KuppingerCole Report

LEADERSHIP COMPASS

by Martin Kuppinger | July 2017

Identity as a Service: Cloud-based Provisioning, Access Governance and Federation (IDaaS B2E)

Leaders in innovation, product features, and market reach for Identity as a Service offerings targeting full Identity and Access Management and Governance capabilities for employees in hybrid environments, but also delivering Single Sign-On to the Cloud and providing support for other groups of users. Your compass for finding the right path in the market.

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

Leadership Compass
Identity as a Service: Cloud-based Provisioning, Access Governance, and Federation (IDaaS B2E)
By KuppingerCole

KuppingerCole Leadership Compass
Identity as a Service: Identity as a Service: Cloud-based Provisioning, Access Governance, and Federation (IDaaS B2E)
Report No.: **70319**

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

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

Advisory Note: Enterprise Role Management - 70285

Executive View: Avatier Identity Management Suite - 71510

Executive View: EmpowerID - 70894

Executive View: Hitachi ID IAM Suite - 72540

Executive View: Omada Identity Suite v11.1 – 70835

Executive View: Oracle Identity and Access Management Suite Plus 11g R2 - 70917

Executive View: SailPoint IdentityIQ - 71319

Executive View: SAP HANA Cloud Platform Identity Authentication and Provisioning - 70290

Executive View: Saviynt Identity Governance and Administration (IGA) 2.0 - 71506

Executive View: Cloud Standards Cross Reference - 71124

Executive View: Microsoft Azure RMS - 70976

Executive View: VMware Identity Manager - 71455

Leadership Compass: Privilege Management - 72330

Leadership Compass: CIAM Platforms - 70305

Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) - 71141

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Access Management and Federation - 70790

Leadership Compass: Access Governance - 70735

Product Report: Microsoft Azure Active Directory - 70977

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 offerings targeting full Identity and Access Management and Governance capabilities for employees in hybrid environments, but also delivering Single Sign-On to the Cloud and providing support for other groups of users. In short, we named this segment IDaaS B2E for the solutions focusing on employees and the enterprise.

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 of 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 simple 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 are 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 offerings in our evaluation.

Notably, many of the solutions we have covered in this Leadership Compass are based on traditional on-premise offerings, but delivered in SaaS style models. On the other hand, a couple of vendors in this market segment have created pure-play SaaS offerings from scratch. This might become a decision criterion for some customers.

1.3 Required Capabilities

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

- Support for hybrid infrastructures; in contrast to IDaaS SSO solutions, which are targeted at cloud services, IDaaS B2E must serve the hybrid environments that are the norm for organizations. Features supporting the management of on-premise applications, from SSO to provisioning, or tight integration with on-premise tools, are. Thus, expected.
- Identity Provisioning capabilities are rated at a higher level than for IDaaS SSO. We expect good support for both cloud services and on-premise environments.
- Access Governance features, at least at a baseline level, are expected as well. This includes advanced auditing capabilities, but also might cover access review, SoD (Segregation of Duties) controls, and other more advanced features.
- 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 B2E.
- 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 will also gain momentum in the customer space, when relying on external Identity Providers.

IDaaS B2E 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 that 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 also 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 the 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 about 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, for example, 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 while we only listed major features, we looked at a variety of other capabilities as well when evaluating and rating the various IDaaS B2E 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 shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

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

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

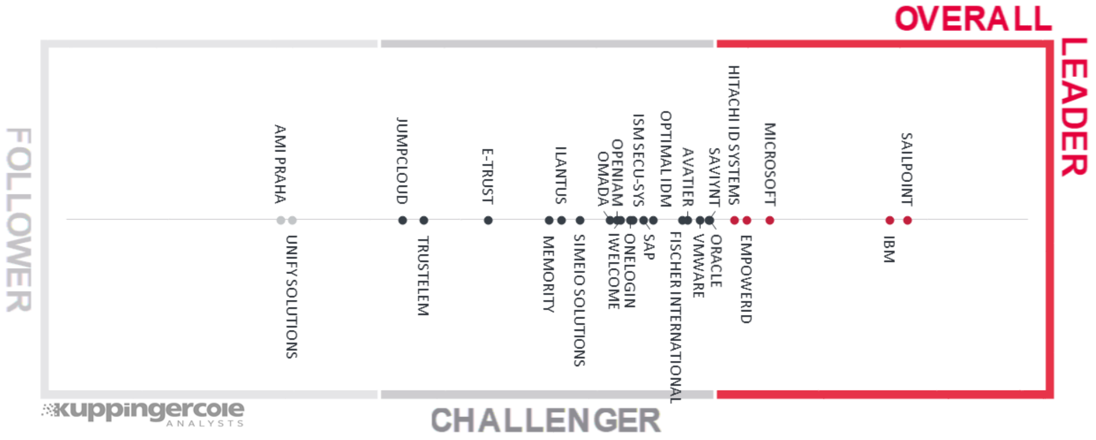


Figure 1: The Overall Leadership rating for the IDaaS B2E market segment

When looking at the Overall Leader segment in the Overall Leadership rating, we see only a handful of companies. This is an indicator of a still emerging market. While many vendors are entering this market segment, few have comprehensive solutions yet. On the other hand, we see several vendors showing strong potential, and we expect them to enter the Overall Leader segment within the next 12-18 months.

The current picture also reflects the fact that vendors in this market segment are originating from other, different, market segments. We see pure-play offerings such as the ones of SailPoint and IBM; solutions that are primarily targeted at IDaaS SSO and CIAM (Consumer IAM), but with advanced capabilities, such as Microsoft; and traditional on-premise Identity & Access Management and Governance solutions provided as a SaaS offering, such as Hitachi ID Systems and EmpowerID.

In the Overall Leader segment, we find only five vendors. SailPoint is in the lead, with IBM being close behind them. Both provide solutions specifically targeted at the requirements of the IDaaS B2E market. The three other players that made it into the Leader's section are Microsoft and EmpowerID, and Hitachi-ID.

While the Leader's segment is rather empty, we see many players in the Challenger's section. Many of these are well positioned in that segment. The vendors that are closest to becoming an Overall Leader are, in alphabetical order, Avatier, Fischer International, Oracle, Saviynt, and VMware, with both Oracle and Savyint missing the Leaders segment by margins. Following these, we find another group of vendors, including (again in alphabetical order) iSM Secu-Sys, iWelcome, Omada, OneLogin, OpenIAM, Optimal IdM, and SAP. These are competing head-to-head in that rating; however, some of them benefit more from product capabilities or innovativeness, while others show a stronger position in the market. We expect some vendors in that group to be able to improve their position significantly within the next 12-18 months.

Other vendors in the Challenger's section are Simeio Solutions, Ilantus and Memority. E-Trust, JumpCloud, and Trustelem (in alphabetical order) also made it into this section. JumpCloud is highly specialized, focusing on a "directory as a service" offering that also can be complementary to other IDaaS solutions.

In the Follower section, we find two vendors. UNIFY Solutions focuses on a broker approach, sitting in between on-premise directories and cloud services with a limited set of capabilities. AMI Praha, a Czech vendor, offers an as yet still too limited set of capabilities, while potentially being interesting for regional, medium-sized customers.

Overall Leaders are (in alphabetical order):

- EmpowerID
- Hitachi-ID Systems
- IBM
- Microsoft
- SailPoint

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.

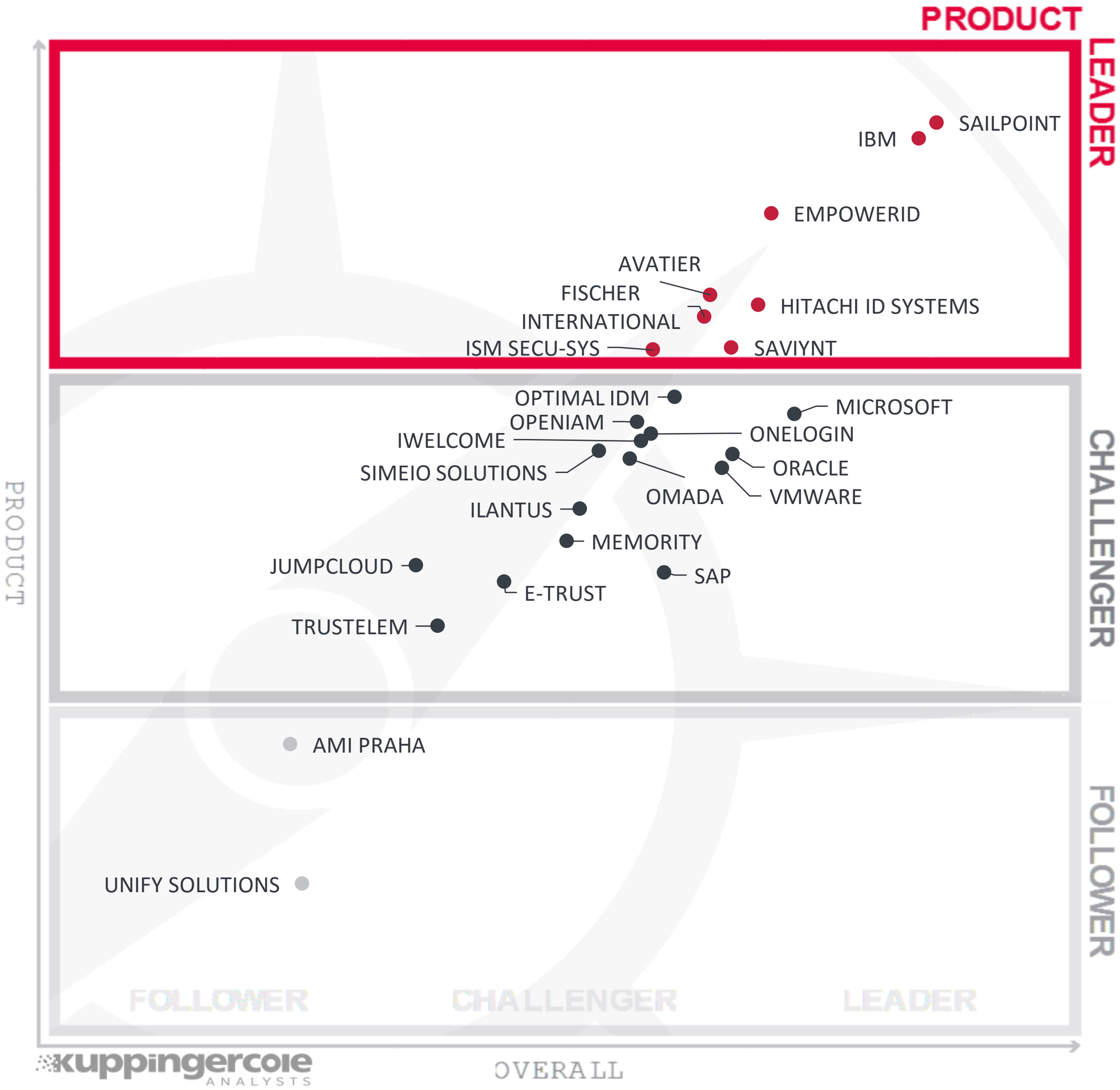


Figure 2: Product leaders in the IDaaS B2E market segment

Product Leadership, or in this case Service Leadership, is the view where we look specifically at the functional strength and completeness of products. Again, we only have a few vendors rated as Leaders, which is an indicator of a still emerging market segment where most vendors still lack functional completeness.

In front, we see SailPoint and IBM, both with specific IDaaS B2E offerings. EmpowerID also is positioned well. They deliver their standard IAM offering also as a SaaS service, but benefit from their functional completeness, in particular, regarding the integration of Identity Federation and Single Sign-On capabilities in the overall offering. Other vendors that made it into the Product Leader's segment are (in alphabetical order) Avatier, Fischer International, Hitachi-ID Systems, iSM Secu-Sys, and Savyint.

Again, the Challenger's section is very crowded. We see a lot of vendors being well positioned, including (in alphabetical order) iWelcome, Microsoft, Omada, OneLogin, OpenIAM, Optimal IdM, Oracle, Simeio Solutions, and VMware. Microsoft is expanding its capabilities for supporting hybrid environments, but falls short when it comes to Access Governance capabilities. Some of these, in particular Oracle, are likely candidates for entering the Leader's segment, by rapidly catching-up in functionality.

Behind these players, we see another group of vendors, with (in alphabetical order), E-Trust, Ilantus, JumpCloud, Memority, SAP, and Trustelem. The reasons for their ratings vary. While some vendors such as JumpCloud (directory as a service) or Saviynt (Access Governance as a service) are focused on specific aspects of IDaaS B2E, others are smaller or regional players.

In the Follower's section, we find AMI Praha, which still should catch up regarding the completeness of their offering, and UNIFY Solutions with their point product positioned as an Identity Broker. While AMI Praha is a regional player as of now, UNIFY Solutions might be used as a complement to other offerings, based on the specific feature set they provide.

Product Leaders (in alphabetical order):

- Avatier
- EmpowerID
- Fischer International
- Hitachi-ID Systems
- IBM
- iSM Secu-Sys
- SailPoint
- Savyint

2.3 Innovation Leadership

Another angle 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 emerging customer requirements.

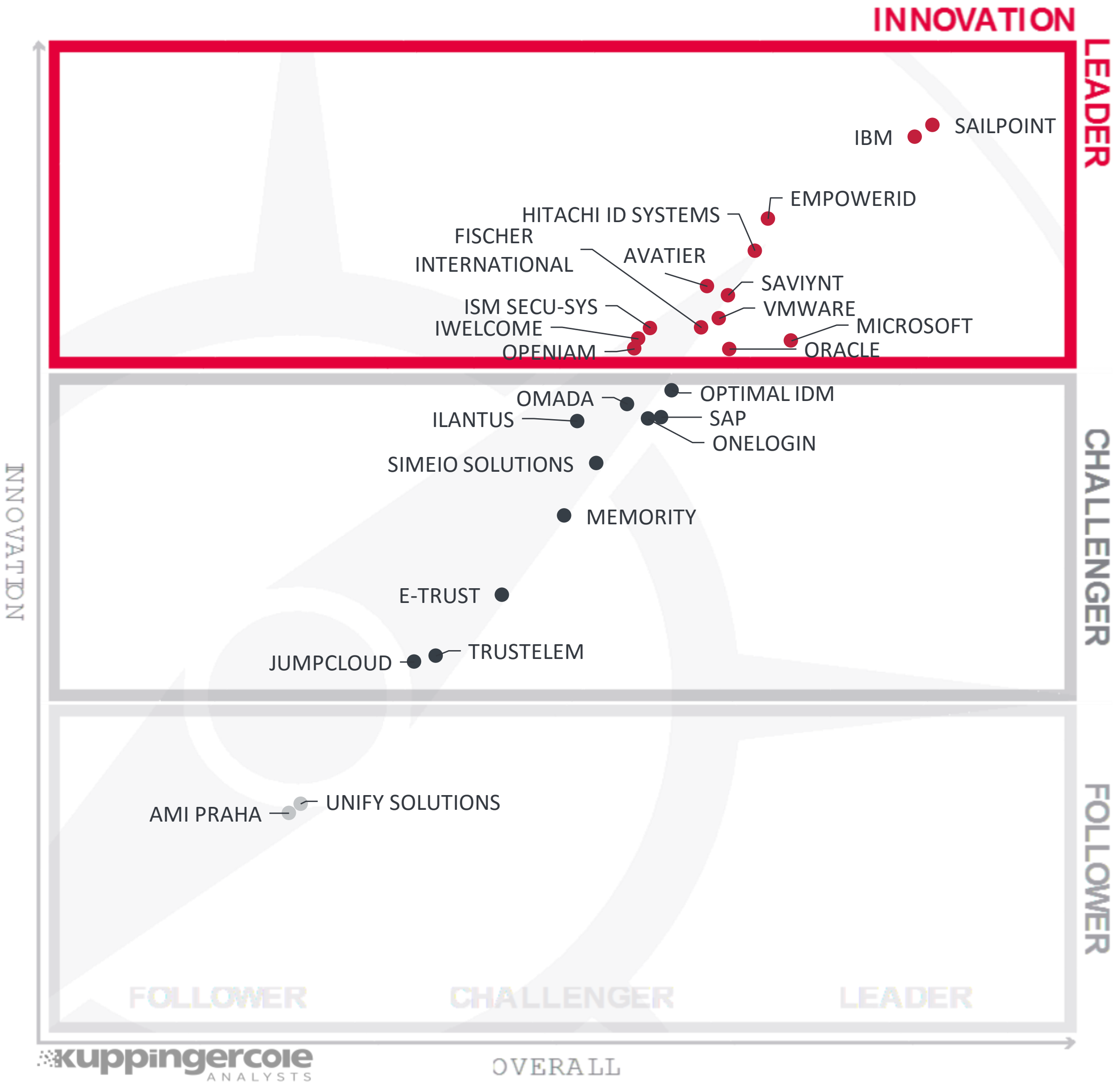


Figure 3: Innovation leaders in the IDaaS B2E market segment

When looking at Innovation Leadership, we see a different picture. While most vendors still show gaps in functional completeness, affecting the Product Leadership rating, many vendors are putting a lot of work into innovative feature areas. Thus, we see many vendors in the Innovation Leader’s segment. Not surprisingly, this is a typical for emerging markets such as the IDaaS B2E market.

Again, SailPoint and IBM are ahead of the others, with EmpowerID and Hitachi-ID following at some distance. After these four vendors, we find several others, including (in alphabetical order) Avatier, Fischer International, iSM Secu-Sys, iWelcome, Microsoft, OpenIAM, Oracle, Savyint, and VMware.

In the Challenger’s section, we find some vendors that are very close to entering the Leader’s segment. This group includes (again in alphabetical order) Ilantus, Omada, OneLogin, Optimal IdM, and SAP. As with the vendors in the Leader’s section, the offerings differ significantly, depending on the roots. Thus, some are stronger in, e.g., Access Governance capabilities, while others are better in supporting SSO to cloud services or provisioning back to the on-premise environments. Closely following this group when it comes to Innovation Leader is Simeio Solutions.

E-Trust, JumpCloud, Memority, and Trustelem (in alphabetical order) are further vendors which are positioned in the Challenger section for Innovation Leadership. All have their specific strengths or are targeted more at regional customers and thus might be an interesting alternative to the leading players in the IDaaS B2E market. JumpCloud as a specialized “directory as a service” provider can be used complementary to other offerings.

Finally, we have the Follower segment, with UNIFY Solutions as provider of an Identity Broker, and AMI Praha as a regional vendor.

Innovation Leaders (in alphabetical order):

- Avatier
- EmpowerID
- Fischer International
- Hitachi ID Systems
- IBM
- iSM Secu-Sys
- iWelcome
- Microsoft
- OpenIAM
- Oracle
- SailPoint
- Savyint
- 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.

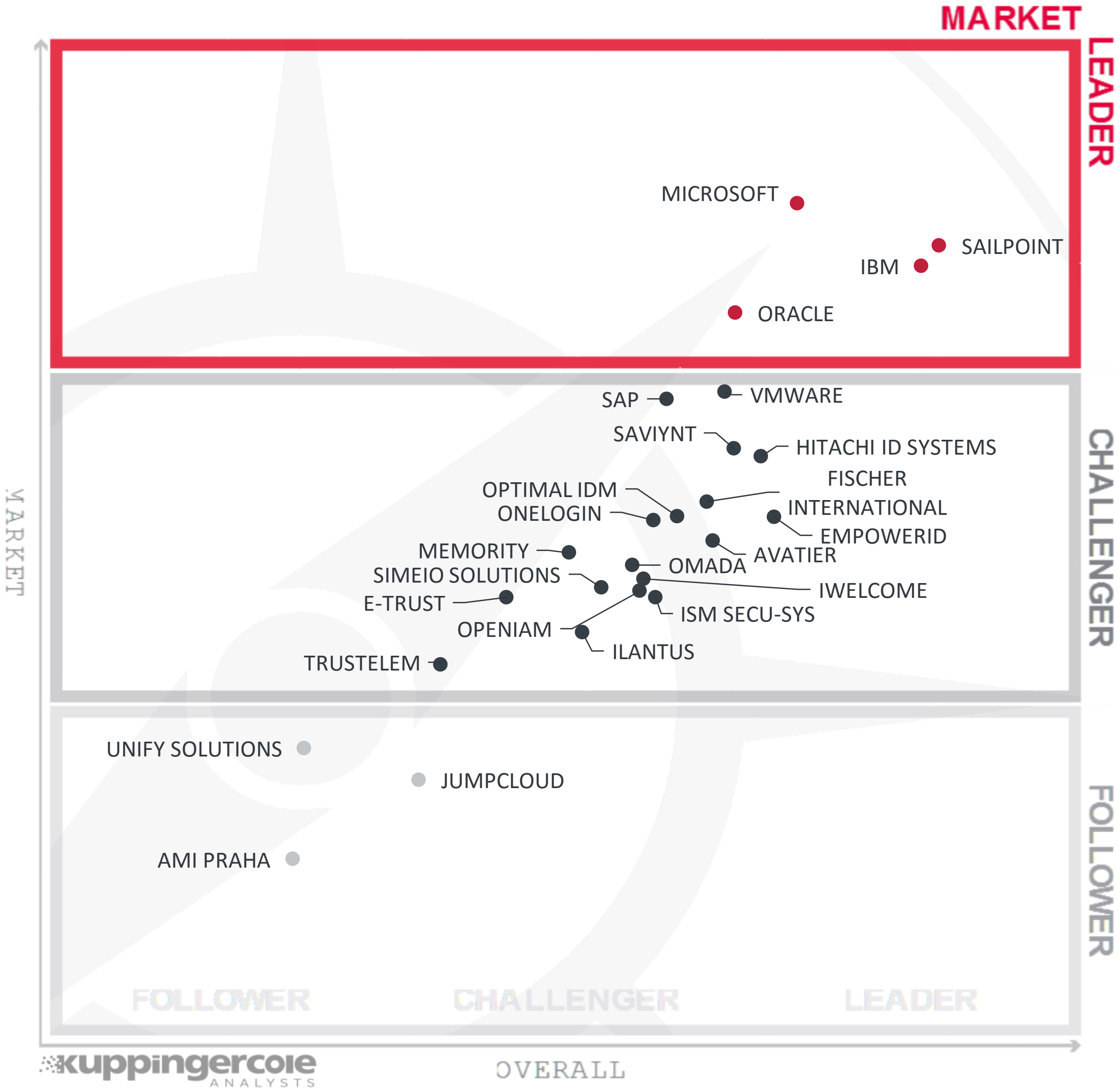


Figure 4: Market leaders in the IDaaS B2E market segment

Here, we see Microsoft in front, followed by SailPoint, IBM, and Oracle. All benefit from a global partner ecosystem, their ability to scale, and – particularly true for Microsoft – from a large installed base.

Close to entering this segment are SAP and VMware. Most of the other vendors are somewhere in the center or to the left of the Challenger section, including (in alphabetical order) Avatier, EmpowerID, E-Trust, Fischer International, Hitachi ID Systems, Ilantus, iSM Secu-Sys, iWelcome, Memority, Omada, OneLogin, OpenIAM, Optimal IdM, Saviynt, Simeio Solutions, and Trustelem.

Some of these are smaller players, while others either lack a global partner ecosystem or have, while being successful with on-premise solutions, a rather small number of customers for their IDaaS B2E offerings.

In the Follower section, we find UNIFY Solutions, JumpCloud, and AMI Praha, which are either regional players such as AMI Praha and UNIFY Solutions or smaller, but highly specialized, vendors.

Market Leaders (in alphabetical order):

- IBM
- Microsoft
- Oracle
- SailPoint

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 for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we 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.

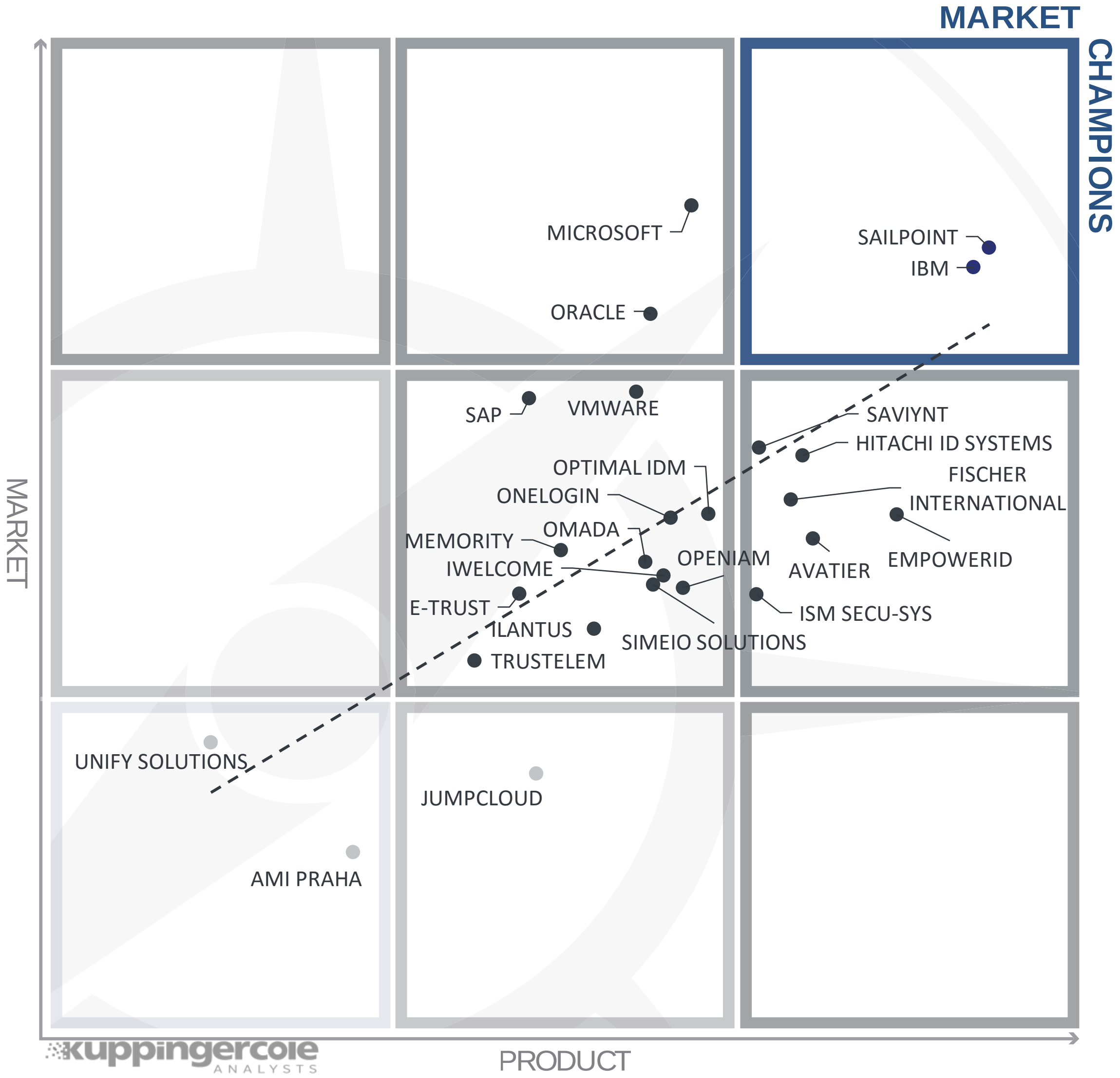


Figure 5: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

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 segment, we find the “Market Champions”. These are for that emerging market segment just two, SailPoint and IBM. Left to them, we see Microsoft and Oracle, which are strong players in the market, also due to their company size, global reach, and strong partner ecosystem, but not (yet) Product Leaders.

On the other hand, we find a number of vendors with interesting product offerings just below the Market Champions, which are not yet considered being Market Leaders. This segment includes, in alphabetical order, Avatier, EmpowerID, Fischer International, Hitachi-ID Systems, iSM Secu-Sys,and Savyint.

The by far most crowded segment is the one in the middle, containing all vendors that are both rated as challengers in the product and market ratings. This segment, in alphabetical order, holds E-Trust, Ilantus, iWelcome, Memority, Omada, OneLogin, OpenIAM, Optimal IdM, SAP, Simeio Solutions, Trustelem, and VMware.

Finally, we see some other vendors being placed below, which include (in alphabetical order): AMI Praha, JumpCloud, and UNIFY Solutions.

3.2 The Product/Innovation Matrix

The second 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 most markets with a significant number of established vendors plus some smaller vendors.

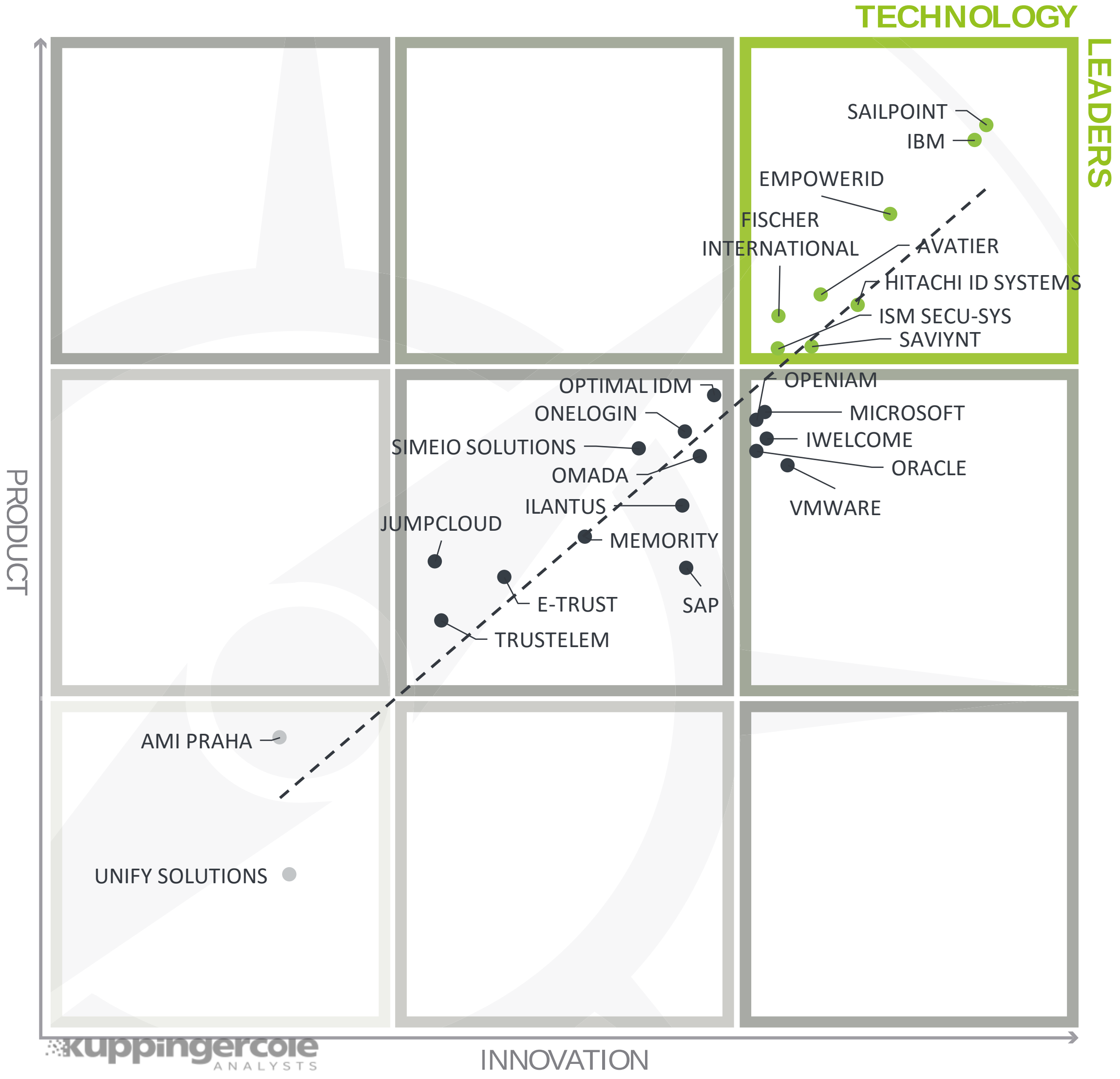


Figure 6: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we see a good correlation between the product and innovation rating, with most vendors being placed close to the dotted line. When looking at the "Technology Leaders" segment, again SailPoint and IBM are in the lead, followed by EmpowerID. Others include Avatier, EmpowerID, Fischer International. Hitachi-ID Systems, iSM Secu-Sys, and Saviynt (in alphabetical order).

In the box below them, we find the other Innovation Leaders, which are (again alphabetically) iWelcome, Microsoft, OpenIAM, Oracle, and VMware.

In the segment in the middle of the graphic, we find the companies that are challengers in both the innovation and product ratings. These include (in alphabetical order) E-Trust, Ilantus, JumpCloud, Memority, Omada, OneLogin, Optimal IdM, SAP, Simeio Solutions, and Trustelem.

Finally, we have AMI Praha and Unify Solutions in the lower left box.

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 to 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.

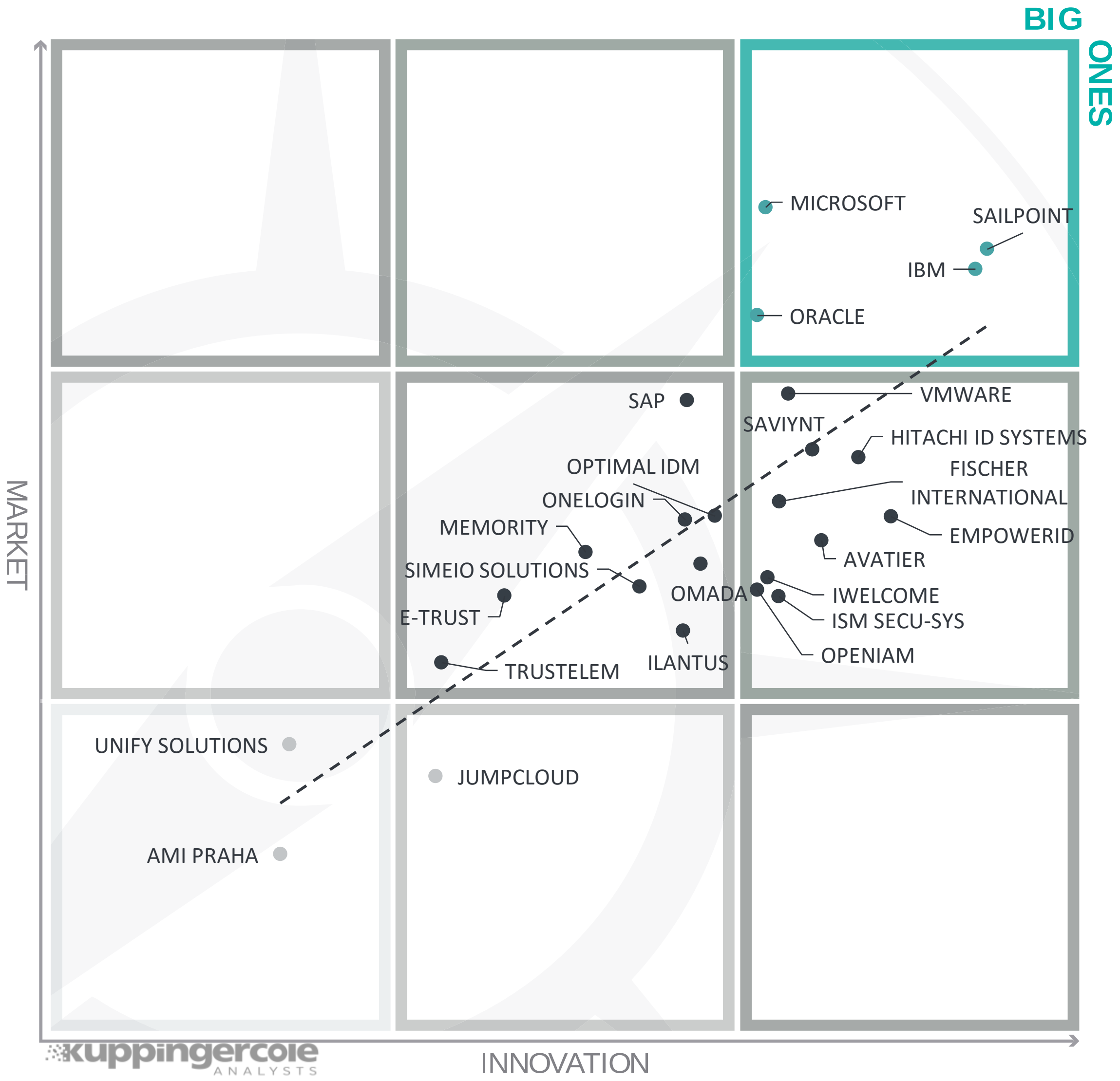


Figure 7: The Innovation/Market Matrix

Vendors 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 the upper right corner, we see the “Big Ones”, SailPoint, IBM, Microsoft, and Oracle. Just below them, we find the mass of vendors that are already rated as Innovation Leaders but considered only being a challenger in the market rating. These include (in alphabetical order) Avatier, EmpowerID, Fischer International, Hitachi-ID Systems, iSM Secu-Sys, iWelcome, OpenIAM, Savyint, and VMware.

In the central section, we find other vendors that are challengers in both the market and innovation ratings. These include (again in alphabetical order) E-Trust, Ilantus, Memority, Omada, OneLogin, Optimal IdM, SAP, Simeio Solutions and Trustelem.

Finally, we find AMI Praha, JumpCloud, and Unify Solutions more towards the bottom of the graphic, with all three vendors being either highly specialized or having a strong regional focus.

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.

4.1 Ratings at a glance

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

Product	Security	Functionality	Integration	Interoperability	Usability
AMI Praha	positive	neutral	weak	neutral	neutral
Avatier	strong positive	positive	strong positive	positive	strong positive
E-Trust	positive	neutral	neutral	positive	positive
EmpowerID	strong positive	positive	positive	strong positive	strong positive
Fischer International	positive	positive	positive	positive	positive
Hitachi ID Systems	strong positive	positive	positive	positive	positive
IBM	strong positive	strong positive	positive	strong positive	strong positive
Ilantus	positive	positive	positive	positive	positive
iSM Secu-Sys	positive	positive	strong positive	positive	positive
iWelcome	strong positive	positive	positive	positive	strong positive
JumpCloud	strong positive	weak	positive	neutral	neutral
Memority	positive	neutral	positive	positive	positive
Microsoft	strong positive	neutral	strong positive	positive	positive
Omada	positive	positive	positive	neutral	positive
OneLogin	not rated[1]	neutral	strong positive	positive	positive
OpenIAM	positive	positive	positive	positive	positive
Optimal IdM	strong positive	neutral	strong positive	positive	positive
Oracle	strong positive	positive	positive	positive	positive
SAP	strong positive	neutral	positive	neutral	positive
SailPoint	strong positive	strong positive	positive	strong positive	strong positive
Saviynt	positive	neutral	neutral	neutral	positive
Simeio Solutions	positive	positive	neutral	strong positive	positive
Trustelem	positive	neutral	positive	positive	neutral
UNIFY Solutions	positive	weak	weak	neutral	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 apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
AMI Praha	weak	critical	weak	weak
Avatier	positive	neutral	neutral	positive
E-Trust	neutral	weak	neutral	positive
EmpowerID	positive	neutral	positive	positive
Fischer International	positive	neutral	neutral	positive
Hitachi ID Systems	positive	neutral	strong positive	positive
IBM	strong positive	neutral	strong positive	strong positive
Ilantus	positive	weak	neutral	neutral
iSM Secu-Sys	positive	weak	neutral	neutral
iWelcome	positive	neutral	neutral	neutral
JumpCloud	neutral	weak	neutral	neutral
Memority	neutral	neutral	positive	neutral
Microsoft	positive	strong positive	strong positive	strong positive
Omada	positive	weak	positive	neutral
OneLogin	positive	neutral	positive	positive
OpenIAM	positive	neutral	neutral	neutral
Optimal IdM	positive	neutral	positive	positive
Oracle	positive	positive	strong positive	positive
SAP	positive	positive	strong positive	positive
SailPoint	strong positive	strong positive	positive	strong positive
Saviynt	positive	positive	neutral	positive
Simeio Solutions	neutral	neutral	neutral	neutral
Trustelem	neutral	weak	weak	neutral
UNIFY Solutions	weak	weak	neutral	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 AMI Praha SkyIdentity

AMI Praha is a Czech software vendor and system integrator which offers a Microsoft Azure-based IDaaS B2E offering named SkyIdentity. The solution is based on the standard IAM software MidPoint, which is pre-integrated to deliver the IDaaS service. MidPoint is an open source solution.

Strengths	Challenges
● Gateway approach for connecting back to on-premise systems, alternatively VPN tunnel ● Run on Microsoft Azure, variety of data centers to choose from ● Full set of standard Identity Provisioning capabilities ● Targeted at small customers	● Small vendor with very limited partner ecosystem ● Limited federation support, limited support for cloud SSO (but integrates to some major services) ● Very limited Access Governance capabilities ● Based on 3rd party (open source) solutions

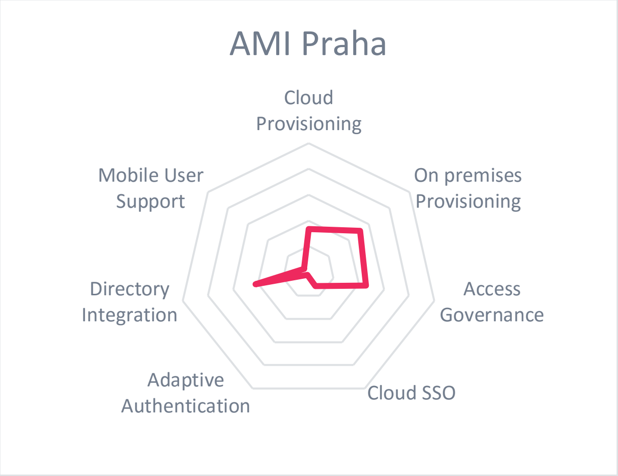
Table 3: AMI Praha major strengths and weaknesses

While the approach taken by AMI Praha is straightforward, the overall feature set is still rather limited, being primarily focused on baseline Cloud SSO and Identity Provisioning capabilities. However, the system at least supports on-premise systems through a gateway-style component or via VPN tunnels, which allows connecting back from the Microsoft Azure environment to the tenant's infrastructures.

While the set of connectors is rather rich, these are provided by 3rd party providers and not developed by AMI Praha itself. Aside from the baseline Identity Provisioning capabilities, we miss more advanced features in most of the areas we look at when rating IDaaS B2E offerings.

Security	positive
Functionality	neutral
Integration	weak
Interoperability	neutral
Usability	neutral

Table 4: AMI Praha rating



SkyIdentity is clearly targeted at medium-sized businesses and not yet a full enterprise-level solution. However, the underlying concept is straightforward and provides potential for enhancing the service to meet more advanced customer requirements. By running the service from Microsoft Azure, customers have a choice of data centers. We recommend AMI Praha continuing its investment to find its sweet spot in the market. For now, the solution is of interest primarily for local customers from medium-sized businesses looking for a SaaS alternative to a costly and complex local Identity Provisioning deployment.

5.2 Avatier

Avatier is a well-established U.S. based vendor that has its roots in the core areas of Identity & Access Management, in particular Identity Provisioning. Avatier has extended its portfolio over the past couple of years, with an emphasis on providing easy-to-use software which also is easy to customize for specific customer requirements. This provides Avatier a good starting point for a SaaS-type offering, even when based on their traditional software.

Strengths	Challenges
● Tightly integrated solution ● Flexible customization ● Leading-edge user interfaces with strong support for mobile users ● Overall strong capabilities for IDaaS B2E	● Basically a single-tenant, MSP-style offering ● Some weaknesses in Identity Federation, but strong SSO capabilities also covering cloud services ● Licensing model not ideally suited for IDaaS

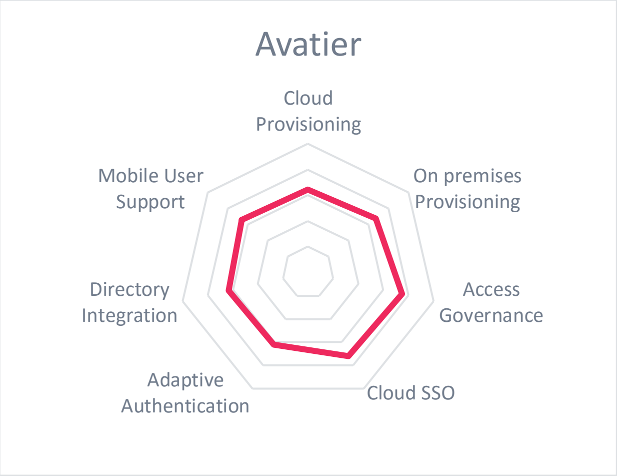
Table 5: Avatier major strengths and weaknesses

Avatier delivers a rich set of features and integrations to its customers, with a clear emphasis on interfacing to on-premise solutions, but a good baseline support particularly for enterprise-class cloud services. The UI is well-suited for today’s requirements of serving mobile users, but also of providing a wealth of self-service interfaces. In this area, we observe one of the biggest strengths of Avatier. Furthermore, all components are tightly integrated and based on the same underlying technology platform.

The solution also delivers strong capabilities for Single Sign-On to both on-premise applications and cloud services, combined with good support or Adaptive Authentication. Avatier is amongst the few vendors that already support the FIDO Alliance protocols for a standards-based integration with strong authentication technologies integrated into mobile devices.

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

Table 6: Avatier rating



As with other vendors that provide a traditional on-premise Identity Management software as a service, Avatier has to face the challenge of delivering that service efficiently to multiple tenants. On the other hand, many IDaaS B2E decisions are strategic, which allows the running of such deployment models successfully. Furthermore, the approach chosen allows Avatier to deliver a very broad set of capabilities to its customers.

5.3 E-Trust Horacius

While they have been in the market for many years, e-Trust still is one of the less well-known vendors in the market with its Horacius Identity & Access Management and Governance offering. The solution is also provided in a SaaS-style deployment model, even while relying on an on-premise software product.

Strengths	Challenges
● Overall strong Identity Provisioning and Access Governance capabilities ● Good set of on-premise connectors ● Service bus approach allows for efficient SaaS deployments	● Focused on Identity Provisioning and Access Governance, lack of Identity Federation ● Somewhat limited regarding SaaS connectors ● Global, but rather small partner ecosystem

Table 7: E-Trust Horacius major strengths and weaknesses

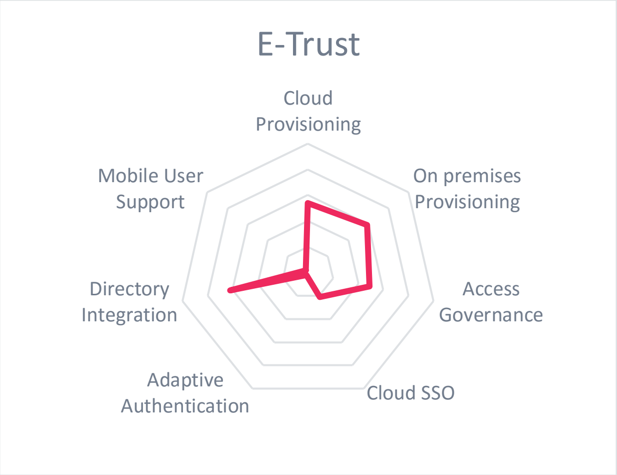
The SaaS offering provided by e-Trust is based on a mature, proven IAM product that provides Identity Provisioning capabilities, but also Access Governance and Access Risk Management features. This is complemented by some self-service interfaces and, overall, at a good capability level.

Technically, Horacius differs from other offerings in relying on a service bus approach for connecting to target systems. This allows decoupling such systems, which is beneficial for SaaS-type delivery models, because integration back to the on-premise target systems via the service bus is straightforward.

An interesting aspect of e-Trust is the additional SOC (Security Operations Center) services that can complement the Horacius offering, improving the overall security services of an organization.

Security	positive
Functionality	neutral
Integration	neutral
Interoperability	positive
Usability	positive

Table 8: E-Trust Horacius rating



As with some of the other vendors who entered the IDaaS B2E market based on an existing on-premise offering for Identity Provisioning and Access Governance, e-Trust shows weaknesses in Identity Federation, which can turn out to be an inhibitor, particularly for customers that have a significant set of cloud services. On the other hand, the baseline functionalities make it an interesting offering for organizations that primarily look for a SaaS solution supporting their on-premise requirements in IAM.

5.4 EmpowerID

EmpowerID with its product also named EmpowerID takes a unique approach to IAM/IAG. It is built from scratch on a Business Process Management/Workflow platform. All standard components rely on that platform and customizations can be made using the same environment. That allows for great flexibility, while the product also delivers a broad set of out-of-the-box features. The service is also offered as a Cloud solution by partners of EmpowerID.

Strengths	Challenges
● Unique, business process-based approach ● Integration back directly to target systems or indirectly via gateway ● Flexible customization based on the central workflow engine, supported by a large number of predefined processes	● Based on an on-premise software solution, but based on a fully multi-tenant approach ● Small partner ecosystem and SaaS service provided only through partners

Table 9: EmpowerID major strengths and weaknesses

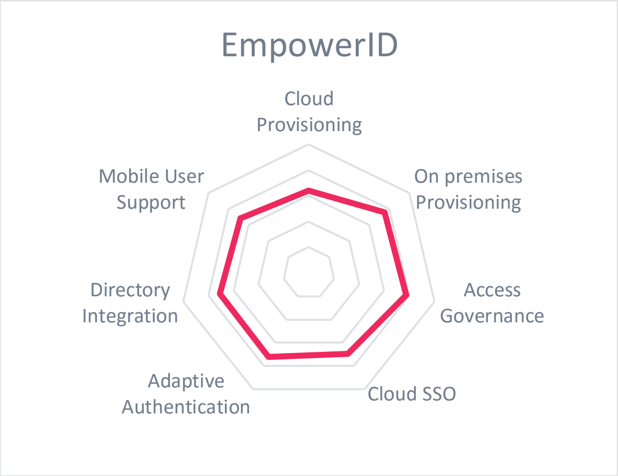
Customization of EmpowerID is very flexible, based on the process-focused approach. As this implies, it is primarily about selecting and customizing graphical workflows, not about coding. The product delivers a very broad feature set for Identity and Access Management, going well beyond Identity Provisioning but with tight integration to these core features. That includes Dynamic Authorization Management capabilities and integrated Identity Federation features. Overall, support for new technologies and standards such as OAuth, OpenID, RESTful APIs, or integrated STS (Secure Token Service) is broad.

However, the product also delivers a broad functionality for common requirements of IDaaS B2E. This includes Single Sign-On capabilities to several Cloud services, built-in and very extensive Identity Federation capabilities, and support for various authentication types.

Integration to existing on-premise systems can be done both via direct integration or via a gateway. While the first approach requires network ports to be opened, the latter allows using one central system which then connects to the various targets.

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

Table 10: EmpowerID rating.



Overall, EmpowerID is a very interesting and innovative solution. It provides a well thought-out and flexible approach for Cloud IAM/IAG with strong Identity Federation and authentication support. The workflow approach might not suit every customer's needs, but is worth evaluating. From the Cloud Service Provider perspective, EmpowerID relies on partners in various regions, but has no offerings of its own. However, being multi-tenant from scratch, one of the basic requirements for providing a Cloud service is met.

5.5 Fischer International Identity

Fischer International Identity is a vendor which is different from all other traditional Identity Management vendors in that the company from the very beginning focused on SaaS delivery models for IAM as a main go-to-market strategy and core competency. The product is available for on-premise deployment as well, which makes up a significant portion of the Fischer sales. However, the entire architecture has been defined for optimally supporting SaaS deployments, requiring only a gateway at the customers' sites. While this approach also suits well for on-premise, it gives Fischer a head start for cloud-based deployments, having, for example, full multi-tenancy support as a logical design principle.

Strengths	Challenges
● SaaS delivery model as standard option ● No coding required, customization is done via configuration and graphical design components ● Well-defined user interfaces for quick-start deployments	● Only one US-based datacenter, which might not be sufficient for customers' needs ● Limited support for authentication mechanisms ● Limited out-of-the-box support for common Cloud services

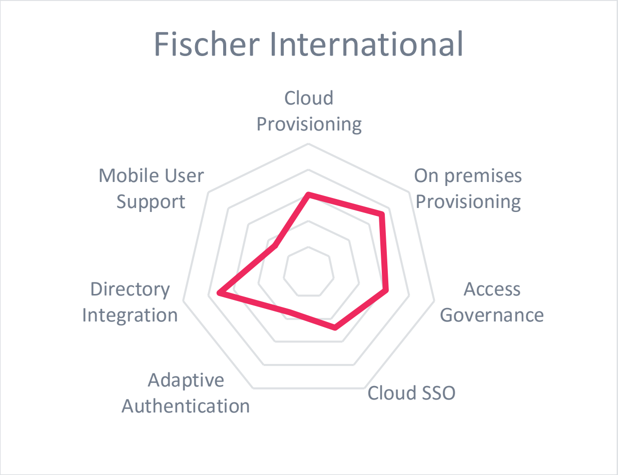
Table 11: Fischer International Identity major strengths and weaknesses

Their SaaS delivery model is supported by several MSPs, including Wipro as a global partner. However, for the Cloud offering, they are relying on Rackspace and a single US-based datacenter, which might be considered a shortcoming primarily for EU customers, but also in some other regions. Due to their SaaS-ready design approach, the clear focus is on providing a large set of features, well-defined standard configurations, and avoiding programming. There is no need for coding, but sometimes intensive configuration is needed. Besides that, there are graphical tools for designing user interfaces and workflows.

Fischer has a good strategy for integration, supporting both an ETL-based approach and a comprehensive set of REST APIs. Furthermore, connectors are fairly simple to create. Thus, even complex scenarios are in scope of this solution. The partner ecosystem of Fischer is still somewhat limited in size but growing and based on a few global, engaged partners.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 12: Fischer International Identity rating



Overall, Fischer provides an interesting approach to IDaaS B2E, supporting both on-premise and SaaS deployments. The approach might not suit the needs of every customer. On the other hand, customization is straightforward and the product focuses on avoiding coding at all. Compared to other vendors, the offering falls short in the breadth of support for authentication mechanisms and with its rather limited out-of-the-box support for connectivity to common Cloud services.

5.6 Hitachi ID Systems Identity and Access Management Suite

Hitachi ID Systems is another well-established player in the IAM market, providing a strong set of offerings in the on-premises market. These offerings are also available in a managed services model and thus can serve the IDaaS B2E requirements of customers. As with other offerings of that sort, Hitachi ID delivers more of an MSP model than a typical SaaS model, which might work out well for some customer scenarios.

Strengths	Challenges
● Overall strong feature set for Identity Provisioning and Access Governance ● Strong Access Governance and role management capabilities ● Good support for Adaptive Authentication and Identity Federation, including integrating MFA capabilities ● Proven solution with a good track record	● Limited number of pre-integrated SaaS services, but good support for enterprise-level services ● SaaS approach relies on AWS, but well-suited for many customer requirements ● Still a relatively small partner network on global scale

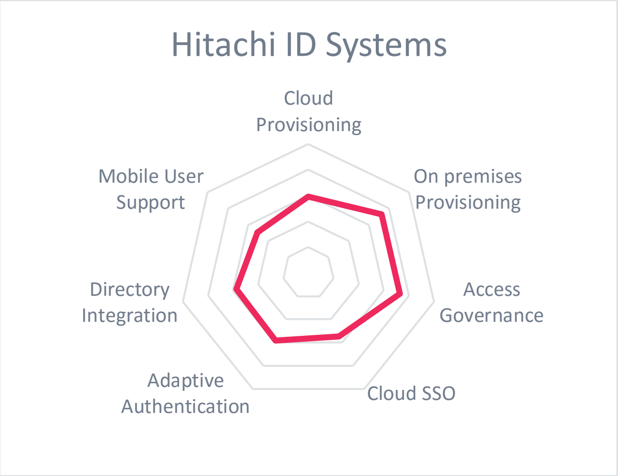
Table 13: Hitachi ID major strengths and weaknesses

As one of the products in the IAM market with a very long-standing history, the Hitachi ID Identity and Access Management Suite is feature-rich. It provides strong Identity Provisioning and Access Governance capabilities, various self-service interfaces, and strong capabilities for Adaptive Authentication including 2FA (Two Factor Authentication) plus support for Identity Federation. Thus, it is a comprehensive solution serving many of today's requirements.

While support for on-premise target environments is strong, the number of pre-integrated SaaS services is still not very large. This is one of the areas where Hitachi ID Systems might add functionality. However, they provide strong standards support and good support for enterprise-level services.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 14: Hitachi ID rating



While Hitachi ID provides a technically strong offering supporting a variety of capabilities, the solution is not one built from scratch as being multi-tenant. However, this deployment model will work well for many organizations looking for a strategic IDaaS B2E solution. Hitachi-ID counts amongst the providers that are worth being evaluated.

5.7 IBM Cloud Identity Service

IBM over the past years has moved from single-tenant, cloud-based deployments of existing IAM tools towards a full, multi-tenant solution that is positioned as 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	Challenges
● 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 15: IBM Cloud Identity Service major strengths and weaknesses

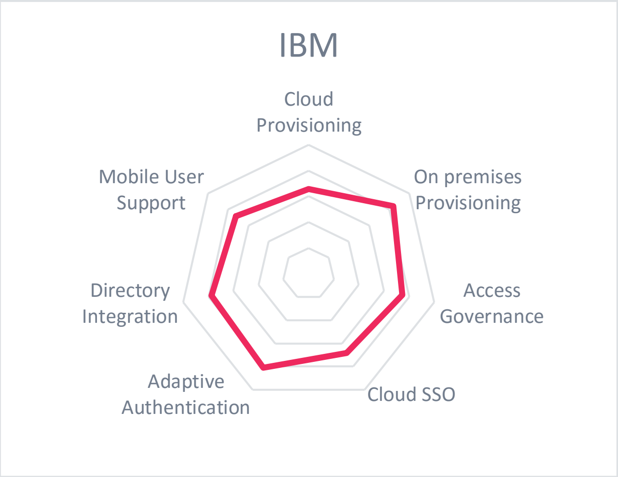
IBM provides a broad set of capabilities, covering the requirements for IDaaS B2E well. This includes tight integration with on-premise applications as well as Access Governance capabilities. However, IBM Cloud Identity Service also serves the IDaaS SSO requirements well, particularly for strategic deployments. 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, e.g., self-registration, profile management, and others. IBM also delivers workflow capabilities that allow for flexible customization of workflows such as self-registration.

Other feature areas such as auditing are 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	strong positive

Table 16: 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.

5.8 Ilantus Xpress IdaaS

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

Strengths	Challenges
● Good support for out-of-the-box integrations, in particular for enterprise-level cloud services, but also on-premise applications ● 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 17: Ilantus Xpress IdaaS major strengths and weaknesses

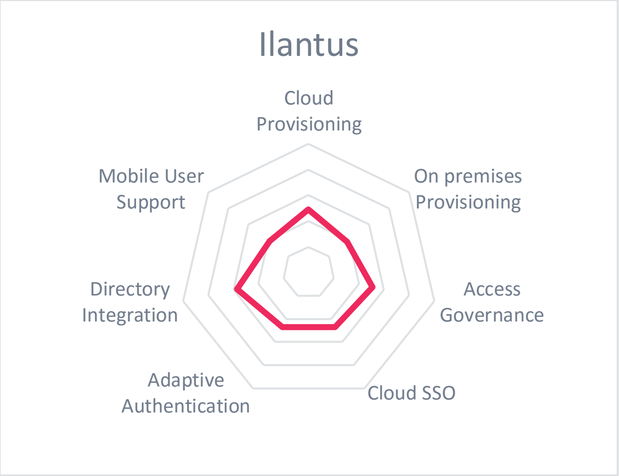
Ilantus provides a solution that covers a variety of aspects around IDaaS. For example, for the primary use cases of IDaaS SSO it delivers a variety of integrations to existing logins, beyond the commonly found IDaaS scope on integration with Microsoft Active Directory. It also delivers broad support 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 18: 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 is about enterprise-level SaaS services. With its capabilities, Ilantus is an interesting contender to the established players in the IDaaS market.

5.9 iSM Secu-Sys bi-cube

German software vendor iSM Secu-Sys is a small vendor that began in the on-premises IAM market. Over the past years, the company has invested in delivering its bi-cube product as a SaaS service, concentrating on adding specific capabilities for the IDaaS requirements, while keeping a clear focus on the IDaaS B2E market segment.

Strengths	Challenges
● Focused on cloud-based deployments out of German datacenters ● Strong Identity Provisioning and Access Governance capabilities ● Baseline strong authentication capabilities plus good integration to 3rd party providers ● Specific strength in solutions for Finance industry customers	● Lack of federation capabilities and broad out-of-the-box support for SaaS services ● Well thought-out but someone rigid concepts ● Very small vendor, focused on close customer relationships ● Small partner ecosystem, focus on Central European region

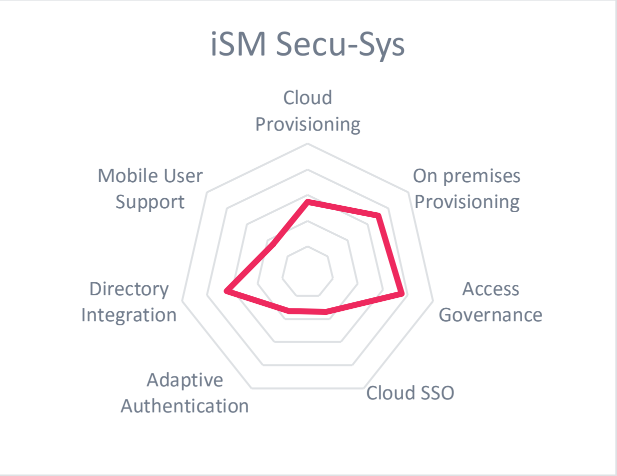
Table 19: iSM Secu-Sys bi-cube major strengths and weaknesses

The offering provides very strong capabilities in the core area of Identity Provisioning and Access Governance. iSM Secu-Sys has most of its customers in the Finance industry. Thus, its solution excels when it comes to Access Governance and Role Management. However, bi-cube now also provides a good set of features for strong authentication, plus integration into various 3rd party solutions.

While the features are well-positioned for the Finance Industry, the concepts in place might turn out to be too rigid for organizations from other industries. Furthermore, the solution lacks some of the capabilities most organizations will require for supporting the growing demand in integrating SaaS services. In particular, the lack of integrated Identity Federation capabilities might turn out to be an inhibitor for choosing bi-cube.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	positive

Table 20: iSM Secu-Sys bi-cube rating



While the deployment from German datacenters can be advantageous to EU-based customers, the size of the vendor and its small partner ecosystem might turn out to be a challenge for customers in other regions. Overall, iSM Secu-Sys bi-cube is an interesting offering, but has some functional gaps and might suffer from the fact of being provided by a small, regional vendor.

5.10 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	Challenges
● Strong integration back to existing on-premise IAM services ● Tight integration with Windows authentication ● Run from 14 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 (multi-instance)

Table 21: iWelcome major strengths and weaknesses

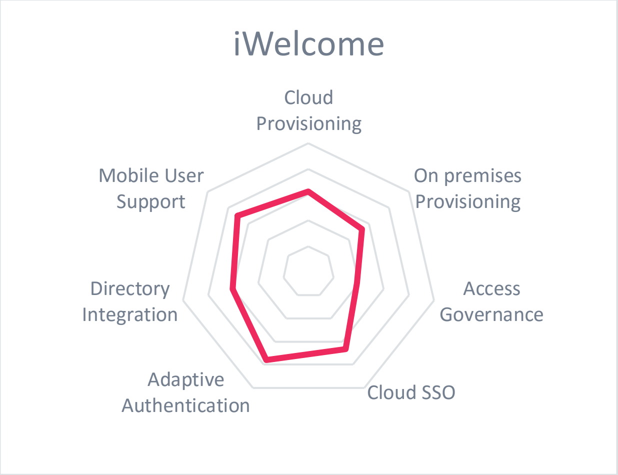
The approach taken by iWelcome allowed them to quickly start offering a service for Cloud User and Access Management, while also supporting integration of external users. In that area, they are leading-edge due to the variety of CIAM features offered, including excellent support for the upcoming EU GDPR 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 standards 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 22: 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 a number of specific strengths.

5.11 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.

Strengths	Challenges
● 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 B2E offering

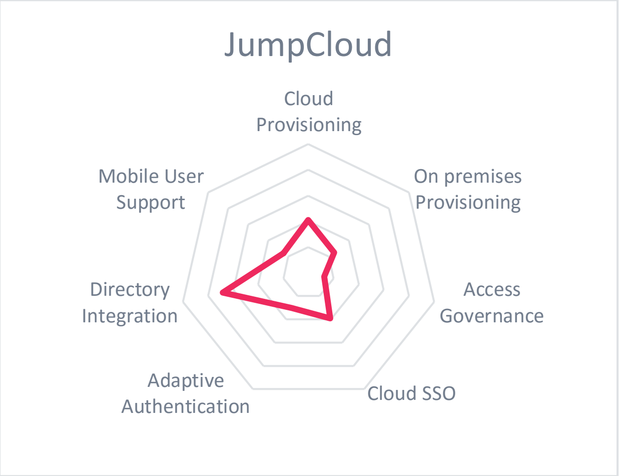
Table 23: JumpCloud major strengths and weaknesses

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, for example, a cloud-based replacement for existing LDAP directory services. 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 are their device management capabilities, which are rarely found in this market. This allows managing 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	weak
Integration	positive
Interoperability	neutral
Usability	neutral

Table 24: 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 B2E vendors lack their own cloud directory capabilities, but can only rely on on-premise services such as Microsoft Active Directory. JumpCloud can fill that gap, providing an extension to other offerings, but also has is place in use cases where the directory capabilities are the essential element, e.g. for SaaS providers themselves that need strong directory capabilities.

5.12 Memority

Memority was founded by French system integrator Arismore. With the acquisition of Arismore by Accenture Security, Memority has become part of that larger group. That gives Memority access to a global network of resources and the potential of expanding its still small market share significantly. Notably, Memority is one of the few offerings with a formal Microsoft Office365/Azure certification.

Strengths	Challenges
● Part of Accenture Security, providing global scale ● Good feature set for Identity Provisioning and Identity Federation ● Baseline Access Governance features ● Adaptive Authentication features available as add-on ● Support for both on-premise and cloud services	● Still low number of customers, but a number of large customers with global deployments ● Individual setup per tenant with extra fee, which however is a common model in that market segment ● 24*7 support not a standard

Table 25: Memority major strengths and weaknesses

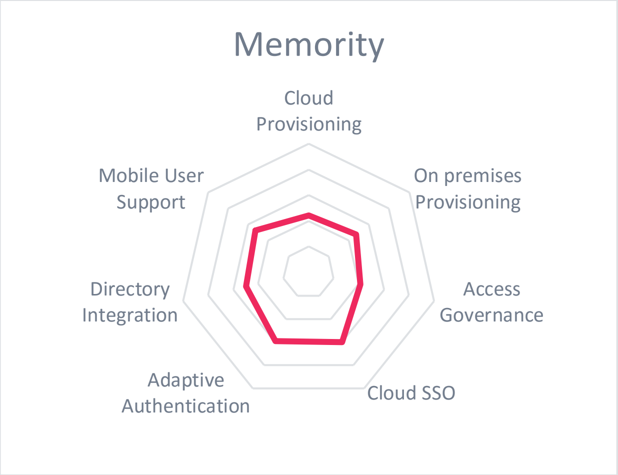
Memority is an IDaaS B2E solution constructed specifically for that purpose. It supports all major feature areas, from good Identity Provisioning and baseline Access Governance capabilities to Access Management and Single Sign-On to cloud services and to Adaptive Authentication. Based on that comprehensive set of capabilities, Memority can offer good support for common IDaaS B2E requirements.

This is especially true for the Adaptive Authentication capabilities, where major features such as support for FIDO Alliance standards, risk- and context-based authentication based on various features, and flexible integration of 3rd party authentication means are supported.

On the other hand, Memority explicitly relies on setup services per tenant, in addition to the pay-per-use model for the service. While such services are not uncommon for IDaaS B2E, together with the fact that 24*7 support is not offered as standard for the base subscription, there are apparently some gaps in the deployment approach chosen by Memority.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	positive
Usability	positive

Table 26: Memority rating



As part of Accenture Security and with EU-based and North American datacenters available, Memority is an interesting alternative to other vendors in the IDaaS B2E market. Based on the new ownership and the overall good set of capabilities, we see good potential for Memority to increase its role in the market.

5.13 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 the access of on-premise users to cloud services through integration with existing Active Directory infrastructures, and of supporting the emerging demand of managing identities and access of business partners and customers.

Strengths	Challenges
● 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 ● Limited support for non-web on-premise environments ● Lack of Access Governance capabilities

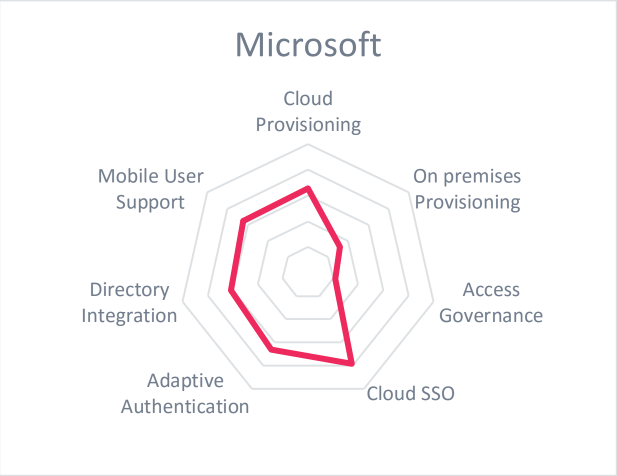
Table 27: Microsoft Azure Active Directory major strengths and weaknesses

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 few years, with several additional capabilities being on the roadmap. However, lack of Access Governance capabilities is a gap for IDaaS B2E.

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

Table 28: Microsoft Azure Active Directory rating



Overall, we see Microsoft Azure AD as a leading-edge offering when it comes to IDaaS, including IDaaS B2E, with their growing support for hybrid environments. 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.

5.14 Omada Identity Suite

Omada is another of the established IAM players that offer their standard offerings as an IDaaS B2E product as well. As with other vendors, this goes in line with some strengths, particular regarding the feature set for supporting on-premise environments, while it also bears some challenges such as a flexible and efficient deployment model for a growing number of tenants.

Strengths	Challenges
● Strong capabilities particular for Access Governance ● Well thought-out, modern user interface ● Good partner network particularly in Europe	● Limited number of own connectors, but generic connector framework ● No full multi-tenancy, but fully scripted deployment ● No federation support, lack in open standards support

Table 29: Omada Identity Suite major strengths and weaknesses

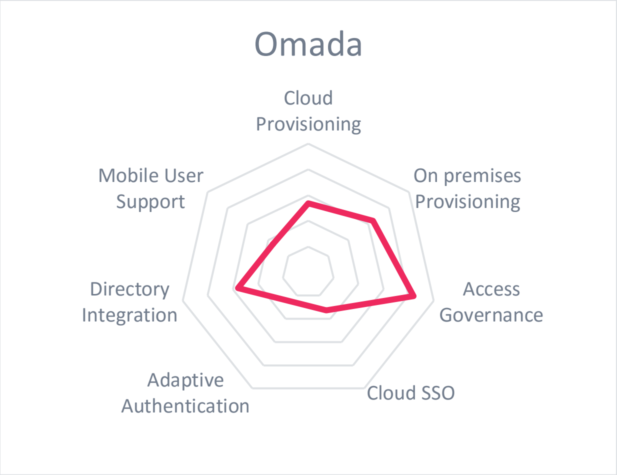
Omada has made a transition over the past several years from an Access Governance add-on for Microsoft Identity Manager towards a complete offering for Identity Provisioning and Access Governance. While Access Governance is a strength of Omada, the number of connectors offered is still somewhat limited, including a fairly low number of connectors for cloud services. However, Omada delivers an efficient connector framework for adding further connectors.

Furthermore, Omada as of now does not deliver Identity Federation capabilities, which are one of the important feature areas we expect to see in IDaaS B2E offerings. Omada has partners in that area. Thus, the primary use case of the offering is providing IAM services for on-premise environments as a managed service.

Notably, in addition to delivering its core product in an MSP/SaaS-style deployment model, Omada has a separate offering for "governance as a service" in place, targeted at rapidly available Access Governance services from the cloud.

Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	positive

Table 30: Omada Identity Suite rating



While Omada has made significant progress over the past few years, we still observe some major gaps when it comes to IDaaS. The offering suits certain use cases well, but is not yet a comprehensive IDaaS B2E offering. Thus, it needs to be carefully evaluated.

5.15 OneLogin

OneLogin is another vendor that started early into the IDaaS market, being originally focusing 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	Challenges
● 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

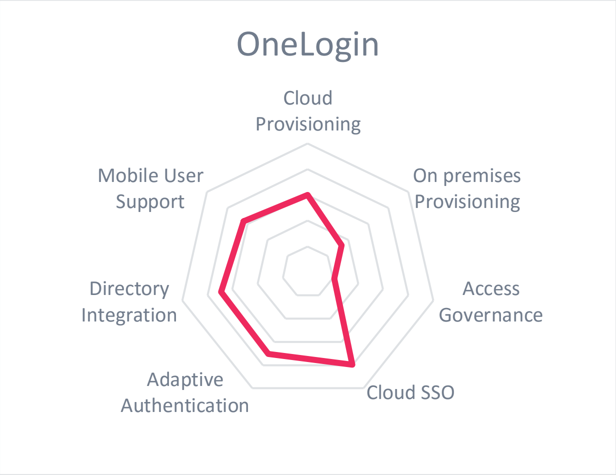
Table 31: OneLogin major strengths and weaknesses

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-facing 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 for 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	neutral
Integration	strong positive
Interoperability	positive
Usability	positive

Table 32: OneLogin rating



As with 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 and makes them a contender in the IDaaS B2E market.

[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.

5.16 OpenIAM

OpenIAM counts among the less known vendors in the IDaaS B2E market segment, taking a different approach than others. They started with an IAM offering deployed in an appliance form factor, which also can be run from the cloud, providing an IDaaS B2E offering. The solution consists of two distinct parts, the OpenIAM Identity Manager delivering Identity Provisioning and auditing features, and the OpenIAM Access Manager, which focuses on Identity Federation, Web Access Management, but also SOA Security.

Strengths	Challenges
● Strong Access Management feature set ● Good Identity Provisioning feature set ● Flexible deployment options, including SaaS deployment ● Well thought-out, modern architecture ● Integrated API Management features	● No fully multi-tenant cloud service ● Relatively small vendor with limited global scale, but growing partner ecosystem

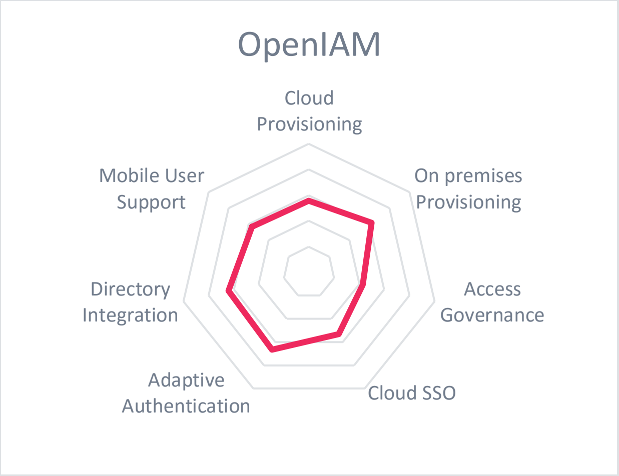
Table 33: OpenIAM major strengths and weaknesses

When looking at the breadth of feature areas covered, OpenIAM supports a very broad range. Beyond standard capabilities such as Identity Provisioning, delegated administration, and baseline Access Governance capabilities, there is, for example, support for XACML and thus Dynamic Authorization Management or SOA, and API security features.

The service-oriented architecture, based on micro services, makes OpenIAM a flexible offering with a high degree of scalability. It leverages various open source components, which are tightly integrated. The user interfaces are fair, but not leading-edge. However, they deliver support for different devices, from traditional desktops to mobile systems. The same holds true for the self-service interfaces provided out of the box.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 34: OpenIAM rating



In sum, OpenIAM is an interesting alternative for IDaaS B2E deployments when customers are looking for a broad set of capabilities they can run on the cloud service of their choice and which they want to adapt to specific requirements. For such use cases, OpenIAM counts into the IDaaS B2E market segment, while not being the typical provider within this market.

5.17 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 IdM’s 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	Challenges
● 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 ● No specific features for mobile management and security ● No leading-edge support for hybrid infrastructures

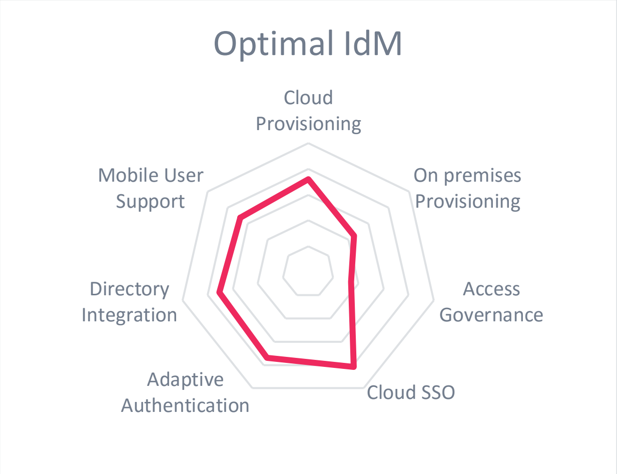
Table 35: Optimal IdM The OptimalCloud major strengths and weaknesses

Optimal IdM 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. For IDaaS B2E use cases, the feature set provided is somewhat limited, particularly with respect to on-premise integration. The offering provides many integrations to SaaS services. Integration to existing directory services is highly flexible, ranging from inbound federation e.g. for 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.

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

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

Table 36: Optimal IdM The OptimalCloud rating



In sum, Optimal IdM’s The OptimalCloud is an interesting offering for the IDaaS market, in particular for enterprise-level deployments. It provides an overall strong set of features, but with some gaps particularly for IDaaS B2E. Furthermore, Optimal IdM has developed a global partner ecosystem, including EMEA and APAC partners, which is essential for enterprise deployments.

5.18 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	Challenges
● Built from the ground up for IDaaS requirements and support of 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

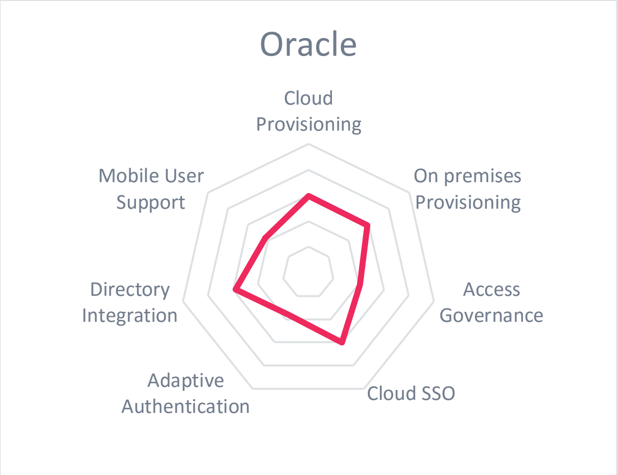
Table 37: Oracle Identity Cloud Service major strengths and weaknesses

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 SSO 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 38: 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.

5.19 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 in conjunction with the Identity Provisioning service is the solution, delivering authentication services to SaaS applications, but also provisioning capabilities from the cloud.

Strengths	Challenges
● 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 and on-premise applications ● Lack of Access Governance features ● Licensing model is usage-based, but capped ● Limited standards support beyond SAML 2.0

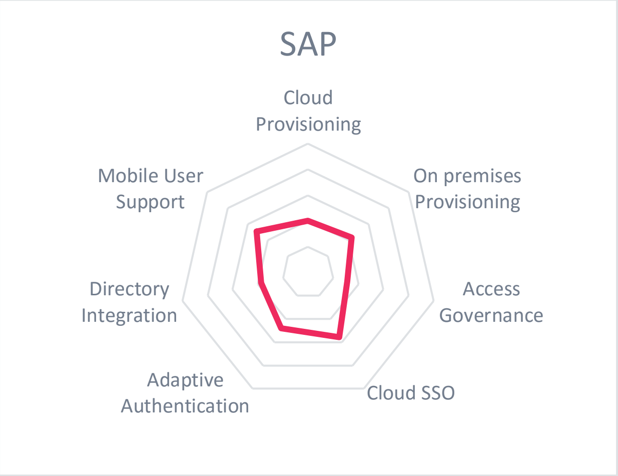
Table 39: SAP Cloud Platform Identity Authentication major strengths and challenges

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 both in the cloud and on-premise.

Security	strong positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 40: SAP Cloud Platform Identity Authentication rating



The SAP CP Identity services show great potential for the IDaaS 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 for integration of such solutions, by providing comprehensive out-of-the-box support, SAP might be well able to become a leading-edge IDaaS vendor.

5.20 SailPoint IdentityNow

IdentityNow is the IDaaS 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	Challenges
● 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, no own datacenters ● Lack of specific mobile management features

Table 41: SailPoint IdentityNow major strengths and weaknesses

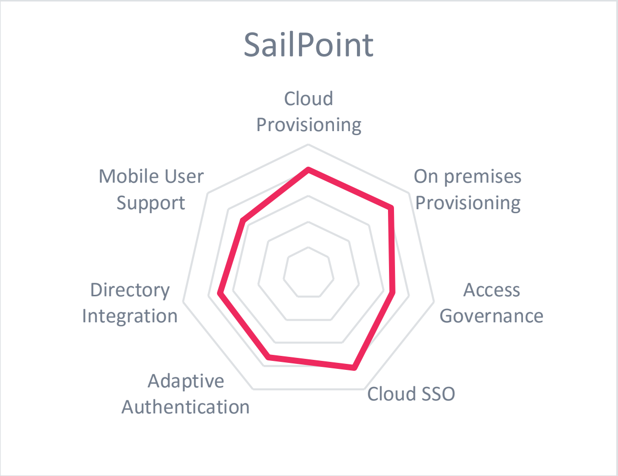
SailPoint IdentityNow consists of a number of feature areas: Single Sign-On, Password Management, Access Certification, User Provisioning, and Access Request Management. Furthermore, it delivers built-in Policy Management and Analysis. In contrast to pure-play IDaaS solutions, the service differs in providing Identity Provisioning and Access Governance capabilities. These are highly relevant 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”, in this case, 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	strong positive
Usability	strong positive

Table 42: 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 both the pure-play IDaaS SSO vendors and the IDaaS B2E vendors by building on existing on-premise solutions, which they have moved to the cloud.

5.21 Saviynt Cloud Access Governance and Intelligence

Saviynt is a vendor focused specifically on Access Governance and Intelligence as a service. However, they also provide strong integration into applications on premises and Identity Provisioning capabilities. This makes Saviynt Cloud Access Governance and Intelligence (CAGI) an interesting alternative in the IDaaS B2E market, but also a complementary offering which can add to other vendors offerings, including some of the IDaaS SSO offerings such as Okta.

Strengths	Challenges
● Strong Access Governance and Intelligence feature set ● Build from scratch as IDaaS solution ● Tight integration into a variety of enterprise-grade SaaS and on-premise services, delivering control of these environments ● Integrates with some IDaaS SSO services such as Okta	● Connectors for enterprise applications are priced separately ● Good but not outstanding support for on-premise applications, aside from enterprise services such as SAP

Table 43: Saviynt Cloud Access Governance and Intelligence major strengths and weaknesses

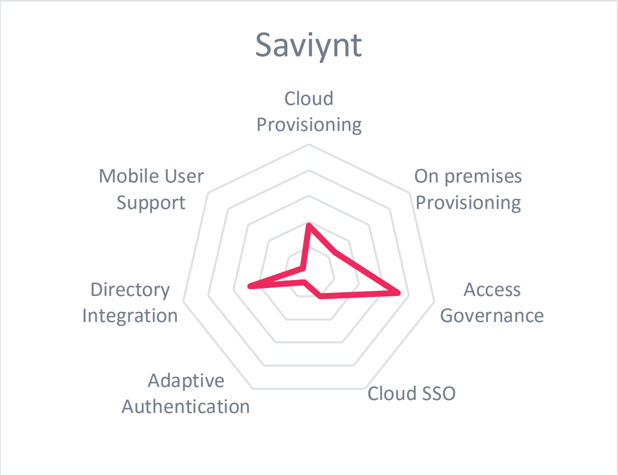
Saviynt started from the beginning as a vendor focusing on a gap many other solutions leave: Access Governance and Intelligence. This gap can be observed in both IDaaS SSO offerings, where Access Governance capabilities are very rare, and in the IDaaS B2E market, where several vendors do not provide advanced capabilities in this highly important area. However, Saviynt is more than a specialist vendor, providing a broad feature set right now.

In the area of Access Governance, Saviynt provides broad, advanced capabilities for reviewing access, classifying data, implementing and enforcing SoD (Segregation of Duties) rules, access risk analysis, and more. They deliver such services for several target environments such as Windows Azure and AWS, but also for enterprise applications such as SAP and the Oracle eBusiness Suite. Furthermore, they integrate with Okta, one of the leading IDaaS SSO solutions, to add Access Governance to this “interface” to other cloud services.

Security	positive
Functionality	neutral
Integration	neutral
Interoperability	neutral
Usability	positive

Table 44: Saviynt Cloud Access Governance and Intelligence rating

Savyint is an option as a standalone IDaaS B2E solution, but also can complement other services due to their outstanding Access Governance capabilities.



5.22 Simeio Identity as a Service

Simeio Solutions is a large system integrator in the IAM market. With their Identity as a Service offering, "powered by Simeio IIC", they provide their own SaaS offering for the IDaaS B2E market. The offering is based on COTS IAM products from various vendors with a well thought-out abstraction layer and a consistent UI. It runs either in one of Simeio's own datacenters (SOC certified) or on Amazon EC2.

Strengths	Challenges
● Broad number of pre-integrated SaaS services ● Good feature set for major IDaaS B2E capabilities ● Large number of customers and huge number of managed identities ● Identity interceptor allows flexible integration back to on-premise environments	● Mix of underlying software components, but abstracted by API layer and by a consistent UI ● More an MSP-style offering than a pure-play SaaS service, but providing

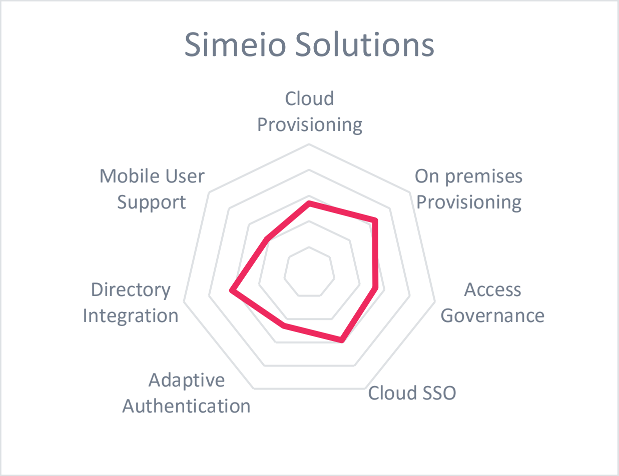
Table 45: Simeio Identity as a Service major strengths and weaknesses

Simeio can build on a long experience in implementing on-premise IAM solutions from various vendors. This gives them the expertise for creating their own IDaaS offering based on COTS software. They abstract these technologies through an API layer and a consistent UI, which remains stable even if underlying technology changes.

On the other hand, the approach chosen allows Simeio to offer a broad set of functionalities for customers, with a well-thought-out integration into on-premise environments through their Identity Interceptor. Thus, the approach chosen by Simeio should serve customers that make a strategic decision to go with Simeio and their COTS software suppliers.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	strong positive
Usability	positive

Table 46: Simeio Identity as a Service rating



While the functionality provided by Simeio Identity as a Service is broad, the dependency on the underlying software remains a challenge. Customers that decide to take this path in fact opt for an MSP service, instead of a multi-tenant IDaaS B2E solution in a traditional approach. However, they then get full support for customizing the IDaaS solutions to their needs, which is beneficial for many customers.

5.23 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 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. The main focus is on IDaaS SSO, but it might also serve as an entry-level offering to IDaaS B2E requirements.

Strengths	Challenges
● 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 47: Trustelem major strengths and weaknesses

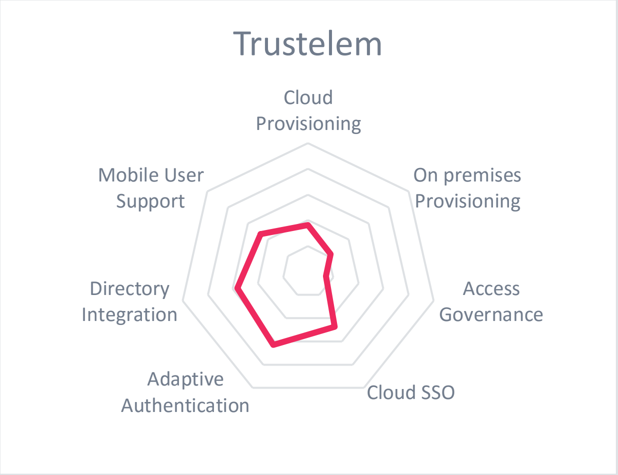
Trustelem, as of now, focuses on the essential building blocks of an IDaaS solution. It integrates with existing directory services such as Microsoft Active Directory and LDAP directories, but also Azure AD, it provides pass-through authentication of Microsoft Active Directory authentication, it allows 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 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 for strong authentication in a standardized way.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	positive
Usability	neutral

Table 48: 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 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.

5.24 UNIFY Solutions Identity Broker

UNIFY Solutions is a system integrator headquartered in Australia. They also provide a software solution that can be deployed as a SaaS offering, delivering partial IDaaS B2E capabilities. In fact, their Identity Broker (IB) is, as the name implies, more a broker component between on-premise directory services and cloud services than a full IDaaS B2E offering.

Strengths	Challenges
● Focused on specific Identity Broker capabilities ● Baseline Access Review capabilities ● Acceptable baseline support for open standards	● Overall very limited functionality, highly specialized offering ● IB configuration requires knowledge of target system data model - a data mapping GUI would assist ● A mature API Management and security environment in which to deploy IB is required ● No global partner ecosystem

Table 49: UNIFY Solutions Identity Broker major strengths and weaknesses

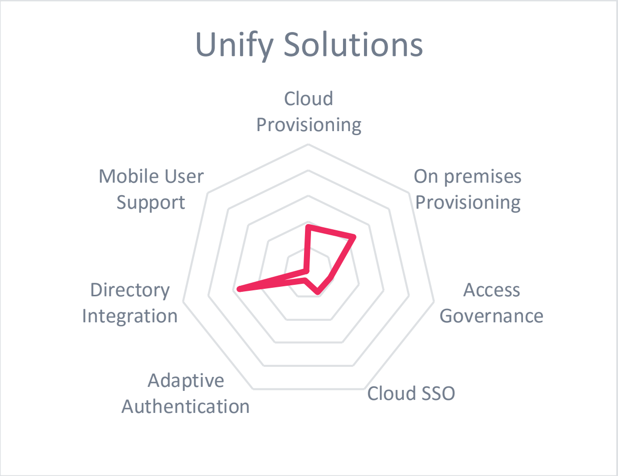
UNIFY Identity Broker V5 is a software application that acts as an identity provider service that transforms a request in one format to one that suits the requirements of the data repository or "source of truth" for identity data. It can be thought of as a "data pump" that can support the requirements of specific APIs exposed by modern-day applications.

It can be deployed in a variety of configurations, depending on customer needs. The application can be deployed to perform periodic batch updates of identity records, to synchronise to a source-of-truth for identity information or to query an identity provider service in real-time. In many cases IB is configured as a data store. This means that identity data will be synchronised to the IB database from which identity queries will be serviced with no call back to the source directory.

The Identity Broker product can be used to provide Identity as a Service (IDaaS) for Cloud-based installations.

Security	positive
Functionality	weak
Integration	weak
Interoperability	neutral
Usability	neutral

Table 50: UNIFY Solutions Identity Broker rating



With its offering, UNIFY Solutions is highly specialized but not a full IDaaS B2E provider. On the other hand, the approach chosen by UNIFY Solutions might serve certain specific customer requirements, particularly where an implementation requires bridging of regionally-based applications to a more fully featured IDaaS B2E vendor's product that does not have off the shelf connectivity for that application.

5.25 VMware Identity Manager

VMware is still primarily perceived as vendor of virtualization solutions. However, with the acquisition of AirWatch in 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 B2E segment.

Strengths	Challenges
● 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 51: VMware Identity Manager major strengths and weaknesses

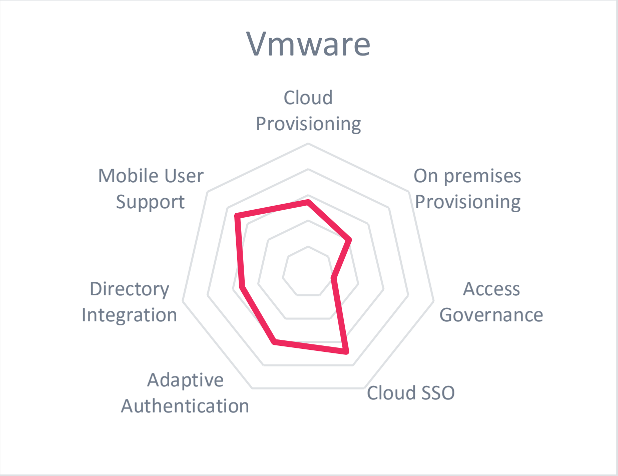
With their Identity Manager offering, VMware build on securing both the device –via AirWatch technology – and the user – with additional identity and SSO services. The solution seamlessly integrates with VMware WorkspaceOne and provides a user experience based on the user's identity and context. This is combined with broad support for a variety of application delivery models, providing seamless, secure access with SSO to these applications, including integration with legacy applications through the Unified Access Gateway.

With its integration of Mobile Security solutions, an application catalog, plus 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 that provided by many of the other players in this market segment.

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 52: VMware Identity Manager rating



Despite several features still lacking, VMware Identity Manager is 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

Aside from 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 for these vendors. Notably, several vendors in the broader IDaaS market that are targeting primarily the IDaaS SSO functionality are covered in the KuppingerCole Leadership Compass on IDaaS SSO.

6.1 Atos

Atos delivers its on-premise IAM solutions, now part of the Evidian product portfolio, as MSP offerings for their customers. While they do not yet provide a full SaaS offering, this might be an option for certain customers.

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 Memority

Memority was founded by French system integrator Arismore. With the acquisition of Arismore by Accenture Security, Memority has become part of that larger group. That gives Memority access to a global network of resources and the potential of expanding its still small market share significantly in future.

Memority is an IDaaS B2E solution constructed specifically for that purpose. It supports all major feature areas, from Identity Provisioning to Access Management and Single Sign-On to cloud services and to Adaptive Authentication. Based on that comprehensive set of capabilities, Memority can offer good support for common IDaaS B2E requirements.

This is especially true for the Adaptive Authentication capabilities, where major features such as support for FIDO Alliance standards, risk- and context-based authentication based on various features, and flexible integration of 3rd party authentication means are supported.

6.4 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.

6.5 Okta

Okta, being a leading vendor in the IDaaS B2C space, might also be considered an option for IDaaS B2E use cases, particularly due to their strong API offering which allows for flexible integration and customization. This is particularly valuable in scenarios where CIAM (Consumer IAM) solutions are in scope, which commonly require a higher level of customization.

6.6 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, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, as well as 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.

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.

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

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.

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.

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

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 B2E, we look at the following seven areas:

Cloud Provisioning — 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.

On-premise Provisioning — Provisioning capabilities, back to on-premise applications.

Access Governance — Integrated Access Governance capabilities, including Access Review, Role Management, SoD (Segregation of Duties) controls, and others.

Cloud SSO — Breadth of SSO functionality for cloud services, in particular, the number of connectors and the support for enterprise-grade SaaS services.

Adaptive Authentication — Flexibility and functionality for adaptive authentication, including support for a variety of authenticators and flexible, risk- and context-based authentication.

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 B2E use cases are still managed.

Mobile User 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.

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

All conclusions, recommendations and predictions in this document represent KuppingerCole´s initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice.

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