KuppingerCole Report

LEADERSHIP COMPASS

by Martin Kuppinger | June 2017

Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO)

Leaders in innovation, product features, and market reach for Identity as a Service offerings targeting Single Sign-On to the Cloud for all types of users, with primary focus on cloud services but some support for on-premise web applications. Your compass for finding the right path in the market.

by **Martin Kuppinger**
mk@kuppingercole.com
June 2017

Leadership Compass
Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO)
By KuppingerCole

Content

Content of Tables

Content of Figures

Related Research

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

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

Advisory Note: Secure your Cloud against Industrial Espionage - 70997

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

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

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

Executive View: Cloud Standards Cross Reference - 71124

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

Executive View: Executive View Microsoft Azure RMS - 70976

Executive View: PingFederate 7 - 70801

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

Executive View: Exostar Services for Life Sciences - 70878

Executive View: PingOne® - 70870

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 70960

Leadership Compass: Access Management and Federation - 70790

Leadership Compass: Access Governance - 70735

Product Report: Microsoft Azure Active Directory - 70977

Scenario: Understanding Cloud Security - 70321

Scenario: Understanding Cloud Computing - 70157

Scenario: Understanding Identity and Access Management - 70129

Vendor Report: SecureAuth Corporation - 70260

1 Introduction

The KuppingerCole Leadership Compass provides an overview of vendors and their product or service offerings in a certain market segment. This Leadership compass focuses on the market segment of Identity as a Service which delivers a Single Sign-On experience to users, with a focus on Single Sign-On to cloud services, but not limited to these. In short, we named this segment IDaaS SSO.

1.1 Market Segment

The IDaaS market has evolved over the past few years and is still growing, both in size and in the number of vendors. However, under the umbrella term of IDaaS, we find a variety of offerings. IDaaS in general provides Identity & Access Management and Access Governance capabilities as a service, ranging from Single Sign-On to full Identity Provisioning and Access Governance for both on-premise and cloud solutions. Solutions also vary in their support for different groups of users such as employees, business partners, and customers, their support for mobile users, and their integration capabilities back to on-premise environments.

For that purpose, we have split the IDaaS market into three distinct market segments. Some vendors serve two or all three segments with their IDaaS services, while others focus on a single segment. The three IDaaS market segment in the KuppingerCole definition are:

- IDaaS SSO: IDaaS focused on providing a Single Sign-On experience to users. While the primary focus is on providing access for employees to cloud services, we also look for support for other groups of users such as business partners and customers, for mobile users, and for downstream SSO back to on-premise applications. Formerly, we referred to this market segment as “Cloud User and Access Management”.
- IDaaS B2E: IDaaS focused on providing Identity Provisioning and Access Governance for on-premise environments, commonly complemented by Identity Federation capabilities and, based on these, at least baseline support for Single Sign-On to cloud services. These services provide a significantly stronger level of integration back to on-premise environments and should deliver Access Governance capabilities, in contrast to IDaaS SSO solutions. A significant portion of these offerings is delivered in Managed Service deployment models, in contrast to full SaaS models. B2E stands for Business-to-Employee, providing functionality focused on employee-centric IAM, but delivered from the cloud. Formerly, we referred to this market segment as “Cloud IAM & IAG”.
- IDaaS Digital: This is a rather new segment, with “Digital” standing for solutions that support the emerging requirements organizations are facing in the Digital Transformation. Such solutions must provide strong support for both customers and business partners and should support more complex interaction and functionality, which can include IoT (Internet of Things) support, secure information sharing capabilities, and others.

All three market segments are covered in separate Leadership Compass documents. Mid-term, we expect to see some convergence. However, there will remain vendors focusing only on certain of these markets, e.g. delivering Cloud SSO capabilities for SMBs or at a departmental level, in contrast to the enterprise-level solutions required for both IDaaS B2E and IDaaS Digital.

1.2 Delivery models

Several vendors provide offerings that can be better described as Managed Services than as Software as a Service (SaaS) offerings. Pure-play SaaS solutions are multi-tenant by design. Customers can easily onboard, usually as simply as booking online and paying with a credit card. On the other side, Managed Service offerings are run independently per tenant. The criteria for considering solutions for this Leadership Compass is based on the customer perspective: from that perspective, two aspects are of highest relevance – elasticity of the service and a pay-per-use license model. If these criteria are met, we include the offerings in our evaluation.

1.3 Required Capabilities

For the segment of IDaaS SSO, at a high level we expect support for the following feature sets:

- Outbound Federation and Single Sign-On, providing access to Cloud services and web applications. This also includes Cloud Provisioning, i.e. the ability to provision users to Cloud services.
- Directory Services for managing the users: These services must provide massive scalability, enabling organizations to deal efficiently not only with their employees, but potentially with millions of customers. They also must provide a highly flexible schema (data structure) that allows managing different types of users and their respective attributes, but also managing relationships between various objects within the directory. Relying just on existing on-premise directory services limits the flexibility and scalability of these services.
- Authentication support, allowing configuration of the authentication requirements, step-up authentication based on risk and context, etc. We also expect to see significant support for upcoming standards that allow flexibly relying on existing strong authentication methods, such as the FIDO Alliance standard.
- Access Management capabilities that allow configuring flexible policies for controlling access to Cloud service and web applications. Beyond just granting access, the ability for at least coarse-grained authorization management is a key capability for IDaaS SSO.
- Inbound Federation and Self-Registration: While inbound federation support focuses on the rapid on-boarding of users from business partners that already have an Identity Federation infrastructure in place, self-registration capabilities are mandatory for other business partners and customers. Identity Federation also will gain momentum in the customer space, when relying on external Identity Providers.

Beyond these capabilities, we see a couple of other feature sets that can add to these services. This includes Access Request portals, allowing users to request access to additional services. It includes the capability for providing access to on-premise applications, which remain in use in most organizations, thus delivering a comprehensive SSO experience beyond just cloud services.

IDaaS SSO also must provide integration with on-premise directories such as the Microsoft Active Directory, allowing employees to access the Cloud services and web applications managed by the service.

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 IDaaS SSO

we considered a series of specific features. These include:

On-premise integration	Approach to integrating back to on-premise IAM environments, for instance Microsoft Active Directory.
Onboarding of externals	Approach and flexibility in onboarding of external users, including configurable workflows and flexible authentication schemes.
Location of datacentres	Location and operation of datacentre, including regional datacentres e.g. in Europe and the question of whether the company owns datacentres or relies on partners.
APIs	Breadth and depth of APIs for managing, configuring and customizing the services.
Reporting capabilities	Built-in reporting capabilities and integration with on-premise Access Governance solutions or SIEM (Security Information and Event Management) solutions.
Preconfigured services	Number of preconfigured cloud services for rapid provisioning.
Depth of pre-configuration	Approach to pre-configuration of cloud services, i.e. level of detail (e.g. only authentication or advanced control of entitlements in these services).
Granularity of access controls	Granularity of access control policies for cloud services that can be configured in these applications.
Strong authentication	Support for strong authentication mechanisms and adaptive authentication, including features such as step-up authentication.
Standards support	Support for established and upcoming industry standards and engagement in standards initiatives.
Baseline cloud capabilities	These includes elasticity, flexibility in upgrades, etc., but also service levels and support.
Cloud security	These features include e.g. business continuity assurance, auditability, and overall security features.

The support for these functions is added to our evaluation of the products. We've also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other offerings available in the market. Among the innovative features in scope, there are

- Support for new standards such as UMA (User Managed Access) and FIDO Alliance standards.
- Flexible, graphical workflow engines for adaptation, e.g. of self-registration processes.
- Advanced cloud provisioning capabilities including, but not limited to, SCIM standard support.
- A comprehensive and consistent set of REST-based APIs.
- Self-service interfaces including access request for all common customer requirements.
- Flexible support for authentication mechanisms.
- Mobile management capabilities.

Please note, that we only listed major features, but looked at a variety of other capabilities as well when evaluating and rating the various IDaaS SSO services.

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 should be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept 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

2.1 Overall Leadership

Figure 1: The Overall Leadership rating for the IDaaS SSO market segment

When looking at the Overall Leader segment, we find several companies. Slightly ahead of the others we see Microsoft, which shows strong ratings in all Leadership categories and which benefits from its exceptionally strong market position.

Right after Microsoft, we see find (in alphabetical order) Centrify, IBM, Okta, and Ping Identity, all at rather the same level. These provide strong offerings for IDaaS SSO, as the other leaders do. VMware, SailPoint, Salesforce and OneLogin also earned an overall strong rating and find their place in the Overall Leader segment. While SailPoint is primarily focused on the IDaaS B2E segment, they provide a solution that is competitive also in the IDaaS SSO market. Salesforce focuses primarily on delivering IDaaS services to their existing customer base, while VMware differs from the others with their tight integration into their Enterprise Mobile Management solution Airwatch, and with capabilities for connecting back to on-premise systems via virtualization technologies. Finally, CA Technologies and Oracle just made it into the Leader's segment.

In the Challenger segment, we find further vendors, with Optimal IdM missing the entry to the Leader segment just by a margin. SecureAuth and SAP also are close to entering the Leader segment. SecureAuth shows its strength when it comes to authentication capabilities, while SAP has an overall strong offering, but suffers slightly from the limited support for non-SAP targets, while on the other hand benefiting from its very strong SAP customer base. Another vendor in this segment is iWelcome, which provides more a Managed Service-style offering and has put their main emphasis on CIAM (Consumer IAM) features but still score well in IDaaS SSO. Other vendors include Ilantus and Trustelem.

Also in the Challenger segment, we see JumpCloud, with a specialized offering centered around providing "directory as a service". They have their specific strengths, which can be a good fit for certain customer scenarios.

Overall Leaders are (in alphabetical order):

- CA Technologies
- Centrify
- IBM
- Microsoft
- Okta
- OneLogin
- Oracle
- Ping Identity
- Salesforce.com
- SailPoint
- VMware

2.2 Product Leadership

The first of the three specific Leadership ratings is about Product Leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

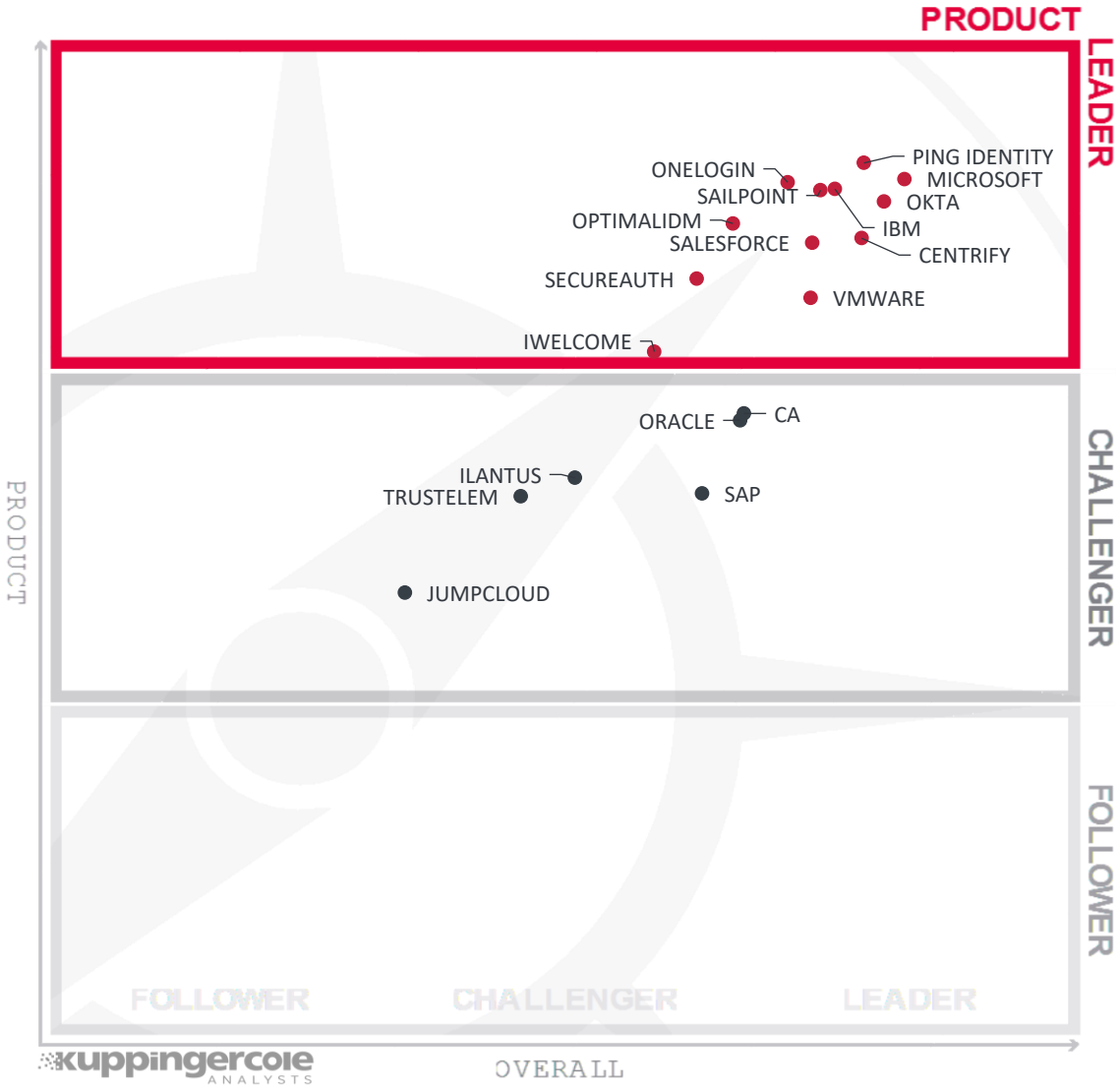


Figure 2: Product leaders in the IDaaS SSO market segment

Product Leadership, or in this case Service Leadership, is the view where we look specifically at the functional strength and completeness of products. We see Ping Identity slightly ahead of the other vendors in this segment. They provide a comprehensive offering, even more so after the acquisition of UnboundID, supported by their strong on-premise offerings.

They are closely followed by a group of vendors, consisting of (in alphabetical order) IBM, Microsoft, Okta, OneLogin, and SailPoint. These provide strong offerings with a differentiating set of features, all of them having specific strengths that set them slightly apart from the other vendors in this segment.

Further close followers in the Leader segment include (again in alphabetical order) Centrify, Optimal IdM, and Salesforce. These all convince with their overall strong feature set. Furthermore, we find SecureAuth, VMware, and iWelcome in the Leader segment, with iWelcome just being at the borderline between the Challenger and the Leader segment.

The significant number of vendors in the Product Leader segment shows a market segment that has matured over the past few years, with a couple of vendors providing leading-edge offerings, even while differing in detail. This is no surprise, given that the LC IDaaS SSO capabilities are the least complex ones of the three different Leadership categories.

In the challenger section, we see CA Technologies and Oracle being very close to becoming a Product Leader. They have made a strategic change in their IDaaS strategy, moving from an IDaaS B2E offering to a newly built IDaaS SSO offering. While they have some differentiating features such as integration with their on premises IAM platforms, they partially still lack breadth, e.g. in supporting cloud services, but with good support for enterprise-level services and well thought-out roadmaps, making them candidates to soon move to the Leaders segment.

Following them, we see (in alphabetical order), Ilantus, SAP, and Trustelem. All of them have their specific strength, but commonly lack some features we expect to see. SAP concentrates on supporting SAP environments, but lacks breadth of support for other cloud services.

Some distance away, we see JumpCloud with their emphasis on “directory as a service”.

Product Leaders (in alphabetical order):

- Centrify
- IBM
- iWelcome
- Microsoft
- Okta
- OneLogin
- Optimal IdM
- Ping Identity
- SailPoint
- Salesforce
- SecureAuth
- VMware

2.3 Innovation Leadership

Another view we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what customers require for keeping up with the constant evolution and emerging requirements they are facing. Innovation is not limited to delivering a constant flow of new releases, but focuses on a customer-oriented upgrade approach, ensuring compatibility with earlier versions especially at the API level and on supporting leading-edge new features which deliver the emerging customer requirements.

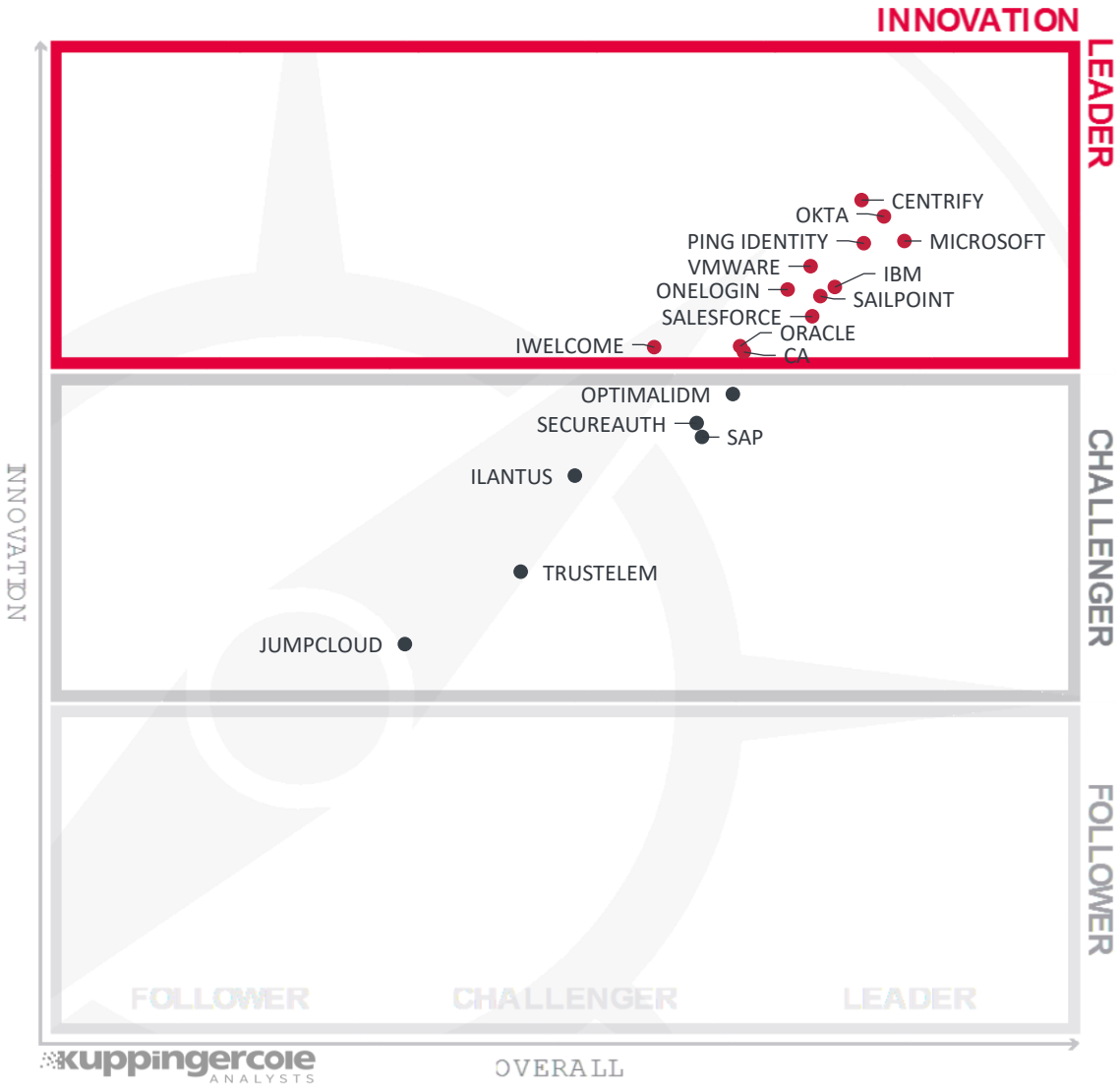


Figure 3: Innovation leaders in the IDaaS SSO market segment

When looking at Innovation Leadership, Centrify is slightly ahead of the others, based on strong mobile support, good integration to on-premise environments, and other specific features such as Privilege Management capabilities. Closely following (in alphabetical order) are Microsoft, Okta, and Ping Identity, all with specific strengths, constantly delivering innovative features.

Other vendors in the Innovation Leader segment include (again in alphabetical order) IBM, OneLogin, SailPoint, Salesforce, and VMware. These too show a constant, good level in innovation, all with their specific strengths. Finally, CA Technologies, iWelcome, and Oracle just passed the borderline to Innovation Leadership. In the case of iWelcome, this is primarily due to their leading-edge feature set for managing customer identities. CA Technologies brings many interesting features for rapid deployment and other innovations, while Oracle is executing on a strong and innovative roadmap for various areas such as Access Governance.

In the Challenger segment, we see Optimal IdM, SecureAuth and SAP being close to becoming a Leader, followed by a couple of other vendors such as Ilantus, Trustelem, and JumpCloud. JumpCloud, as stated in the context of other Leadership ratings in this document, is a specialized vendor focusing on “directory as a service”.

Innovation Leaders (in alphabetical order):

- CA Technologies
- Centrify
- IBM
- iWelcome
- Microsoft
- Okta
- OneLogin
- Oracle
- Ping Identity
- SailPoint
- Salesforce.com
- VMware

2.4 Market Leadership

Finally, we looked at Market Leadership, i.e. the number of customers, the partner ecosystem, the global reach, and related factors affecting the leadership in a market. Market Leadership, from our point of view, requires global reach.

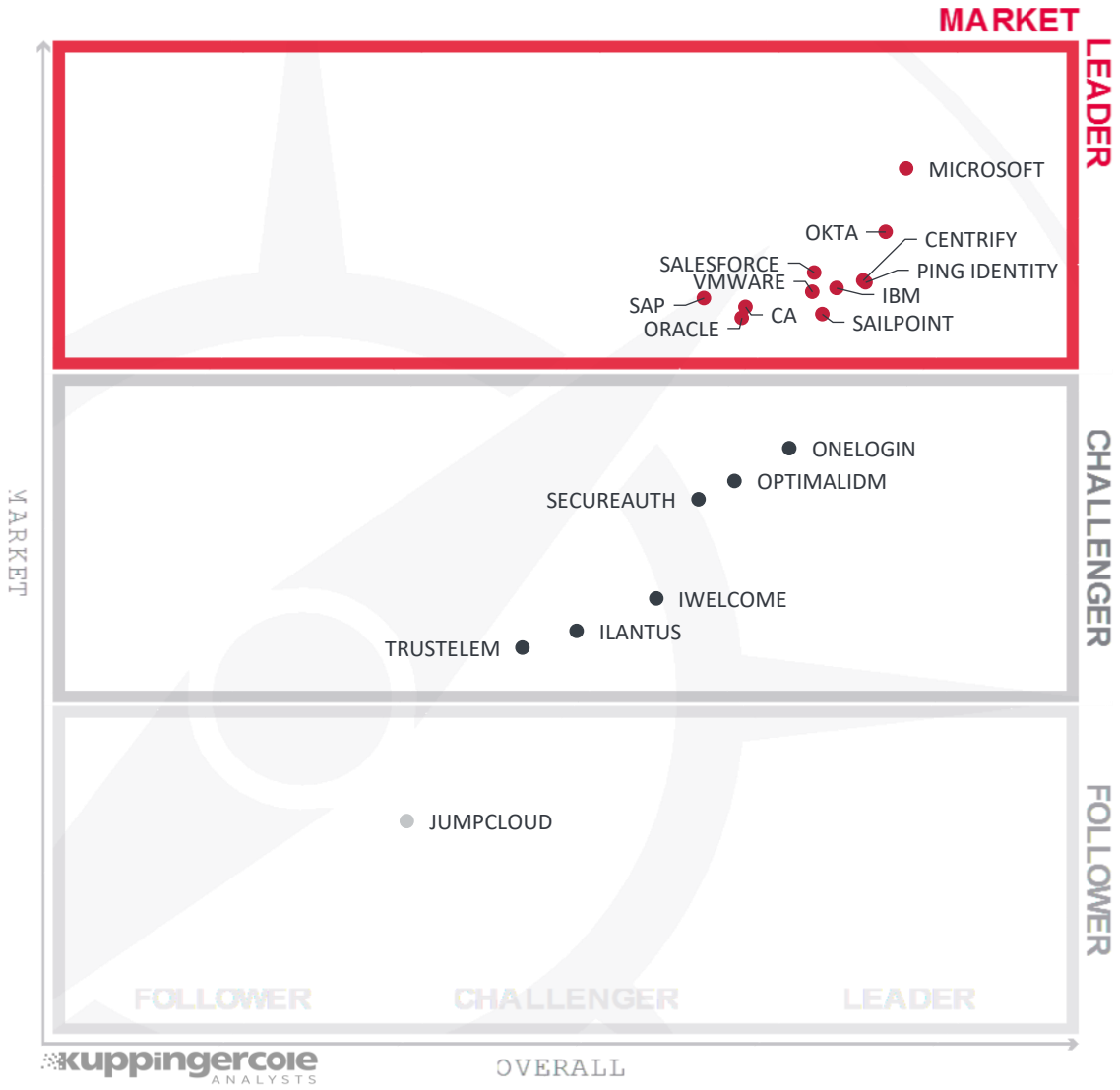


Figure 4: Market leaders in the IDaaS SSO market segment

Microsoft is the clear Market leader, due to its strong customer base derived from traditional Active Directory deployments, Microsoft Office 365, and Microsoft Azure. Furthermore, Microsoft has an exceptionally strong partner ecosystem.

Okta is following, also with a very large customer base. However, in contrast to, e.g. Microsoft, their partner ecosystem and global reach is limited. Following Microsoft and Okta, we see a series of other vendors, which all made it into the Market Leader segment. These are (in alphabetical order) CA Technologies, Centrify, IBM, Oracle, Ping Identity, SailPoint, Salesforce, SAP, and VMware.

While some of these benefit from a large number of installations, such as SAP, others primarily benefit from their global reach and partner ecosystem, such as Oracle and CA Technologies.

In the Challenger section, we see OneLogin in front, followed by Optimal IdM and SecureAuth. All three are well-positioned in the market, but not at the level of a Market leader yet. Other, smaller vendors in that segment include (in alphabetical order) Ilantus, iWelcome, and Trustelem.

Finally, we see a one vendor in the Follower section, which is the point solution vendor JumpCloud.

Market Leaders (in alphabetical order):

- CA Technologies
- Centrify
- IBM
- Microsoft
- Okta
- Oracle
- Ping Identity
- SailPoint
- Salesforce.com
- SAP
- VMware

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for, say, a product leader, but also for a vendor that is, e.g., 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 deliver additional 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 looks at 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.

In the upper right corner, we find the Market Champions. Microsoft is leading, with their strong market position, followed by several other vendors that are all positioned close to each other. These include, in alphabetical order, Centrify, IBM, Okta, Ping Identity, SailPoint, Salesforce, and VMware.

Left to that segment, we see vendors that are not yet Product Leaders, but have a very strong position in the market. Not surprisingly, this segment is populated by the large vendors CA Technologies, Oracle, and SAP.

Right below the Market Champions, we find a couple of vendor with strong product offerings, that are not yet as large in the market as the leading vendors. These include (in alphabetical order) iWelcome, OneLogin, Optimal IdM, and SecureAuth.

The other vendors, Ilantus, Trustelem, and JumpCloud, are positioned in the lower segments and more towards the left.

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

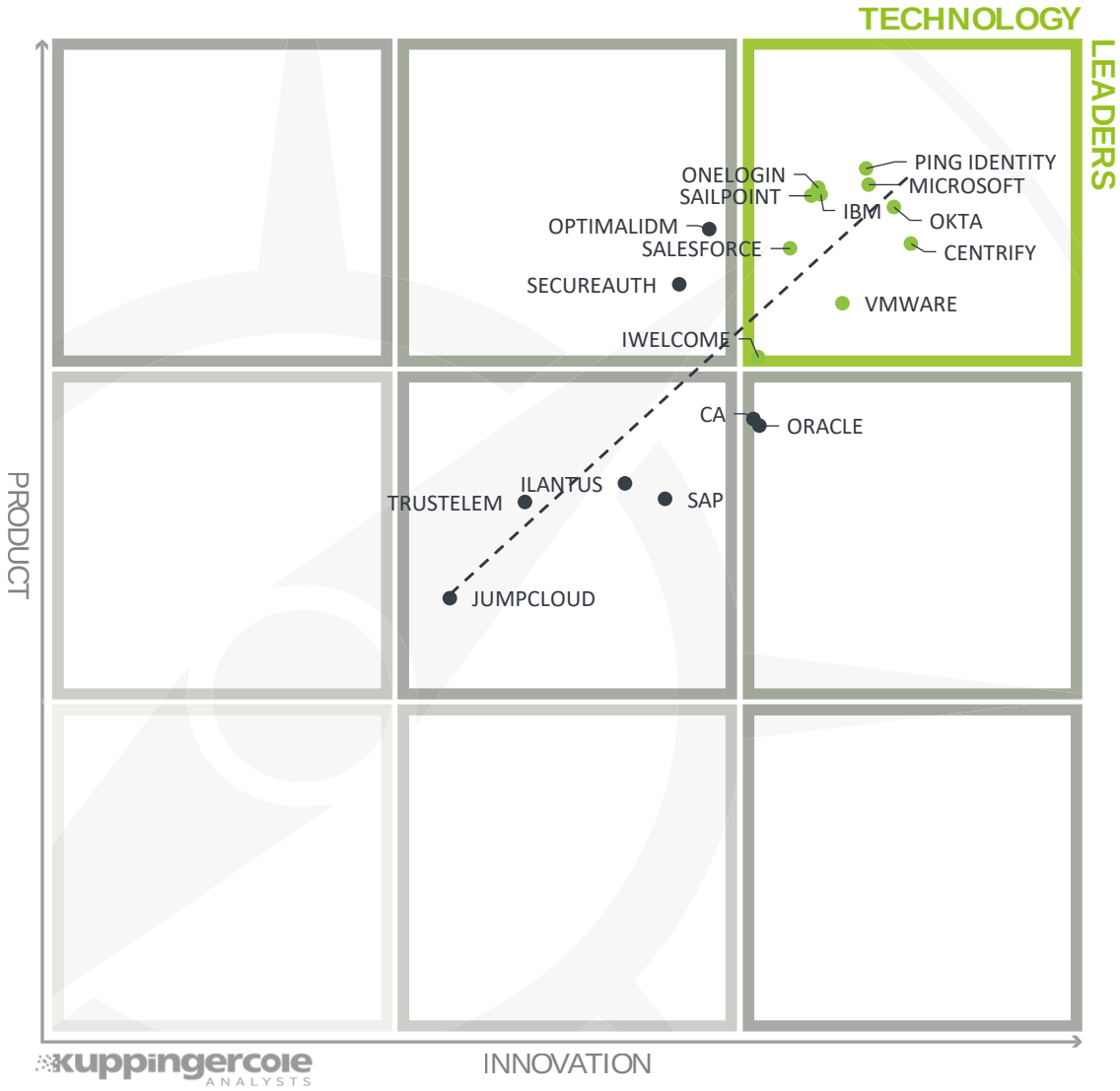


Figure 6: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here we look at the Technology Leaders. On top, we find a group of vendors, which are all positioned close to each other. These include (in alphabetical order) Microsoft, Okta, and Ping Identity. Close to these, we find Centrify, IBM, OneLogin, and SailPoint. Other vendors that made it into this section are iWelcome, Salesforce, and VMware, with iWelcome just entering that segment.

In the segment to the left, we find Optimal IdM and SecureAuth, both with strong product offerings but not rated as Innovation Leaders, while we find CA Technologies and Oracle in the segment just below the Technology Leaders, being not yet Product Leaders but already being rated Innovation Leaders.

In the segment in the middle of the graphic, we see the remaining vendors (in alphabetical order), i.e. Ilantus, JumpCloud, SAP, and Trustelem.

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

Figure 7: The Innovation/Market Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Vendors above the line are performing well in the market compared to their relative weak position in the Innovation Leadership rating, while vendors below the line show, based on their ability to innovate, the biggest potential for improving their market position.

In this comparison, we look at the “Big Ones”, i.e. vendors that have a strong market position and continue driving innovation, thus being in a good position of keeping their already strong position.

In that upper right segment, we see Microsoft slightly ahead due to their market position, while others show some more innovativeness. Other vendors in that segment include, in alphabetical order, CA Technologies, Centrify, IBM, Okta, Oracle, Ping Identity, SailPoint, Salesforce, and VMware.

In the segment to the left, we find SAP, with a strong market position but not leading in innovation, while the segment below contains some innovative vendors such as iWelcome and OneLogin, that don’t yet have the market reach the leaders have.

The segment in the middle contains vendors that are both challengers in innovation and in market, with Ilantus, Optimal IdM, SecureAuth, and Trustelem. Below them, we find JumpCloud as a highly specialized vendor.

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 IDaaS SSO. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

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

Product	Security	Functionality	Integration	Interoperability	Usability
CA	strong positive	positive	positive	positive	positive
Centrify	strong positive	positive	strong positive	positive	positive
IBM	strong positive	strong positive	positive	strong positive	positive
Ilantus	positive	positive	positive	positive	positive
iWelcome	strong positive	positive	positive	positive	strong positive
JumpCloud	strong positive	neutral	positive	neutral	neutral
Microsoft	strong positive	positive	strong positive	strong positive	positive
Okta	positive	strong positive	strong positive	strong positive	positive
OneLogin	Not rated[1]	positive	strong positive	strong positive	positive
Optimal IdM	strong positive	positive	strong positive	strong positive	positive
Oracle	strong positive	positive	positive	positive	positive
Ping Identity	strong positive	strong positive	positive	strong positive	positive
SAP	strong positive	neutral	positive	neutral	positive
SailPoint	strong positive	strong positive	positive	positive	strong positive
Salesforce	strong positive	positive	positive	positive	positive
SecureAuth	strong positive	positive	positive	positive	positive
Trustelem	positive	neutral	positive	positive	neutral
Vmware	strong positive	positive	positive	positive	positive

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

[1] Due to a recent incident, we did not rate OneLogin security. Ask KuppingerCole for the current rating, as we update this based on the progress of OneLogin in responding on that incident.

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 also include specific product aspects.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
CA	positive	positive	strong positive	positive
Centrify	strong positive	strong positive	positive	positive
IBM	positive	positive	strong positive	strong positive
Ilantus	positive	weak	neutral	neutral
iWelcome	positive	neutral	neutral	neutral
JumpCloud	neutral	weak	neutral	neutral
Microsoft	strong positive	strong positive	strong positive	strong positive
Okta	positive	strong positive	positive	positive
OneLogin	positive	positive	positive	positive
Optimal IdM	positive	neutral	positive	positive
Oracle	positive	positive	strong positive	positive
Ping Identity	strong positive	positive	positive	strong positive
SAP	positive	positive	strong positive	positive
SailPoint	positive	positive	positive	strong positive
Salesforce	positive	positive	strong positive	strong positive
SecureAuth	positive	neutral	neutral	neutral
Trustelem	neutral	weak	weak	neutral
Vmware	positive	positive	strong positive	positive

Table 2: Comparative overview of the ratings for vendors

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

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

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

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

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

5 Product/service evaluation

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

5.1 CA Identity Service

CA Technologies is one of the established players in the overall IAM market. While they have a strong presence in on-premise IAM, it took a while until they came up with an offering for the IDaaS SSO market. CA Identity Service thus is still rather new on the market, but already provides an interesting feature set and can be backed by on-premise IAM solutions, in particular CA Single Sign-On (formerly SiteMinder).

Strengths/Opportunities	Weaknesses/Threats
• Bi-directional integration to connected services • Good provisioning capabilities to cloud services • Support for major enterprise-level cloud services • Integration with CA Single Sign-On	• No integrated, comprehensive workflow capabilities • Low number of cloud services supported out-of-the-box, but very good support for enterprise-level SasS services • Lack of advanced features such as baseline Access Governance

Table 3: CA Identity Service major strengths and weaknesses

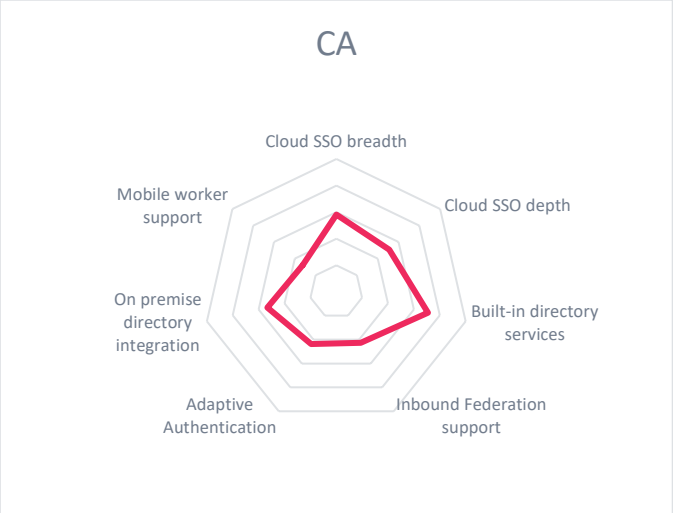
CA Identity Service is a typical IDaaS SSO solution, providing SSO to cloud services, including built-in 2FA (Two Factor Authentication). In contrast to other offerings, the number of cloud services that are supported out-of-the-box is rather low. However, major services for enterprise customers, ranging from Microsoft Office 365 to ServiceNow or Cisco WebEx, are on the list. Furthermore, connection to other services via SAML or indirectly via CA Single Sign-On is supported.

The integration with CA Single Sign-On counts as one of the features that differentiate CA Identity Service from other solutions in this market segment. It allows connectivity to on-premise web applications as well as to cloud services that do not support SAML.

Another area where CA Identity Service shows strong capabilities is user provisioning and connectivity to services. Provisioning is flexible, yet lacking full workflow support. Connectors to services work bi-directionally, which stands in contrast to many other offerings in the market. On the other hand, in addition to the limited out-of-the-box support of cloud services, advanced features, such as at least a baseline Access Governance functionality, are missing.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 4: CA Identity Service rating.



When looking at the Cloud Service Provider infrastructure, CA Technologies offers cloud services from their own operated and managed data centers and through partner operated and managed data centers. Based on that, CA can cover certain regions and comply with the common regulations in place. Overall, CA Identity Service is an interesting option in the emerging IDaaS market and has a potential for playing a strong role in the IDaaS SSO market with the expected growth in capabilities.

5.2 Centrify Identity Service

Centrify has emerged from being a provider of Microsoft Active Directory to Unix integration to become a leading supplier of IDaaS SSO solutions. With Centrify Identity Service, the vendor plays a strong role in this market segment, building on both a strong baseline capability and a number of innovative capabilities such as the strong Mobile Management features.

Strengths/Opportunities	Weaknesses/Threats
• Integrated Mobile Management features • Support for managing Mac endpoints • Integration with Centrify Privilege Service • Broad out-of-the-box support for cloud services	• Limited self-service interfaces

Table 5: Centrify Identity Service major strengths and weaknesses

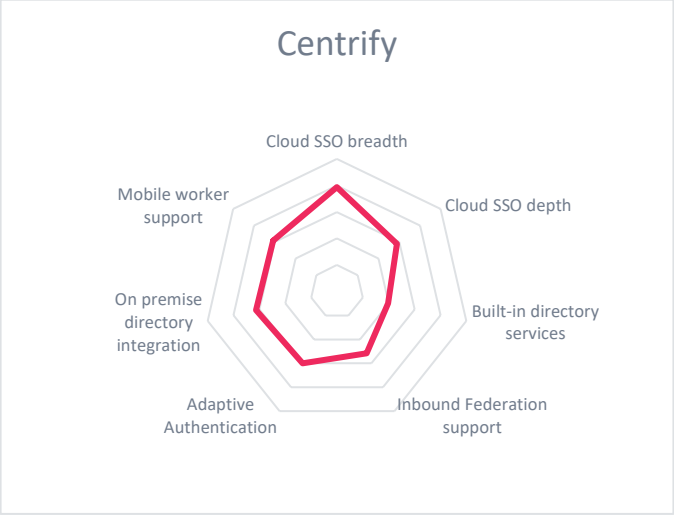
Centrify Identity Services combines the SSO to cloud services with a set of other features. One is its strong Mobile Management capability, which is of importance for securing access of the mobile users that are the common user type for many organizations today. Furthermore, management of Apple Macs is also supported. Both services include endpoint-related security features.

On the other hand, the service also delivers strong baseline capabilities, including a vast number of cloud services that are supported out-of-the box, including business applications such as SAP systems. In contrast to many other solutions, it also provides built-in workflow capabilities. This allows, for example, for customization of self-service registration.

Directory integration is good, as can be expected given the history of Centrify. While the primary focus of the service is on employee access to cloud services, it also provides support for business partners and customers. A unique capability is its integration with Centrify's Privilege Service, i.e. cloud-based Privilege Management.

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

Table 6: Centrify Identity Service rating



Centrify Identity Service has matured to become a leading-edge offering in the IDaaS market, with many customers. While there are still some gaps, there are many other capabilities which are rarely found. Centrify Identity Services counts among the offerings that are a logical candidate for shortlists.

5.3 IBM Cloud Identity Service

IBM over the past several years has moved from single-tenant, cloud-based deployments of existing IAM tools towards a full, multi-tenant solution that is positioned as an enterprise IAM from the cloud. While the main target is providing a solution for the market segment we define as IDaaS B2E, IBM also is a strong player in the IDaaS SSO segment, providing easy-to-use and broad support for integrating with cloud services.

Strengths/Opportunities	Weaknesses/Threats
• Very feature-rich offering, including Access Governance capabilities • Customizable workflows • Can be flexibly tailored to customer requirements, but provided as standard SaaS app • Strong adaptive authentication feature set	• No specific mobile capabilities, but available through IBM portfolio • Good support for enterprise cloud services, but overall number not outstanding

Table 7: IBM Cloud Identity Service major strengths and weaknesses

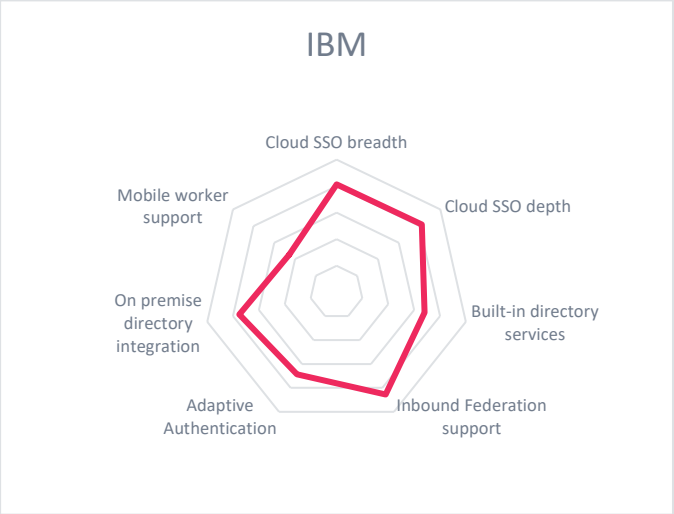
IBM provides a broad set of capabilities, well beyond the standard IDaaS SSO feature set. This includes tight integration with on-premise applications as well as Access Governance capabilities. However, IBM Cloud Identity Service also serves the IDaaS SSO requirements well, particularly for strategic deployments. It delivers strong support for federation standards, social logins, and interfaces out-of-the-box to a variety of enterprise-level SaaS services.

Furthermore, it comes with a large range of self-service apps, including, for example, self-registration, profile management, and others. IBM also delivers workflow capabilities that allow for flexible customization of, e.g., self-registration workflows.

Other areas such as auditing are also feature-rich and at enterprise-level. Support for mobile systems is at a baseline level; however, IBM has its own offerings in this area that can complement the IBM Cloud Identity Service.

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

Table 8: IBM Cloud Identity Service rating



IBM Cloud Identity Service counts among the leading solutions in the IDaaS market segment, targeted at enterprise customers. It provides a high degree of flexibility, in contrast to many of the other IDaaS offerings in the market. However, it is not positioned as a "pay with credit card and use it" solution. From our perspective, organizations looking at a strategic IDaaS solution should include IBM Cloud Identity Service in their evaluation.

5.4 Ilantus Xpress IDaaS

Ilantus Technologies is a specialized vendor in the IAM domain. Being primarily a system integrator, it has recently moved to becoming an IDaaS vendor specializing in an enterprise-level solution covering both IDaaS SSO and IDaaS B2E requirements.

Strengths/Opportunities	Weaknesses/Threats
• Good support for out-of-the-box integrations, in particular for enterprise-level cloud services, but also on-premise applications such as SAP • Flexible customization, including workflow and Access Governance capabilities • MFA support • Broad integration with existing logins	• Small partner network, but based on large partners with global scale • Focus on enterprise customers, no point-and-click access to service • Relatively small vendor, primarily focused on the U.S. market

Table 9: Ilantus Xpress IDaaS major strengths and weaknesses

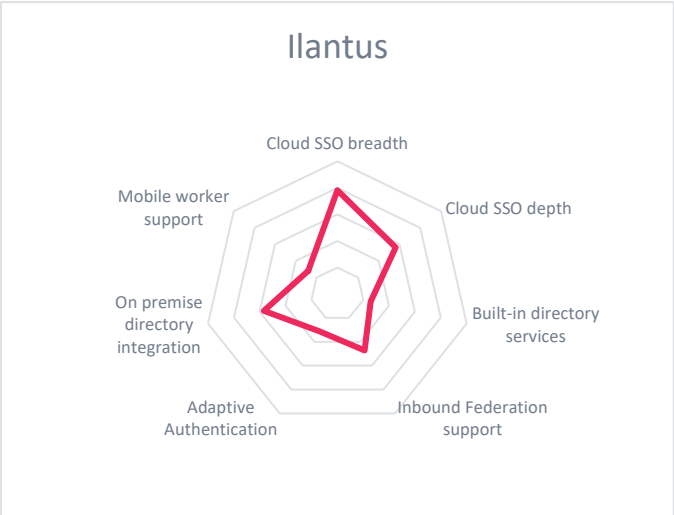
Ilantus provides a solution that covers a variety of aspects around IDaaS. For the primary use cases of IDaaS SSO, it delivers a variety of integrations to existing logins, beyond the commonly found IDaaS scope on integration with Microsoft Active Directory. It also delivers broad support for MFA (Multi Factor Authentication), however it is not strong when it comes to advanced adaptive authentication capabilities such as risk-based and context-based authentication.

The solution also comes with a set of self-service interfaces such as for password reset. In general, it provides a strong degree of flexibility in customization, including workflow support. Furthermore, there is support for advanced capabilities in Identity Provisioning and Access Governance, which make Ilantus Xpress IDaaS a solution that also can cover the IDaaS B2E use cases.

As with some of the IDaaS offerings, Ilantus Xpress IDaaS is not a solution that is supposed to just be ordered via credit card, but targeted at enterprise customers making a strategic IDaaS decision. The deployment thus can be flexibly customized, based on pre-packaged integrations, templates, and use cases.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 10: Ilantus Xpress IdaaS rating



Ilantus counts amongst the IDaaS SSO providers that focus on enterprise use cases. They provide strong support beyond IDaaS SSO capabilities, while covering these well, particularly when it comes to enterprise-level SaaS services. With its capabilities, Ilantus is an interesting contender to the established players in the IDaaS market.

5.5 iWelcome

iWelcome is a VC-backed vendor based in the Netherlands that provides an IDaaS and CIAM (Consumer IAM) service. The service is run from datacenters within the EUwith data residency within the EU. Over the past two years, iWelcome has gradually moved into the CIAM space, while still maintaining a good position for IDaaS SSO and IDaaS B2E market.

Strengths/Opportunities	Weaknesses/Threats
• Strong integration back to existing on-premise IAM services • Tight integration with Windows authentication • Run from EU datacenters • Well thought-out approach for covering security and privacy concerns particularly of EU customers	• Still limited number of out-of-the-box integrations to Cloud services, but strong standard support for simple integration • Relies on 3rd party data centers • No full multi-tenancy, but isolated environments per tenant

Table 11: iWelcome major strengths and weaknesses

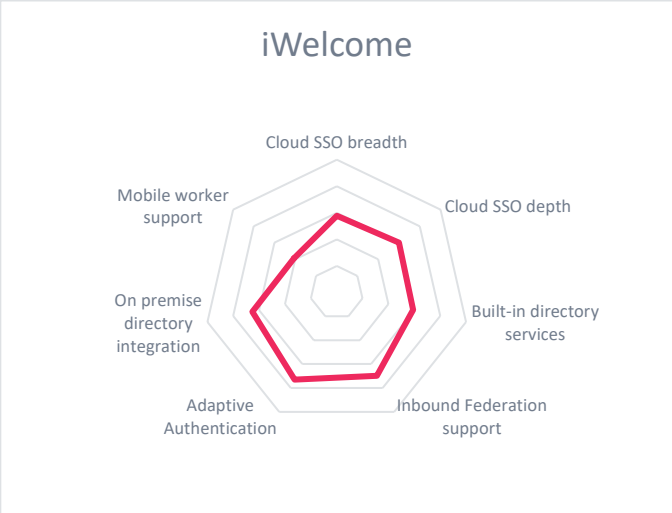
The approach taken by iWelcome allowed them to quickly start offering a service for Cloud User and Access Management, while also supporting integration of external users. In that area, they are leading-edge due to the variety of CIAM features offered, including excellent support for the upcoming EU GDPR requirements.

The biggest challenge of iWelcome's approach might be support for a growing number of instances as they run their service multi-instance and not multi-tenant. Factually, all instances are segregated, but iWelcome has a well-thought-out approach on scaling. Furthermore, the clear segregation provides advantages from a security perspective. Furthermore, they provide strong integration back to existing on-premise IAM services. This also includes tight integration with primary Windows authentication.

The list of Cloud services supported out-of-the-box is still rather small, but includes several complex business applications. In addition, iWelcome provides strong standard support for rapid integration of Cloud services. We expect to see a further growing number of such preconfigured integrations.

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

Table 12: iWelcome rating



iWelcome potentially will benefit from the fact that their services are run from EU-located datacenters. This is quite attractive for EU-based customers, which should have a look at iWelcome. The datacenters are not owned by iWelcome, but well chosen. Overall, iWelcome is an interesting player in the emerging IDaaS market with some specific strengths.

5.6 JumpCloud

JumpCloud is one of the single-service providers in the IDaaS market. They differ from other IDaaS services in their focus on a "directory as a service" offering. Instead of putting their emphasis on SSO capabilities or enhanced Identity Provisioning and Access Governance features, JumpCloud is essentially a directory service deployed from the cloud – the one directory to use when there is no directory service on premises. Thus, while it can cover IDaaS SSO requirements, it is not a 100% fit for this market segment.

Strengths/Opportunities	Weaknesses/Threats
• Strong directory service capabilities • Support for device management from directory, based on scripts • RADIUS support • LDAP and REST-based interfaces to directory service	• Limited out-of-the-box support for SaaS services, based on SAML protocol only • Relatively small vendor, no partner ecosystem at global scale • Baseline MFA and Adaptive Authentication support • Specific focus on "directory as a service", no complete IDaaS SSO offering

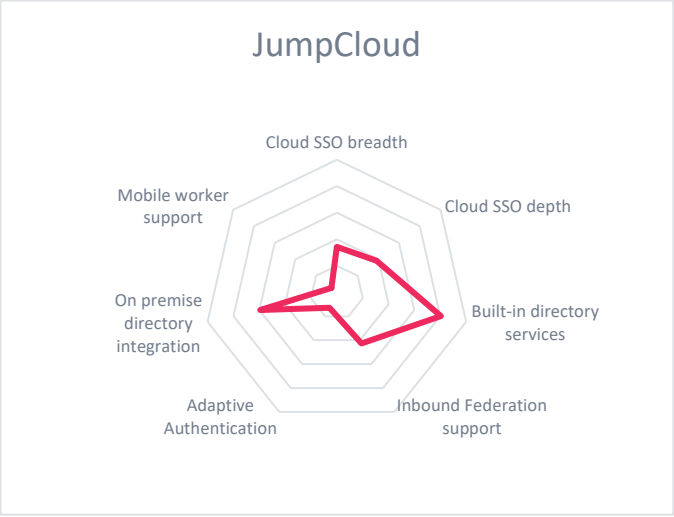
Table 13: JumpCloud major strengths and weaknesses

JumpCloud provides good capabilities when it comes to directory service features. This includes LDAP and REST-based interfaces for user management, RADIUS support for integrating with other authentication providers, password management capabilities and a directory-style user management. Based on these capabilities, it can serve as a cloud-based replacement for existing LDAP directory services, for example. However, it also might complement SaaS offerings as their directory service or might be used as a cloud-based directory in conjunction with other IDaaS offerings, given that some of these lack their own cloud-based directory service capabilities.

A specific strength of JumpCloud is their device management capabilities, which are rarely found in similar products. This allows managing, e.g., Windows, Mac, and Linux devices from the cloud directory, based on well thought-out scripting capabilities. Furthermore, the service delivers group management capabilities.

Security	strong positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	neutral

Table 14: JumpCloud rating



JumpCloud, due to its specific feature set, can not only be an IDaaS SSO offering, but also a complement to other provider's offerings. Several of the IDaaS SSO vendors lack their own cloud directory capabilities, but can only rely on others such as on-premise Microsoft Active Directory. JumpCloud can fill that gap, providing an extension to other offerings, but also has its place in use cases where the directory capabilities are the essential element, e.g, for SaaS providers themselves that need strong directory capabilities.

5.7 Microsoft Azure Active Directory

Microsoft entered the IDaaS market rather early with its Azure Active Directory (Azure AD), which comes in various editions. Aside from the different levels of capabilities available in the core Azure AD, there are extensions such as the B2C (Business to Customer) and B2B (Business to Business) feature sets, which support advanced capabilities. Additional features and add-on services are under development. With Azure AD, Microsoft plays a key role in the evolution of the IDaaS market. The product is targeted at both enabling access of on-premise users to cloud services through integration with existing Active Directory infrastructures, and on supporting the emerging demand of managing identities and access of business partners and customers.

Strengths/Opportunities	Weaknesses/Threats
• Proven scalability and performance, being the underlying service for Microsoft Office 365 • Broad number of preconfigured integrations to cloud services • Innovative and well thought-out approach on IDaaS SSO • Broad standards support	• Microsoft executes on roadmap, but some expected features still lacking

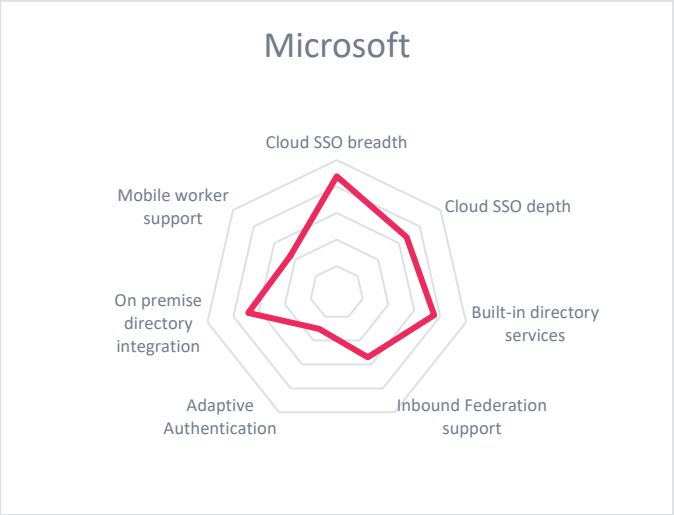
Table 15: Microsoft Azure Active Directory Premium major strengths and weaknesses

Azure AD is one of the most interesting offerings in the IDaaS market. There is a free edition, but with limited functionality regarding scalability, two-factor authentication, etc. This is complemented by a basic and two premium editions with an extended feature set, plus other variants such as Azure AD B2B collaboration, Azure AD Domain Services, and Azure AD B2C. There is tight integration back to the on-premise Microsoft Active Directory through both synchronization and federation services. Furthermore, Microsoft delivers Identity Protection risk-based capabilities.

The service provides several interesting features such as flexible schemas and many preconfigured integrations to cloud services. Several other important features have been added over the past years, with several additional capabilities being on the roadmap. Once released, that will further strengthen the position of Azure AD in that market segment.

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

Table 16: Microsoft Azure Active Directory Premium rating



Overall, we see Microsoft Azure AD as a leading-edge offering when it comes to IDaaS – not only IDaaS SSO, but overall IDaaS approaches at the enterprise level. Microsoft has an excellent position in this market. While running the solution from their own data centers, Microsoft has a well-thought-out approach for respecting local regulations such as in the EU.

5.8 Okta, Inc.

Okta is one of the most prominent providers in the IDaaS market, powered by significant funding from venture capital firms. Their focus is on delivering Single Sign-On to cloud services for enterprise users. However, over time they have added capabilities for dealing with business partners and customers through an API, with several customer wins in that area as well. Furthermore, they have added mobile management capabilities and other features.

Strengths/Opportunities	Weaknesses/Threats
• Very high number of preconfigured cloud services for SSO, including provisioning capabilities • Well thought-out approach to cloud Single Sign-On • Integrated support for strong authentication • Integrated mobile management features	• Relies on third party datacenters, runs on AWS • Acceptable but not leading-edge support for external users such as business partners and customers currently, but with a growing set of capabilities

Table 17: Okta major strengths and weaknesses

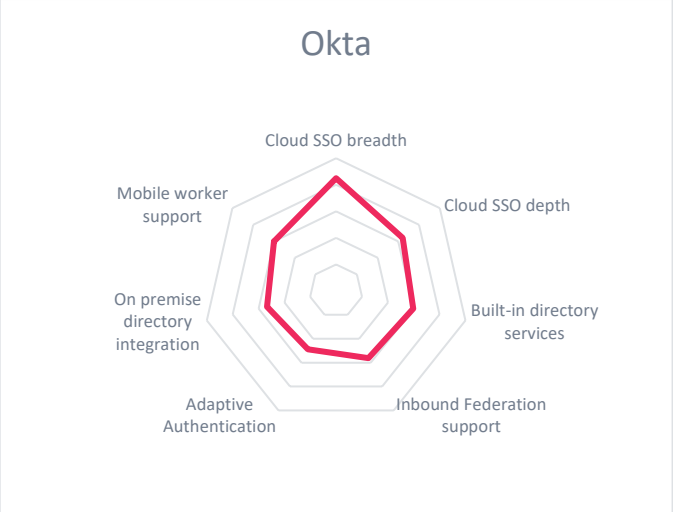
When looking at the use case of providing Single Sign-On of employees to cloud services, Okta is very well-positioned. They have excellent support for existing cloud services, claiming to support thousands of these services out-of-the-box – and they provide provisioning capabilities for a significant number of such services. However, in the area of supporting business partners and customers, while there is a strong API, we still miss out-of-the-box features.

Among their strengths aside from the Cloud Single Sign-On capabilities we rate the good standards support and integrated support for strong and adaptive authentication, plus the ability to support other authentication mechanisms.

Running the service on AWS (Amazon Web Services) is an acceptable option, especially given that AWS is providing one of the most secure offerings. With the evolution AWS has made regarding regional support for data centres, this should work out well for most customers.

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

Table 18: Okta rating



Okta clearly is amongst the leaders for IDaaS SSO. However, we still see room for improvement when it comes to enterprise-level requirements for full IDaaS for hybrid environments, across all groups of users, out-of-the-box.

5.9 OneLogin

OneLogin is another vendor that started early into the IDaaS SSO market, being originally focused on employee SSO to cloud services as the main use case. However, this has changed since then and OneLogin is expanding its capabilities, in particular for supporting on-premise applications and mobile security features. They provide a strong offering with good integration to existing directory services, advanced user provisioning services to cloud services, and other capabilities.

Strengths/Opportunities	Weaknesses/Threats
• Very broad support for preconfigured cloud services and integration toolkits • Good integration back to on-premise infrastructures • Strong mobile security features	• No graphical workflows • Limited support for business partner and consumer use cases • EU-based datacenter in place, but still need to expand their global presence

Table 19: OneLogin major strengths and weaknesses

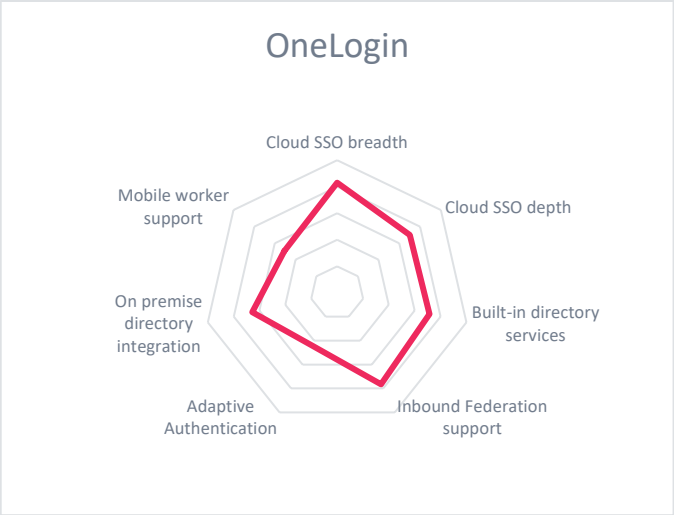
Like some of the other vendors with strong support for the IDaaS SSO use case, OneLogin supports a large number of preconfigured cloud services that can be easily connected. Additionally, they provide SAML and SCIM integration toolkits to SaaS providers. OneLogin is well-above average when it comes to provisioning user accounts into these services and de-provisioning them again. The service also provides good integration back to on-premise user directories.

The customer-facting security features of the service, including adaptive authentication, password vaulting, and reporting features are well thought-out, as are some features for user convenience such as search capabilities and support for mobile users. On the other hand, support for common scenarios supporting business partners and customers, such as flexible self-registration based on graphical workflows, is still missing.

The service has been run from OneLogin's own US-based datacenters since the beginning, with OneLogin adding datacenters in other regions.

Security	not rated[2]
Functionality	positive
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 20: OneLogin rating



As for some other vendors, the ongoing challenge for OneLogin is further expanding its capability set beyond the baseline IDaaS SSO use case. OneLogin has focused on mobile features and support back to on-premise environments, which gives them a strong position for enterprise deployments of IDaaS SSO. We rate them among the leading vendors in the IDaaS SSO market segment.

[2] Due to a recent incident, we did not rate OneLogin security. Ask KuppingerCole for the current rating, as we update this based on the progress of OneLogin in responding on that incident.

5.10 Optimal IdM The OptimalCloud

With its IDaaS offering named The OptimalCloud, Optimal IdM has positioned itself in the emerging IDaaS market. Optimal IdM defines its offering as "a private or public federated cloud service", based on Optimal IdMs Virtual Identity Server, VIS. Thus, the solution is one of the various enterprise-level offerings that can be deployed as a cloud service but are managed on a per-tenant basis.

Strengths/Opportunities	Weaknesses/Threats
• Strong federation support both inbound and outbound • Advanced support for delegated administration • Well thought-out features for MFA • Flexible directory integration capabilities	• No advanced workflow and Access Governance capabilities • Limited focus on consumer-centric use cases • No specific features for mobile management and security

Table 21: Optimal IdM The OptimalCloud major strengths and weaknesses

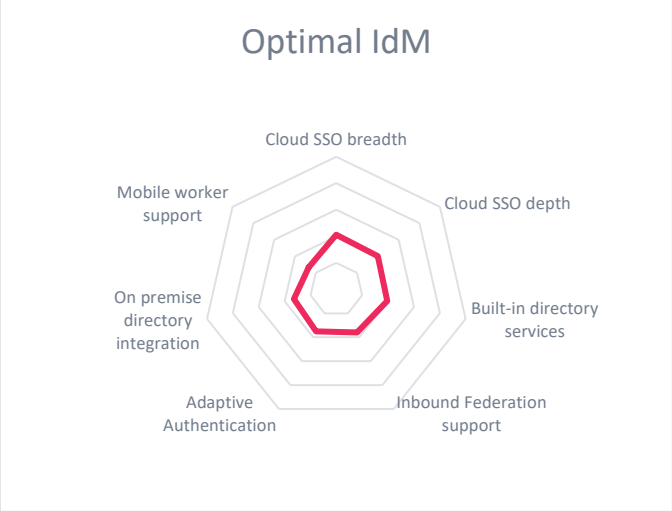
Optimal IdM, while not being among the most well-known IDaaS SSO vendors, delivers a strong feature set that serves the requirements of enterprise customers well, particularly when it comes to pure-play IDaaS SSO use cases for enterprise users and business partners.

The offering provides many integrations to SaaS services. Integration to existing directory services is highly flexible, ranging from inbound federation e.g. from business partners, to local directory services and a full broker mode, which allows managing and authenticating users in their current directory services without the need of synching them to a cloud directory. However, they also provide a private directory in the cloud.

Another strength is the capability for delegated administration, which is stronger than what most of the competitors in the market are offering. Authentication capabilities are at normal level, including an integrated MFA (Multi Factor Authentication) approach, which is, in fact, a 2FA (Two Factor Authentication) solution. On the other hand, advanced features for customization such as graphical workflows, Access Governance, and mobile management are lacking.

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

Table 22: Optimal IdM rating



In sum, Optimal IdM's The OptimalCloud is an interesting offering for the IDaaS SSO market, in particular for enterprise-level deployments. It provides an overall strong set of features, but with some gaps. Furthermore, Optimal IdM has developed a global partner ecosystem, including EMEA and APAC partners, which is essential for enterprise deployments.

5.11 Oracle Identity Cloud Service

Oracle counts among both the leading software vendors and the leading cloud service providers. Their new IDaaS platform has been built new from the ground up and isn't just an MSP offering of the existing on-premise Oracle Identity Management Suite.

Strengths/Opportunities	Weaknesses/Threats
• Built from the ground up for IDaaS requirements and support for hybrid environments • Good support for cloud standards such as OAuth and for API-based integration • Integrates back to Oracle Identity Management Suite • Good integration with Microsoft Active Directory	• Already good feature set, but several advanced features yet roadmap items • Only baseline Access Governance support yet • Lack of support for specific mobile management features

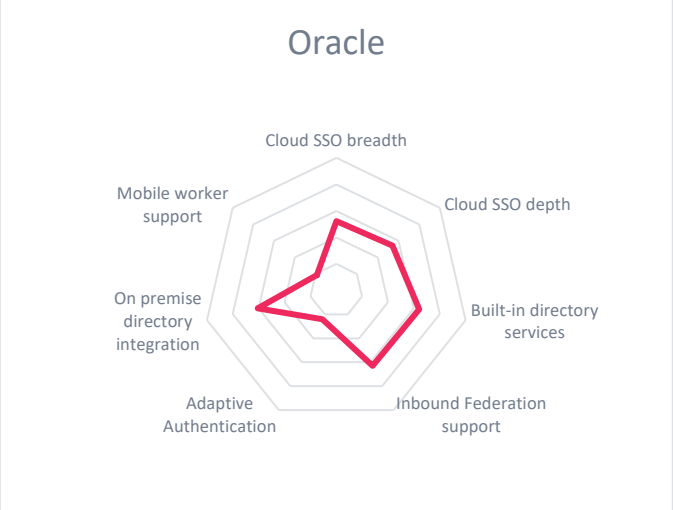
Table 23: Oracle Identity Cloud Service major strengths and weaknesses

The Oracle Identity Cloud Service delivers a variety of features we expect to see in the IDaaS market. This includes strong support for standards such as OAuth 2.0, OpenID Connect, SCIM, or SAML 2.0, as well as for REST APIs which support provisioning to cloud services. The service also comes with a good set of self-service user interfaces, supporting, e.g., profile management, password self-services, and management of the users' own applications. Furthermore, Oracle takes a broad approach on delivering IDaaS and has started to innovate in many areas, including Access Governance and Adaptive Authentication.

Furthermore, integration with the on-premise Oracle Identity Management Suite, but also with Microsoft Active Dirctory, is strong. Beyond that, there now is a gateway allowing integration with on-premises solutions for customers not running the Oracle Identity Management Suite on premises. The integration capabilities overall are strong, when it comes to the core IDaaS use cases. More advanced capabilities such as advanced mobile management features are lacking. On the other hand, Oracle has started adding Access Governance capabilities and shows a well thought-out roadmap in this and other areas.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 24: Oracle Identity Cloud Service rating



Oracle Identity Cloud Service is an interesting offering, targeted at enterprise customers. Oracle focuses on standard-based integration, but also integrates back with its own on-premise IAM offerings. The service provides good above-baseline features and Oracle shows a promising roadmap. With Oracle being a late entrant into the market and already delivering an interesting solution, we expect them to catch up quickly and thus already being an interesting option for customers.

5.12 Ping Identity PingOne Cloud

Ping Identity is an established pioneer in the market for Identity Federation and Cloud IAM. The company is highly engaged in standards initiatives, driving the development of standards in the field of IAM. PingOne Cloud is their IDaaS solution, providing both Identity Federation and Directory Service capabilities.

Strengths/Opportunities	Weaknesses/Threats
• Good support for a variety of use cases, beyond IDaaS SSO • Strong standards support • Integrates with Ping's own directory service • Good integration with on-premises environments and tight integration into other Ping Identity products	• Very limited workflow capabilities for onboarding and self-registration • Only 3rd party datacenters in the EU, but has its own datacenters in US

Table 25: Ping Identity PingOne Cloud major strengths and weaknesses

PingOne Cloud service is operated from Ping Identity's own datacenters in Denver and Boston and runs in AWS (Amazon Web Services) data centers in the U.S. and other locations such as Ireland. It provides a secure IAM experience for users of various devices, including a variety of mobile devices. The service is available in several versions, with varying features and scalability.

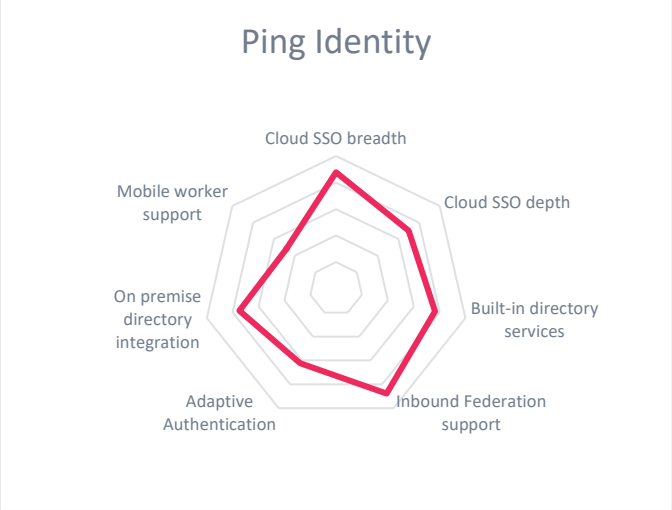
It provides a unified interface where users can view and quickly access their approved apps. This interface is accessible from devices such as mobile phones and desktops. It supports a vast number of preconfigured applications, including enterprise-level SaaS applications.

Access to applications can be via basic SSO, i.e. username/password, or Federated SSO, based on standards such as SAML 2.0. Customers can onboard additional applications and integrate them into the directory of available Cloud applications. Customers can also manage how users access these apps through group access control and context-based authentication policies. The product supports various ways for integrating with on-premise IAM infrastructures. Furthermore, it comes along with its own directory service, after the acquisition of UnboundID by Ping Identity. This also extends the scope beyond employee and business partner use cases to an even stronger support for customer-facing scenarios.

The service also provides broad support for adaptive authentication, including its own 2FA (Two Factor Authentication) capabilities.

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

Table 26: Ping Identity PingOne Cloud rating



Overall, Ping Identity with its PingOne Cloud offering and other tools for integration back to on-premise environments, is one of the leading vendors in the IDaaS SSO market. Based on their strong offering, they should be considered when evaluating enterprise-level providers for IDaaS SSO.

5.13 SAP Cloud Platform Identity Authentication

SAP, as one of the leading enterprise software vendors, entered the IDaaS market a while ago. The portfolio now consists of three distinct cloud services, which, however, can work in a tightly integrated manner. For IDaaS SSO, SAP Cloud Platform Identity Authentication is the primary service, delivering authentication services to SaaS applications.

Strengths/Opportunities	Weaknesses/Threats
• Excellent integration with SAP environments • Complemented by additional SAP IDaaS services • Integrated MFA capabilities • Large number of customers	• Very limited out-of-the-box support for non-SAP SaaS services • Licensing model is usage-based, but capped • Limited standards support beyond SAML 2.0

Table 27: SAP HANA Cloud Platform Identity Authentication major strengths and challenges

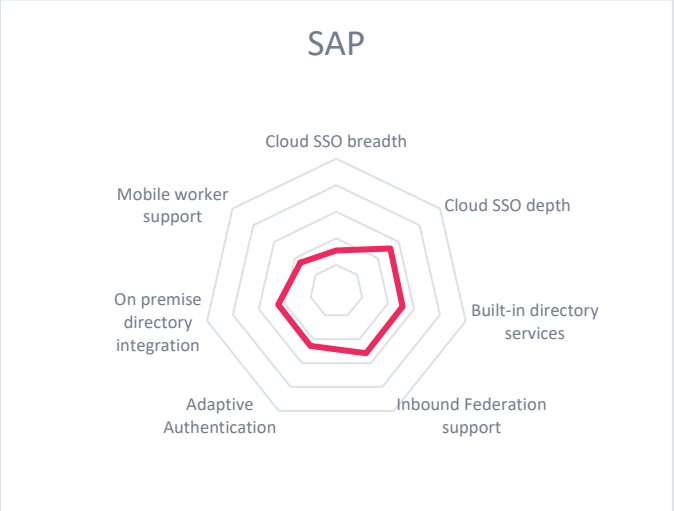
SAP Cloud Platform Identity Authentication or, in short, SAP CP Identity Authentication, is one of three IDaaS offerings SAP currently has in its portfolio. SAP CP Identity Provisioning adds provisioning capabilities to both cloud services and on-premise applications, while SAP Cloud Identity Access Governance delivers additional access analysis services.

With its services, SAP is, not surprisingly, successful in its traditional customer base, where the offerings deliver tight integration and good support for the required capabilities. On the other hand, we observe some gaps in fully supporting the common set of standards such as OpenID Connect or SCIM, but in particular out-of-the-box support for non-SAP environments.

A challenge for customers might occur due to the usage-based licensing model, which counts the number of authentications, instead of working with a flat fee per user/month. This model has to be carefully evaluated.

Security	strong positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 28: SAP HANA Cloud Platform Identity Authentication rating



SAP Cloud Platform Identity Authentication shows great potential for the IDaaS SSO market, with outstanding yet not surprising integration into SAP environments. The main challenge of the SAP offering is the limited out-of-the-box support for non-SAP environments. While there is standard support allowing integration of such solutions, by providing a comprehensive out-of-the-box support, SAP might be well able to become a leading-edge IDaaS SSO vendor.

5.14 SailPoint IdentityNow

IdentityNow is the IDaaS SSO offering provided by SailPoint. While the primary focus is on the IDaaS B2E use case, IdentityNow also serves well as an offering for enterprise-level IDaaS SSO use cases. With IdentityNow, SailPoint is well-positioned for the emerging demand of both pure-play IDaaS deployments and integrated delivery for hybrid environments.

Strengths/Opportunities	Weaknesses/Threats
• Enterprise-grade approach to IDaaS, supporting both SSO and B2E use cases • Broad out-of-the-box support for SaaS services, including enterprise-class services • Provides a high degree of standardization for common IAM/IAG functions	• Some few features, particularly around in-depth Access Governance, still lacking • Relies on 3rd party IaaS providers for delivery only, no own datacenters • Lack of specific mobile management features

Table 29: SailPoint IdentityNow major strengths and weaknesses

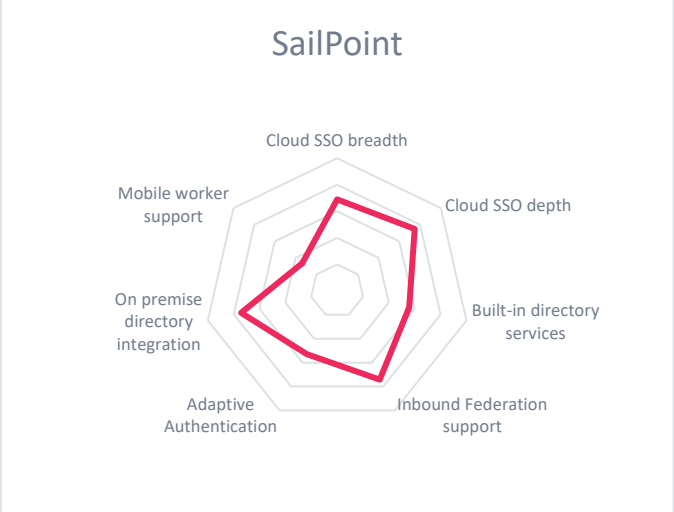
SailPoint IdentityNow consists of a number of feature areas: Single Sign-On, Password Management, Access Certification, and User Provisioning, and Access Request Management. Furthermore, it delivers built-in Policy Management and Analysis. In contrast to pure-play IDaaS SSO solutions, the service differs in its Identity Provisioning and Access Governance capabilities. While the latter are sort of an extra for IDaaS SSO services, provisioning capabilities are highly important for tight integration especially into enterprise-class SaaS offerings.

Furthermore. SailPoint provides a managed virtual appliance that runs on-premise and delivers connectivity and reverse proxy capabilities. The term “managed” means that it is managed from the Cloud but runs locally. From there, local integration to existing applications can be configured, in combination with SailPoint’s IdentityIQ offering.

SailPoint has chosen a different path with its initial focus on IDaaS B2E, but also reached a strong level of maturity for the IDaaS SSO market, particularly when looking at enterprise customer requirements in hybrid environments.

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

Table 30: SailPoint IdentityNow rating



SailPoint IdentityNow is an interesting offering in the IDaaS market, serving both IDaaS SSO and IDaaS B2E use cases at a strong level. While there are some gaps such as mobile management features, other capabilities make the solution an interesting option to the pure-play IDaaS SSO vendors.

5.15 Salesforce Identity

Salesforce.com is an established player in the SaaS market, primarily known for its CRM (Customer Relationship Management) offering. The portfolio has expanded massively over the years, now providing broad support for various types of applications, primarily centered on those for customer relationship and sales/marketing. Salesforce Identity adds to these services by providing IDaaS SSO capabilities. Salesforce itself understands these capabilities as a logical enhancement of their services, providing a unified experience for customers and well-integrated identity and access management capabilities for their tenants.

Strengths/Opportunities	Weaknesses/Threats
• Significant number of preconfigured Cloud services • Integrated support for social logins • Backend integration provided through a partnership • Strong workflow features	• Limited support for existing legacy web applications that do not support federation standards

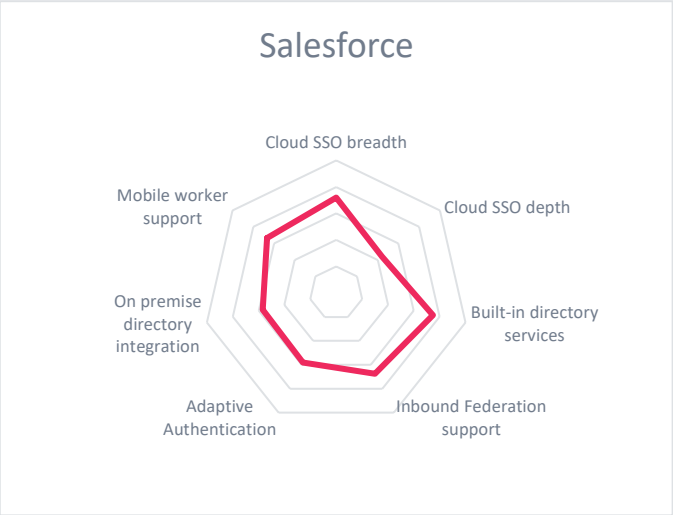
Table 31: Salesforce Identity and Salesforce Identity Connect major strengths and weaknesses

The approach Salesforce.com takes is targeted at their customers and other external users, but also provides flexible integration to on premise directory services. In contrast to most other players in the IDaaS market, Salesforce Identity already provides consumer-centric features such as support for social logins. The standards support, particularly for modern standards, is very good. Thus, it is generally sufficient for what commonly is required.

While there is support for a broad number of preconfigured Cloud services, there is no support for integrating back to web applications which don't support federation standards, including existing on-premise web applications. This is also a challenge given the fact that a significant portion of today's cloud services do not support SAML 2.0 and other standards. On the other hand, there is strong support for workflows, supporting, for instance, self-registration of users and authentication workflows.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 32: Salesforce Identity and Salesforce Identity Connect rating



Overall, Salesforce Identity is an interesting, enterprise-grade offering particularly for organizations looking at onboarding their customers and business partners and managing their identities and access. The service is run from Salesforce.com datacenters and is one of the more comprehensive offerings for IDaaS. It is independent but tightly integrated with other services provided by Salesforce.com and an interesting alternative to the pure play vendors in the IDaaS market segment.

5.16 SecureAuth IdP

SecureAuth is one of the vendors in the market that have been around for quite some time. As the name implies, their specific strength is not only providing IDaaS capabilities but strong authentication as a service. In contrast to most other offerings, SecureAuth supports both cloud-based and on-premise deployments.

Strengths/Opportunities	Weaknesses/Threats
• Strong support for strong and adaptive authentication mechanisms • Tight integration especially with on-premise Microsoft Active Directory • Strong standards support and broad out-of-the-box support for services • Well thought-out approach on security and data privacy	• Cloud deployment based on external data centers only (AWS) • No integrated directory service, but good support for on premises directories and JumpCloud cloud directory • Limited support for business partners and customer-centric use cases

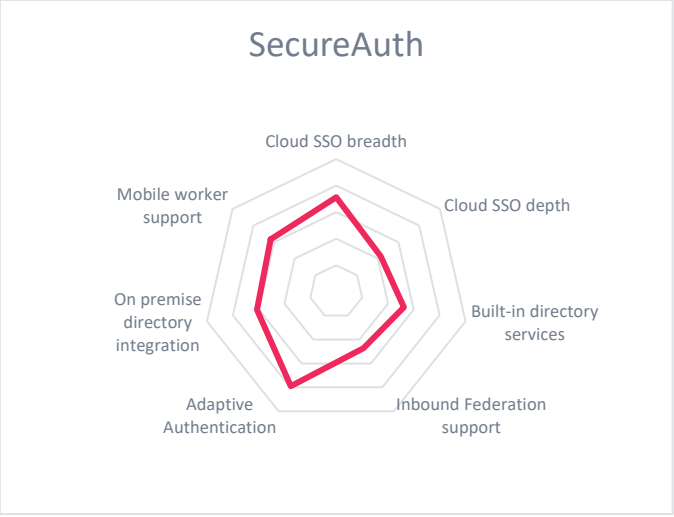
Table 33: SecureAuth IdP major strengths and weaknesses

When looking at the broader feature set of IDaaS SSO, SecureAuth is primarily targeted at strong authentication, mobile access, and cloud SSO for enterprise users. Supporting the emerging use cases around customers and business partners and managing their access to both existing web applications and Cloud services is not yet the primary scope of SecureAuth. However, SecureAuth is increasingly targeting that domain as well.

On the other hand, they provide strong features for strong and adaptive authentication, with more than twenty different approaches currently supported, including soft tokens and a variety of other technologies. Also, support for mobile users is strong. Support for standards is also strong. Likewise, the integration with backend IAM services is good, in particular with Microsoft Active Directory. The user store is always kept on-premise.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 34: SecureAuth IdP rating



When deployed as a cloud service, SecureAuth offers AWS (Amazon Web Services) as provider. They do not own datacenters, which is quite common in the market. For customers looking for strong integration with enterprise infrastructures and strong authentication, SecureAuth is an interesting pick despite their shortcomings regarding non-employee users.

5.17 Trustelem

Trustelem is one of the few players in the market that is not headquartered in the U.S., but in France. They provide a standard IDaaS SSO solution with good support for MFA (Multi Factor Authentication), being one of the rare players in the market segment that already supports the FIDO Alliance standards.

Strengths/Opportunities	Weaknesses/Threats
• Good support for MFA and client certificate authentication • Integration with Azure AD • Good baseline out-of-the-box support for enterprise-grade SaaS services • Runs in EU-based data centers only • Low price	• Overall list of connectors still too short • Most advanced features still missing, e.g. risk- and context-based authentication • Limited support for business partners and customer-centric use cases • Lack of support for mobile management features

Table 35: Trustelem major strengths and weaknesses

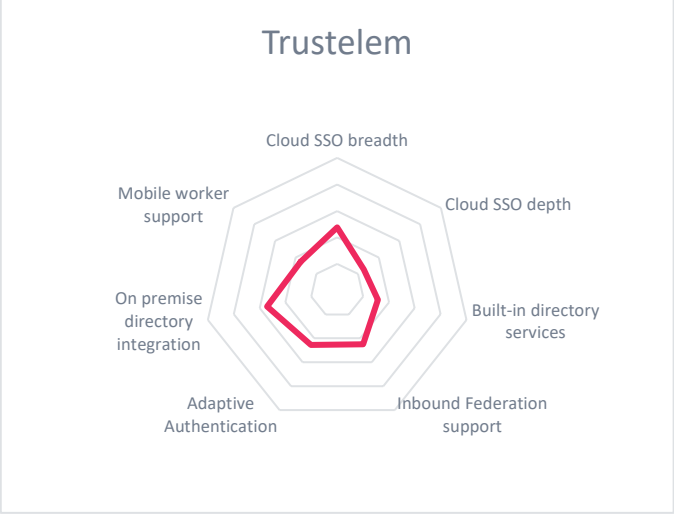
Trustelem, as of now, focuses on the essential building blocks of an IDaaS SSO solution. It integrates with existing directory services such as Microsoft Active Directory and LDAP directories, but also Azure AD, it provides pass-through authentication of Microsoft Active Directory authentication, it allows adding a variety of additional authentication factors for both traditional and mobile devices, and it integrates with a series of SaaS services.

The service does not deliver any of the more advanced feature sets we frequently see in IDaaS SSO solutions, be it specific support for business partners and customers, be it workflow capabilities and extensive self-service interfaces, or be it mobile management features.

On the other hand, the support for MFA or 2FA (Two Factor Authentication) is above average, particularly through tight integration with some specific second factors such as Neowave and Inwebo, both being particularly relevant in France, and for FIDO U2F devices. FIDO Alliance standards allow integrating with mobile devices and other devices providing some form of strong authentication in a standardized way.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	positive
Usability	neutral

Table 36: Trustelem rating



Trustelem, with its roots in France and its focus on EU-based data centers, as of now is primarily an option for EU-based customers. While the feature set is not outstanding, baseline capabilities for IDaaS SSO are provided at a fair price. Furthermore, support for directory integration and 2FA/MFA is strong. This makes it an interesting option to the established players.

5.18 VMware Identity Manager

VMware is still primarily perceived as vendor of virtualization solutions. However, with the acquisition of Airwatch early 2014, the company has gone well-beyond virtualization and is increasingly targeting the field of secure application delivery to users. This includes VMware Identity Manager, which is available as a SaaS offering and serves the emerging IDaaS market, also covering the IDaaS SSO segment.

Strengths/Opportunities	Weaknesses/Threats
• Strong integration into on-premise environments based on virtualization • Leading edge mobile management capabilities	• Not a very well-known offering of the vendor, yet a key component of Workspace ONE • Lack of Access Governance capabilities

Table 37: VMware Identity Manager major strengths and weaknesses

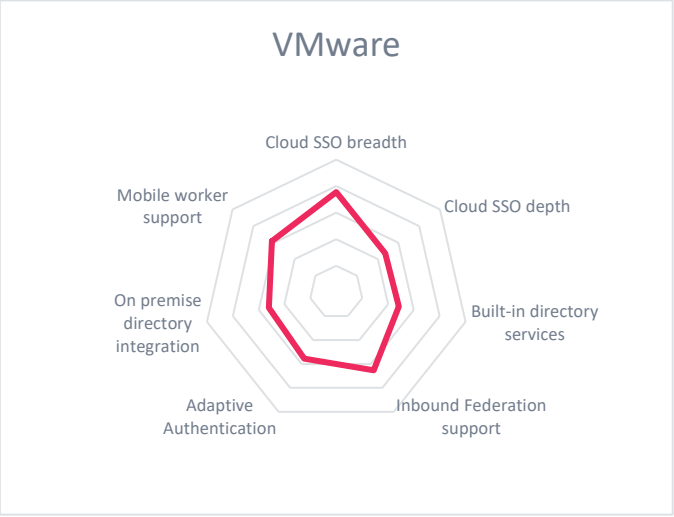
With their VMware Identity Manager offering, they build on securing both the device via Airwatch technology, and the user with additional identity and SSO (Single Sign-On) services. The solution seamlessly integrates with VMware;s WorkspaceOne and provides a user experience based on the user's identity and context. This is combined with broad support for a variety of application delivery models, providing seamless, secure access with SSO to these applications.

With its integration of Mobile Security solutions, an application catalog, the support for a variety of application deployment options, and Identity Management features, VMware Identity Manager is bringing in new concepts to IDaaS solutions. VMware Identity Manager supports both the trend towards mobile and frequently unmanaged devices and the increasing use of cloud applications, while not ignoring the need for access to traditional on-premise applications. Thus, its scope is larger than what many of the other players in this market segment provide today.

However, there is also room for improvement. One area we see is the need for broader out-of-the-box support of user directories, in particular the various cloud-based directories. Together with that, extended support in particular for the emerging FIDO Alliance standards would be nice-to-have features.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 38: VMware Identity Manager rating



Despite some features still lacking, VMware Identity Manager is definitely a solution to look at. The integration of various features builds the groundwork for a new approach to both Mobile Security and IDaaS. We recommend evaluating VMware Identity Manager when looking for solutions for IDaaS in hybrid environments and secure access from mobile devices to a variety of applications.

6 Vendors and Market Segments to watch

In addition to the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting for that market. Some had 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 IDaaS SSO or are not yet mature enough to be considered in this evaluation. We provide short abstracts on these vendors. Notably, several vendors in the broader IDaaS market that are targeting primarily the IDaaS B2E functionality who are covered in more detail in the KuppingerCole Leadership Compass on IDaaS B2E.

6.1 8K Miles Group

8K Miles Group is a System Integrator that provides an own IDaaS offering, EzIAM, but also other services such as Federated SSO as an IDaaS service. They deliver a broad set of services and support common SaaS services as a target. The US-based provider might be an alternative to established IDaaS vendors.

6.2 Bitium

Bitium is one of many start-ups in the IDaaS market and headquartered in the Los Angeles area. It is a single-product company, offering the Bitium IDaaS service in three variants, with differences in pricing and feature set. The editions differ in the breadth of integration capabilities and advanced security features such as MFA (Multi Factor Authentication) support and advanced Credential Management.

Bitium is one of the IDaaS vendors worth looking at, with their strength around Adaptive Authentication and good directory and HRMS system integration. The latter is what makes them a potential player in the IDaaS B2E market as well, although not being leading-edge. Particularly interesting for customers focusing more on cloud than on-premise services, but given tight integration with existing directory services and identity sources, plus good security features, Bitium can be a good choice.

6.3 Cion Systems

CionSystems is a relatively small vendor focused on supporting Microsoft environments. It provides several tools for such environments, including an IDaaS offering named Cloud Identity Minder. As a specialized vendor with primary focus on Microsoft environments, its scope is rather narrow. The solution can be installed on-premises or run in the cloud.

The solution provided by CionSystems differs from other solutions in the market on the one hand by its rather narrow scope, being focused on the Microsoft application landscape. On the other hand, it can be run from the cloud but based on using standard IaaS (Infrastructure as a Service) environments such as Microsoft Azure or Amazon AWS, but not in the typical cloud deployment model fully operated by the vendor.

6.4 Cloudentity

Cloudentity is a Seattle-based CIAM & IDaaS vendor. Their cloud-first identity solution is based on micro-services for increased scalability. The Cloudentity licensing model is also tied to micro-service usage, rather than per user or per transaction fees. Moreover, the micro-service architecture allows Cloudentity to support and augment other CIAM, IAM, and IDaaS solutions.

The Cloudentity risk engine aggregates threat and fraud intelligence from multiple sources, performs identity proofing, and can evaluate internal, external, and data attributes. Cloudentity offers MFA, and supports SAML, OAuth, OIDC, and SCIM. They take an innovative approach to integrating device identity: devices can register as top-level entities, and relationships can be managed between devices according to policies without association to human users. This allows for modeling complex relationships and operationalizing machine-to-machine interactions. Cloudentity supports the nascent OAuth2 Device Flow specification, which is an increasingly popular method for linking consumer identities to SmartHome automation and wearable IoT devices.

6.5 Google

Google delivers their Google Identity Platform which allows organizations building their authentication system around the Google services, based on Google Sign-In. It delivers low-end 2FA (Two Factor Authentication) support and integrates via standards with other services, including the Google G Suite. This solution is of particular interest for customers that made a strategic decision for Google G Suite and want to integrate additional services into that environment with a seamless SSO experience. However, Google as of now is not offering a full-featured IDaaS SSO solution.

6.6 LastPass

LastPass is an established player in the area of user password management. However, based on that cloud service, they also can act as an IDaaS SSO provider, who delivers a seamless SSO experience to a variety of services by storing and injecting credentials. This service also is available as an enterprise service with additional capabilities. While not being a full-featured IDaaS SSO offering, it might be considered as an alternative to such solutions.

6.7 NetIQ CloudAccess

NetIQ provides their solution, CloudAccess, as a virtual appliance, which is targeted to run within the enterprise on-premise IT infrastructure. Thus, it does not fall into the category evaluated in this KuppingerCole Leadership Compass, while potentially being an alternative to Cloud-based solutions particularly for IDaaS services for employees. It might be evaluated as an alternative to the solutions reviewed in this KuppingerCole Leadership Compass.

6.8 ViewDS Cobalt

ViewDS, an Australia-based vendor, provides its Cobalt solution in the IDaaS market space. In contrast to other solutions, Cobalt is not targeted at end user organizations, but at SaaS providers that need a strong identity foundation for their own SaaS offerings. Thus, Cobalt does not exactly fit into the IDaaS market segments KuppingerCole is evaluating, but might be an interesting solution for specific use cases. This also might include “community cloud” environments, which are operated by a group of organizations.

7 Methodology

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

It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

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

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

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains products which lag behind in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even 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, 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 – 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[3]). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

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

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

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

Interoperability—interoperability also can have many meanings. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to insure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[4]) for more information about the nature and state of extensibility and interoperability.

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

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

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

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

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 the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

7.3 Vendor rating

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

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

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

Ecosystem – this dimension looks at the ecosystem of the vendor. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

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

7.4 Rating scale for products and vendors

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

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

7.5 Spider graphs

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

Cloud SSO breadth	Breadth of SSO functionality for cloud services, in particularly based on the number of connectors and the support for enterprise-grade SaaS services.
Cloud SSO depth	Depth of integration with cloud services, with specific emphasis on provisioning capabilities and support for cloud services that do not offer integration via SAML, OAuth 2.0, and SCIM.
Built-in directory services	Functionality and scalability of integrated directory services, allowing the management of users both locally and at scale. Scale is essential for emerging use cases such as managing customers.
Inbound Federation support	Ability to federate external users in from existing sources, based on federation standards. This can be relevant for employee-centric use cases, but is essential for integration of business partners.
Adaptive Authentication	Flexibility and functionality for adaptive authentication, including support for a variety of authenticators and flexible, risk- and context-based authentication.

On-premise directory integration	Integration capabilities with existing on-premise directory services, including, but not limited to, Microsoft Active Directory. In these directory services, most users for employee-centric IDaaS SSO use cases are still managed.
Mobile worker support	Support for mobile workers, including authentication capabilities and specific mobile management features, enhancing security of mobile access to cloud services.

The spider graphs add an extra level of 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 IDaaS. The better the rating per category, the closer the value is located to the edge.

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.
- Denial of participation: Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular market segment.
- Lack of information supply: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

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

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