KuppingerCole Report

LEADERSHIP COMPASS

by John Tolbert | June 2017

CIAM Platforms

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

by **John Tolbert**
jt@kuppingercole.com
June 2017

Leadership Compass
CIAM Platforms
By KuppingerCole

Content

Content of Tables

Content of Figures

Related Research

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

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

Advisory Note: Secure your Cloud against Industrial Espionage - 70997

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

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

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

Executive View: Cloud Standards Cross Reference - 71124

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

Executive View: Executive View Microsoft Azure RMS - 70976

Executive View: PingFederate 7 - 70801

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

Executive View: Exostar Services for Life Sciences - 70878

Executive View: PingOne® - 70870

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 70960

Leadership Compass: Access Management and Federation - 70790

Leadership Compass: Access Governance - 70735

Product Report: Microsoft Azure Active Directory - 70977

1 Introduction

Consumer Identity and Access Management (CIAM) is a sub-genre of traditional Identity and Access Management (IAM) that has emerged in the last few years to meet evolving business requirements. Many businesses and public sector organizations are finding that they must provide better digital experiences for and gather more information about the consumers who are using their services. Enterprises want to collect, store, and analyze data on consumers in order to create additional sales opportunities and increase brand loyalty. Know Your Customer (KYC) initiatives, particularly in the financial sector, are another example of the business driver motivating exploration and adoption of CIAM.

CIAM goes beyond traditional IAM in commonly supporting some baseline features for analyzing customer behavior, as well as integration 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. Some solutions in this space provide connections to various identity proofing services to strengthen the veracity of the consumer attributes. CIAM systems generally feature weak password-based authentication, but also support social logins and other authentication methods. Information collected about consumers can be used for many different purposes, such as authorization to resources, or for analysis to support marketing campaigns, or Anti-Money Laundering (AML) initiatives. Moreover, CIAM systems must be able to manage many millions of identities, and process potentially billions of logins and other transactions per day.

In order to reduce money laundering, cyber-crime, terrorist financing, and fraud, regulators are requiring banks and financial service providers to put into place mechanisms for "Knowing Your Customer". Government regulators expect banks to utilize analytics to develop baseline patterns for all their customers, and to be able to spot deviations from individuals' normal parameters. Suspicious transactions must be flagged for investigation, specifically to prevent the aforementioned criminal activities. Having IAM systems dedicated to hosting consumer identities and their associated profiles is a good first step toward KYC.

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

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

The entire market segment is somewhat young compared to traditional IAM and still evolving. We expect to see more changes and perhaps more entrants within the next few years.

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

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

1.1 Market Segment

The CIAM market is growing, with some vendors offering mature solutions providing standard and deluxe features to support millions of users across almost every industrial sector. As will be reflected in this report, the solutions in this space are quite diverse. Some vendors have just about every feature one could want in a CIAM product, while others are more specialized, and thus have different kinds of technical capabilities. For example, some smaller vendors are targeting the government-to-citizen (G2C) market as well as business-to-consumer (B2C). We often see support for national e-IDs, x.509 certificates, and higher assurance authentication mechanisms in these vendors' products compared to the rest.

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

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 more rapidly than traditional IAM.

A new category is emerging within CIAM, that of CIAM developer platforms. CIAM developer platforms are not always completely assembled products and services. Rather, these platforms are collections of tools, code, and templates. CIAM developer platforms may contain many open source elements, and generally leverage well-known standards. KuppingerCole is tracking developments in this area and will examine these CIAM developer platforms in future research papers.

1.2 Delivery models

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

1.3 Required Capabilities

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

- Deployment options: On-premise, cloud, or hybrid options.
- Social logins: Allow users to login via Facebook, LinkedIn, Twitter, Google, Amazon, etc.
- Multi-factor authentication: SmartCards, tokens, OTP, Biometrics, OOB mobile push apps, etc.
- Risk adaptive authentication: Conduct user behavioral analytics and threat intelligence evaluated to match the appropriate authentication mechanism to the level of business risk
- Cyber threat and/or fraud intelligence: Consume internal or external cyber threat or fraud information, such as known bad domains, compromised credentials, accounts suspected of fraud, etc., for the purpose of evaluation by the risk engine to choose the right authentication mechanisms and permit/deny access or transaction completion.
- Business intelligence: Transform data about user activities into information for marketers
- Privacy and consent management: Explicit user consent must be received for the use of their information
- Enhanced user experience: White-labeled CIAM solutions allow seamless branding, and self-registration and social logins increase successful consumer interaction with websites
- IoT device identity information: As IoT devices increase in popularity, consumers and business customer users will have greater need to associate their IoT devices with their digital identities. These identity associations between subject and IoT object will allow for more secure and private use of smart home, wearables, medical, and even industrial devices.

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

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 majority offer CIAM as SaaS.

When evaluating the services, besides looking at the aspects of

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- core features of CIAM

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

Authentication	Social logins, mobile support, multi-factor authentication
Consent	Facilities within the UI to allow consumers to unambiguously opt-in to services and 3rd party usage of their data. Ability to export and delete consumer profiles as requested. Family management
IoT	Extensions to the CIAM platform to allow consumers to register, activate, and monitor usage of IoT devices by associating consumer identity with device identity. The use of OAuth2 Device Flow specification is a good means to achieve this

Marketing	Once consent is given, transforming information for marketing campaigns, creating special offers, encouraging brand loyalty. Includes identity analytics features, such as the ability to generate and customize reports on user actions, as well as representing aggregated activity on enterprise dashboards in real-time
Mobile	Mobile authentication options, native app SDKs for customer developers, mobile apps for managing consumer information, mobile management apps for CIAM systems
Registration	Self-registration, self-maintenance of attributes, consistent branding, bulk provisioning
Risk Analysis	Evaluation of user attributes, environmental factors, and other information to determine authentication and authorization levels required per transaction
SSO	Solutions use standards such as SAML, OpenId, OIDC, and OAuth for identity federation amongst a customer's websites. It can also include proprietary connectors for internally hosted applications and SaaS applications, such as CRM, Marketing Automation, etc.

Each of the categories above will be considered in the product evaluations below. We've also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other offerings available in the market.

- Support for new standards such as GSMA Mobile Connect, Kantara Initiative UMA (User Managed Access), FIDO Alliance, and Global Platform Secure Element and Trusted Execution Environment standards.
- Flexible self-registration processes that can be white-labeled by tenants.
- Advanced cloud provisioning capabilities, such as Graph API and SCIM standard support.
- A comprehensive and consistent set of REST-based APIs for identity, marketing, and security analytics.
- Self-service portals for viewing and editing consent.
- Advanced support for authentication mechanisms, especially mobile biometrics.
- Mobile app integration capabilities (SDKs).
- Integration with national e-IDs and passports.

Please note, that we only listed major features, but looked at other capabilities as well when evaluating and rating the various CIAM platforms.

2 Leadership

Selecting a vendor of a product or service must not be only based on the comparison provided by a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

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

- Product Leadership
- Innovation Leadership
- Market Leadership

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

We find several companies in the Leader section. Gigya leads the field, showing strong ratings in all Leadership categories.

At the time of this update, ForgeRock, Janrain, and Salesforce have crossed into the Leader section. ForgeRock has added several innovative capabilities to their Identity Platform, particularly in support of IoT identity integration and microservices. Janrain supports 50 different IoT applications and facilitates GDPR compliance for customers. Salesforce continues to add features, also around device identity for IoT.

In the Challenger segment, Ping Identity is on the cusp of becoming an Overall Leader. Just behind Ping Identity, we find CA Technologies, IBM, and iWelcome. Each of these companies has taken a different track in developing CIAM solutions. iWelcome has excellent consent management capabilities to help EU customers comply with GDPR. CA and IBM leverage their strong IAM base to provide robust, scalable, and secure solutions for their customers. IBM also has in-car telematics and mobility applications for their consumer-facing customers. Login Radius and Okta have shifted further to the right. Okta's recent IPO helps improves their market position. Rounding out the Challenger block is EmpowerID, Microsoft, and SecureAuth. Microsoft's market share and recent releases have pushed it into the center.

EmpowerID and SecureAuth have CIAM offerings derived from high security IAM technologies which may make them a good fit for customers with these types of requirements.

In the Follower segment, we see that Avatier is branching out to pursue CIAM.

Overall Leaders are (in alphabetical order):

- ForgeRock
- Gigya
- Janrain
- Salesforce

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

Figure 2: Product leaders in the CIAM market segment

Product Leadership, or in some cases Service Leadership, is where we examine the functional strength and completeness of products. Gigya is in front, with their full-featured suite addressing a wide range of CIAM business requirements. They are closely followed by iWelcome. iWelcome's platform is tailored to meet the needs of consumer identity needs of EU customers, with fine-grained consent options and detailed auditing. ForgeRock, Janrain, Ping Identity, and Salesforce are also found in the Product Leader section. ForgeRock Identity Platform, while not offered as SaaS, can be run in the cloud, and offers much flexibility to customers. Janrain is cloud-based, having deployed in Amazon Web Services starting back in 2006, focusing on high availability. Salesforce is also cloud-based, and provides rich marketing

functionality. Ping Identity's CIAM solution suite is available for either on-premise or cloud deployment, and offers customers scalable, standards-based support to achieve their objectives.

The growth in the number of Product Leaders since 2016 shows that there has been rapid innovation in this field. More vendors are adding a wide array of appealing and useful features into their products and services.

In the Challenger section, we see CA Technologies being very close to becoming a Product Leader. Tight integration with their IAM stack, including their API Gateway, and good mobile support are hallmarks of their CIAM offering. IBM is following closely with high security authentication and administration options that make it a challenger to the Product Leaders.

Following them, we see (in alphabetical order), EmpowerID, Login Radius, Microsoft, Okta, and SecureAuth. All of them have their specific strengths, but commonly lack some features we expect to see.

In the Follower segment, we find Avatier, with a history in strong security B2B environments, moving into the B2C world.

Product Leaders (in alphabetical order):

- ForgeRock
- Gigya
- iWelcome
- Janrain
- Ping Identity
- Salesforce

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested cutting-edge features, while maintaining compatibility with previous versions.

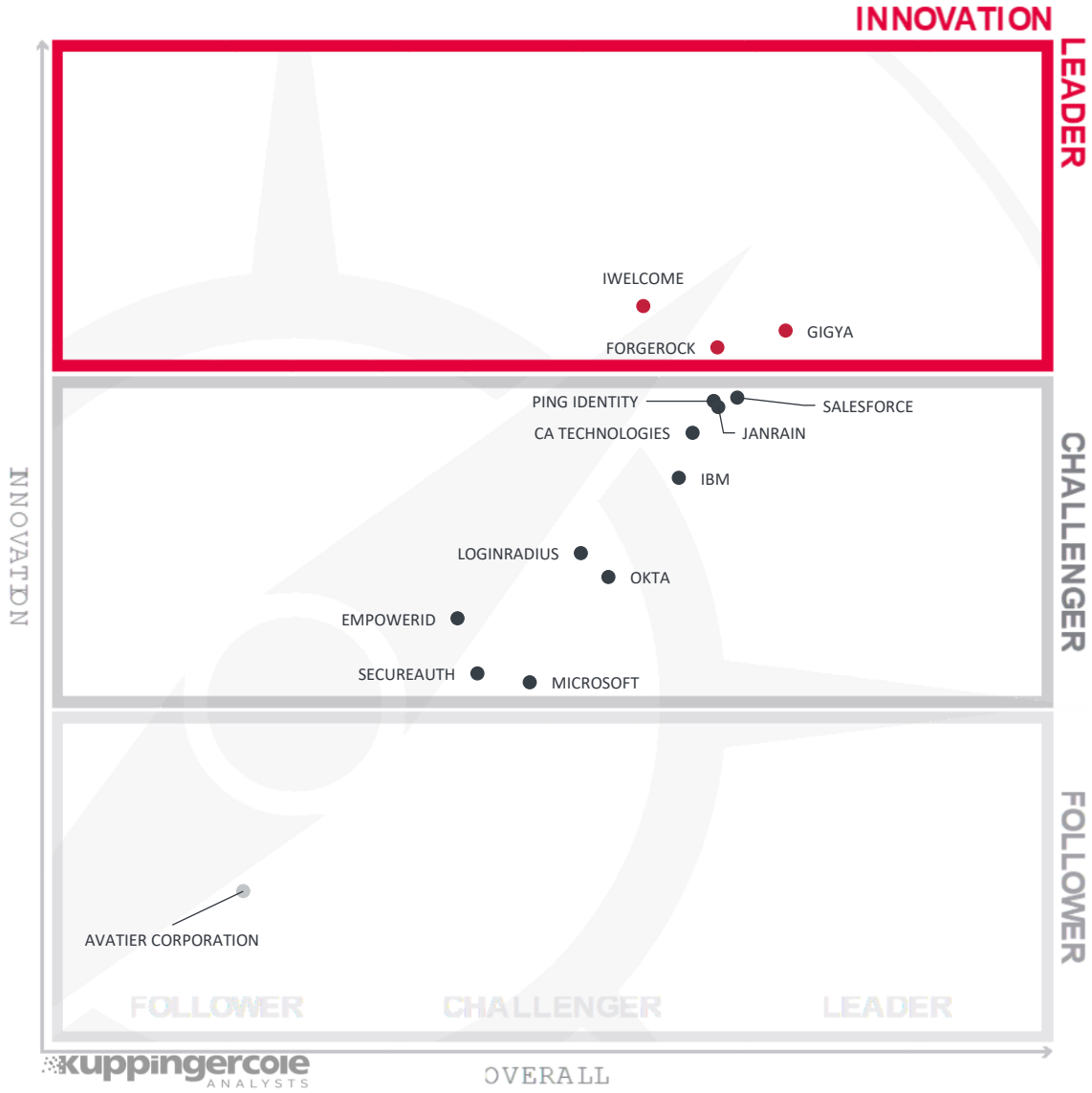


Figure 3: Innovation leaders in the CIAM market segment

When looking at Innovation Leadership, iWelcome is slightly ahead of all others, based on excellent consent management, marketing capabilities, and an extensible data model. Closely following (in alphabetical order) are ForgeRock and Gigya, constantly delivering new features at customer request, such as IoT device identity linking with consumer identities.

In the Challenger segment, we see CA Technologies, Janrain, Ping Identity, and Salesforce on the verge of becoming Leaders. Each of these vendors has made significant enhancements to their products that address real business needs. In the remainder of the Challenger block, in alphabetical order, we find EmpowerID, IBM, Microsoft, Okta, and SecureAuth. They are building in more CIAM baseline functionality and we expect them to improve in the months ahead.

Avatier appears in the Follower section.

Innovation Leaders (in alphabetical order):

- ForgeRock
- Gigya
- iWelcome

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

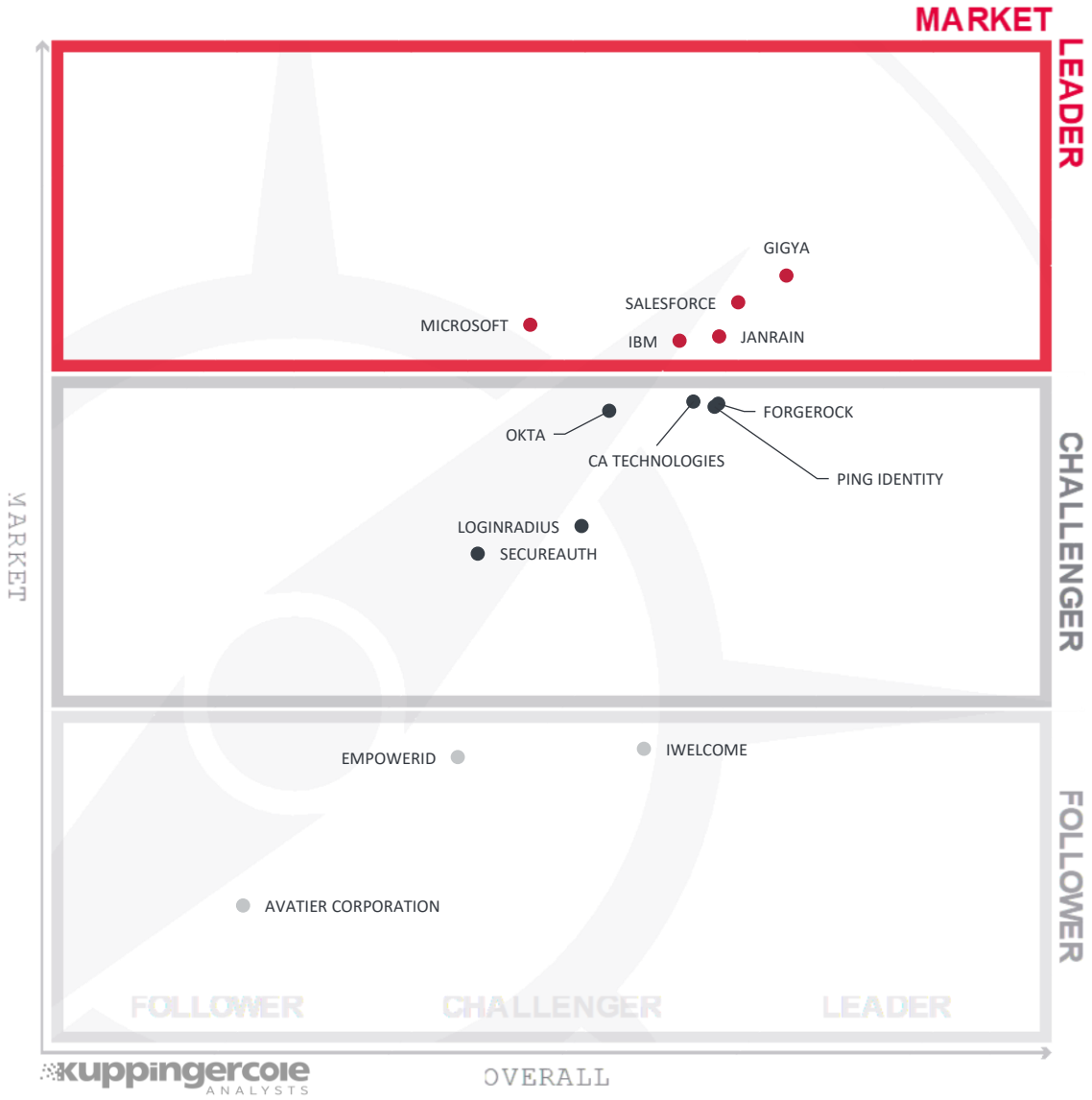


Figure 4: Market leaders in the CIAM market segment

Gigya is the Market leader, due to its large global customer base, partner and support network.

IBM, Janrain, Microsoft, and Salesforce are also Market Leaders. As very large software companies and service providers, we are not surprised by their strong position in this market. They each also have customers around the world, with large and experienced partners for implementations and support.

We find CA Technologies, ForgeRock, Okta, and Ping Identity at the top of the Challenger segment. These companies have captured large numbers of customers, and have very good support ecosystems. Login Radius and SecureAuth complete the Challenger section of the Market Leadership analysis.

Finally, we see Avatier and iWelcome in the Followers section. iWelcome is full featured but only focused on the EU market. Avatier was focused on B2B but is moving into B2C. Each of these companies' products fill a niche and are interesting to certain customers.

Market Leaders (in alphabetical order):

- Gigya
- IBM
- Janrain
- Microsoft
- Salesforce

3 Correlated View

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

3.1 The Market/Product Matrix

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

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

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

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

In the upper right box, we find Gigya, Janrain, and Salesforce. These vendors are leading in both the product and market ratings.

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

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

In the center of the graphic, we find (in alphabetical order) CA Technologies, Login Radius, Okta, and SecureAuth. These all have respectable positions in both the Product Leadership and Market Leadership ratings and thus are interesting options to the leading vendors.

iWelcome resides in the lower right, which indicates excellent product strength compared to market position. EmpowerID is in the lower center, while Avatier is in the lower left. These have smaller market shares and products that may be concentrated on specific feature sets for targeted customers.

3.2 The Product/Innovation Matrix

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

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

This chart shows a quite interesting picture. Most vendors are near the line, showing a balanced ratio of product capabilities and innovation. ForgeRock, Gigya, and iWelcome are the technology leaders, with many advanced features.

The spaces below technology leaders are empty. In the top center, we find Janrain, Ping Identity, and Salesforce, with strong products containing many innovative features.

Most vendor products reside in the center of the chart: CA Technologies, EmpowerID, IBM, Login Radius, Microsoft, Okta, and SecureAuth.

In the lower left sector, we find Avatier, who is just entering the CIAM market.

3.3 The Innovation/Market Matrix

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

Figure 7: The Innovation/Market Matrix

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

Gigya occupies the top left sector, having both an excellent position in the market and presenting innovative capabilities to their customers. ForgeRock and iWelcome appear on the leftmost side also, indicating very strong innovation, but having less market share.

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

Once again, the majority of the vendors surveyed fall into the center of the chart: CA Technologies, Login Radius, Okta, Ping Identity, and SecureAuth. CA Technologies and Ping Identity are closest to crossing into the top right sector.

EmpowerID is found in the lower center, offering some innovative features but not yet capturing a large share of the market. Avatier, as a new entrant, has some high security features derived from their B2B offering, but small market share.

4 Products and Vendors at a glance

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

4.1 Ratings at a glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in table 1.

Product	Security	Functionality	Integration	Interoperability	Usability
Avatier	weak	weak	weak	neutral	positive
CA Technologies	strong positive	positive	positive	positive	positive
EmpowerID	positive	positive	neutral	neutral	positive
ForgeRock	strong positive	strong positive	positive	positive	strong positive
Gigya	positive	strong positive	strong positive	positive	strong positive
IBM	positive	positive	strong positive	strong positive	positive
iWelcome	strong positive	strong positive	positive	strong positive	strong positive
Janrain	strong positive	positive	strong positive	positive	strong positive
LoginRadius	positive	positive	positive	positive	strong positive
Microsoft	positive	positive	positive	neutral	neutral
Okta	strong positive	positive	strong positive	positive	neutral
Ping Identity	strong positive	positive	strong positive	strong positive	positive
Salesforce	positive	positive	strong positive	positive	strong positive
SecureAuth	strong positive	neutral	positive	neutral	positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Avatier	weak	weak	weak	weak
CA Technologies	positive	positive	strong positive	Positive
EmpowerID	neutral	weak	weak	weak
ForgeRock	strong positive	positive	positive	strong positive
Gigya	strong positive	strong positive	neutral	strong positive
IBM	neutral	strong positive	strong positive	strong positive
iWelcome	strong positive	weak	weak	weak
Janrain	positive	strong positive	neutral	strong positive
LoginRadius	neutral	neutral	weak	positive
Microsoft	neutral	strong positive	strong positive	positive
Okta	neutral	positive	positive	strong positive
Ping Identity	positive	positive	positive	positive
Salesforce	positive	strong positive	strong positive	strong positive
SecureAuth	neutral	neutral	neutral	neutral

Table 2: Comparative overview of the ratings for vendors

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

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

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

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

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

5 Product/service evaluation

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

5.1 Avatier

California-based Avatier is an enterprise IAM vendor moving into CIAM. Their focus is on rapid deployment of basic IAM services to customers. Avatier has mostly been deployed on-premise, but is being run in IaaS by some customers. Avatier is launching a new SaaS which can store customer profiles.

Strengths	Challenges
• Hybrid IAM to CIAM • Good selection of strong MFA mechanisms • Basic built-in identity governance	• More IAM than CIAM, but broadening capabilities • Needs risk adaptive authentication • No native marketing analytics and interfaces • No IoT device identity integration

Table 3: Avatier's major strengths and challenges

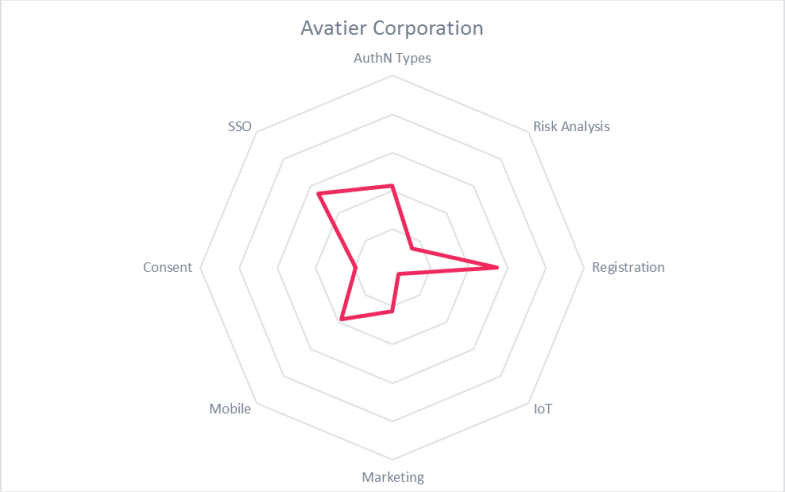
Avatier supports authentication mechanisms including Knowledge-based Authentication (KBA), email/phone/SMS OTP, Symantec VIP, Duo, Google Authenticator, RSA SecurID, HID, SmartCards, CipherLock, and Microsoft MFA. The Avatier mobile app features fingerprint, voice, facial recognition biometrics, but doesn't support FIDO. Avatier can accept social logins including Facebook, Microsoft, LinkedIn, Twitter, etc. SAML and OAuth are supported for federation. Users can self-register, or be provisioned via LDAP or SCIM. Risk factor evaluation and adaptive authentication are not possible within the product today.

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

Users can select which attributes are shared from social logins at registration time, but cannot indicate consent to additional usages. Moreover, users cannot delete their accounts and profiles. The product does not support family management.

Security	weak
Functionality	weak
Integration	weak
Interoperability	neutral
Usability	positive

Table 4: Avatier rating



Avatier is a privately owned IAM company moving into CIAM. The product has good authentication options. However, it lacks identity and marketing analytics, risk adaptive authentication, IoT integration, and privacy management functions. As the Avatier product evolves, we expect the feature set to include more B2C features.

5.2 CA Technologies Identity Portfolio

Well known for enterprise IAM, CA Technologies tightly integrated suite is also used in B2C environments that need higher security. CA Identity Portfolio comprises Identity Management and Governance, Privileged Access Management, Single Sign-On, Advanced Authentication, and Directory products. The product can be deployed on-premise on Red Hat or SUSE Linux, or Windows Server. CA also offers Identity Portfolio as SaaS through partners.

Strengths	Challenges
• Many strong authentication options • Robust risk engine for adaptive authentication • Mobile API Gateway (MAG), API Management, Bluetooth, and QR code support for IoT integration	• Primarily on-premise solution, but SaaS options are becoming available • Complex customer profile storage may require database schema changes • Marketing analytics via APIs to 3rd party products

Table 5: CA's major strengths and challenges

For authentication, CA Identity Portfolio includes social logins, KBA, and OTP (email, phone, and SMS). Several 3rd-party authenticators interoperate with the platform. Step-up authentication is also available via a mobile push app. CA is a sponsor member of the FIDO Alliance, and we expect to see FIDO protocol support in the medium term. The risk engine analyzes up to 200 different risk factors, including user behavioral profiling. Different authentication methods can be triggered based on risk scores. LDAP and SCIM interfaces are available for provisioning. The product integrates with SIEM/RTSI via syslog, and with GRC and SRM systems via APIs.

Marketing analytics is not a current focus for CA's customers. But CA Identity Portfolio does allow for integration with 3rd-party big-data, identity, and marketing analytics via REST APIs. Some customers are integrating IoT sensors and device identities into the directory by Bluetooth and QR code registration. Identity management of these IoT devices can be achieved with CA API Management and MAG.

User dashboards facilitate consent collection. CA Identity Portfolio supports user data export and deletion. Family management can be accomplished with some customization using the provided APIs.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 6: CA's rating

CA Identity Platform is a leader in the enterprise IAM market, being mature and widely deployed. CA Technologies has an excellent worldwide partner ecosystem. Integration with Advanced Authentication makes the product a clear pick for shortlists when looking for an CIAM solution with high security requirements.

5.3 EmpowerID

EmpowerID provides a CIAM solution derived from enterprise IAM. EmpowerID is strongly focused on workflow. Workflow is useful for organizations that need to customize CIAM functions but do not want to write and maintain lots of custom code. EmpowerID ships with more than 750 ready-to-use workflows with covering user provisioning, entitlement management, SaaS integration, and identity federation. The product is available as on-premise virtual appliance.

Strengths	Challenges
• Visual workflows obviate the need for coding • Many authentication options • IoT device tracking via asset management console • Fine-grained consent management	• Smaller vendor, but with a growing customer base and support ecosystem • On-premise, Windows only solution • Risk engine needs additional sophistication for fraud reduction

Table 7: EmpowerID's major strengths and challenges

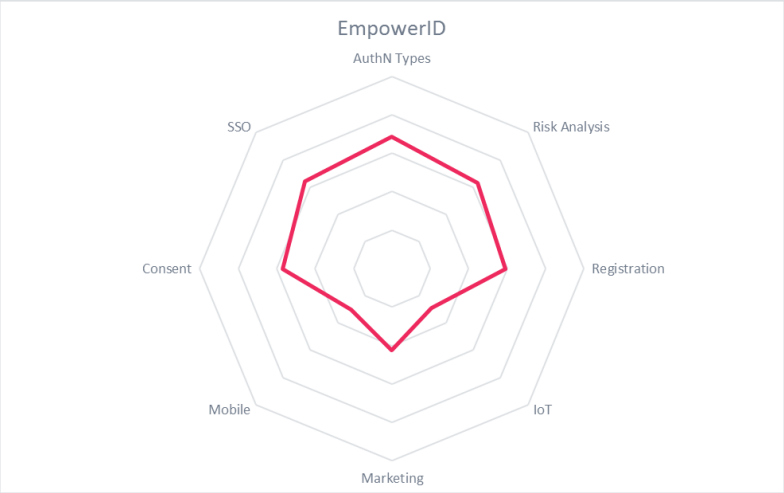
EmpowerID's authentication options include Knowledge-based Authentication (KBA), OATH TOTP, email/phone/SMS OTP, FIDO U2F, Yubico Yubikeys, Duo Security's Push, RADIUS; social logins including Facebook, Microsoft, LinkedIn, Twitter, Yahoo, Salesforce, Paypal, Box, Twilio, Amazon AWS, and GitHub. It also contains a risk engine capable of processing minimal risk factors while evaluating against configurable static policies. EmpowerID also features SaaS integration to Google Apps, Office365, Salesforce, Amazon, and Box.

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

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

Security	positive
Functionality	positive
Integration	neutral
Interoperability	neutral
Usability	positive

Table 8: EmpowerID rating



EmpowerID is a privately owned IAM company moving into CIAM. The product has good authentication options and excellent consent management features that will help customers comply with GDPR. It lacks some capabilities in terms of marketing analytics and risk adaptive authentication. These features plus the customizable workflow engine make it an appealing choice for some environments.

5.4 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.

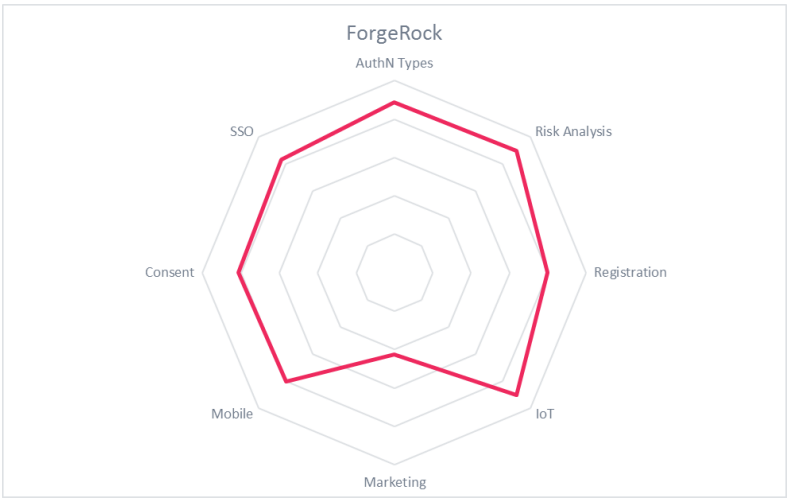
Strengths	Challenges
• Large scale CIAM deployments • Wide array of authentication methods • Risk adaptive authentication chaining • IoT integration via OAuth2 Device Flow, microservices, and mobile push authorization • UMA support for consent management	• ForgeRock does not provide cloud hosting services • No OOTB Business Intelligence functionality

Table 9: ForgeRock's major strengths and challenges

ForgeRock Identity Platform provides numerous choices for how customers can authenticate. Users may login from social networks or use OpenIDs, SMS OTP, FIDO-enabled devices, and mobile applications. Administrators can write risk-based policies to evaluate numerous environmental factors and attributes to chain various authenticators together to support business 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	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 10: ForgeRock rating

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.

5.5 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 has recently become certified as a HIPAA business associate and W3C WCAG 2.0. Their product accommodates most all social logins and integrates with many SaaS vendors. The service itself is entirely cloud-based, and it hosts customer profile data as well. Gigya has improved their progressive profiling capabilities and decreased average implementation time.

Strengths	Challenges
• Large customer base / ecosystem • High performance • IdentitySync UI for ETL between user repositories • Detailed Marketing Analytics and Reporting • Excellent consent management features	• Strong authentication options would enhance the product • No support for FIDO, OAuth2 Device Flow, or UMA

Table 11: Gigya's major strengths and challenges

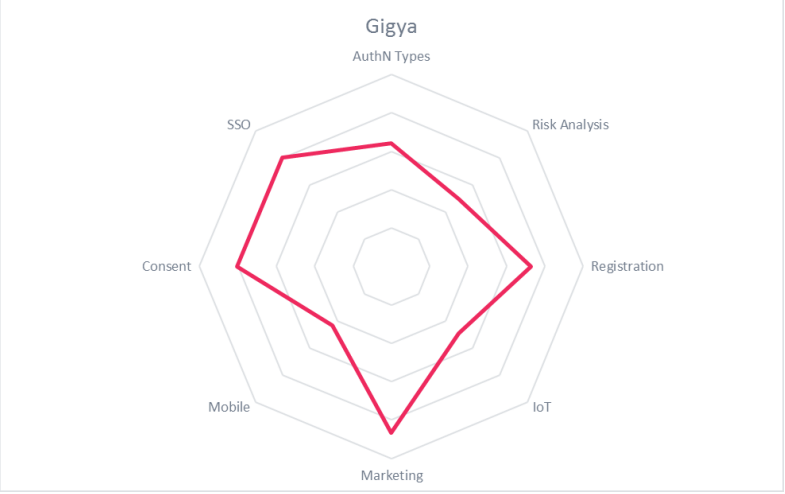
Registration occurs via social media accounts, custom SAML or OpenID providers, a mobile phone, or email address. Gigya has OOTB integrations with Socure, Trulioo, and LexisNexis for identity verification. The console has an improved UI Builder for drag-and-drop site creation. Network Protected Identity provides real-time analysis and alerting on in-network credential compromises. It also has some risk analytics capabilities, evaluating device IDs, IP addresses, locations, and blacklisted locations. If the score returned is too low, the risk engine can call for step-up authentication mechanisms such as SMS/email OTP.

The reporting and analytics functions can track key user activities including registrations, logins, shares, referral traffic, comments, etc. These reports can help clients measure 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 some GDPR compliant features built-in, such as storing proof of consent, right to export data, data deletion upon request, and data age/retention policies. Gigya has multiple data centers for localizing user data.

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

Table 12: Gigya's rating



Gigya is well-established amongst the leading products in the CIAM market. 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.

5.6 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 underpinned by IBM's IAM tools. With customers and partners across the globe, IBM's CIS is a major player in the market.

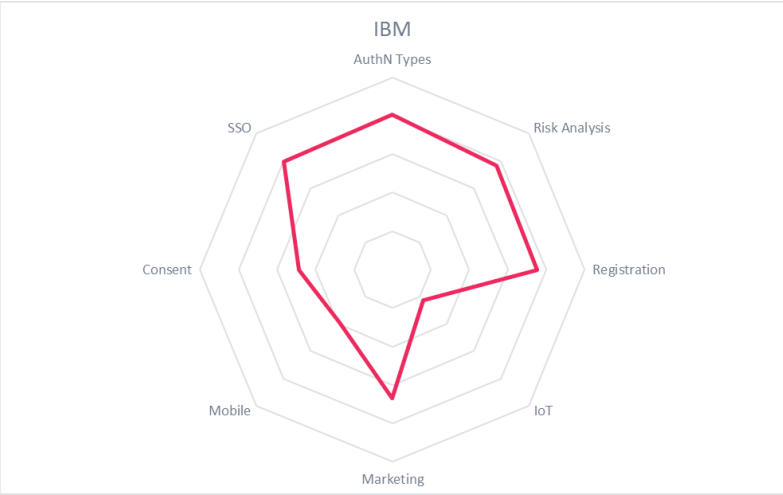
Strengths	Challenges
• Excellent administrative security • Large number of authentication options • Multi-protocol federation capabilities • Limited IoT integration	• Users cannot unregister themselves • No family management yet, but on roadmap • No FIDO or OAuth2 Device Flow support

Table 13: IBM's major strengths and challenges

IBM CIS provides self-registration and profile management features, and 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. For identity federation, it supports SAML, OIDC, OAuth, WS-Federation, WS-Trust, and Kerberos. For provisioning, Graph API, 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 works with IBM Security Intelligence for real-time threat feeds. CIS interoperates with Salesforce, and various Big Data analytics platforms for enhanced marketing analyses, but provides identity analytics natively. IBM is working with auto makers on IoT / Connected Car strategies.

For consent management, CIS does allow users to choose which attributes they want to pass at registration time, and they can edit information afterward. IBM has been improving their consent options. Users can delete their profiles but cannot currently de-register from the service. This feature will be added in 2H2017. Family management capabilities are due to be added by May 2018 for GDPR compliance.



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

Table 14: IBM's rating

IBM CIS is strong in terms of 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 is Privacy Shield certified. The offering would benefit from additional built-in reports and more fine-grained consent options.

5.7 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 initially located within Europe, with plans to expand into new regions. iWelcome uses some market leading open source components in its software platform; therefore, it supports standards, such as SCIM, UMA, and XACML. iWelcome is a microservices cloud-based offering, and it hosts customer profiles as well as identities.

Strengths	Challenges
• Very granular consent model • Strong support for GDPR compliance • Strong support for federation standards and social login • OAuth2 Device Flow for IoT identity linking	• Small but growing partner ecosystem • Heavily centered on EU currently • Limited identity and marketing analytics

Table 15: iWelcome's major strengths and challenges

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

Table 16: iWelcome's rating

As an up-and-coming challenger, iWelcome focuses on delivering CIAM solutions that foster GDPR compliance for the EU market by providing excellent consent management mechanisms. Their solution provides innovative CIAM functionality, but 3rd party products must be used to realize the full potential of the intelligence gathered from CIAM. Organizations in the EU that need flexibility in their consumer identity systems should include iWelcome in RFPs.

5.8 Janrain

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

Strengths	Challenges
• Very large enterprise customer base • Fine-grained consent management • Excellent integration with social networks • IoT integration via OAuth2 Device Flow • Privacy Shield certified	• Lack of standards-based provisioning options • Proprietary mechanism for bulk import of identities

Table 17: Janrain's major strengths and challenges

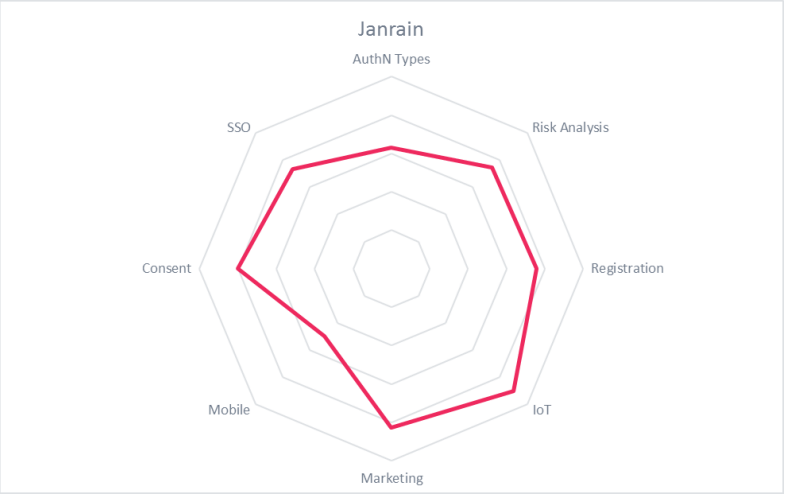
With an emphasis on social network integration, Janrain accepts Facebook, Twitter, Microsoft, Google, and 30 other types of social logins. Besides social logins, Janrain also accepts password-based and SMS OTP authentication, and SAML, OAuth, and OIDC federation. Janrain allows bulk identity import, but does not use LDAP or SCIM for that function.

Identity and marketing analytics are Janrain's forte. Examples of built-in reports include demographics such as gender, age, location, nationality; segmentation analysis such as generation, age range, income bracket; events including logins, registrations, social providers used; "likes" such as favorite TV shows, sports teams, books; and social engagement including top commenters and time spent on site. Janrain also permits 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 change. Family relationships can be defined to allow parents to govern the access rights of children.

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

Table 18: Janrain's rating



Janrain is a key player in the CIAM market. The solution focuses on high availability and harvesting user data for marketing analysis. It provides almost all the features expected in an advanced CIAM solution. Strong authentication options are on the roadmap. Janrain is mature and scalable, and should be seriously considered by organizations that need HA and comprehensive marketing analytics features.

5.9 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.

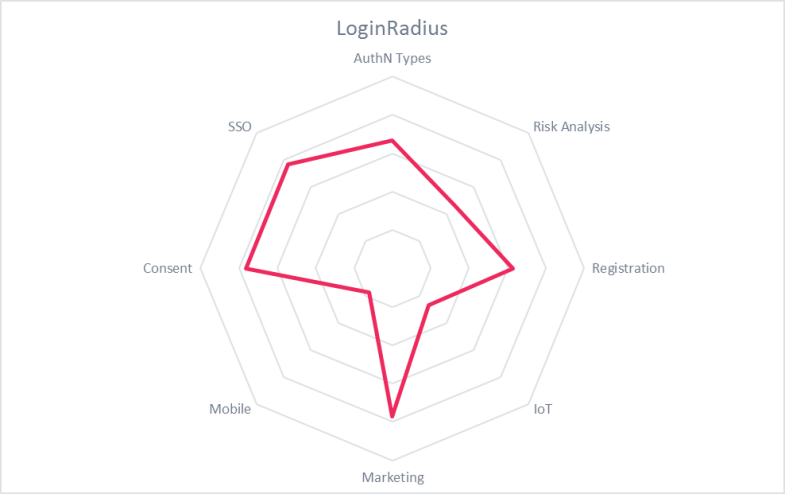
Strengths	Challenges
• Strong social login/Graph API support • Large customer base • Broad support by 3rd party marketing, e-commerce, and CRM solutions • IoT identity association by REST API	• Focused on low-risk, high volume customers and use cases • No automatic notification of privacy settings changes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

Table 19: LoginRadius's major strengths and challenges

LoginRadius supports social and OIDC logins including Facebook, Twitter, Google, Microsoft, and 38 other providers. Two-factor authentication, including SMS OTP and Google Authenticator, is available. LoginRadius features IoT device linking through a REST API, which allows user-to-device permission mapping.

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.

Consumers may choose which social network attributes to share at registration. Users may edit, export, or delete their stored data at any time. LoginRadius does not automatically notify consumers when privacy terms change. Family management can be achieved within the user and permission data model.



Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 20: LoginRadius's rating

LoginRadius is strong in social network registration and login. Supporting additional authentication methods and fraud detection feeds would make the service 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.

5.10 Microsoft Azure Active Directory B2C

Microsoft Azure Active Directory B2C is a cloud-based identity and access management service focused on facilitating business to consumer applications. Built upon Microsoft Azure AD, the B2C offering is architected to scale and perform well with hundreds of millions of users and over one billion logins per day. 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	Challenges
• Integration with PowerBI allows for reporting and marketing analytics • Adaptive risk engine evaluates 100+ factors • Strong attack detection through robust cyber threat intelligence network • Resilient against cyber attacks	• Limited support for 3rd party SaaS app integration • Support for AD and 3rd party IDaaS coming later in 2017 • Needs stronger fine-grained administrative capabilities for application & policy management • User consent management absent • No IAM connectors, FIDO, LDAP, SCIM, or UMA support

Table 21: Microsoft's major strengths and challenges

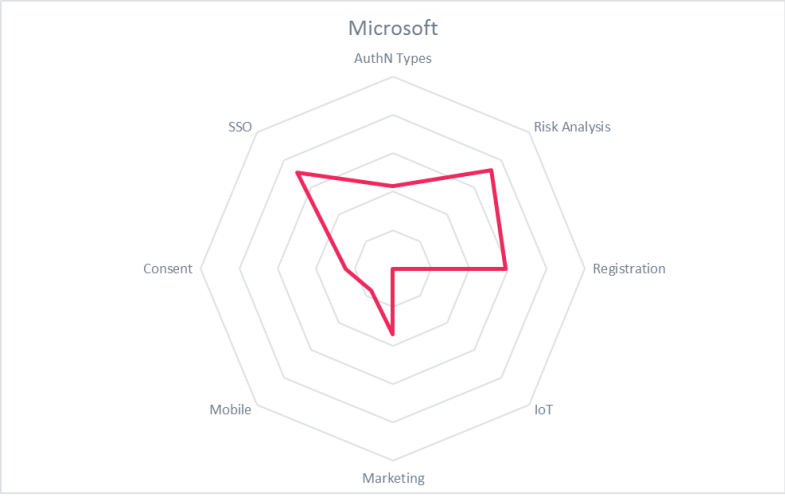
Microsoft Azure AD B2C accepts password-based, SMS OTP, and social login authentication. MFA options are available through partners. Integration between Azure AD and AD B2C is coming later in 2017. A mobile authenticator app is on the horizon as well. AD B2C accepts OIDC and OAuth federation, but not SAML (administrators can authenticate via SAML). It does not currently support bulk provisioning or integrating with other IDaaS. This offering 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 or similar analytic tool to transform the data into business intelligence.

Microsoft Azure AD B2C has coarse-grained functionality that allows user data to be stored within the region of each individual user. Users are notified about which attributes will be shared from source accounts only at registration time.

Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	neutral

Table 22: Microsoft's 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.

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

Table 23: Okta's major strengths and challenges

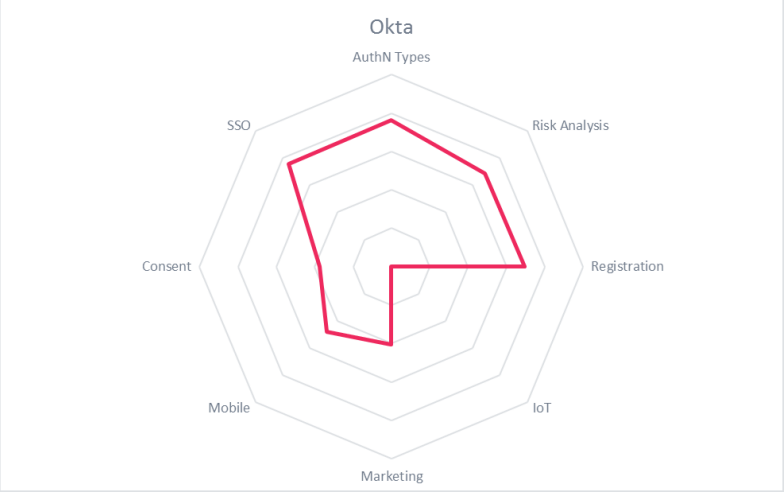
The Okta Platform accepts social logins from Facebook, Google, Microsoft, and LinkedIn. It also supports SMS OTP, FIDO U2F, and federated authentication from SAML, OIDC, and OAuth. The flexibility of Okta platform allows it to accept user information from many standard sources, such as Microsoft AD, and allows Okta to integrate with many SaaS apps or any database. Okta's policy framework can evaluate user, group membership, device ID, location, and IP address. 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 and delete their own data, but a consumer dashboard is not provided. Family management is possible via the Okta API. Okta does not support UMA for consent management. To facilitate GDPR compliance, Okta has two data centers within the EU.

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

Table 24: Okta's rating



Okta is a challenger to the established players in the market for consumer identity management. Its marketing analytics features lag 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 majority of its customers are in North America. Okta's strong cloud presence make it worth considering in CIAM RFPs.

5.12 PingIdentity Platform

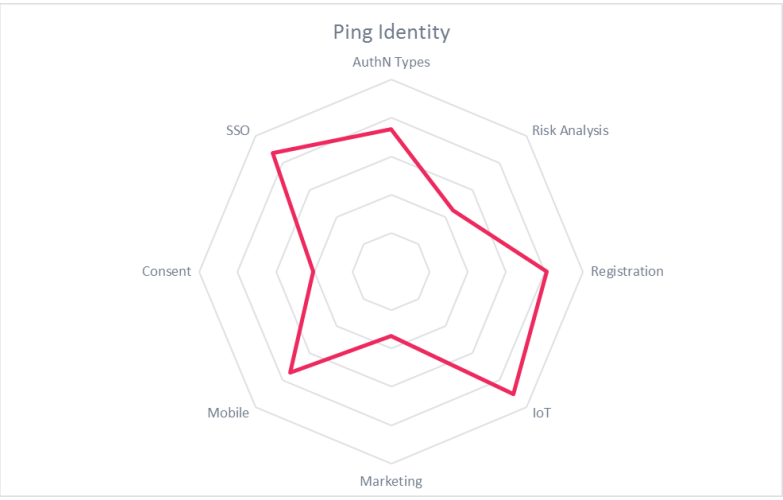
PingIdentity has been a pioneer in identity federation since its inception. Ping was purchased by Vista Equity Partners and then acquired UnboundID in 2016. PingIdentity was among the first to adapt to consumer-facing requirements. The services are available for both on-premise and cloud deployment, and the PingOne platform can host customer profiles.

Strengths	Challenges
• Many authentication options including Mobile Connect • Many OOTB connectors to SaaS / IDaaS • Many large scale, high performance on-premise and cloud deployments • IoT integration via OAuth2 Device Flow • Cyber Threat Intelligence integration	• 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 • Adaptive risk engine improvements coming in 2017

Table 25: PingIdentity's major strengths and challenges

Ping CIAM users can login with SMS/email/phone OTP, RECAPTCHA, or native mobile apps. Ping currently relies on partner integrations for supporting FIDO U2F and UAF. Ping provides an SDK to embed multi-factor authentication features into any mobile app. This includes transaction approvals for purchases, password changes, or other transactions, as well as the ability for customers to self-manage multiple trusted mobile devices. Social logins from Facebook, Twitter, Microsoft, Google, and 30 other identity providers are accepted. It also supports all forms of identity federation. Bulk provisioning and bi-directional synchronization is possible via LDAP and SCIM. This solution can serve as an identity bridge to IDaaS, SaaS, and on-premise AD, IAM, and SSO implementations. Reports show basic identity analytics. More advanced identity and marketing analytics require 3rd party applications, for which APIs are provided. IoT identity integration is achieved via OAuth2 Device Flow.

Customers choose which attributes to share at registration time and may edit them afterward. However, users aren't prompted to consent when service terms change. Only administrators can delete user data. Family management can be implemented as group management, there is no explicit family UI.



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

Table 26: PingIdentity's rating

PingIdentity Platform provides customer engagement capabilities that will be further enhanced as UnboundID features are 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 giving users the ability to delete their profiles, would strengthen the product suite. It is a high performing and scalable system which should be evaluated when conducting RFPs.

5.13 Salesforce Identity

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

Strengths	Challenges
• Very large customer base with many large-scale deployments • Excellent support for most standards • Very good built-in identity and marketing analytics • IoT identity with OAuth2 Device Flow	• Extra licensing fee to connect to on-premise AD • CIAM functionality focused on serving Salesforce.com ecosystem • Needs additional consent management features

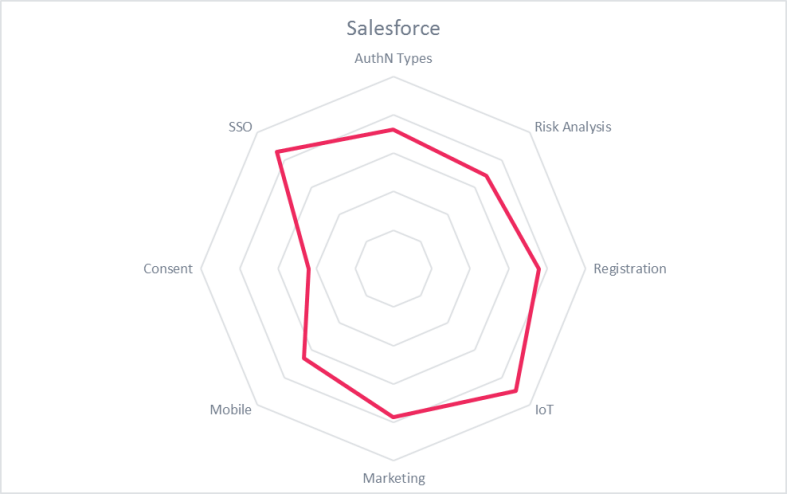
Table 27: Salesforce's major strengths and challenges

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. They provide a Mobile SDK which can be leveraged by developers to create mobile and IoT integration apps. The platform defines standard and high assurance authentication levels, and the GUI allows administrators to define workflows for triggering high assurance logins. Salesforce Identity also allows customers to associate IoT devices with user identities. Salesforce Identity handles key generation, and uses OAuth2 Device Flow for registration. 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 it 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 obtain 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 28: Salesforce's rating



Salesforce Identity is a robust and scalable CIAM solution that provides much flexibility for customers. For existing Salesforce customers, Salesforce Identity may be a natural choice for B2C.

5.14 SecureAuth IdP

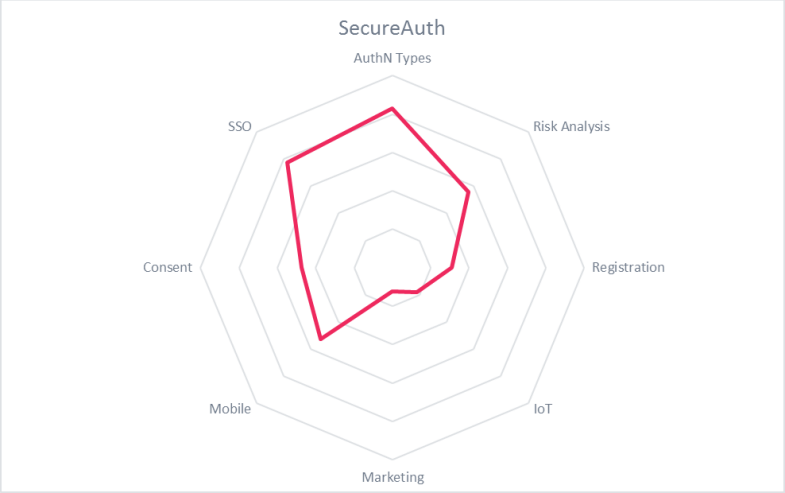
SecureAuth is a well-established provider of IAM products and solutions. The company has a large customer base, primarily centered in North America. Their Windows Server 2012-based CIAM product, is available primarily for on-premise deployments as a hardened virtual appliance. It can also run in hybrid mode with the SecureAuth Cloud Access IDaaS, which features customer profile storage.

Strengths	Challenges
• Very large number of authentication options • Tight integration with the robust SecureAuth adaptive authentication risk engine • Cyber Threat intelligence integration • Phone Fraud Prevention	• Ecosystem centered on North America, but expanding • No built-in identity or marketing analytics • Additional consent management features needed • Limited IoT integration

Table 29: SecureAuth's major strengths and challenges

Built on SecureAuth's strong authentication product, this solution offers nearly every authentication method as an option. FIDO is on the roadmap. 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 numerous 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. SecureAuth now ships with Phone Fraud Prevention, to allow customers to block recently ported numbers, classes of numbers, or by telco/carrier.

The product offers OOTB connectors to SIEM/RTSI tools. It can also integrate with 3rd-party IDaaS. SecureAuth does not have built-in reporting capabilities for identity and marketing analytics. SecureAuth IdP does allow consumers to granularly consent to attribute usage via the self-registration portal, and to edit them afterward. It allows users to de-register and delete their stored profile information. The product does not currently support UMA or family management. IoT identity support is currently limited to Apple Watch and Android Wear.



Security	strong positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 30: SecureAuth's rating

SecureAuth IdP excels in authentication and adaptive risk factor processing. They have a large customer base, and their deployments are designed for high performance and security. To deliver full CIAM functionality, the solution needs to develop marketing analytics and business intelligence features. For organizations whose CIAM requirements include strong security and lots of authentication options, SecureAuth should be on the consideration list.

6 Vendors and Market Segments to watch

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

6.1 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.

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

6.2 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.

6.3 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.

6.4 Pirean

With offices in London and Sydney, Pirean serves both the IAM and CIAM markets. For CIAM, their products provide self-registration and maintenance, such as password resets; social registration and login through Facebook, Google, and Twitter; MFA through their mobile authenticator; SSO by SAML, OpenID, WS-Trust and OAuth; and identity analytics for security intelligence. Pirean's target markets are retail, banking, insurance, and government. KuppingerCole may look at their product suite in more detail in future reports.

6.5 Privo ID

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

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

6.6 Safelayer

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

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

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

6.7 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.

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 Authentication 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.

6.8 Ubisecure

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

Ubisecure customers can authenticate with passwords, Mobile Connect, ETSI MSS, TUPAS, NemID, SMS OTP, OTP TAN, MeonTrust MePIN smartphone biometrics authenticator app, and all the major social logins plus VKontakte, Amazon, and GitHub. Ubisecure supports federation with SAML, OIDC, WS-Federation, and OAuth. It supports LDAP and REST for bulk provisioning. Ubisecure currently only looks at a small number of risk factors. It does not have the ability to utilize external cyber threat intelligence feeds.

The product sends data to SIEM/RTSI tools using syslog. Ubisecure does not have built-in reporting capabilities for identity and marketing analytics, but they do ship with Pentaho Data Integration. Their CIAM solution does allow consumers to granularly consent to attribute usage via the self-registration portal, and to edit them afterward. It allows users to de-register and delete their stored profile

information. Family management can be implemented in the data model, and parent/children relationships can be modeled as service contracts.

6.9 UXP Systems

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

7 Methodology

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

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

7.1 Types of Leadership

We look at four types of leaders:

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

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

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

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

7.2 Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management[1]). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Unresolved security vulnerabilities and hacks are also understood as weaknesses. This rating is based on the severity of such issues and the way a vendor deals with them.

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

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

Interoperability can have several elements. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or

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

standards that are important outside of the product family. Extensibility is related to interoperability, and is measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status to insure its importance is understood by both the vendor and the customer. As we move forward, simly providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

Usability refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes good documentation can facilitate adequate accessibility. However, we have strong expectations that user interfaces will be logically and intuitively designed. Moreover, we expect a high degree of consistency across user interfaces of a product or different products of a vendor. We also believe that vendors should follow common, established approaches to user interface design.

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

- Increased People Participation—Human participation in systems at any level is the highest area of cost and highest potential for breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product Security, Functionality, Integration, Interoperability, and Usability which the vendor has provided is of highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns, and will result in weak infrastructure.

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

7.3 Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

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

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

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

7.4 Rating scale for products and vendors

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

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

7.5 Spider graphs

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

Authentication	Social logins, mobile support, multi-factor authentication
Consent	Facilities within the UI to allow consumers to unambiguously opt-in to services and 3rd party usage of their data. Ability to export and delete consumer profiles as requested. Family management
IoT	Extensions to the CIAM platform to allow consumers to register, activate, and monitor usage of IoT devices by associating consumer identity with device identity. The use of OAuth2 Device Flow specification is a good means to achieve this
Marketing	Once consent is given, transforming information for marketing campaigns, creating special offers, encouraging brand loyalty. Includes identity analytics features, such as the ability to generate and customize reports on user actions, as well as representing aggregated activity on enterprise dashboards in real-time
Mobile	Mobile authentication options, native app SDKs for customer developers, mobile apps for managing consumer information, mobile management apps for CIAM systems
Registration	Self-registration, self-maintenance of attributes, consistent branding, bulk provisioning
Risk Analysis	Evaluation of user attributes, environmental factors, and other information to determine authentication and authorization levels required per transaction
SSO	Solutions use standards such as SAML, OpenId, OIDC, and OAuth for identity federation amongst a customer's websites. It can also include proprietary connectors for internally hosted applications and SaaS applications, such as CRM, Marketing Automation, etc.

The spider graphs provide comparative information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas, while being strong in other areas. These might be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic decisions on CIAM.

7.6 Inclusion and exclusion of vendors

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

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

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

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

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

8 Copyright

The Future of Information Security – Today

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

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

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

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