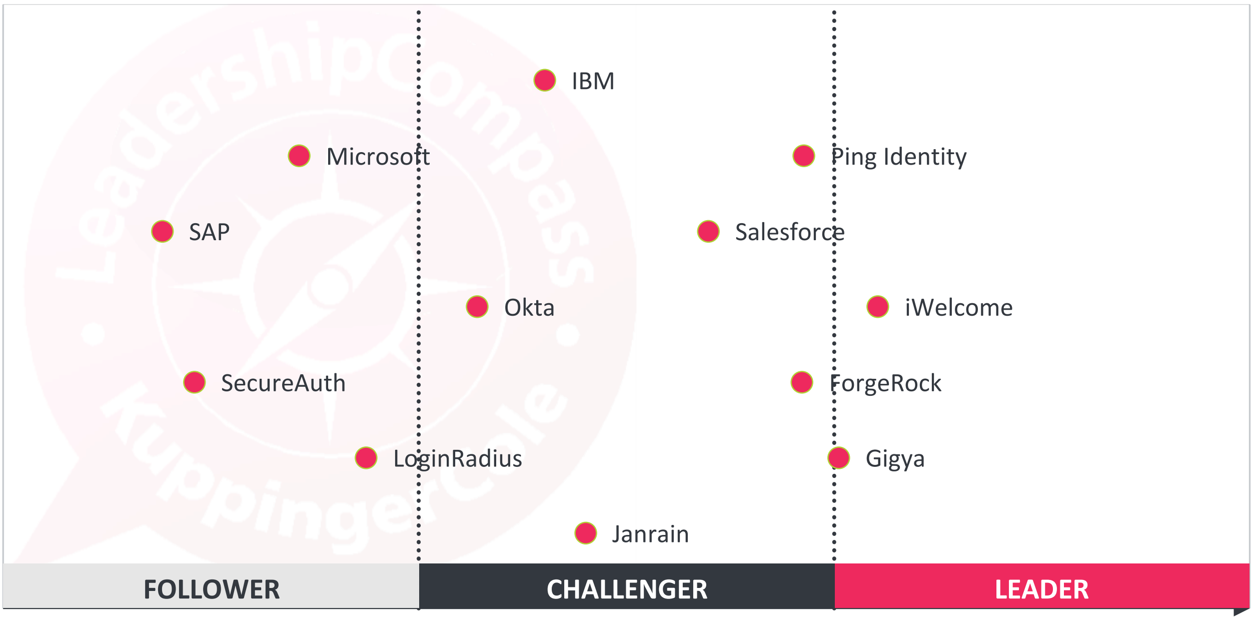


Fig. 9: Innovation Leaders in the CIAM market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

Here we see iWelcome and Gigya in front. Both of them showed significant innovation and strong support of the list of features we consider as innovative in the CIAM market, starting with broad support of multiple authentication methods and privacy consent management.

ForgeRock, PingIdentity, and Salesforce are leading the Challenger segment, all being very close to entering the Leaders segment. The other vendors, such as IBM, Janrain, and Okta are also well placed in the Challenger segment, indicating that they show significant innovation in this market.

LoginRadius, Microsoft, SAP, and SecureAuth make up the Followers section. They have some innovative features, however due to the still relatively small feature set they lack support for some of the innovative features we'd like to see.

Again, in some cases products that appear more to the left of that figure do not necessarily fail in innovation but are focused on specific requirements or highly focused approaches

Some vendors have demonstrated a significant amount of innovation in recent time, driving standards evolution forward. UMA would be the significant example here. Others are innovative with respect to new features such as fine-grained consent options for privacy management. Overall, this view reflects the fact that there is still a lot of innovation happening in the CIAM market, with significant room for some of the vendors to enhance their offerings.

Innovation Leaders (in alphabetical order):

- Gigya
- iWelcome

11 Product Evaluation

This section contains a quick rating for every product we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and KuppingerCole Executive View Reports available, providing more detailed information.

11.1 ForgeRock Identity Platform

ForgeRock has grown from a start-up to become a leading vendor in the traditional IAM and CIAM space. They have taken the open source approach to product delivery, but their technology and support are enterprise grade today. 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 a variety of cloud environments.

Strengths/Opportunities	Weaknesses/Threats
● Large scale CIAM deployments ● Wide array of authentication methods (from social logins to mobile apps) ● Flexible authentication chaining ● Fully multi-tenant cloud options ● UMA support for consent management	● ForgeRock does not provide cloud hosting services ● No OOTB Business Intelligence functionality ● Strong toolset, but limited set of pre-defined CIAM specific features such as consent management

Table 1: ForgeRock Identity Platform major strengths and weaknesses.

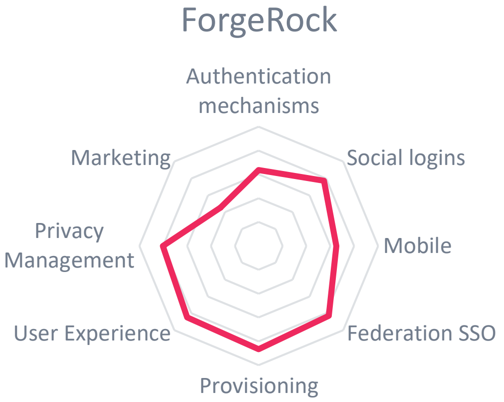
ForgeRock Identity Platform provides numerous choices for how customers can authenticate. Users may login with social logins and OpenIDs from the major networks, SMS OTP, FIDO-enabled devices, and mobile applications. Administrators can write flexible policies to "chain" various authenticators together to support risk-based step-up authentication requirements.

Though Identity Platform does not have built-in identity analytics and business intelligence reporting facilities, 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, but the onus is on the administrators to create consent management practices and processes to do so. ForgeRock will release GDPR templates which users can customize for their own organizations.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	neutral

Table 2: ForgeRock Identity Platform rating.



ForgeRock is venture-financed and currently investing heavily in product development. This results in rapid improvements in an already solid product. ForgeRock also has a large partner ecosystem on global scale. ForgeRock has a sizable list of customers with installations supporting up to 150 million external users. With its many innovative features and flexible architecture, ForgeRock Identity Platform should be on the short list for organizations considering deploying CIAM solutions.

11.2 Gigya Identity Enterprise

Gigya’s Identity Enterprise is a CIAM tool suite that was created to address what their founders saw as deficiencies in the traditional IAM approach. Gigya was one of the first companies to offer MySpace login and Facebook Connect. Their product has expanded considerably to accommodate most all social logins and integration with many SaaS vendors. The service itself is entirely cloud-based, and it hosts customer profile data as well. Gigya’s goal is to help clients turn site visitors into known users.

Strengths/Opportunities	Weaknesses/Threats
● Large customer base with correspondingly large ecosystem ● High performance ● Native ETL functionality ● Detailed Marketing Analytics and Reporting ● Excellent privacy compliance capabilities	● Password-based administration ● Manual re-consent process

Table 3: Gigya major strengths and weaknesses.

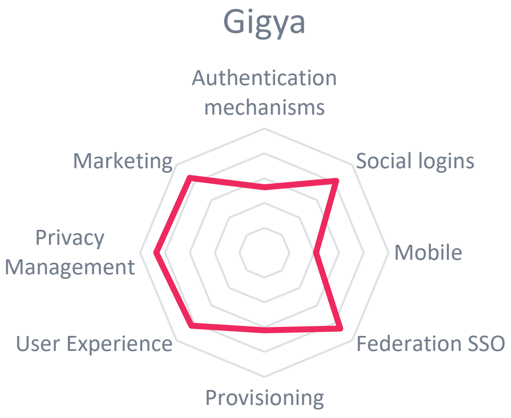
First-time visitors may register with social media accounts, custom SAML or OpenID identity providers, a mobile phone number or a traditional email/password combination. Gigya has out-of-the-box integrations with Socure, Trulioo, and LexisNexis for identity verification. It also has limited risk analytics capabilities, to process information such as device IDs, IP addresses, locations, and blacklisted locations. If the score returned is too low, the risk engine can call for step-up authentication mechanisms such as SMS/email OTP, or phone verification.

The reporting and analytics functions can track key user activities including registrations, logins, shares, referral traffic, comments, etc., that graphically represent client’s KPIs on a dashboard. These reports can help clients measure, for example, the efficacy of marketing initiatives. Clients can filter based on age, location, gender, and any other attributes from customer profiles. The dashboard can also be used to track activities across all of a client’s digital properties, in cases where a company owns multiple brands.

Gigya provides consent management, and already has GDPR compliant features built-in, such as storing proof of consent, right to export data, data deletion upon request, and data age and retention policies. Moreover, Gigya has multiple data centers for localizing user data.

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

Table 4: Gigya rating.



Gigya is well-established amongst the leading products in the CIAM market, being mature and widely deployed. Their focus on consumer experience and integrated marketing tools provide a powerful platform for not only managing user identities but also for creating usable intelligence on market trends. This makes the product a clear pick for shortlists when looking for CIAM solutions.

11.3 IBM Cloud Identity Service (CIS)

Cloud Identity Service is IBM's multi-tenant cloud-based IDaaS. In addition to hosting enterprise identities, and serving B2B use cases, CIS is also used by many clients across a variety of industries to provide consumer identity services. As the name implies, the service is entirely cloud-based, and IBM hosts customer profile data for clients as well. CIS is derived from and in fact underpinned by IBM's IAM tools. With customers across the globe and a worldwide partner network, IBM's CIS is a major player in the market.

Strengths/Opportunities	Weaknesses/Threats
● Strong administrative security ● Large number of authentication options ● Multi-protocol federation capabilities ● Integration with identity suites	● No ability to delete user entries ● Users not provided consent options upon change of terms ● No family management ● Limited built-in reports

Table 5: IBM Cloud Identity Service major strengths and weaknesses.

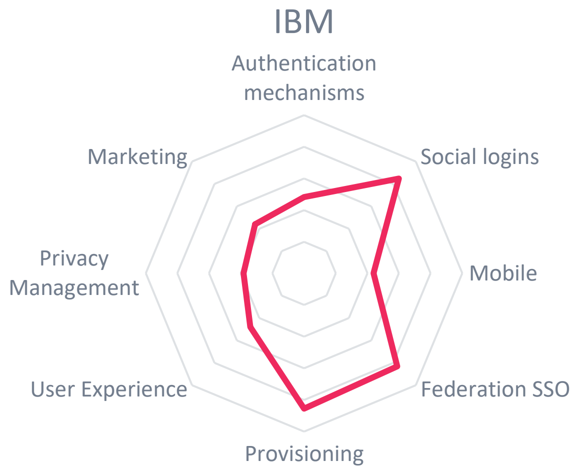
IBM CIS accepts a wide array of authenticators, from password to TOTP/HOTP. It also integrates with all the major social network providers, plus Yahoo, Windows Live, RenRen, QQ, Weibo, and Wechat. To facilitate identity federation, it supports SAML, OIDC, OAuth, WS-Federation, WS-Trust, and Kerberos. For provisioning, LDAP and SCIM interfaces are available.

CIS integrates well with other IBM solutions in the Identity Governance, Security, and enterprise business application space. For example, CIS integrates with SIEM/RTSI tools such as QRadar. CIS has a risk engine that processes device fingerprint, IP address and reputation, geolocation for step-up authentication decisions. CIS interoperates with Salesforce, Big Data, and various analytics platforms for enhanced marketing analyses, but also provides identity analytics natively.

In terms of consent management, CIS does allow users to choose which attributes they want to pass at registration time, and they can edit information afterward. When privacy terms change, users are not automatically notified and are not presented with consent options. Users can delete their profiles but cannot currently de-register from the service. This feature will be added in 2017. There are no family management capabilities in the current version of the service.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 6: IBM CIS rating.



IBM CIS is strong in terms of traditional IAM features: administrative security, authentication options, and interoperability with 3rd party products. Organizations needing both traditional IAM and CIAM should consider CIS as a possible solution. IBM has announced its intentions to become fully GDPR compliant by May 2018. The offering would benefit significantly from additional built-in reports and more fine-grained consent options.

11.4 iWelcome

iWelcome is a venture capital backed vendor of IDaaS and CIAM solutions headquartered in the Netherlands. In fact, the CIAM functionality is a core feature of their overall IDaaS program. iWelcome's customer and support ecosystem are entirely located within Europe. iWelcome uses some market leading open source components in its software platform: MongoDB, Elastic, and ForgeRock OpenAM; therefore, it supports the same standards, such as SCIM, UMA, and XACML. iWelcome is a cloud-based offering, and it hosts customer profiles as well as identities.

Strengths/Opportunities	Weaknesses/Threats
● Very granular consent model ● Strong support for GDPR compliance ● Strong support for federation standards and social logins	● Small but growing partner ecosystem ● Heavily centered on EU, no global reach ● Limited identity and marketing analytics

Table 7: iWelcome major strengths and weaknesses.

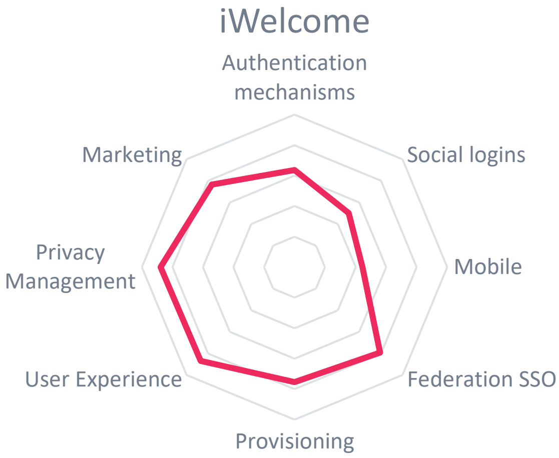
iWelcome accepts Facebook, Microsoft, Google, Twitter, LinkedIn, and many other social logins, as well as SAML, OAuth, and OIDC federation. For step-up authentication, iWelcome accepts SMS OTP, KBA, FIDO U2F, and their own mobile push app. The risk engine processes location and IP address information, and can trigger step-up events in accordance with client-defined policies.

For real-time security intelligence, iWelcome utilizes the ELK stack (Elasticsearch, Logstash, and Kibana) as well as provides syslog forwarding options. For identity and marketing analytics, iWelcome leverages the MongoDB BI connector, which allows export of data to a plethora of 3rd party data analytics applications.

As an EU-based company, iWelcome's CIAM offering is strong in preparation for GDPR. Their data centers are located in the EU. It provides very granular consent and privacy management functions. During registration using social network credentials, users can select which attributes they want to share with iWelcome clients. Also, at any point after registration, users may edit their choices. Moreover, if iWelcome client's privacy terms change, the users are notified and may decide on permissible uses of their PII. The solution also supports de-registration and deletion of data. iWelcome also supports family management. Users may define relationships and parents can govern children's' activities.

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

Table 8: iWelcome rating.



iWelcome focuses on delivering CIAM solutions which are GDPR compliant for the EU market. Their IDaaS solution provides adequate CIAM functionality, but 3rd party products must be used to realize the full potential of the intelligence gathered from CIAM.
Given their small customer base and ecosystem, iWelcome is an up-and-coming challenger in the mature CIAM market. The consent and privacy management features make it an interesting option for EU-based companies. If GDPR compliance is a top issue in your organization, iWelcome may be a potential solution.

11.5 Janrain

Janrain is a venture capitalist financed provider of CIAM solutions, based in Portland, Oregon. The company was launched in 2002 with an aim to provide user management and login capabilities for the nascent social media market. Today the company has many large enterprise clients around the world serving millions of consumers. Janrain was a founding member of the OpenID foundation and supports open standards today. The Janrain suite of solutions is only offered as a cloud service, and they host customer profile data.

Strengths/Opportunities	Weaknesses/Threats
● Very large enterprise customer base ● Support for standards ● Excellent integration with social media ● Privacy Shield certified	● Lack of standards-based provisioning options ● Proprietary mechanism for bulk import of identities

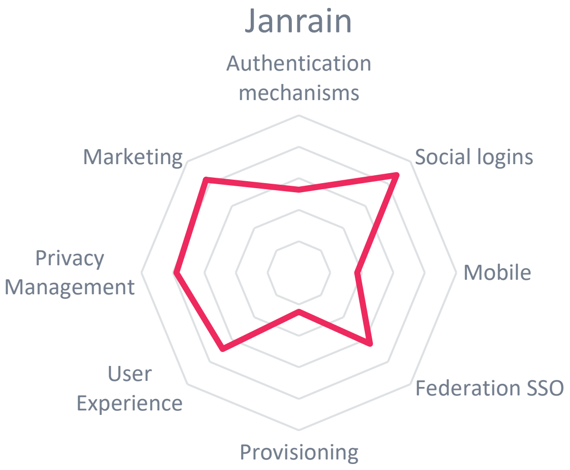
Table 9: Janrain major strengths and weaknesses.

With an emphasis on social network integration, Janrain accepts Facebook, Twitter, Microsoft, Google, and 30 other types of social logins. Besides social logins, Janrain also accepts password-based and SMS OTP authentication, and SAML, OAuth, and OIDC federation. Additional authentication options would improve the overall offering. Janrain allows bulk identity import, but does not use LDAP or SCIM for that function. Identity and marketing analytics are Janrain's forte. Examples of 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 favorite TV shows, sports teams, books; and social engagement including top commenters and time spent on site. Janrain also permits programmatic access via APIs to integrate with a wide range of 3rd party market analysis tools as well, e.g. Google Analytics and Tableau.

Janrain does allow for granular selection of attributes to be shared from social network registration. Users may also edit and delete their information at any time after registering. Janrain provides the capabilities for their tenants to automatically notify users and have them re-consent after privacy policies changes. By employing group management techniques, clients can represent family relationships and allow parents to govern the access rights of children.

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

Table 10: Janrain rating.



Janrain has established itself as a key player in the CIAM market. The solution focuses on social media integration and harvesting user data for marketing analysis. It does provide all the basic features expected in a CIAM solution. The Janrain suite could be improved by offering additional login methods and more options for adaptive authentication. However, the product is mature and scalable, and should be seriously considered by organizations that need the strong analytics features provided by the Janrain suite of solutions.

11.6 LoginRadius

Established in 2011, LoginRadius is venture capital backed CIAM vendor based in Vancouver, Canada. The company provides cloud-based CIAM services 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.

Strengths/Opportunities	Weaknesses/Threats
● Strong social login support ● Large enterprise customer base ● Broad support by 3rd party marketing, e-commerce, and CRM solutions	● Few authentication mechanisms apart from social ● No automatic notification of privacy settings changes ● No family management capabilities

Table 11: LoginRadius major strengths and weaknesses.

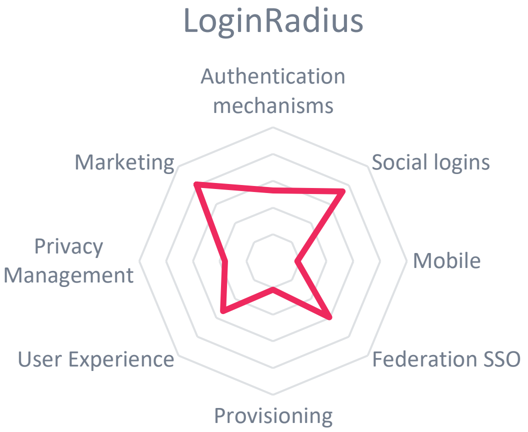
LoginRadius supports social logins including Facebook, Twitter, LinkedIn, Google, Microsoft, and 37 other providers. Users can login with any OpenID. Two-factor authentication, including SMS OTP and Google Authenticator, is on the near-term roadmap.

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. Additionally, data can be exported to and analyzed by 20 major analytics platforms, including Adobe Analytics, Google Analytics, and Marketo; 6 CRM solutions including Microsoft Dynamics and Salesforce; and e-Commerce, advertising, and content management platforms. LoginRadius has obtained certification for ISO 27001/2, FISMA, HIPAA, and PCI DSS L1.

The solution provides consent management. Consumers may choose which data points to share from social network providers at registration time. Users may edit, export, or delete their stored data at any time. LoginRadius does not automatically notify consumers when privacy terms change. Family management is not available at this time. The company is in the process of becoming GDPR compliant.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	strong positive

Table 12: Login Radius rating.



LoginRadius is a relatively young entrant into the CIAM market. Its feature set is strong in social network registration, login, and utilization. Its openness lends itself to a broad partner system to fill out the gaps in functionality. Supporting additional authentication methods and fraud detection feeds would make the LoginRadius solution stronger. Overall, the LoginRadius offering is an interesting alternative in the CIAM market and deserves evaluation in decision making processes, particularly for those organizations without high security requirements and that are consumer facing.

11.7 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. Cloud services have been one of the primary drivers in Microsoft's business portfolio. Azure is one of the global leaders in the cloud infrastructure market, second only to Amazon's AWS.

Strengths/Opportunities	Weaknesses/Threats
● Integration with PowerBI allows for reporting and marketing intelligence gathering ● Scalability and high performance	● No support for 3rd party SaaS app integration ● No support for 3rd party IDaaS ● No support for customer authentication via SAML ● Identifiers and profiles not encrypted ● Weak administrative security ● No automatic notification of privacy changes ● No LDAP, SCIM, IAM, or AD interfaces

Table 13: Microsoft Azure AD B2C major strengths and weaknesses.

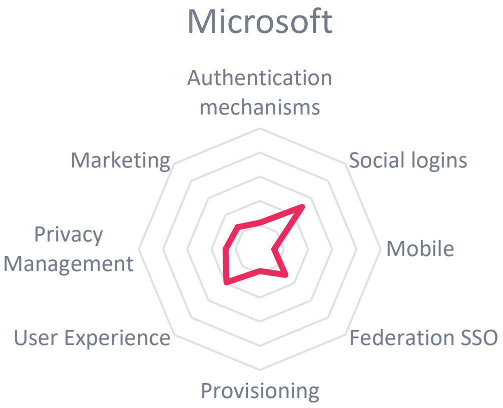
Microsoft Azure AD B2C accepts password-based, SMS OTP, and social login authentication. It also supports Multi Factor Authentication (MFA). This can be selected via the Azure Portal, and is available for an extra per-transaction cost. Microsoft Azure AD MFA utilizes the following factors: phone calls, SMS OTP, mobile app notification (with simple verify function button), and mobile app verification. It also accepts OIDC and OAuth federation, but not SAML (administrators can authenticate via SAML). It does not currently support bulk provisioning or integrating with other IDaaS. This service would benefit from additional authentication methods and bulk provisioning mechanisms.

Microsoft Azure AD B2C features a RESTful API, through which integration with systems such as SIEM/RTSI, 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 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. Users are notified about which attributes will be shared from source accounts only at registration time. This service is only available in preview mode and is not fully operational in the EU.

Security	neutral
Functionality	neutral
Integration	positive
Interoperability	weak
Usability	neutral

Table 14: Microsoft Azure AD B2C rating.



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

11.8 Okta Platform

Okta platform is a cloud-based 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.

Strengths/Opportunities	Weaknesses/Threats
● Large user base ● Strong security model ● Adaptive MFA ● Multiple security certifications	● Heavily centered on North American market ● Consumers are not able to granularly select attributes from social registration ● Strong focus on enterprise SSO

Table 15: The Okta Platform major strengths and weaknesses.

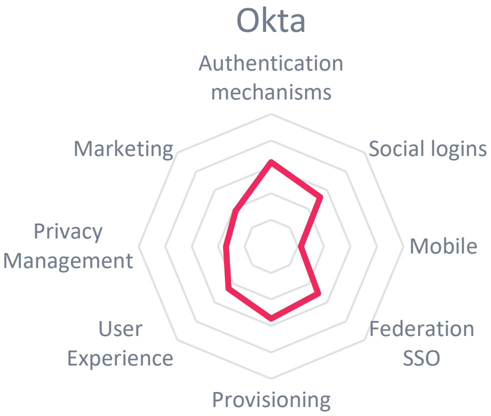
The Okta Platform accepts social logins from Facebook, Google, Microsoft, and LinkedIn. It also supports SMS OTP, FIDO U2F, and federated authentication from SAML, OIDC, and OAuth. The flexibility of Okta platform allows it to accept user information from a number of standard sources, such as Microsoft AD, and also allows Okta to integrate with a large number of SaaS apps or any database. Okta's policy framework can evaluate user, group membership, device ID, location, and IP address. Its risk engine can receive intelligence about IP reputation, breached credentials, other cyber threats, and can then be configured to require step-up authentication from the methods listed above.

The Okta System Log collects basic 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.

The Okta Platform accepts social network registrations, but does not ask the user for consent when attributes are pulled from the social database. Users can edit, export, and delete their own data after registration. Family management is possible via the Okta API. Okta does not support UMA for consent management.

Security	strong positive
Functionality	neutral
Integration	neutral
Interoperability	neutral
Usability	neutral

Table 16: Okta Platform rating.



Okta is a challenger to the established players in the market for consumer identity management. Its marketing analytics features lag behind other solutions in this space. Additional consent and privacy management features would improve the offering. However, Okta Platform does focus on security and performance. While it does have a reasonable support ecosystem in the EU, the vast majority of its customers are in North America. To prepare for GDPR compliance, Okta has two data centers within the EU.

11.9 PingIdentity Platform

PingIdentity has been a pioneer in identity federation since its inception. With the recent purchase by Vista Equity Partners, and their acquisition of UnboundID, Ping is a strong brand in the digital identity space. Although Ping's portfolio began as traditional identity federation and IAM, the products were among the first to adapt to consumer-facing requirements. The services are available for both on-premise and cloud deployment, and as a result of the UnboundID purchase, the PingOne platform can host customer profiles.

Strengths/Opportunities	Weaknesses/Threats
• Largest number of authentication options • Excellent multi-protocol support, including FIDO and SCIM • Many OOTB connectors to SaaS / IDaaS • Many large scale, high performance on-premise and cloud deployments	• Consumers cannot delete their profiles • Limited identity analytics • No built-in marketing functionality • Main presence in North America as of now, but growing in other regions

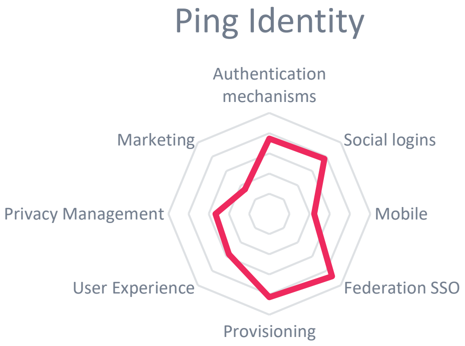
Table 17: PingIdentity major strengths and weaknesses.

Ping provides all the common authentication options and more, including SMS/email/phone OTP, RECAPTCHA, native mobile apps, FIDO U2F, and FIDO UAF. Social logins from Facebook, Twitter, Microsoft, Google, LinkedIn, and 30 other identity providers can be accepted. It also supports all forms of identity federation, such as SAML, OAuth, and OIDC. Bulk provisioning and bi-directional synchronization is possible via LDAP and SCIM. The PingIdentity Platform also can serve as an identity bridge to IDaaS, CRM, SaaS, and on-premise AD, IAM, and SSO implementations. Dashboards display real-time utilization. Reports show basic identity analytics such as logins, consent drop off rates, and opt-in/opt-out actions. More advanced identity and marketing analytics require 3rd party applications, for which APIs are provided.

Customers may choose which attributes to share at registration time and may edit them afterward. Fine-grained consent options are available. However, users are not prompted to re-consent when service terms change and users may only disable their accounts. Only administrators can delete user data. Family management can be implemented as group management, there is no explicit family UI.

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

Table 18: PingIdentity rating.



PingIdentity Platform is a robust IAM solution, offering a plethora of authentication and interoperability options. The addition of UnboundID provides customer engagement capabilities that will further enhance the platform as the technologies become integrated. Though it does not have built-in CRM or marketing analytics, it provides many OOTB connectors and APIs to facilitate integration with specialty solutions. Adding consent options, such as providing notifications when service terms change and giving users the ability to delete their profiles, would strengthen this already strong product suite. It is a high performing and scalable system which should be evaluated when conducting RFIs.

11.10 Salesforce Identity

Salesforce is a pioneer in PaaS and SaaS with their flagship CRM solution, and it is not a surprise that they also offer consumer identity services as well. Their identity platform has grown from servicing their own CRM platform and other tools to being a multi-purpose identity provider for many organizations. Salesforce has thousands of customers with many millions of managed identities, and thousands of SAML, OAuth, and OIDC connections, with automated federation protocol brokering. Salesforce Identity can be whitelabeled, to offer customers complete brand control. The solution is cloud-based only.

Strengths/Opportunities	Weaknesses/Threats
● Very large customer base with many large-scale deployments ● Excellent support for most standards ● Very good built-in identity and marketing analytics ● IoT identity support	● Extra licensing fee to connect to on-premise AD ● CIAM functionality focused on serving Salesforce.com ecosystem ● Needs additional consent options for GDPR compliance

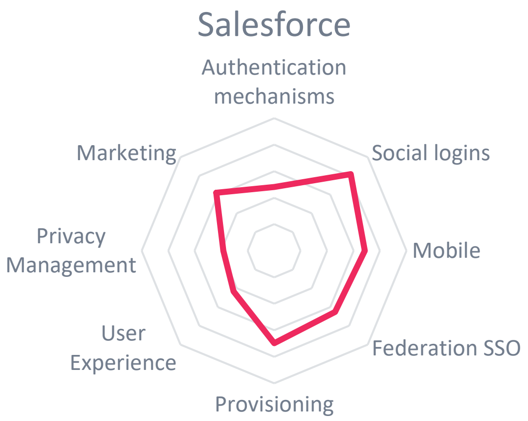
Table 19: Salesforce Identity major strengths and weaknesses.

Salesforce Identity accepts logins from all the common social networks, SMS OTP, and FIDO U2F. Salesforce also has Lightning login, a mobile app that utilizes built-in biometrics for challenge/response authentication. 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. To enable this feature, users register IoT devices via mobile apps provided by the vendors. Salesforce Identity handles key generation, and then IoT devices are represented by OAuth asset tokens. Many analytics features and reports are available within Salesforce Identity. For example, reports on logins, authenticator types used, registration sources, location, gender, consent info, other associated identities are available directly in Salesforce "Contact". 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.

Though Salesforce Identity does not have built-in fraud protection, administrators can configure feeds of 3rd party risk intelligence into the risk engine, and can require higher assurance authentication if any defined criteria fail. Salesforce Identity provides the tools for tenants to collect granular consent and manage families' digital access, but there are no default settings in place for those schemes.

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

Table 20: Salesforce Identity rating.



In summary, Salesforce Identity is a robust and scalable CIAM solution that provides much flexibility for the customers. For organizations that are already using Salesforce CRM or PaaS, adding Identity may be a natural choice. Thus, the service should be an option when looking for CIAM solutions.

11.11 SAP HANA Cloud Platform (HCP) Identity Authentication and Provisioning services

SAP, the world's 3rd largest software company headquartered in Germany, entered the cloud computing space 5 years ago and has quickly grown to offer numerous SaaS solutions. Accordingly, SAP has developed its own identity platform so that customers may integrate with their services: SAP HANA Cloud Platform Identity Authentication and SAP HANA Cloud Platform Identity Provisioning. SAP offers customer profile hosting as well.

Strengths/Opportunities	Weaknesses/Threats
● Very large customer base ● Provides identity services for SAP Cloud ● GDPR compliant consent management features ● LDAP and SCIM support	● No identity or marketing analytics ● No support for FIDO

Table 21: SAP HCP major strengths and weaknesses.

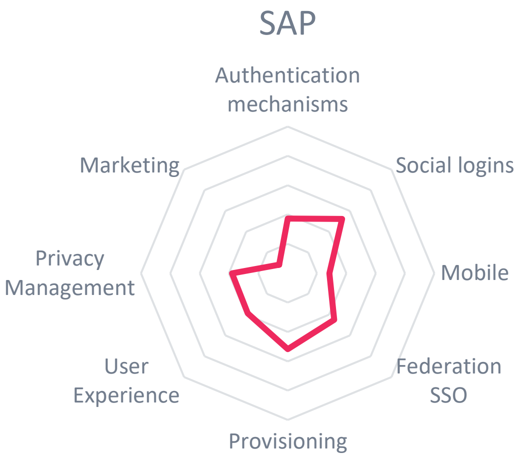
For customer authentication, SAP HCP Identity Authentication accepts password, SMS OTP, SAP mobile authenticator, and social logins (Facebook, Twitter, Google, and LinkedIn) as well as SPNEGO Kerberos. In federated use cases, it only accepts SAML and OAuth. Users can self-register. The product can be integrated and complemented by SAP HCP Identity Provisioning that can provision users via LDAP and SCIM interfaces. It can integrate HCP Identity Provisioning can integrate with SAP's on-premise identity management, SAP Identity Management.

SAP HCP Identity Provisioning does interface with SAP Hybris Cloud for Customer and SAP Jam, but there are no OOTB connectors to other CRM, identity analytics, or marketing analytics tools. Also, it doesn't have interface capabilities to SIEM/RTSI solutions, and cannot receive and process 3rd party fraud and threat intelligence information.

SAP HCP Identity Authenticaiton allows users to select which attributes to share from social registration, edit that information after registration, and it does notify users and ask them to re-consent when terms of service change. Moreover, in accordance with GDPR, it allows consumers to de-register and to delete their profiles altogether, and it provides privacy policy templates for various legal jurisdictions. However, it does not support family management or the UMA protocol.

Security	neutral
Functionality	weak
Integration	neutral
Interoperability	weak
Usability	neutral

Table 22: SAP HCP Identity rating.



SAP HCP is a robust solution in terms of number of deployments and market ecosystems. The offering needs additional features, such as supporting FIDO, providing adaptive authentication functionality, connecting with other IDaaS/SaaS, and either including marketing analysis tools or building interfaces for 3rd party analytics tools. For organizations with big SAP investments already, SAP HCP Identity Authentication and Provisioning should be on the consideration list.

11.12 SecureAuth IdP

SecureAuth is a well-established provider of IAM products and solutions. The company has a large customer base, primarily centered in North America. The product, which runs only on Windows Server 2012, is available for on-premise deployment. SecureAuth just launched Cloud Access, their IDaaS solution. It will also feature customer profile storage.

Strengths/Opportunities	Weaknesses/Threats
• Very large number of authentication options • Integration with SecureAuth adaptive authentication and risk engine	• Newly available in the cloud • Small customer base and ecosystem outside of North America • Needs tools or interfaces for analytics • Additional consent management features needed

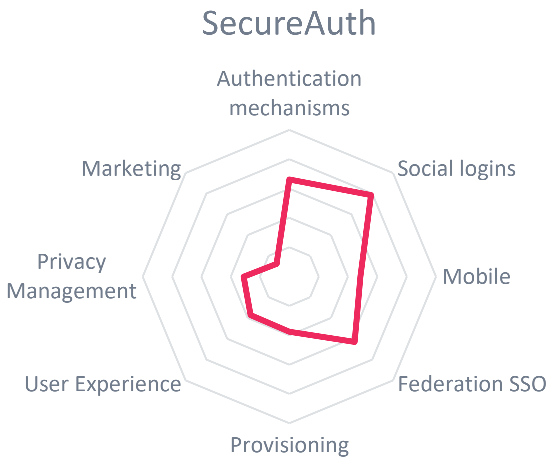
Table 23: SecureAuth IdP major strengths and weaknesses.

Built on SecureAuth's strong authentication product, this solution offers nearly every authentication method as an option, except FIDO. It supports LDAP for bulk provisioning. SecureAuth's adaptive risk engine permits administrators to write complex policies requiring different authentication methods for various resource access scenarios. It can also evaluate a large number of risk factors before granting access, such as device ID, geo-location, geo-velocity, etc. The SecureAuth risk engine can also receive and process 3rd party fraud and threat intelligence.

The product offers OOTB connectors to SIEM/RTSI tools. It can also integrate with IDaaS such as Microsoft Azure AD, Oracle, and Ping. SecureAuth does not have dashboards and reporting capabilities for identity and marketing analytics. SecureAuth IdP does allow consumers to granularly select attributes from social network providers at registration time, and to edit them afterward. SecureAuth IdP notifies customers about potential fraud activity, but does not notify for terms of service changes. It allows users to de-register and delete their stored profile information. The product does not currently support UMA or family management.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	neutral

Table 24: SecureAuth IdP rating.



SecureAuth IdP excels in authentication and adaptive risk factor processing. It is also quite strong with regards to security functionality. They have a large customer base, and their deployments are designed for high performance. Their cloud offering is new though. It may take time to scale as well as the on-premise solutions. To deliver full CIAM functionality, the solution needs to develop marketing analytics and business intelligence features, and/or provide OOTB connectors or standards-based interfaces to 3rd party products. For organizations whose CIAM requirements include strong security and lots of authentication options, SecureAuth should be on the consideration list.

12 Products 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 25.

Product	Security	Functionality	Integration	Interoperability	Usability
ForgeRock Identity Platform	strong positive	positive	positive	positive	neutral
Gigya Identity Enterprise	positive	strong positive	strong positive	positive	strong positive
IBM Cloud Identity Service	positive	positive	positive	positive	positive
iWelcome	positive	strong positive	positive	strong positive	strong positive
Janrain	strong positive	positive	positive	neutral	strong positive
LoginRadius	positive	neutral	positive	neutral	strong positive
Microsoft Azure AD B2C	neutral	neutral	positive	weak	neutral
Okta Platform	strong positive	neutral	neutral	neutral	neutral
PingIdentity Platform	strong positive	strong positive	positive	strong positive	positive
Salesforce Identity	positive	positive	strong positive	positive	strong positive
SAP Cloud Platform Identity	neutral	weak	neutral	weak	neutral
SecureAuth IdP	positive	neutral	positive	neutral	neutral

Table 25: Comparative overview of the ratings for the product capabilities.

In addition, we provide in table 26 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
ForgeRock	positive	neutral	weak	strong positive
Gigya	positive	positive	neutral	strong positive
IBM	neutral	neutral	strong positive	positive
iWelcome	positive	weak	weak	weak
Janrain	neutral	positive	weak	neutral
LoginRadius	weak	neutral	weak	weak
Microsoft	weak	positive	strong positive	positive
Okta	neutral	weak	weak	strong positive
PingIdentity	positive	positive	positive	positive
Salesforce	positive	strong positive	strong positive	positive
SAP	weak	neutral	strong positive	positive
SecureAuth	critical	neutral	weak	positive

Table 26: Comparative overview of the ratings for vendors.

Table 26 requires some additional explanation in case that a vendor has got a “critical” rating.

In the area of *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, privacy consent management, marketing analytics capabilities, and others. However, in this analysis all vendors scored at least neutral regarding this criterion.

The *critical* ratings are applied for *Market Position* in the case of vendors which have a very limited visibility (with that particular product and in general) 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 the area of *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 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 the own consulting and system integration business. However, our strong believe is that growth and successful market entry of companies into a market segment relies on strong partnerships.

12.1 The Market/Product Matrix

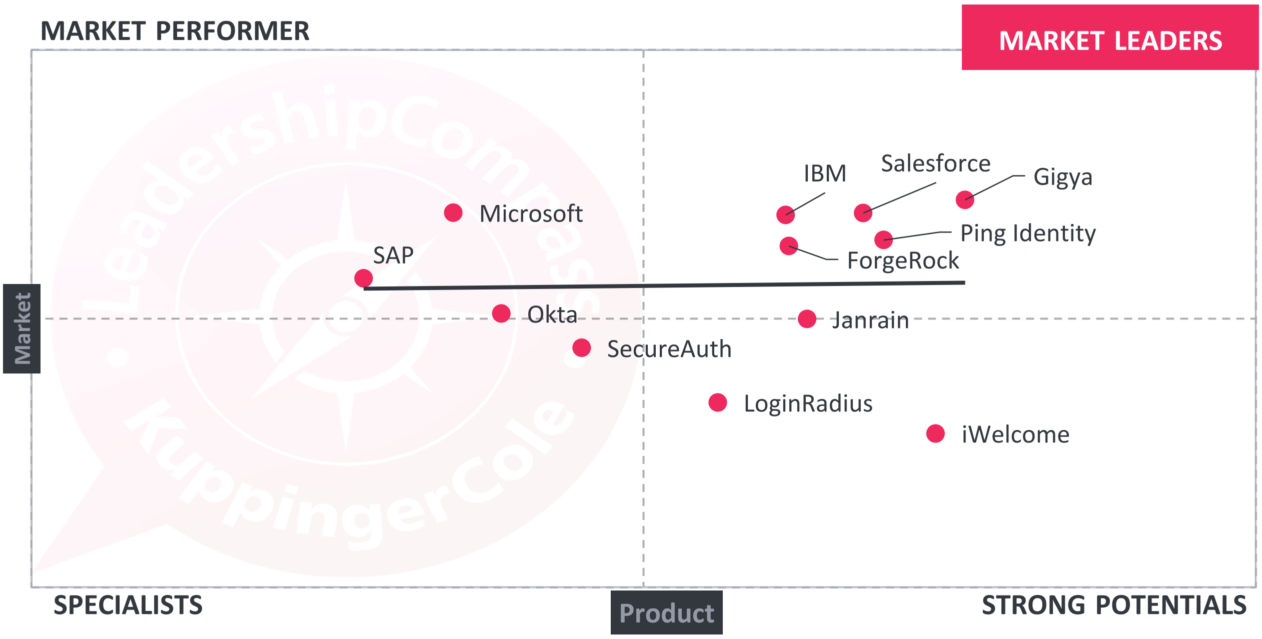


Fig. 10: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

Beyond that analysis, we have compared the position of vendors regarding combinations of our three major areas of analysis, i.e. Market Leadership, Product Leadership, and Innovation Leadership.

These comparisons, for instance, use the rating in Product Leadership on the horizontal axis and relate it with the rating in other areas, which is shown on the vertical axis. The result is split into four quadrants. The upper right quadrant contains products with strength both in the product rating and in the second rating we've looked at in the particular matrix, e.g. innovation. The lower right quadrant contains products that are overall quite strong but are lacking in the dimension shown on the vertical axis.

For example, this can be products that have strong technical capabilities but are relatively new to the market, resulting in a small customer base. The upper left quadrant contains products which are typically below average in the product rating but have specific strengths regarding the second dimension we look at in the particular matrix. They might be highly innovative or very mature and established, but not being leading edge when looking at the product rating. Finally, the lower left quadrant contains products suffering on both axes. However, these products might have specific strengths that are highly valuable for some specific use cases.

In that 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 often the very large vendors, while vendors below the line frequently are innovative but focused on specific regions.

We've defined four segments of vendors to help in classifying them:

Market Leaders: This segment contains vendors which have a strong position in our categories of Product Leadership and Market Leadership. These vendors have an overall strong to excellent position in the market.

Strong Potentials: This segment includes vendors which have strong products, being ranked high in our Product Leadership evaluation. However, their market position is not as good. That might be due to various reasons, like a regional focus of the vendors or the fact that they are niche vendors in that particular market segment.

Market Performers: Here we find vendors which have a stronger position in Market Leadership than in Product Leadership. Typically, such vendors have a strong, established customer base due to other market segments they are active in.

Specialists: In that segment we typically find specialized vendors which have – in most cases – specific strengths but neither provide full coverage of all features which are common in the particular market segment nor count among the software vendors with overall very large portfolios.

This chart shows an interesting distribution of the vendors. On one hand, we see a number of companies in the Market Leaders segment. These include the overall leaders such as ForgeRock, Gigya, IBM, Salesforce, and PingIdentity.

The Strong Potentials segment also contains a number of vendors, with iWelcome, Janrain, and LoginRadius.

Microsoft, Okta, and SAP are the Market Performers. Both have large customer sets due to the other niches within the IAM market that they are serving.

SecureAuth is in the Specialists category. Specialists, as the name implies, generally offer specialized products, or in other cases, serve smaller specialized markets with a constrained feature set directed by those markets. SecureAuth is a specialist in the category of offering a wide array of strong and adaptive authentication mechanisms.

12.2 The Product/Innovation Matrix

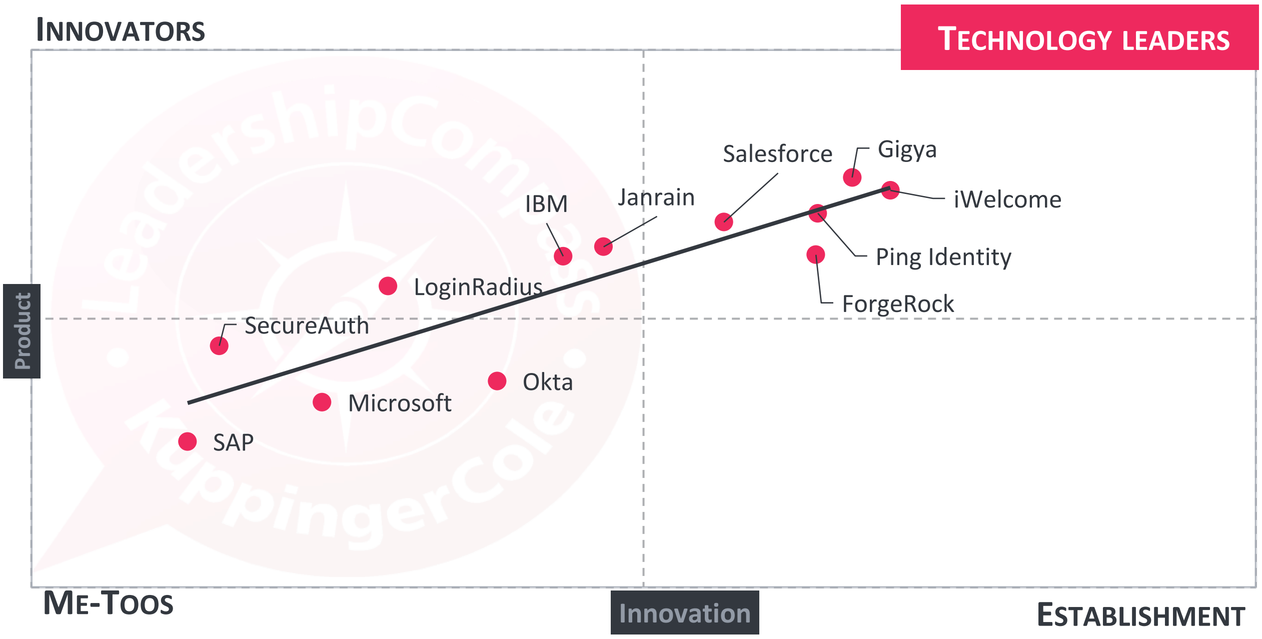


Fig. 11: The Product/Innovation Matrix. Vendors below the line are less innovative, vendors above the line are, compared to the current Product Leadership positioning, more innovative.

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 typical for mature markets with a significant number of established vendors plus a number of smaller vendors.

Again we've defined four segments of vendors. These are

Technology Leaders: This group contains vendors which have technologies which are strong regarding their existing functionality and which show a good degree of innovation.

Establishment: In this segment we typically find vendors which have a relatively good position in the market but don't perform as strong when it comes to innovation. However, there are exceptions if vendors take a different path and focus on innovations which are not common in the market and thus do not count that strong for the Innovation Leadership rating.

Innovators: Here we find highly innovative vendors with a limited visibility in the market. It is always worth having a look at this segment because vendors therein might be a fit for specific customer requirements.

Me-toos: This segment mainly contains those vendors which are following the market. There are exceptions in the case of vendors which take a fundamentally different approach to providing specialized point solutions. However, in most cases this is more about delivering what others have already created.

In this chart, ForgeRock, Gigya, iWelcome, PingIdentity, and Salesforce are found in the Technology Leaders segment, with a strong correlation between Innovation and Product rating. This is typical for more mature markets, where most vendors deliver a broad set of features, including at least a significant portion of the more innovative features.

Janrain, LoginRadius, and IBM are the Innovators. Though they have a good customer base, their products may not have sufficient visibility in the market.

There are no Establishment vendors, as described in this context.

The Me-Toos are comprised of Microsoft, SAP, and SecureAuth. The products offered here have value for their customers, although the products are generally not pushing the technological envelope.

12.3 The Innovation/Market Matrix

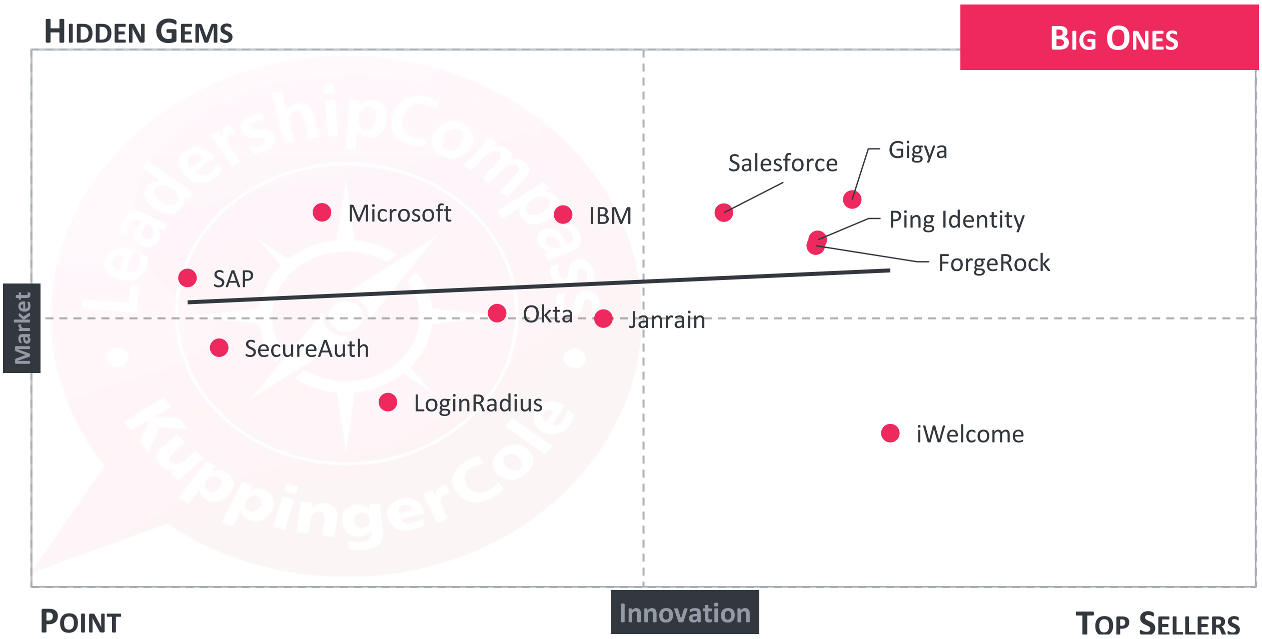


Fig. 12: The Innovation/Market Matrix. Vendors below the line are performing well in the market compared to their relatively weak position in the Innovation Leadership rating, while vendors above the line show based on their ability to innovate, the biggest potential for improving their market position.

The third relation 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 but might also fail, especially in the case of smaller vendors.

The four segments we have defined here are

Big Ones: These are market leading vendors with a good to strong position in Innovation Leadership. This segment mainly includes large software vendors.

Top Sellers: In this segment we find vendors which have an excellent market position compared to their ranking in the Innovation Leadership rating. That can be caused by a strong sales force or by selling to a specific community of repeat customers, i.e., a loyal and powerful group of contacts in the customer organizations.

Hidden Gems: Here we find vendors which are more innovative than would be expected when looking at their Market Leadership rating. These vendors have a strong potential for growth, however they also might fail in delivering on that potential. Nevertheless, this group is always worth a look due to their specific position in the market.

Point Vendors: In that segment we find vendors which typically either have point solutions or which are targeting specific groups of customers, like SMBs, with solutions focused on these, but not necessarily covering all requirements of all types of customers and thus not being amongst the Innovation Leaders. These vendors might be attractive if their solution fits the specific customer requirements.

Here we see a number of companies being both highly innovative and having a strong position in the market. These companies, being placed in the Big Ones segment, include ForgeRock, Gigya, PingIdentity, and Salesforce.

iWelcome is the lone top seller, due to its unique consent management capabilities in the market segment.

The Hidden Gems segment contains IBM, Microsoft, Okta, and SAP. Though they are strong in the market already, it could be that customers have not recognized the value of their offering in this segment.

Point Vendors include Janrain, LoginRadius, and SecureAuth. Janrain is almost in the Hidden Gems category.

13 Overall Leadership – the combined view

Finally, we've put together the three different ratings for Leadership, i.e. Market Leadership, Product Leadership, and Innovation Leadership and created an Overall Leadership rating. This is shown below in figure 13.

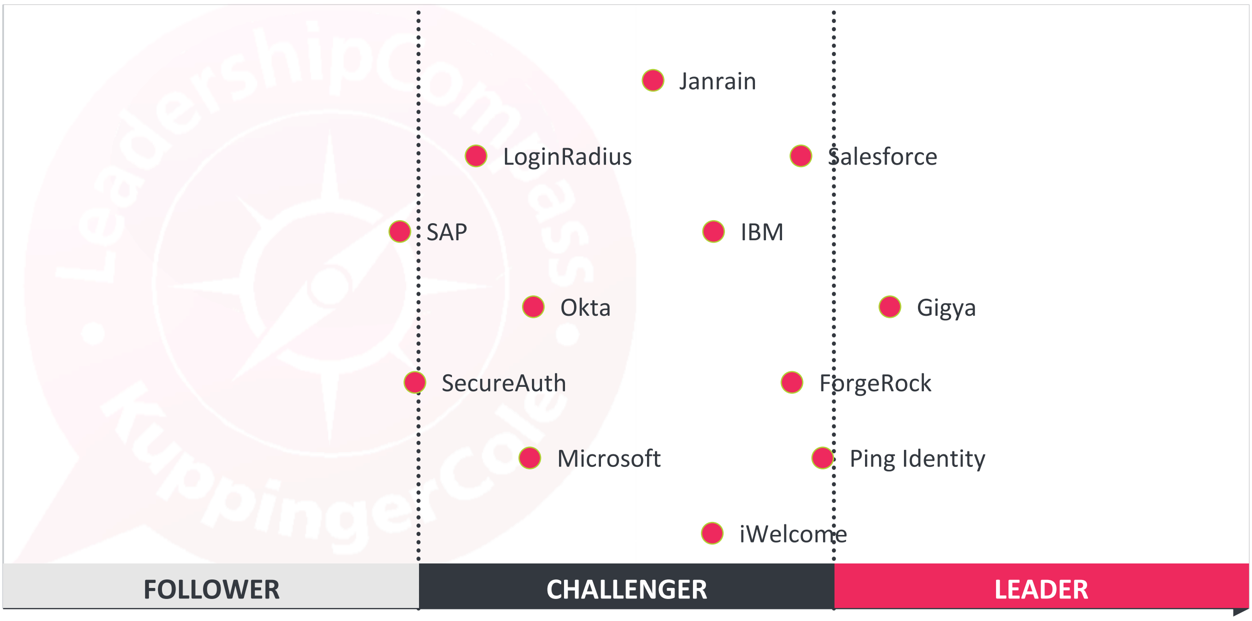


Fig. 13: The Overall Leadership rating for the CIAM market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

In the market for CIAM, we currently see only Gigya in the Leader segment for Overall Leadership. Gigya has a strong feature set and large customer base.

The Challenger segment is very crowded, with most vendors being placed in that segment. Here we find a variety of players, including large and established vendors such as Microsoft and IBM, which provide scalable offerings, however they may not always be as feature-rich and innovative as the companies in the Leaders segment. ForgeRock, iWecome, PingIdentity, and Salesforce almost made it into the Leader space, and as such are regarded as strong challengers. Furthermore, we find a number of specialists in the Challengers section, including Janrain, LoginRadius, and Okta.

Finally, we have SAP and SecureAuth being placed in the Followers section. These vendors generally have product offerings that delivers baseline capabilities, but still do not have the breadth of functional coverage as other products in the market. However, they are on their way towards becoming a challenger for the more established players in the market and might be a good choice for certain specific use cases and customer requirements.

Again: Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping to the features provided by the vendor's products is mandatory. Overall Leaders are (in alphabetical order):

- Gigya

14 Vendors and Market Segments to watch

Besides the vendors covered in this KuppingerCole Leadership Compass on CIAM, there are several other vendors which either declined to participate in this KuppingerCole Leadership Compass, have only a slight overlap with the topic of this document, or are not (yet) mature enough to be considered in this document. This includes the following vendors:

AvocoSecure

AvocoSecure is a privately-owned UK company offering Cloud and CIAM services. Their product is called Trust Platform, and it is relatively new in the marketplace. 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. It is 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 also accepts federated login via SAML, OIDC, and OAuth.

Using REST API, Trust Platform can feed data to SIEM/RTSI 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 does provide strong privacy consent management functionality. Consumers must approve attributes from social networks, and they are prompted to re-accept when terms or conditions change. Users may also edit or delete their information at any time after registration as well. Trust Platform does support UMA, and AvocoSecure has been a participant in the development of that standard. The product has a built-in family management features handled through granular access by delegation - digital death handling is also on the near term roadmap.

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.

Bitium

Bitium, based in California, is a provider of IAM solutions for mid-market to enterprise companies. 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. They may be considered for review in future KuppingerCole publications.

Ilantus

Ilantus is a well-established US-based company that provides a suite of IAM products. They have a large global customer base. Their flagship product is identity governance and administration. The Ilantus suite includes Xpress Governance, Xpress Sign-On, Xpress Password & Password Reset-as-a-Service, and Xpress Access. They offer managed IGA and IAM services, and have been moving to the cloud, as evidenced by the Xpress IDaaS solution. Xpress IDaaS can enable enterprise SSO to SAP, Salesforce, Microsoft Office 365, Netuite, Wordkay, and Google Apps. The functionality provided is well-suited for CIAM use cases. Ilantus' products will be examined in future KuppingerCole research.

Ubisecure

Ubisecure has internationally recognized expertise in delivering PKI solutions at the national and enterprise scale. Their products also include access management and identity federation solutions. Their integrated product solutions deliver rich CIAM functionality, particularly in terms of strong authentication support and IoT device identity management. Ubisecure will be considered in future KuppingerCole evaluations.

15 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**

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

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