kuppingercole
ANALYSTS

KuppingerCole Report

LEADERSHIP COMPASS

by **Martin Kuppinger** November 2019

Identity as a Service (IDaaS) - IGA

An emerging market, IDaaS IGA is largely characterized by cloud-based delivery of Identity Provisioning and Access Governance capabilities for business irrespective of the application and service delivery models. Improved time-to-value proposition prioritizes adoption of IDaaS for traditional IGA use cases, helping IDaaS IGA to increasingly become the preferred choice of customers for IAM purchases globally. This Leadership Compass discusses the market direction and provides a detailed evaluation of market players to offer necessary guidance for IAM and security leaders to make informed decisions.

by **Martin Kuppinger**
mk@kuppingercole.com
November 2019

Leadership Compass
Identity as a Service ((IDaaS) - IGA
By KuppingerCole

Content

Content of Tables

Content of Figures

Related Research

Executive View: Ilantus Compact Identity - 80052

Executive View: Ilantus IDaaS Next - 70252

Executive View: IBM Security Access Manager (ISAM) - 79066

Executive View: IBM Security Identity Governance and Intelligence - 71113

Executive View: IBM Cloud Identity - 79065

Executive View: Micro Focus Data Protector - 80193

Executive View: EmpowerID - 70894

Executive View: Simeio IAM for SMB - 79071

Executive View: Microsoft Azure Information Protection - 72540

Executive View: Microsoft Azure Stack - 72592

Executive View: Oracle Data Safe - 80076

Executive View: Oracle Identity Cloud Service - 80156

Executive View: Saviynt Identity Governance and Administration (IGA) - 70370

Leadership Compass: Access Governance & Intelligence - 71145

Leadership Compass: Privileged Access Management - 79014

Leadership Compass: Identity Governance & Administration - 71135

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

Leadership Compass: CIAM Platforms - 79059

Leadership Compass: Database and Big Data Security - 79015

Leadership Compass: Access Management and Federation - 71147

Leadership Compass: Consumer Authentication - 80061

Buyer's Guide: Identity-as-a-Service (IDaaS) - 71526

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 (IDaaS) with a focus on IGA (Identity Governance and Administration, i.e. Identity Provisioning and Access Governance) technologies. IDaaS IGA, as the market is termed, has observed a significant growth in terms of new IAM (Identity and Access Management) purchases and is emerging as one of the fastest-growing markets of IAM characterized by cloud-based delivery of traditional IAM services.

The overall IDaaS market, driven largely by web-centric use-cases in its early days, now offers full-fledged delivery of IAM capabilities irrespective of application delivery models. The significant growth of the IDaaS market can be attributed to the ever-increasing demand of organizations to achieve better time-to-value proposition over on-premises IAM deployments and to extend IAM capabilities to meet the security requirements of growing SaaS portfolio.

1.1 Market Segment

IDaaS is a growing market segment of IAM characterized by delivery of traditional IAM services in an as-a-service model, with immediate to at least very rapid deployment and standardized capabilities, in contrast to individual implementations per customer. The market, driven largely by cloud-centric use-cases in its early days, now offers full-fledged delivery of IAM capabilities irrespective of application delivery models. The IDaaS market has registered significant growth over the last few years primarily driven by the need of organizations to:

   a)   Achieve better time-to-value proposition over on-premises IAM deployments

   b)   Extend IAM capabilities to meet the security requirements of growing SaaS portfolio

   c)   Adopt global IAM standards and practices with access to industry expertise

   d)   Reduce internal IAM costs and efforts to keep up with the market trends

   e)   Limit internal IAM failures in project delivery and ongoing operations

IDaaS vendors have originated from distinct backgrounds and therefore their abilities to support the primary IDaaS use-cases vary significantly. Most of the IDaaS vendors come from different backgrounds including:

   1.   Access Management vendors that offered broader IAM capabilities required for large IAM implementations but could not easily extend these functions to support rapidly emerging cloud and consumer access use-cases.

   2.   IGA (Identity Governance and Administration) vendors that traditionally offered support for identity administration and access governance on-premises but neither could extend these capabilities to applications in the cloud, nor could support access management beyond basic authentication and authorization

3. Traditional SSO (Single Sign-On) vendors that have evolved over time to support web and cloud access use-cases but are deficient on common Identity Governance and Administration (IGA) functions required by most organizations for basic IAM implementation

The IDaaS market consolidates Access Management functions with IGA and Access Governance capabilities thrown in – all delivered and managed as a service. Today, all IDaaS vendors predominantly deliver a cloud-based service in a multitenant or dedicatedly hosted fashion to serve the common IAM requirements of an organization's hybrid IT environment. The common IAM capabilities served by most IDaaS vendors can be grouped largely in three categories:

IDENTITY ADMINISTRATION	ACCESS MANAGEMENT	ACCESS GOVERNANCE
✔ Ready, Cloud-native provisioning connectors ✔ Automated User Provisioning ✔ Common Directory Sync ✔ Self-Service Profile and Password Management	✔ Consistent Authentication ✔ Common Password ✔ Single Sign-On ✔ Federation, Social Identity Integration	✔ Centralized Role Management ✔ Common Access Reporting ✔ Common Access Certification

Figure 1: IDaaS Capability Matrix

Identity Administration: This represents the group of capabilities required by organizations to administer identity lifecycle events including provision/ de-provision of user accounts, maintaining identity repository, managing access entitlements and synchronization of user attributes across the heterogeneous IT environment. A self-service user interface allows for requesting access, profile management, password reset, and synchronization. Configurable connectors, either cloud-native or based on gateways back to on premises environments, offer automated user provisioning to both on-premises as well as SaaS applications. Other common identity administration capabilities include administrative web interface, batch import interface, delegated administration, SPML, and SCIM support.

Access Management: This refers to the group of capabilities targeted at supporting access management requirements of organizations ranging from authentication, authorization, single sign-on and identity federation for both on-premises and SaaS applications delivered as a cloud service. The underlying support for industry standards such as SAML, OAuth and OpenID Connect can vary but are largely present in most IDaaS offerings. API security and web access management gateways are fast becoming a differentiator for IDaaS vendors looking to offer competitive access management capabilities and so is social identity integration – which now represents a basic qualifier for consumer access use-cases.

Access Governance: Access governance represents the group of capabilities that are least mature and still frequently absent from the portfolio of IDaaS vendors, partly due to architectural limitations and partly due to ownership issues. While many organizations still prefer to keep access governance on-premises for better control and auditing purposes, several others are moving it to the cloud for ease of integration and better time to value as their SaaS portfolio continues to grow. IDaaS vendors may have some serious limitations in how they could support integration with legacy on-prem systems for common access governance capabilities such as auditing and reporting, and so it is important for IAM leaders to ensure they assess their access governance requirements aligned with their IAM vision before starting to evaluate IDaaS vendors for their access governance capabilities.

Generally speaking, supporting hybrid IT environments is amongst the main challenges for IDaaS, across all areas. Connecting back to legacy web applications is more challenging than with most on-premise solutions, and Identity Provisioning as well. This needs to be kept in mind and carefully considered during choosing an IAM solution. The strength and weaknesses of IDaaS solutions in connecting back to on-premise environments are an important factor throughout our evaluation in this Leadership Compass.

As the IDaaS market continues to evolve, its adoption is inhibited by several factors including the concerns of data residency, dependency on providers internal security controls and the ability to address scenarios that require extensive customizations to address organization's internal process complexity and where organizations believe these could be better solved with on-premises IGA or access governance product deployments. However, we observe a clear trend to shifting also more complex use cases such as access governance to IDaaS.

In the later parts of this document, we also discuss the evaluation criteria important for IAM leaders to help decide whether they should move to an IDaaS platform for their IAM requirements or a conventional on-prem IAM deployment should suffice their IAM requirements in the short to midterm.

Depending on the key focus, architectural type and product origin, which affect their overall ability to support IDaaS functions, most IDaaS vendors can be classified in two major categories - either as Access Management or IGA focussed IDaaS vendors:

1. IDaaS Access Management (IDaaS AM)

There are primarily 2 types of AM focussed IDaaS vendors:

The first type is the traditional SSO vendors that progressed overtime as WAM vendors to mostly address web-centric use-cases along with identity federation but originally lacked the ability to address IAM requirements for cloud-based infrastructure and applications. Over the last few years, these vendors have made significant changes to their product architecture to make them cloud-ready, however, there remain certain limitations in addressing cloud AM requirements.

The second category of IDaaS AM vendors are the vendors that are born in the cloud to primarily manage access management requirements of SaaS and IaaS applications but have architectural limitations in how these could be easily extended to address access management for on-prem applications.

2. IDaaS Identity Governance and Administration (IDaaS IGA)

The IGA focused IDaaS vendors are the ones that have traditionally been offering identity administration capabilities including identity provisioning, lifecycle management and access governance across on-premises IT applications and systems. The key focus of these vendors on managing user identities in an increasingly complex IT environment combined with the demand and adoption trends of identity-centric solutions in the market has led these vendors to focus lesser and lesser on building access management capabilities. The move to the cloud, however, required them to support basic access management functions, in addition, to be able to support the delivery of all IGA capabilities to compete with the new IDaaS entrants. The depth of IGA functions delivered by these vendors in a cloud-based delivery model to support a hybrid IT environment not only remains questionable due to the technological limitations but also due to the consumption archetypes of on-premises IT applications and systems.

The IDaaS market continues to evolve with a significant push from organizations looking to adopt cloud-based delivery of security services including IAM. With IDaaS vendors slowly bridging on the gap with traditional on-premises IAM software in terms of depth of functionalities, particularly IGA, they present a strong alternative for organizations to replace existing on-premises IAM deployments.

Besides replacing traditional on-premises deployments for workforce IAM, IDaaS has evolved as a strong enabler of CIAM offering the required availability and scalability. With IDaaS starting to dominate new IAM purchases for most use-cases across the industry verticals, traditional IAM vendors are gearing up to deliver more cohesive IDaaS capabilities as part of their security services, including tighter integrations with Cloud Access Security Broker (CASB), Enterprise Mobility Management (EMM) and User Behavior Analytics (UBA).

IDaaS is only delivered as SaaS, hosted and managed by the IDaaS vendor itself. Vendors that use the on-premises software provided by other vendors to offer hosted and managed IAM services are not considered IDaaS vendors. Mostly combined in separate service bundles based on adoption and usage trends, most services are priced per managed identity or active users per month. Some functions such as user authentication or fraud detection can be charged on per transaction basis depending on the function's delivery and consumption.

The use cases for IDaaS technology adoption and their primary characteristics as observed by the industry are listed below:

- Web Access Management - Many organizations have the need to deliver basic authentication and authorization for the variety of internal web applications they have across their IT environment. IDaaS offers basic authentication and session management capabilities including single sign-on, coarse-grained authorization and identity federation required by these organizations to meet the most common web access management demands.

- Hybrid Access Management - Many organizations today have an urgent need to extend internal access management policies to the range of SaaS and IaaS platforms being integrated into their IT application portfolio. IDaaS can provide a seamless extension of on-premises IAM capabilities to the applications and infrastructure in the cloud in an effective and secure manner. There are, however, limitations in how they can support internal legacy IT systems versus SaaS applications.

- Workforce IAM - With most traditional IAM deployments suffering from internal inefficiencies, staffing, and budgeting concerns, IDaaS promises a flexible approach for organizations looking to on-board a workforce IAM program to deliver better time to value and agility. With IDaaS commonly offering capabilities across identity administration, access management and access governance, more advanced features such as access certification, role lifecycle management, SOD controls management etc. may not be adequately supported or entirely absent.

- Consumer IAM - IDaaS delivery model with its significant business value in terms of better flexibility and time to value has become a strong enabler of CIAM – offering the required scalability and availability. Most IDaaS vendors are aggressively building on or acquiring capabilities to better support CIAM use-cases, for eg., Okta acquired Stormpath and Ping Identity acquired UnboudID to strengthen their CIAM features. Most IDaaS vendors today support capabilities required by organizations to support CIAM programs including social identity integration, progressive customer profiling, fraud and risk intelligence as well as identity analytics.

There may be more use cases that are driven by the organization and business-specific access management requirements; however, most will fit well into one of these categories.

1.2   Market Direction

IDaaS IGA offers a springboard for organizations to start using foundational IAM elements delivered from the cloud and move rest of the IAM functions as they find it appropriate and at a pace that matches the organizational security maturity and cloud strategy. The IDaaS market, with its ease of adoption and cloud-native integrations, is slowly overtaking the on-premises IAM market.

IDaaS IGA market continuing on a growth spree allows the following technology trends to speed up the adoption by aligning them to match better with the organization's IAM priorities that security and IAM leaders must take note of. The IDaaS market continues to evolve with a significant push from organizations looking to adopt cloud-based delivery of security services including IAM. With IDaaS vendors slowly bridging on the gap with traditional on-premises IAM software in terms of depth of functionalities, particularly IGA, they present a strong alternative for organizations to replace existing on-premises IAM deployments.

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. These 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.

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. Factually, the need for multi-tenancy appears to be disappearing with modern software architectures and deployment models. Container-based deployment allow for quickly bringing up new instances, and the underlying microservice architectures simplify updates across tenants, specifically by segregating customizations from the standard. Thus, 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.

Specifically to IDaaS IGA, we are observing more vendors providing such capabilities, either focused on specific use cases such as Access Governance and, in particular, Access Analytics and Access Review, or by delivering a more comprehensive set of IGA capabilities. However, the IDaaS IGA market is still in a relatively early stage of maturity. Currently, most of the leading solutions have been ported from traditional on premises deployments by moving them to container-based deployments and gradually migrating them to more modern, microservices-based software architectures. There are few cloud-born offerings available for now, but we expect to see them evolving. Specifically, we observe that leading IDaaS AM vendors are starting to add more advanced IGA features to their offerings.

In some cases, vendors build on a mix of new IDaaS IGA offerings that have their strength in connecting to cloud services, while they rely on existing on premises IGA solutions to connect back to hybrid environments. We don't consider this being a favourable solution, unless the on premises component is delivered in a "black box" approach as a single packaged deployment and fully managed from the IDaaS IGA service. Otherwise, customers have to deal with two separate solutions, adding massive complexity to their environments.

1.3   Required capabilities

For the market segment of IDaaS IGA, on a high level, we expect the vendors to support the following set of features and capabilities:

Capability	Description
Directory Services & Integration	Support existing Directory Services, both on premises and in the cloud, as both source and target of identity information.
Flexible User Onboarding	Integration to HR/HCM systems and other sources for identity information and support for mapping identity data from different sources.
Breadth of Connectors	Connectors to a broad variety of target systems, both cloud services and on premises applications and systems. Provisioning of users to cloud services, beyond just SSO, is considered a key capability.
Depth of Connectors	For certain target systems, connectors must support deep integration, beyond just creating accounts and simple group/role mapping. This specifically affects business applications with complex entitlement structures such as SAP.
Provisioning Flows	The flow of information from target to source system shall be flexibly configurable.
Workflow Capabilities	Flexible workflows e.g. for access requests and approvals that can be configured to the specific customer's demand, without coding. Furthermore, we expect pre-configured workflows/Identity Management processes to be part of such solutions, for simplifying deployments of IDaaS IGA solutions.
User Self Services	Pre-configured user self-services e.g. for password management or access requests. Again, required customization should be feasible by configuration, not coding.
Mobile Interfaces	Support for access of key functionality such as access approval and reviews via modern, mobile UIs.
Access Request Management	Access requests are a key capability of every IDaaS IGA solution, requiring users to be able to identify the assets (applications, services,…) they need access to and the specific entitlements. Access Request Management includes flexible approval workflows.

Access Reviews	For Access Reviews, we observe a need in the market to keep these lean and efficient. Beyond regular review campaigns, solutions should also support risk-based and other types of reviews that reduce the workload for reviewers and focus on high-risk items.
Access Analytics	Additionally, analytics that identifies such high-risk users and entitlements is a feature we like to see in IDaaS IGA solutions.
SoD Management	SoD (Segregation of Duties) management is another important capability. As of not, it is not a commonly found feature in IDaaS IGA, but we expect solutions to deliver at least a good baseline capability in this area.
Flexible Entitlement Management	Managing entitlement constructs such as groups and roles should be supported with a good level of flexibility, i.e. not requesting customers to e.g. mandatorily use a multi-tiered role models. Multiple models can ideally co-exist for separate use cases.
Baseline IDaaS AM Capabilities	While the focus of IDaaS IGA is on Identity Provisioning and Access Governance, solutions commonly deliver at least some baseline Access Management capabilities, which allow customers to deliver a core IDaaS based on a single offering.
Central Administrative UI	All administrative features should be integrated into a single UI. This specifically also includes management of components that can or must be installed on premises.
Strong set of APIs	All features should be exposed via APIs, allowing flexible integration and customization of capabilities wherever required.
Hybrid Support	Supporting the hybrid environments most businesses still have today is a key capability. IDaaS IGA must not be limited to SaaS only target environments to deliver on its promise.
Modern Architecture	Finally, the architecture of IDaaS IGA should be based on a well-thought-out microservices architecture and delivery in container-based deployments or fully multi-tenant public cloud environments. However, the latter might impose (perceived, not necessarily real) challenges regarding regulatory compliance and confidentiality. From our perspective, analysing and validating the software architecture of solutions is an essential criteria in any tools choice today, because of the significant impact software architecture has on customization, integration, but also the ability of the vendor for further and rapidly developing its solutions.

Table 1: Capability matrix for IDaaS IGA, showing the most relevant high-level capabilities we expect to see in this group of products.

Besides these technical capabilities, we evaluate participating IDaaS IGA vendors on the breadth of supported IDaaS capabilities, operational requirements such as support for high availability and disaster recovery, strategic focus, partner ecosystem, quality of technical support and the strength of market understanding and product roadmap. Finally, we also assess their ability to deliver a reliable and scalable IDaaS IGA service with desired security, UX and TCO benefits.

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

When looking at the Overall Leadership in LC IDaaS IGA, we see several vendors that have achieved this rating. The number is still comparatively low, when looking at other Leadership Compass documents, which is due to the still relatively young and immature market segment.

Figure 2: The Overall Leadership rating for the IDaaS IGA market segment

In this rating we see Microsoft ahead of the other vendors, which is primarily due to their strong market presence with Microsoft Azure Active Directory. While they are still several functional gaps, Microsoft benefits from its global presence and the very large number of customers. Following Microsoft, we see Saviynt and Microsoft head-to-head, with Saviynt delivering the more feature-rich solution, while IBM as Microsoft benefits from its overall market position and global ecosystem. SailPoint (with the IdentityNow offering targeted primarily at the mid-market being in scope of this Leadership Compass) and EmpowerID are two more vendors that have achieved a Leader position in Overall Leadership. Finally, there is Okta,

which beyond the leading-edge Access Management capabilities also started delivering Lifecycle Management features. Okta, as some others, benefits from its strong position in Market Leadership.

Following these vendors, we find a group of challengers in the Overall Leadership rating, which include (in alphabetical order) Avatier, Fischer International, Ilantus, Micro Focus, SAP, and Simeio Solutions. All deliver interesting yet very different solutions in the IDaaS IGA space. Micro Focus builds primarily on a "cloudified" deployment of former on premises capabilities and SAP focus on the Access Governance capabilities with only baseline Identity Lifecycle Management, while others provide rather full-fledged solutions.

Other challenges include Tools4ever, E-TRUST, and Accenture Memory. Tools4ever is primarily targeted medium-sized business and the mid-market and thus does not deliver the same breadth in integration and Access Governance capabilities as some others do. E-TRUST, based in Brazil, provides an interesting alternative but e.g. yet lacks a global ecosystem. Accenture Memory also has a still small customer base, but provides an interesting alternative as an IDaaS solution covering both IGA and AM requirements.

Overall Leaders are (in alphabetical order):

- EmpowerID
- IBM
- Microsoft
- Okta

- SailPoint
- Saviynt

2.2   Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services. **Product Leadership**, or in this case factually Service Leadership, is where we examine the functional strength and completeness of products/services.

Figure 3: Product Leaders in the IDaaS IGA market segment

Here, Saviynt takes the leadership, with a comprehensive offering focused on IGA capabilities that is feature-rich and competitive to the leading-edge on premises solutions in IGA. Following them, we find a group of other companies that have entered the Leader's segment. EmpowerID and SailPoint are slightly ahead of IBM, all providing a good set of IGA capabilities.

As noted already, the rating for SailPoint applies to their cloud services IdentityNow, that has less depth and breadth of features than their flagship product IdentityIQ, which is only available in on premises and MSP deployments, thus not meeting the inclusion criteria of this Leadership Compass. While IBM delivers a good set of capabilities, certain more complex features specifically for on premises environments will require the integrated use of their ISIGI offering.

After this group of vendors, we find (in alphabetical order) Avatier, Fischer International, Ilantus, and Microsoft. Both Avatier and Fischer International deliver broad IAM capabilities that are available in different deployment models. Ilantus is demonstrating a broad feature set that is constantly expanded and already delivering to a significant range of IGA requirements. Microsoft and its Azure Active Directory currently lack strength in supporting on premises environments and deliver only baseline Access Governance capabilities. However, Microsoft rates strong in baseline capabilities and other areas and is quickly expanding the specific IGA capabilities.

In the Challenger section, we see (in alphabetical order) Micro Focus, Okta, and Simeio Solutions on top. All these vendors are close to becoming rated as Leaders. As partially already mentioned in the section on Overall Leadership, these three vendors have very different entries to the IDaaS IGA market, with Simeio Solutions initially delivering on premises IGA as managed service and now providing an own IDaaS service.

Further Challengers include (again in alphabetical order) Accenture Memory, E-TRUST, SAP, and Tools4ever. While SAP focuses on a subset of capabilities and Tools4ever is targeting the mid-market – with a very good feature set for these group of customers – the other two vendors also have a good feature set, yet lacking the full breadth and depth of others.

Product Leaders (in alphabetical order):

- Avatier
- EmpowerID
- Fischer International
- IBM
- Ilantus
- Microsoft
- SailPoint
- Saviynt

2.3 Innovation Leadership

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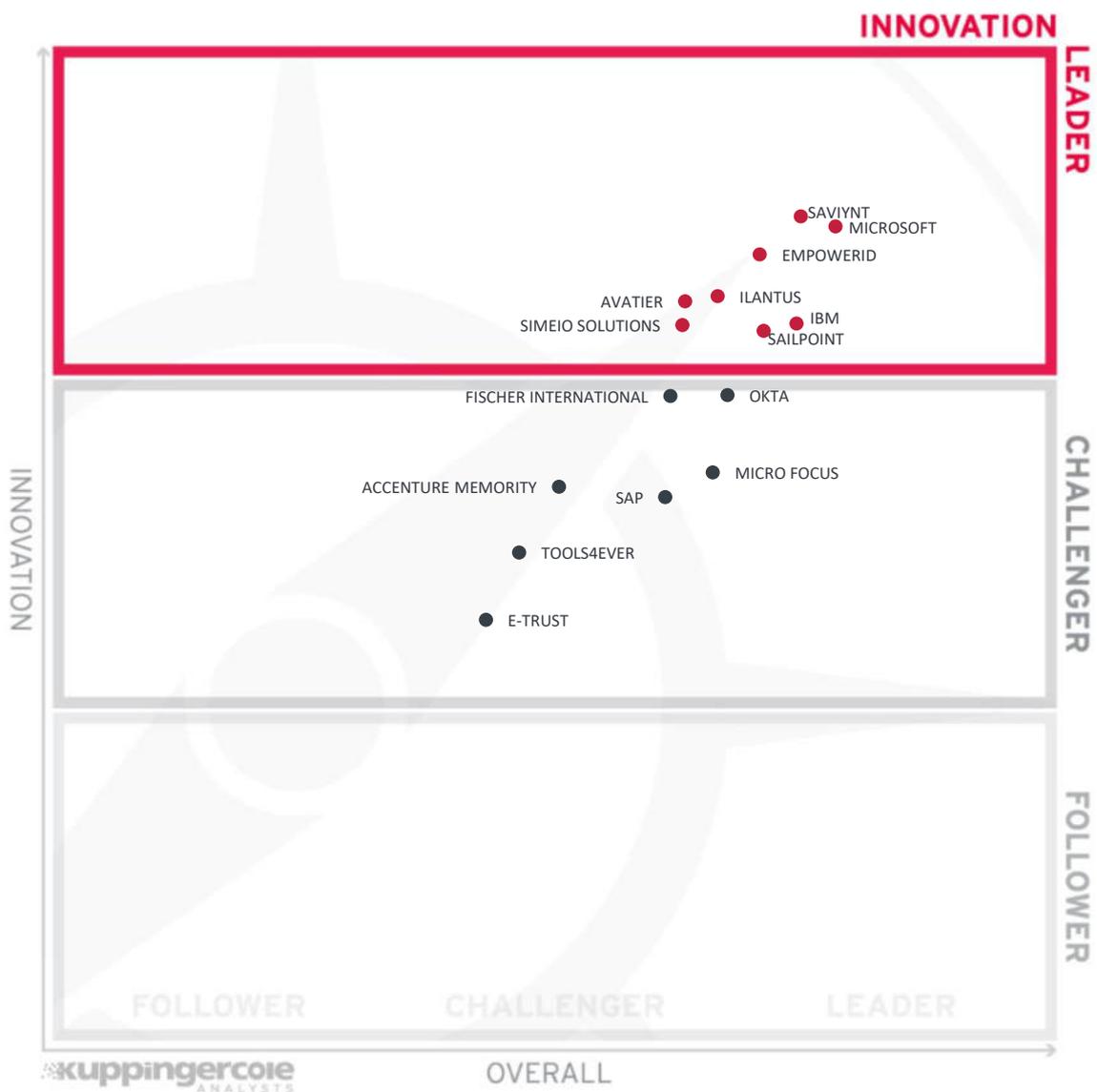

Figure 4: Innovation Leaders in the IDaaS IGA market segment

In this segment, we see a head-to-head competition for Innovation Leadership between Saviynt, Microsoft, and EmpowerID. Saviynt comes with a very strong IGA feature set, complementing these by new capabilities.

Microsoft excels specifically with integrations around security and other Azure and Microsoft EMS features. EmpowerID comes with a number of strong capabilities in certain areas such as SoD, but also the depth of integration to target systems beyond what we commonly find in other solutions.

Other vendors (in alphabetical order) in the Leader's segment include Avatier, IBM, Ilantus, SailPoint, and Simeio Solutions. All these vendors provide a good level of innovative features around IGA and are constantly innovating their offerings.

Closely following the group of Leaders we see Fischer International and Okta. While Fischer International delivers a broad set of IGA capabilities, Okta is tackling this segment from a perspective of a cloud-born solution that is expanding into IGA, focusing on lightweight implementation and usage of IGA features within their Lifecycle Management capabilities.

The other vendors amongst the Challengers in Innovation Leadership include Micro Focus with a mix of mature and modern capabilities, SAP with an innovative solution but primarily focused on Access Governance, Tools4ever with their strength for mid-market, and finally E-TRUST and Accenture Memory with some innovative features, but also the need for catching up in other areas.

Innovation Leaders (in alphabetical order):

- Avatier
- EmpowerID
- IBM
- Ilantus
- Microsoft

- SailPoint
- Saviynt
- Simeio Solutions

2.4   Market Leadership

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

Figure 5: Market Leaders in the IDaaS IGA market segment

In this Leadership graphic, we see the large players in front, with Microsoft being ahead of Microsoft and Micro Focus. Micro Focus still has rather few IDaaS customers, but a global presence and a strong partner ecosystem. Okta, SAP, and SailPoint also count amongst the Leaders.

The Challenger section for Market Leadership is very crowded, with Saviynt, EmpowerID, Ilantus, Simeio Solutions, Fischer International, Avatier, Tools4ever, Accenture Memority, and E-TRUST being placed in this segment. All vendors lack the one or other strength we expect from Leaders, such as a global presence or a significant customer base.

Market Leaders (in alphabetical order):

- IBM
- Micro Focus
- Microsoft

- Okta
- SailPoint
- SAP

3   Correlated View

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

3.1   The Market/Product Matrix

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

Figure 6: 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.

KuppingerCole Leadership Compass
IDaaS IGA
Report No.: **80051**

Here, we find IBM, Microsoft, and SailPoint in the upper right area, with Leadership positions in both Product Leadership and Market Leadership. Micro Focus, Okta, and SAP are placed to the left, having not yet achieved a Product Leadership rating, while being large players with a strong go-to-market. We expect these vendors to evolve their IGA capabilities gradually.

In the section right to the middle, we find the vendors that have achieved a Product Leadership rating but count not yet amongst the Market Leaders. Here, we find (in alphabetical order) Avatier, EmpowerID, Fischer International, Ilantus, and Saviynt. All show a strong potential if they manage to further grow their global ecosystem and their customer base – many of these vendors currently are limited to certain geographies.

In the middle section, we find the other vendors that made it to a Challenger rating in both Product Leadership and Market Leadership, which are Accenture Memority, E-TRUST, Simeio Solutions, and Tools4ever. All of these are interesting alternatives to the other vendors, with specific strengths that make them specifically interesting for certain types of use cases and customers.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. This distribution and correlation is tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.
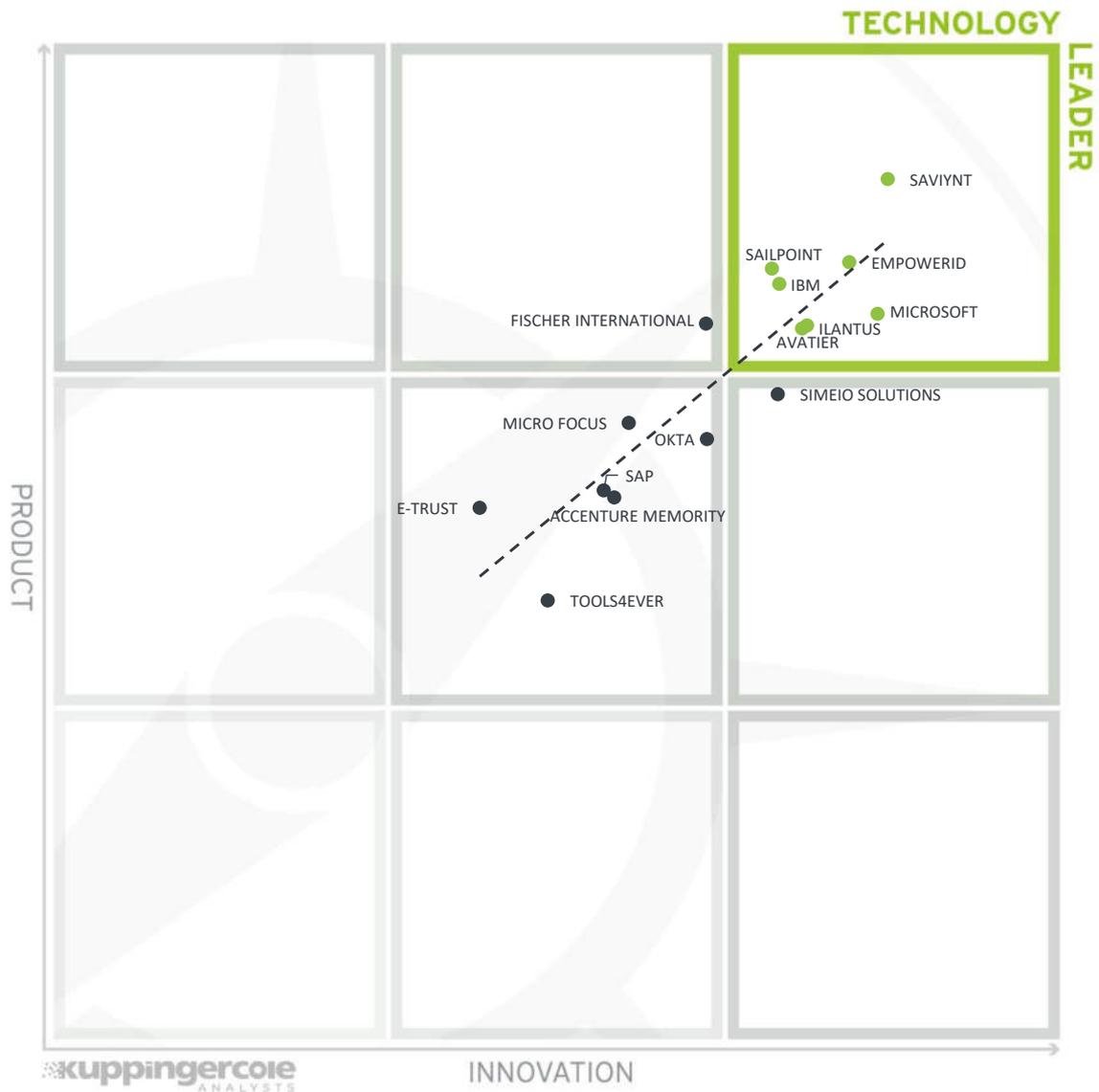
Figure 7: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we see – in alphabetical order – Avatier, EmpowerID, IBM, Ilantus, Microsoft, SailPoint, and Saviynt as Technology Leaders, with the latter being somewhat ahead of the others, being strong in both product and innovation ratings. The other vendors also count amongst the strongest contenders in the emerging IDaaS IGA market segment.

Fischer International, being just placed left to these vendors, being slightly less innovative according to our rating than the Technology Leaders are. Below the Technology Leaders we find Simeio Solutions, with being close to entering the Technology Leaders box.

Finally, we find (in alphabetical order) Accenture Memority, E-TRUST, Micro Focus, Okta, SAP, and Tools4ever in the middle section, ether with offerings that are still evolving or being specialized on certain aspects of this market.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.
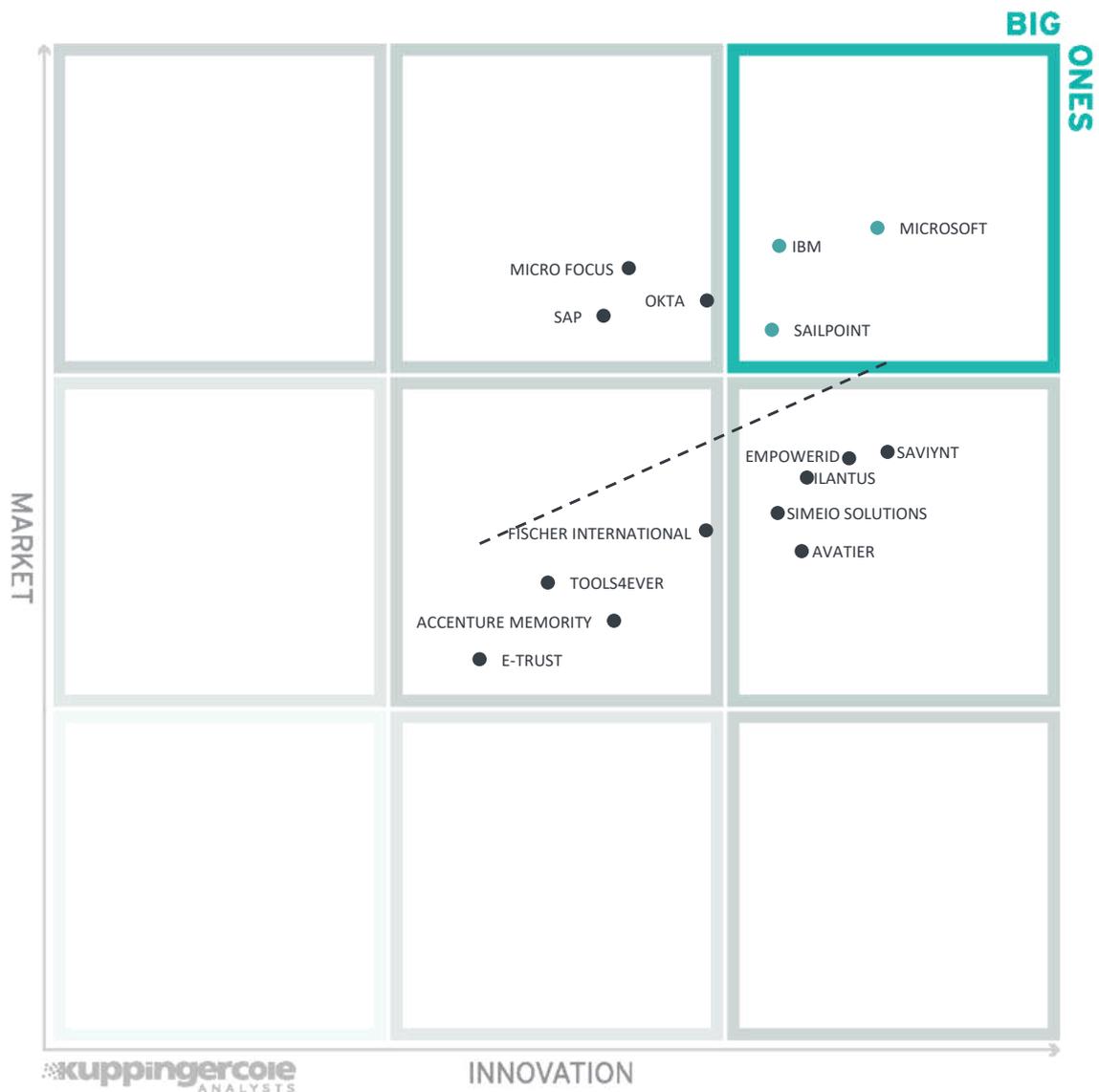
Figure 8: The Innovation/Market Matrix. Vendors above the line are performing well in the market compared to their relatively weak position in the Innovation Leadership rating; while vendors below the line show an ability to innovate, and thus the biggest potential for improving their market position.

Finally, the Big Ones such as IBM, Microsoft, and SailPoint are in the top-right box, with other large players in the IT market such as Micro Focus, Okta, and SAP being placed left of these.

Below the Big Ones, we find the innovative yet not as big vendors, including (in alphabetical order) Avatier, EmpowerI, Ilantus, and Saviynt.

In the box to the middle, we find the remaining vendors such as Fischer International, Tools4ever, Accenture Memory, and E-TRUST.

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 IGA. 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 2.

Product	Security	Functionality	Integration	Interoperability	Usability
ACCENTURE MEMORY	positive	positive	positive	positive	positive
AVATIER	positive	strong positive	positive	positive	strong positive
EMPOWERID	positive	strong positive	positive	strong positive	strong positive
E-TRUST	positive	strong positive	positive	positive	positive
FISCHER INTERNATIONAL	positive	strong positive	positive	positive	positive
IBM	strong positive	strong positive	positive	positive	positive
ILANTUS	positive	strong positive	positive	positive	strong positive
MICRO FOCUS	positive	strong positive	neutral	positive	positive
MICROSOFT	strong positive	positive	strong positive	strong positive	strong positive
OKTA	strong positive	positive	positive	strong positive	strong positive
SAILPOINT	strong positive	strong positive	strong positive	positive	strong positive
SAP	strong positive	positive	positive	positive	positive
SAVIYNT	strong positive	strong positive	strong positive	strong positive	strong positive
SIMEIO SOLUTIONS	strong positive	strong positive	positive	strong positive	strong positive
TOOLS4EVER	positive	positive	positive	positive	positive

Table 2: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 3 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
ACCENTURE MEMORITY	positive	neutral	positive	neutral
AVATIER	strong positive	neutral	positive	neutral
EMPOWERID	strong positive	positive	positive	positive
E-TRUST	neutral	neutral	neutral	weak
FISCHER INTERNATIONAL	positive	positive	positive	neutral
IBM	strong positive	strong positive	strong positive	strong positive
ILANTUS	strong positive	positive	positive	positive
MICRO FOCUS	positive	positive	positive	strong positive
MICROSOFT	strong positive	strong positive	strong positive	strong positive
OKTA	positive	strong positive	strong positive	strong positive
SAILPOINT	strong positive	positive	strong positive	strong positive
SAP	positive	positive	strong positive	strong positive
SAVIYNT	strong positive	positive	positive	positive
SIMEIO SOLUTIONS	strong positive	positive	positive	positive
TOOLS4EVER	positive	neutral	positive	neutral

Table 3: Comparative overview of the ratings for vendors

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.

Spider graphs

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

Target System Support	Breadth and depth of connectivity to target systems, both on premises and in the cloud.
Access Request & Workflows	Capabilities for enabling self-service and managed access request and the approval of such requests, plus the workflow capabilities required for these and other capabilities.
Access Governance	Integrated capabilities for Access Governance and Analytics, including Access Review and SoD controls, but also flexible support for entitlement models.
Authentication & Federation	Baseline capabilities for Access Management, i.e. SSO to target applications etc.
Mobile Support	Support for access to essential features via mobile devices with adequate interface design.
Architecture	Modern architectures, based on microservices and deployment via containers or as multi-tenant public cloud services.
Self Service Interfaces	Modern, advanced, and feature-rich interfaces for self-services such as credential management and access request that are easy to customize without coding.
Hybrid Environment Support	Strong support not only for cloud services but also for existing systems that run on premises in the infrastructure of organizations or in MSP deployments, but following traditional on premise deployment models.

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

5.1   Accenture Memority

Memority is a unit within Accenture Security delivering an IDaaS solution. Memority started as an independent software vendor and has become part of that larger group three years ago. Thus, Memority benefits from the global network of resources and the potential of expanding its still relatively small market share and focus on the French market significantly. They understand themselves as provider of an Identity Fabric that connects all types of users to all types of services.

Strengths	Challenges
● Part of Accenture Security, providing global scale	● Still low number of customers, but a number of large customers with global deployments
● Good feature set for Identity Provisioning and Identity Federation	● Lack of visibility in the market
● Baseline Access Governance features	● In migration from former monolithic solution to a modern microservices architecture, showing significant progress
● Adaptive Authentication features included, 2FA for administrative access as standard	
● Support for IoT use cases and manufacturing environments	
● Full IDaaS solution, but on premise deployments supported as well	

Table 4: Accenture Memority's major strengths and challenges

Memority is an IDaaS solution that supports both the IDaaS IGA and IDaaS AM use cases. It supports all major feature areas, from good Identity Provisioning and baseline Access Governance capabilities to Access Management, 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 IGA requirements and beyond.

While the functionality provided is rather broad, depth of capabilities is not yet at the top-level of the market but emerging. Memority, amongst other enhancements, has a strong focus on adding consistent API layers to its solution. Beyond that, Accenture Memority is very flexible in supporting specific customer requirements. While moving away from a per-tenant approach in deployment towards standardized deployments and operations, they still differ in that area from other vendors. A specific strength is the IoT support of the offering.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 5: Acccenture Memority's rating

As part of Accenture Security and with EU-based datacenters available, Memority is an interesting alternative to other vendors in the IDaaS IGA market, specifically the ones requiring customization for industry-specific use cases with the support of Accenture group. Based on the fact that Memority is part of Accenture and the overall good set of baseline capabilities, we see good potential for Memority to improve its role in the market.

ACCENTURE MEMORITY
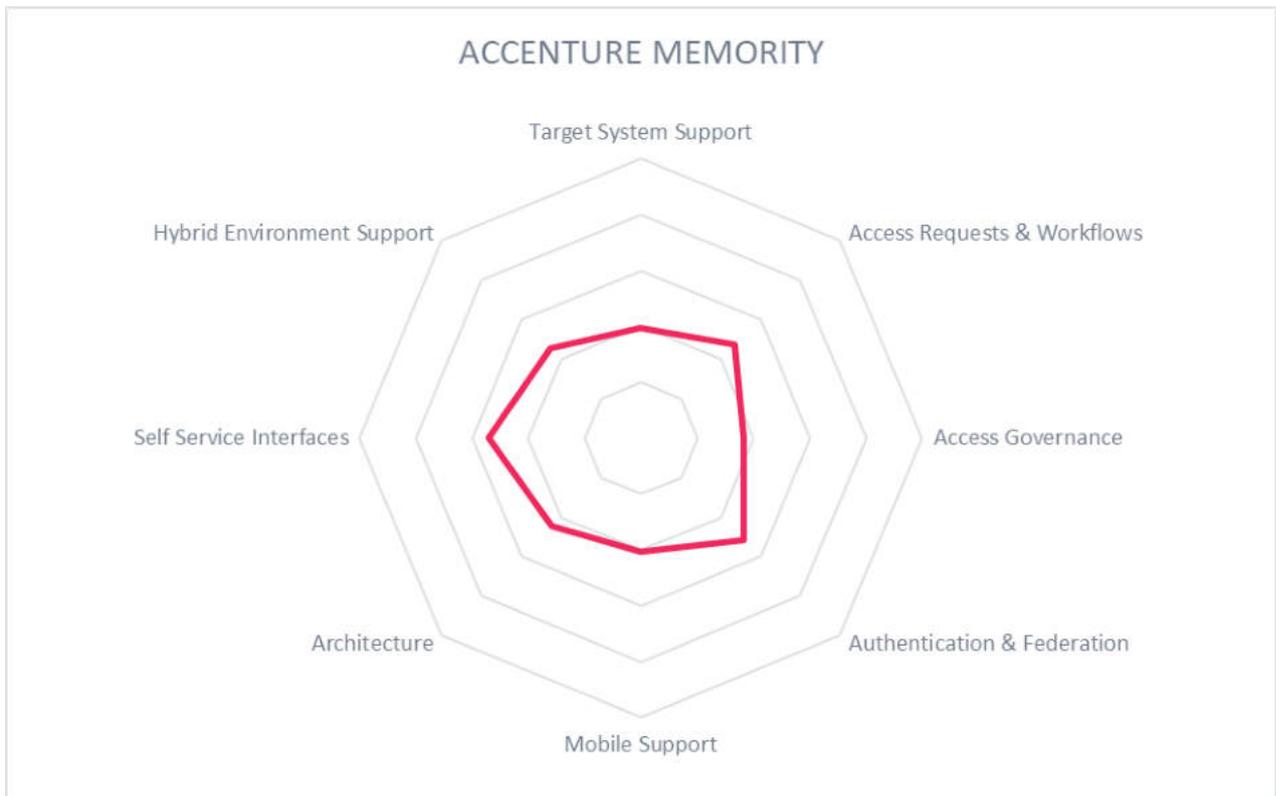
5.2   Avatier Identity Anywhere

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. Avatier Identity Anywhere has evolved from the former Avatier offerings, but has been widely re-architected, now being delivered as a containerized solution that can run in various environments, including as-a-service deployments.

Strengths	Challenges
● Tightly integrated solution	● Some weaknesses in Identity Federation, but strong SSO capabilities also covering cloud services
● Flexible customization based on configuration	
● Leading-edge user interfaces with strong support for mobile users	● No global partner ecosystem
● Overall strong capabilities for IDaaS IGA	
● Fully containerized solution	

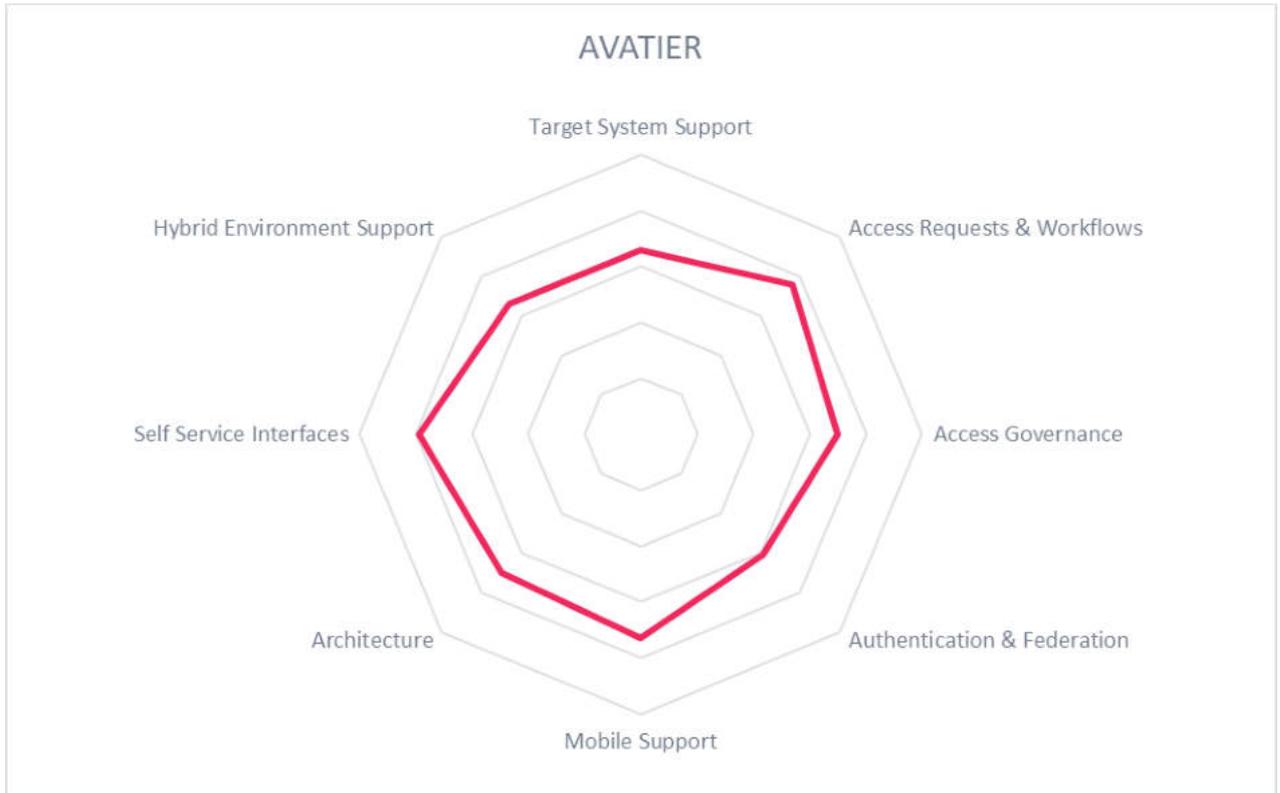Table 6: Avatier's major strengths and challenges

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.

Avatier recently released an AI chatbot which allows users to manage their identity using multiple chat channels, such as Slack, Skype, and Microsoft Teams. It also delivers an IOS and Android Avatier Identity Anywhere app that provides a seamless experience for users on the go. 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 showing a strong commitment on supporting identity standards..

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

Table 7: Avatier's rating

With the evolution Avatier has made over the past few years, they moved from a traditional IAM vendor that just delivers its solutions in an MSP-type deployment to broader support for the requirements of as-a-service deployments. The consequent use of microservices as an architectural paradigm and delivery via containers allows for quickly setting up instances for customers and managing these, supporting different types of clouds.

AVATIER

- Target System Support
- Access Requests & Workflows
- Access Governance
- Authentication & Federation
- Mobile Support
- Architecture
- Self Service Interfaces
- Hybrid Environment Support

5.3 EmpowerID

EmpowerID offers a broad range of of IAM capabilities, including Identity Provisioning and Access Governance. All services build on a common platform, but are provided as distinct services within IDaaS portfolio of EmpowerID. EmpowerID is one of the few vendors in the market delivering a comprehensive IAM Suite covering all areas of IAM. While some such as PAM are baseline capabilities, EmpowerID comes with a strong feature set in IGA.

Strengths	Challenges
● Integrated platform covering a broad range of IAM capabilities, including IDaaS Access Management	● Lacks support for multi-tenancy
● Both deep and broad integration with on premises applications and cloud services	● Conversion of architecture from former Windows base is work in progress
● Strong workflow capabilities allowing for flexible customization	● Still relatively small vendor, but fast growing ecosystem in both North America and Europe
● In-depth support for SoD controls for SAP and other complex environments	
● Good self-service interfaces	

Table 8: EmpowerID's major strengths and challenges

Identity Provisioning and Access Governance are at the core of the EmpowerID offering. The product is centered around its workflow capabilities, that allow streamlining the Identity and Access Lifecycle. EmpowerID comes with strong support for more complex challenges, including SoD support for complex target environments such as SAP, down to the level of transactions.

Being a product that is targeted at delivering an integrated suite of IAM capabilities, EmpowerID also provides good Access Management capabilities as part of the offering. Furthermore, deployment is supported in various models ranging from on premises to full as-a-service.

EmpowerID Virtual Directory provides an implementation of LDAP virtual directory server to create consolidated views, enable synchronization of user data across disparate user directories and support CRUD operations through internal workflows. Mostly supporting RBAC, an assignable ABAC engine from EmpowerID can offer granular control for authorization requests, in addition to using Open Policy Agent (OPA) for real-time microservices authorization.

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

Table 9: EmpowerID's rating

Overall, EmpowerID offers a decent IDaaS with few required on-prem components for better control of data and applications on-premises. Several advanced access management features are available.

EmpowerID makes a good candidate for organizations looking for an integrated solutions covering all major areas of IAM that can be run both on premises or in as-a-service models to begin their IDaaS transition.
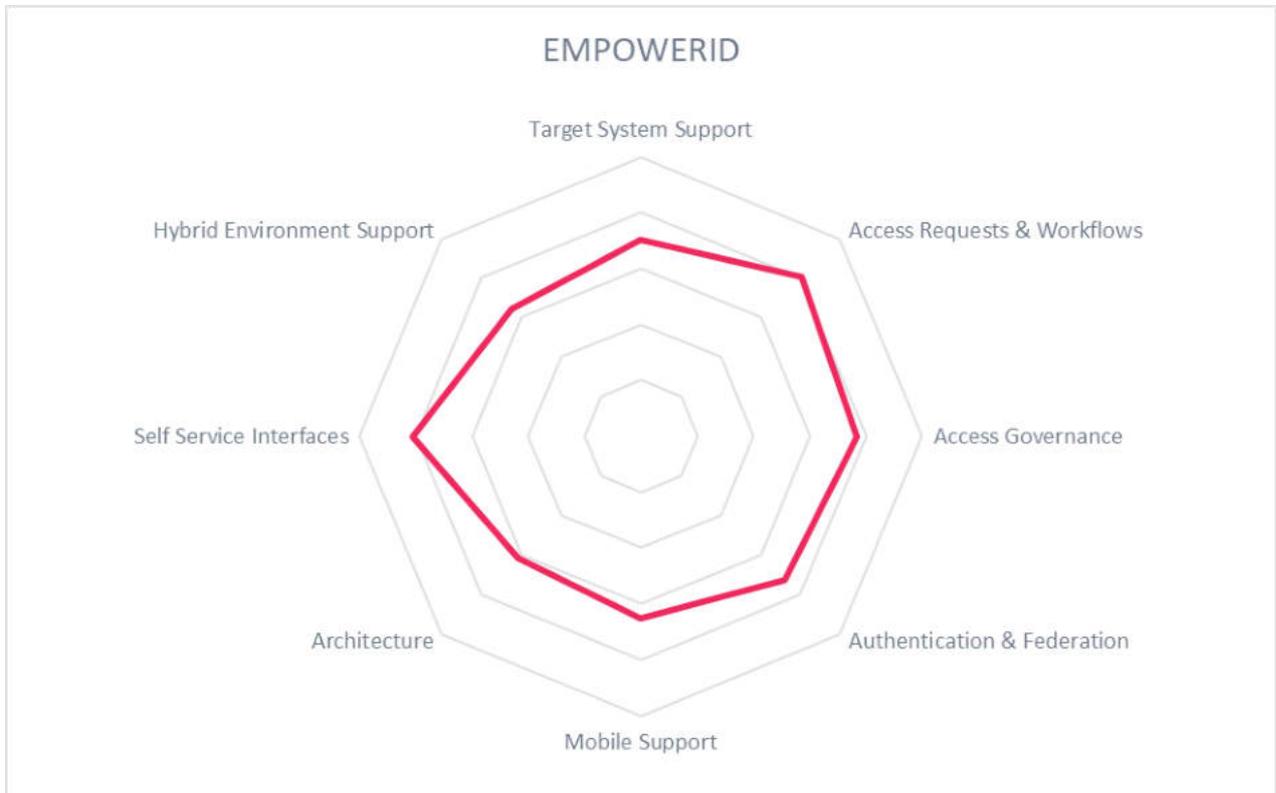
5.4   E-TRUST Horacius Identity Management

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	● No IDaaS Access Management capabilities
● Good set of on-premise connectors	● Based on on premises solutions, single-tenant SaaS deployment
● Established, mature offering	
● Service bus approach allows for efficient SaaS deployments	● Global, but rather small partner ecosystem, no global presence yet

Table 10: E-TRUST's major strengths and challenges

The SaaS offering provided by E-TRUST is based on a mature, proven IAM product that provides Identity Provisioning and Access Governance capabilities, plus additional Access Risk Management and Access Analytics features. This is complemented by a set of 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. This specifically allows for secure operations of the SaaS solution.

Security	positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	positive

Table 11: E-TRUST's rating

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

E-TRUST
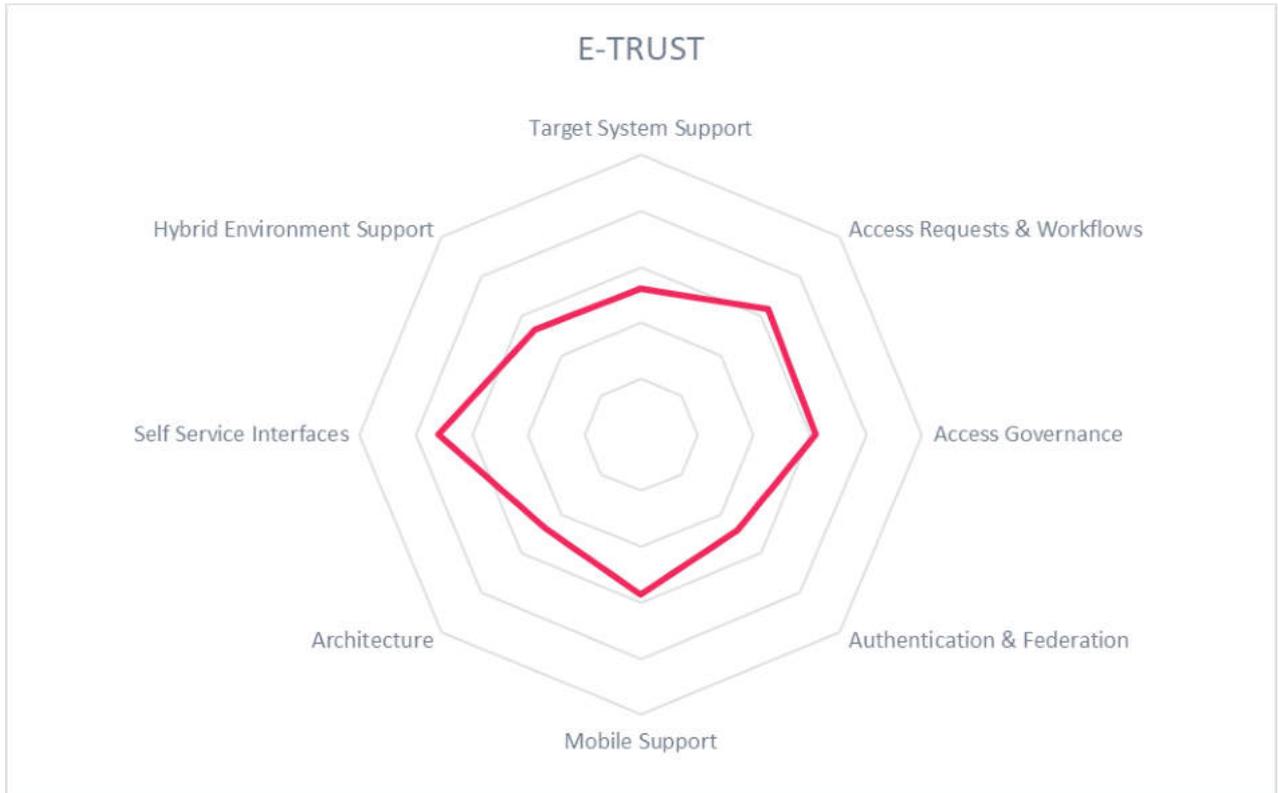
5.5 Fischer International Identity-as-a-Service

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. 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 SaaS deployments including full multi-tenancy support.

Strengths	Challenges
● SaaS delivery model as standard option	● Very limited global partner ecosystem and presence
● No coding required, customization is done via configuration and graphical design components	● No Identity Analytics and overall limited Access Governance capabilities
● Well-defined user interfaces for quick-start deployments	
● Broad set of certifications for the data centers in use	

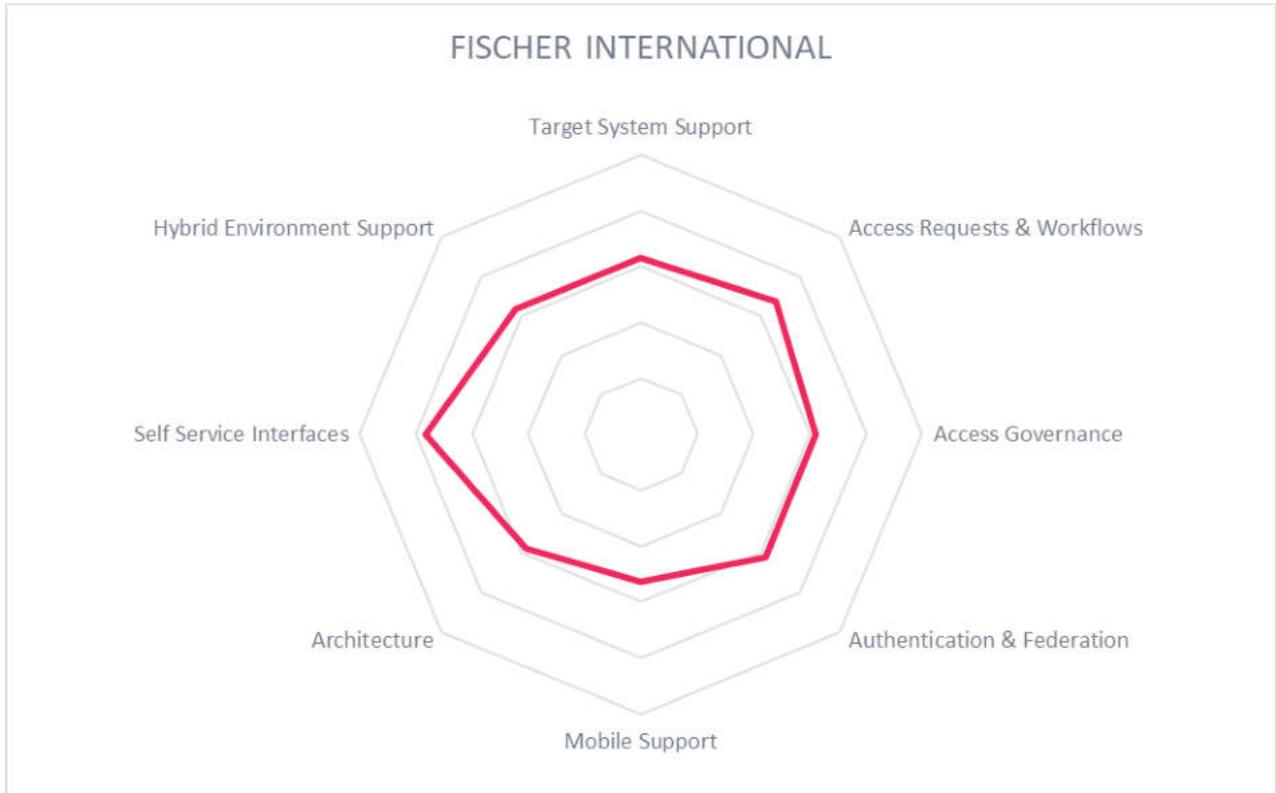Table 12: Fischer International's major strengths and challenges

Their SaaS delivery model is supported by several CSPs and partners, including Wipro as a global partner. Fischer International nowadays supports the use of data centers outside of the U.S., which has been a limitation in former times. 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 straightforward 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	strong positive
Integration	positive
Interoperability	positive
Usability	positive

Table 13: Fischer International's rating

Overall, Fischer provides an interesting approach to IDaaS IGA, 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.

FISCHER INTERNATIONAL

Target System Support

Access Requests & Workflows

Access Governance

Authentication & Federation

Mobile Support

Architecture

Self Service Interfaces

Hybrid Environment Support

5.6   IBM Cloud Identity

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. IBM Cloud Identity is one of the solutions that cover both the IDaaS IGA and the IDaaS Access Management market, allowing customers to build on a single offering. However, more complex requirements in hybrid environments require additional use of existing IBM on premises solutions for IAM, i.e. ISAM and ISIGI.

Strengths	Challenges
● Feature-rich offering, including Access Governance capabilities	● Might require use of IBM on premises solutions for advanced hybrid support
● Customizable workflows	● Overall limited number of out-of-the-box connectors in the SaaS solution
● Can be flexibly tailored to customer requirements, but provided as standard SaaS app	
● Supports also IDaaS Access Management requirements	

Table 14: IBM's major strengths and challenges

IBM provides a broad set of capabilities, covering the requirements for IDaaS IGA well. This includes tight integration with on-premise applications as well as Access Governance capabilities. However, IBM Cloud Identity Service also serves the IDaaS Access Management 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, however lacking breadth for consumer-grade 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.
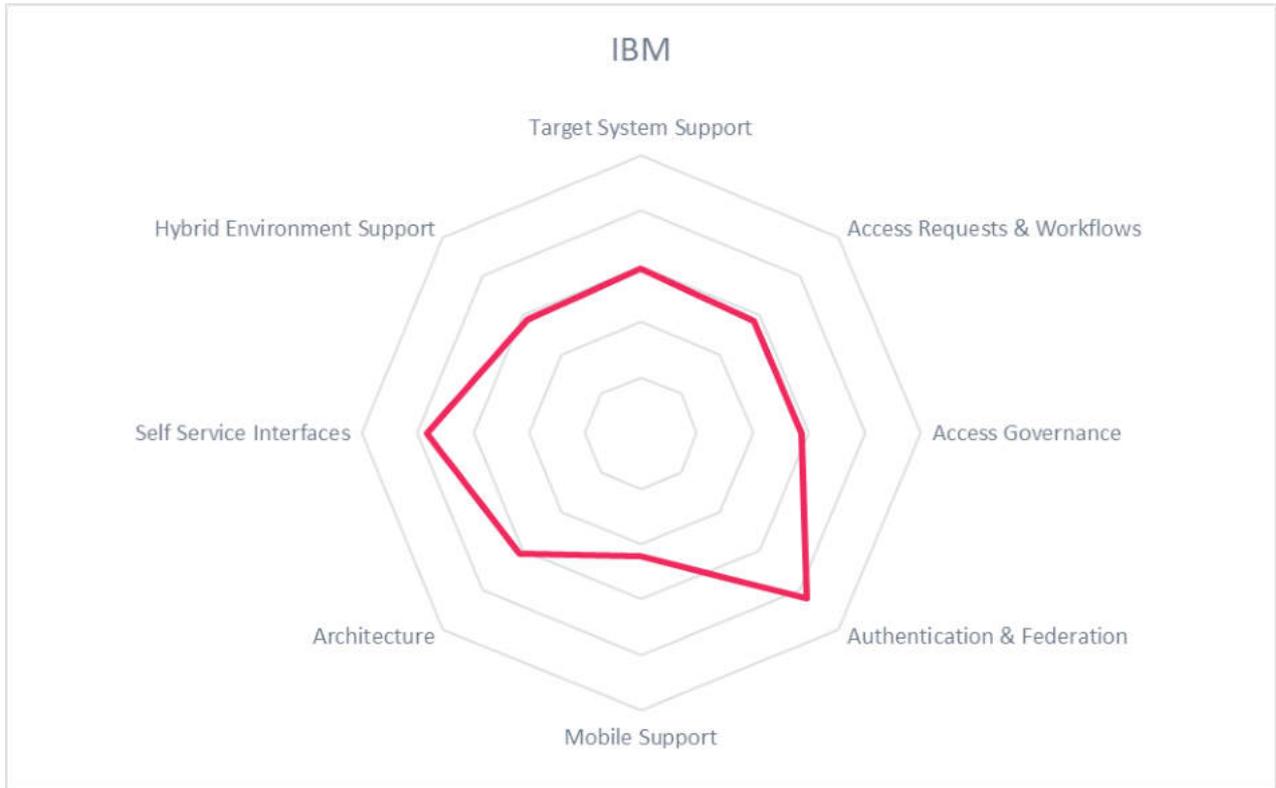
Other feature areas such as auditing are feature-rich and at enterprise-level. Support for mobile systems is at a baseline level; however, IBM with MaaS 360 has its own offerings in this area that can complement the IBM Cloud Identity Service.

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

Table 15: IBM's rating

IBM Cloud Identity Service counts among the leading solutions in the IDaaS IGA 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.

IBM

Target System Support

Access Requests & Workflows

Access Governance

Authentication & Federation

Mobile Support

Architecture

Self Service Interfaces

Hybrid Environment Support

5.7   Ilantus Compact Identity

Ilantus, which started as a system integrator, has moved into the IDaaS market over the past years, now providing a set of IDaaS offerings targeted at different types of customers. Their flagship solution Identity Plus focuses on delivering IGA capabilities, also as a service. It is deployed from Microsoft Azure and AWS data centers and meets also more complex requirements on IGA. Additionally, Ilantus offerings also cover the IDaaS Access Management requirements in the market.

Strengths	Challenges
● IDaaS solution focused on supporting IGA requirements of mid-market and large customers	● A small but selective partner ecosystem
● Good support for IGA capabilities	● Customer presence is still primarily focused on the US and few Asian countries, still low in EMEA
● Support for multi-tenant deployments, but also for running multiple tenants for a single customer	● Out-of-the-box reporting is somewhat limited, but Ilantus provides additional Access Analytics
● Flexibility for customization including policy and workflow customizations	
● Increased focus on enhancing user and administrative experience	

Table 16: Ilantus' major strengths and challenges

Ilantus provides a broad range of capabilities for IGA, from Identity Lifecycle Management to access request and approval workflows and Access Intelligence. Entitlements can be assigned based on rules, and Ilantus focuses on minimizing the amount of manual access requests by building on a well-thought-out approach for rule-based role assignments and birth-right provisioning. They are also strong in supporting mover processes.

The workflow capabilities are flexible and support multi-level approvals. Workflows can be configured within the UI with a easy-to-use workflow builder. Other important features include support for time-bound access, auto de-provisioning, and temporary suspension. For Access Governance, Ilantus delivers standard Access Review support, including multi-level campaigns, but also additional Access Intelligence capabilities. Ilantus also plans to add CIAM, risk-based analytics, CIAM and PAM within the solution.

The product integrates with Microsoft Active Directory and other solutions, including HR solutions, and covers a good range of target systems. Furthermore, it provides integration to Ilantus' own IDaaS Access Management as well as to Microsoft Azure Active Directory, Okta, and others.

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

Table 17: Ilantus' rating

Ilantus has emerged from a niche player to one of the leading vendors in the IDaaS market. Deployed in public cloud (Azure and AWS cloud), Ilantus Compact Identity offers the flexibility to be deployed in various models. As an easy to onboard and use solution, it makes a good choice of IDaaS for organizations that are looking to start their IAM journey without significant effort and investment, favoring a lean IAM operating model that delivers good IGA capabilities and integrates with IDaaS Access Management offerings.
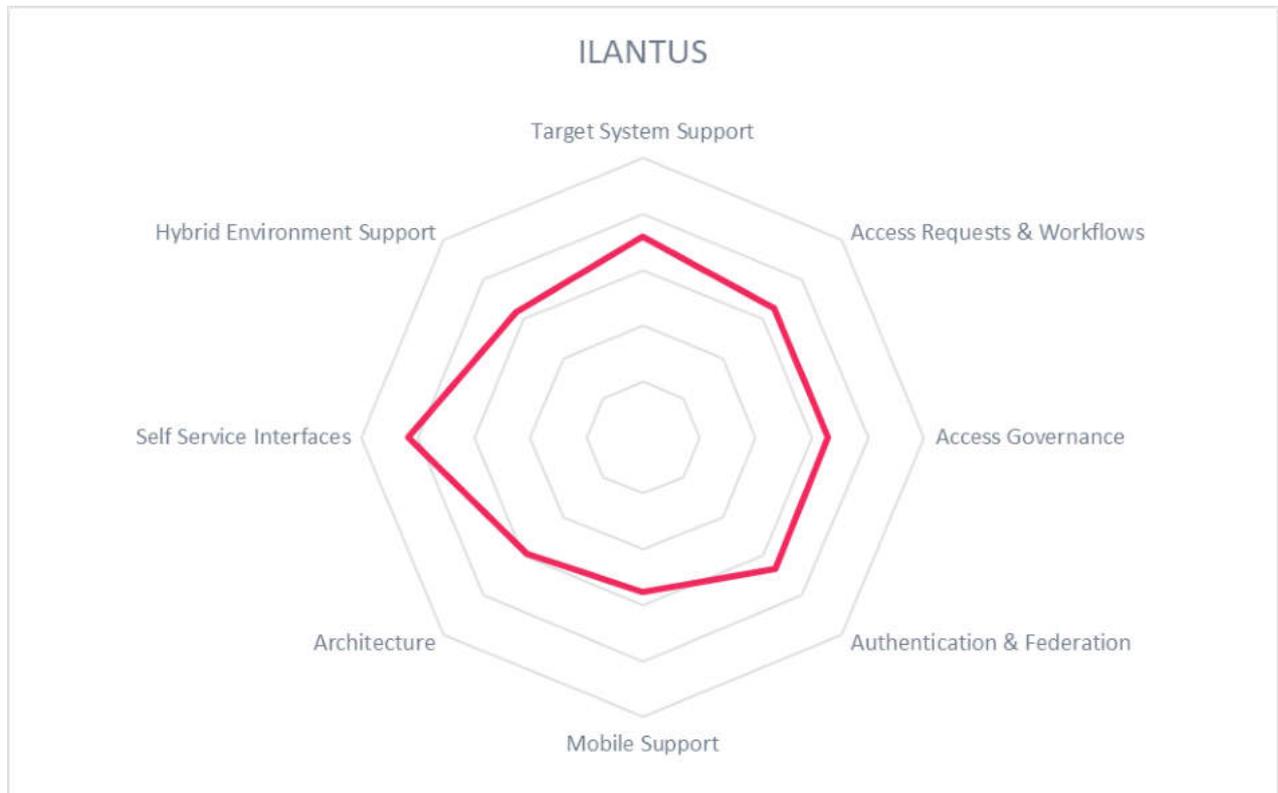
5.8 Micro Focus

Micro Focus has gathered several solutions in the IAM space, specifically through the former acquisition of NetIQ and thus the earlier Novell products. While these products originate from on premises solutions, Micro Focus is shifting combined offerings into an as-a-service model. They follow a single-tenant approach, but are ready to deliver these services from public cloud environments now. Thus, they can deploy IDaaS capabilities now.

Strengths	Challenges
● Strong capabilities based on the strength of the existing on premises solutions	● Single-tenant solution, delivered per individual customer
● Additional features such as identity Governance have been added over the past years	● Builds on existing on premises solutions that have been shifted to the cloud, thus more complex to configure and run than some other services
● Feature-rich offering	● Still a very new offering in its early stage as a IDaaS deployment
● Strong support for a very broad range of target systems	
● High degree of flexibility	

Table 18: Micro Focus' major strengths and challenges

As with all approaches that build on on-premises solutions, there are strengths and challenges. The obvious strength comes from the feature-richness and the maturity of the solutions the Micro Focus cloud solution builds on. On the other hand, there is more complexity involved in running and managing such solutions than it is for cloud-born IDaaS offerings. Furthermore, Micro Focus just started offering this new solution.

From a feature perspective, Micro Focus provides a strong set of connectors that are proven. Few vendors have as much experience in connecting target systems as Micro Focus has. While the strength arises specifically from connectors to on premises systems, Micro Focus also shows progress in connecting to cloud services.

Feature-wise, all major areas of IGA are covered. Micro Focus has added various capabilities such as Identity and Access Governance over the past years, becoming a vendor that goes well-beyond the Identity Lifecycle/Provisioning capabilities of the past.

Security	positive
Functionality	strong positive
Integration	neutral
Interoperability	positive
Usability	positive

Table 19: Micro Focus' rating

Due to the history and approach taken by Micro Focus, this solution needs to be carefully evaluated. It is an apparent option for customers already running Micro Focus IAM solutions on premises. However, it also provides a broad set of features, which make it an interesting option for more complex hybrid environments.

On the other hand, the offering is somewhere in between a traditional MSP-type deployment of an on premises solution and a full IDaaS offering, thus customers looking for pure-play IDaaS might not be served well by this product.
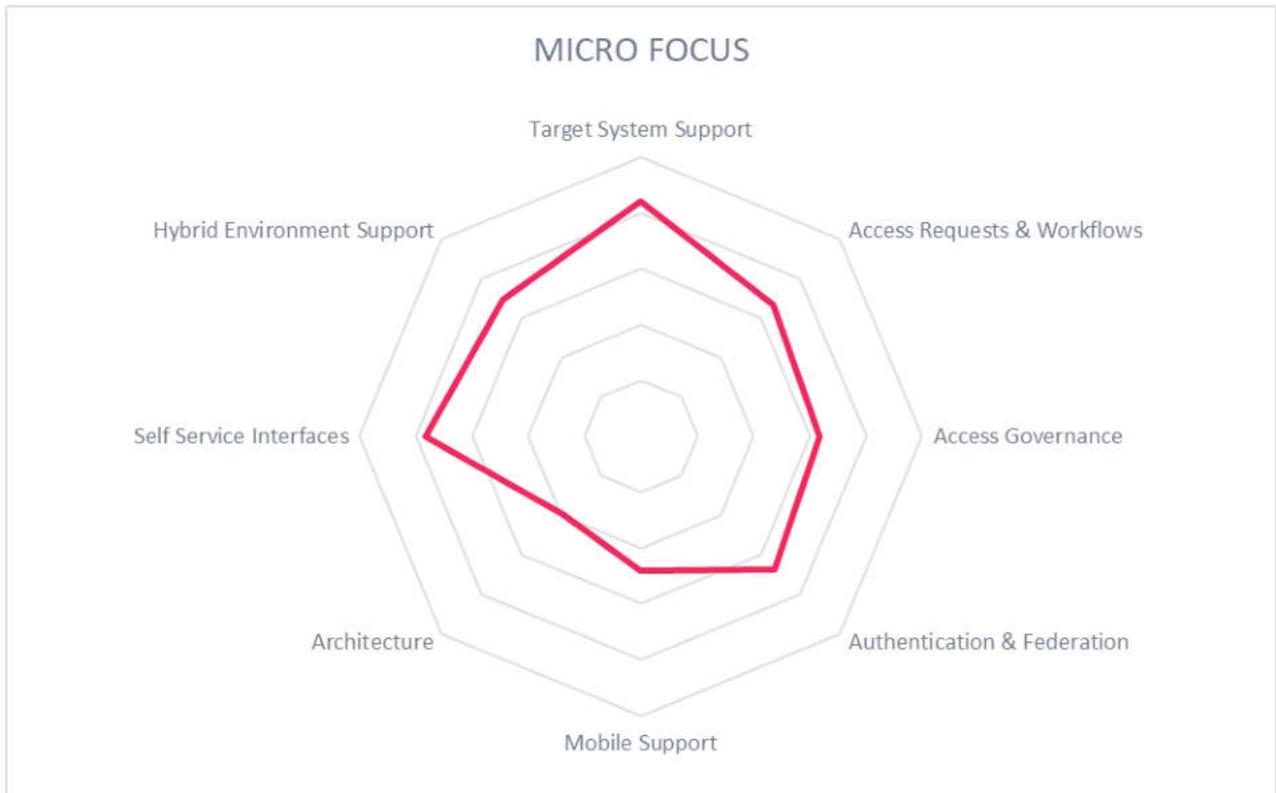
5.9 Microsoft Azure Active Directory

Microsoft offers Azure Active Directory (Azure AD) as its primary IDaaS platform. Azure AD Connect helps connecting on-premises Active Directory (AD) to the cloud and provide real-time data synchronization across on-premises and cloud directories enabling the use of a single identity across Office 365, Azure and other SaaS applications. Azure AD Connect provisions users, groups and other AD objects ensuring data synchronization between on-premises and cloud identity infrastructures.

Strengths	Challenges
● Tight integration with on premises Microsoft Active Directory	● Currently, most advanced IGA capabilities such as role management, SoD, or advanced access reviews are lacking
● Strong adaptive authentication strengthened by Microsoft Defender and Intune integration	● Significant limits in hybrid support, lack of advanced on premises connectors
● Baseline capabilities in IGA	● Limited API support for exposing IGA capabilities to developers
● Increasingly DevOps friendly with strong developer community support	● Strong focus on integration with Microsoft-only technology stack
● Huge installed customer base	
● Good support for popular SaaS integrations	

Table 20: Microsoft's major strengths and challenges

While Microsoft Azure AD is strong when it comes to Access Management capabilities, its IGA capabilities are still rather limited. Support for connecting back to on premises solutions for Identity Lifecycle Management and Access Governance are very limited. Azure AD App Proxy supports access to applications in a hybrid infrastructure environment for Access Management, but not the IGA use cases.

Also, other capabilities such as Active AD Identity Protection, Azure AD Conditional Access, or the deep integration with Microsoft 365 and Enterprise Mobility + Security Services (EMS) apps to control access based on the risk score are focused on Access Management use cases.

Microsoft Azure AD offers only baseline capabilities for access requests, their approval, and for Access Governance. While these capabilities will be extended over time, Azure AD currently is a solution that is primarily targeted at supporting SaaS applications, but not that much the hybrid environments of customers.

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

Table 21: Microsoft's rating

A large base of active users for third-party apps and active applications integrations make Azure AD the largest and most popular IDaaS platform globally – for Access Management. Microsoft Azure AD is an ideal choice for organizations with limited IAM expertise in-house and looking for a solution that's easy to procure, integrate and operate to meet standard access management requirements. However, customers need to be aware that the IGA capabilities are still early stage and only will evolve over time.

We expect Microsoft to increase its position in IDaaS IGA over time, but for now, customers must carefully evaluate whether the solution is already delivering what they need.
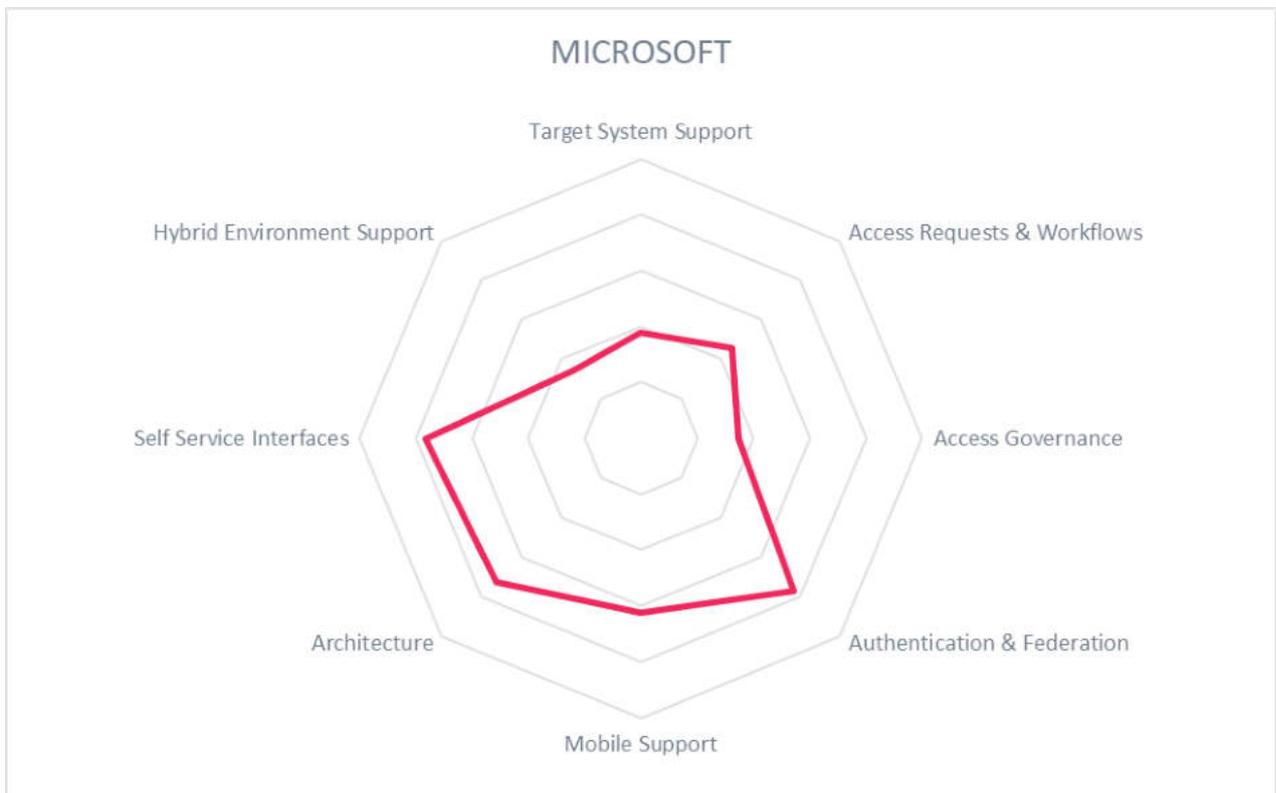
5.10 Okta Identity Lifecycle Management

Okta counts amongst the leading vendors in the IDaaS Access Management market, delivering a comprehensive, unified IDaaS platform to the market targeting both workforce and consumer Identity Management use cases. The solution comes with a unified directory, but also Identity Lifecycle Management, which makes it at least an entry-level solution for the IDaaS IGA market segment.

Strengths	Challenges
● Large customer base and global partner ecosystem	● Very limited Access Governance capabilities, based just on reporting
● Strong in IDaaS Access Management	● Limited connectors for on premises applications aside of SCIM but integration SDK available as Okta OPP (on premises provisioning)
● SCIM support for connecting to on premises services, plus few connectors	
● Strong support for SaaS applications	
● Good support for integration with HR/HCM systems	● Limited support for complex IGA workflow requirements
● Comprehensive exposure of capabilities via APIs	

Table 22: Okta's major strengths and challenges

Okta is most known for its Access Management capabilities, where the vendor started. However, over the past years, Okta has significantly extended the capabilities of its IGA platform, including adding support for Identity Lifecycle Management. This is targeted on Identity Provisioning, with only limited support for Access Governance. The latter is basically limited to reporting, lacking Access Intelligence or comprehensive support for Access Review.

Okta delivers out-of-the-box integrations to roundabout 200 systems for Identity Provisioning, most of them SaaS services. However, there is also connectivity back to on premises applications, with some direct connectors e.g. to the Oracle E-Business Suite, and with a SCIM connector that allows adding other applications in a standardized manner. Beyond that, the API of Okta can be used for further integrations, and there is a SDK provided.

Lifecycles can be orchestrated on the platform, providing some level of workflow support. However, compared to other products, there are still gaps when it comes to the full breadth of frequently rather complex workflows in IGA. The number of supported HR systems is good, however primarily focused on SaaS-based offerings.

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

Table 23: Okta's rating

Okta Lifecycle Management can be an interesting solution for customers, specifically when Access Governance requirements are not high on their list. For the Provisioning capabilities, Okta provides a quick start and a very flexible API, but lacks from deep on premises support.

Thus, it depends very much on the current state of the IT infrastructure of customers whether Okta Lifecycle Management is an adequate solution. Customers that primarily run SaaS applications and consequently follow a cloud first strategy will be already well-served, while customers with complex hybrid IT infrastructures might lack support for the on premises part of their IT.
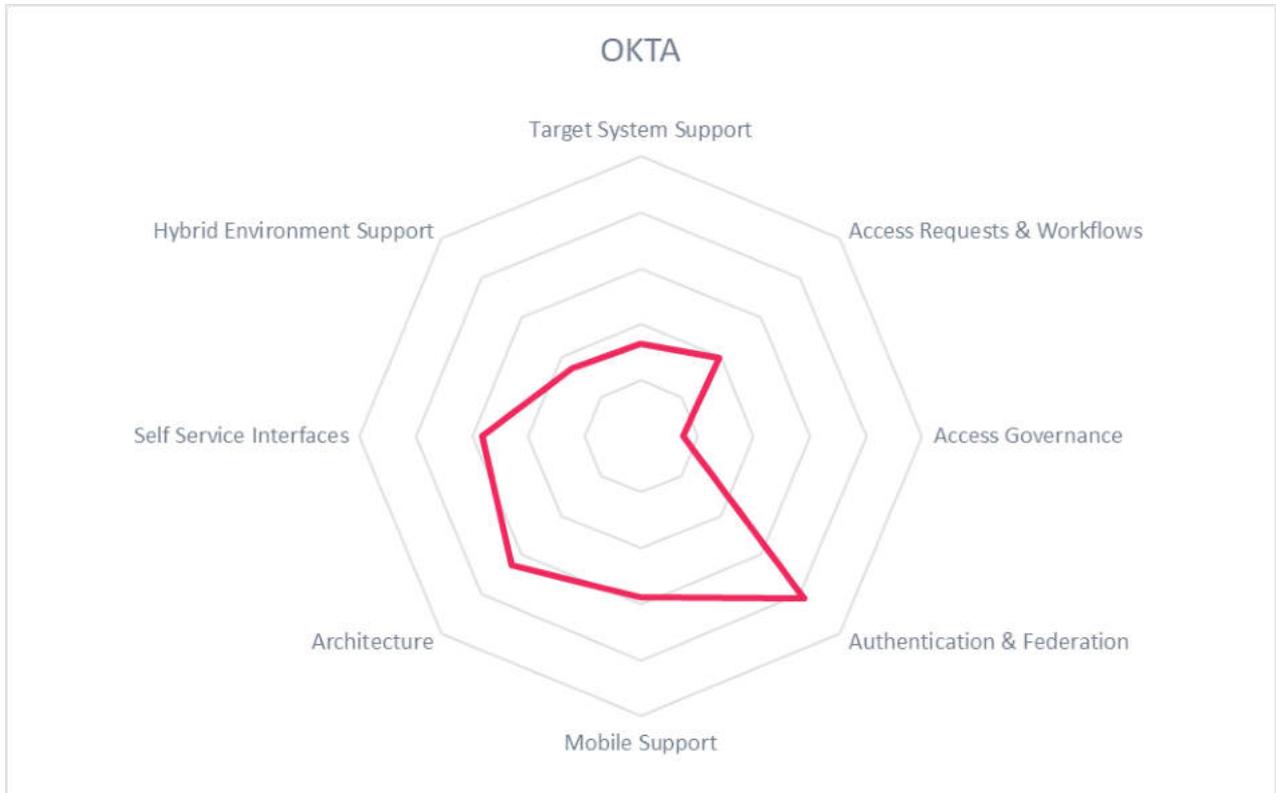
5.11 SailPoint IdentityNow

IdentityNow is the IDaaS offering provided by SailPoint. It is purely focused on IDaaS IGA use cases and does not support any IDaaS Access Management capabilities. This is consistent with the SailPoint corporate strategy of focusing on IGA only. IdentityNow is targeting both the mid-market and large enterprise use cases that require easy-to-use, out-of-the-box IGA capabilities instead of more complex models, with SailPoint also offering an MSP deployment of its software product IdentityIQ for complex enterprise use cases. SailPoint focused on IdentityNow in its response to this Leadership Compass.

Strengths	Challenges
● Easy-to-use capabilities for IGA	● Not as feature-rich as the SailPoint software product IdentityIQ
● Broad connector support	
● Clear focus on IGA and customers looking for a turnkey IGA solution	● No own data centers
	● Not focused on complex, large enterprise customers
● Provides a high degree of standardization for common IGA features	

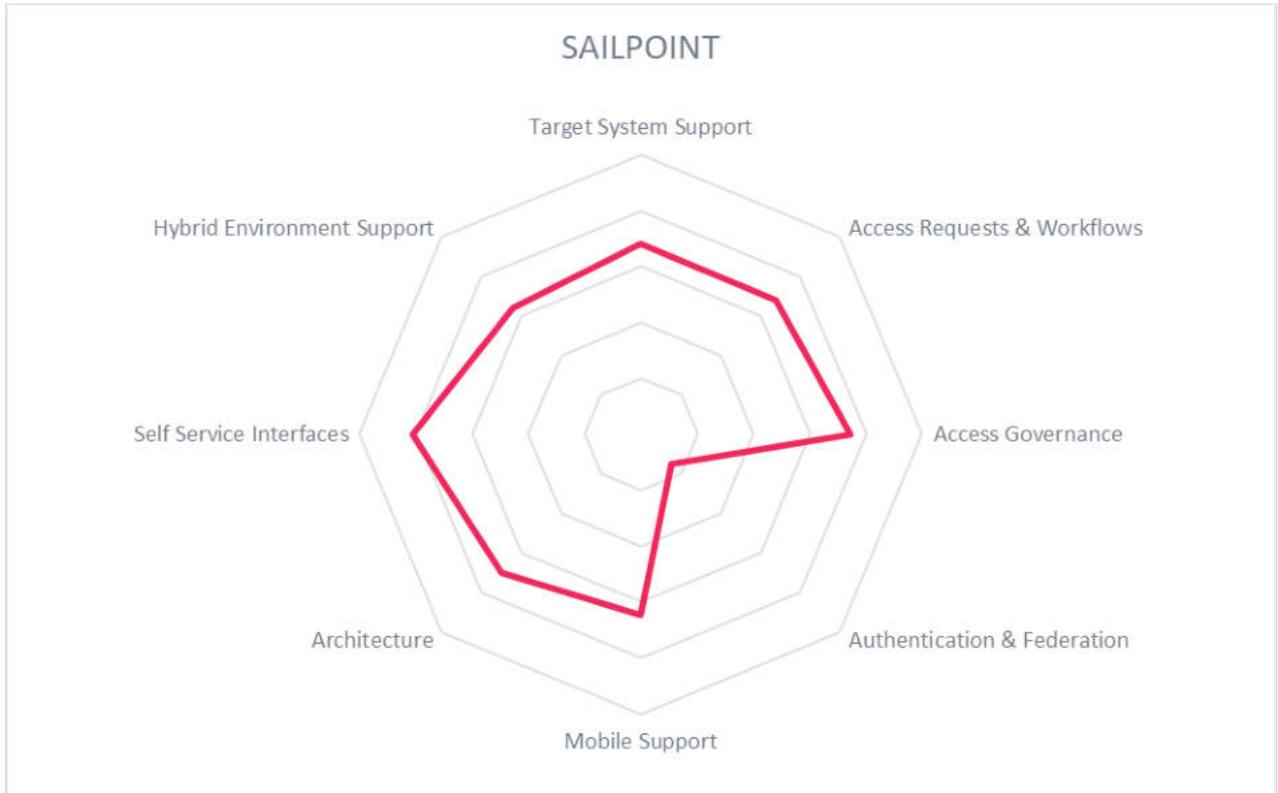Table 24: SailPoint's major strengths and challenges

SailPoint IdentityNow supports common IGA capabilities, including User Provisioning, Access Request Management, and a good but not leading-edge Access Governance capabilities. The product is focused on easy deployment and simple customization and configuration. However, the main emphasis is on providing strong out-of-the-box capabilities in a standardized manner for the target customers.

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.

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

Table 25: SailPoint's rating

SailPoint IdentityNow is an interesting offering in the IDaaS IGA market, with its clear focus on providing sort of a turnkey IDaaS IGA solution for businesses that require pre-configured, highly standardized solutions for rapid deployment. However, customers need to be aware of the fact that IdentityNow is not intended to deliver the same breadth of capabilities as SailPoint IdentityIQ.

SAILPOINT

Target System Support
Access Requests & Workflows
Access Governance
Authentication & Federation
Mobile Support
Architecture
Self Service Interfaces
Hybrid Environment Support

5.12 SAP Cloud Identity Access Governance

SAP Cloud Identity Access Governance is a pure-play IDaaS IGA solution, however focused primarily on the Access Governance part of IGA, including assignment of entitlements. It provides only baseline support for Identity Lifecycle Management yet, which – in the SAP ecosystem – is also provided by either their Identity Manager or, with SAP-only focus, by SAP Access Control. For customers using SuccessFactors, HR events triggering provisioning to certain targets is already supported. The solution comes with certain interesting capabilities and plays an important role in supporting the broader SAP ecosystem, i.e. the cloud-based applications such as Concur and SuccessFactors.

Strengths	Challenges
● Good support for SAP solutions	● Still very baseline support for Identity Lifecycle Management
● Modern UI, cloud-born offering	
● Delivers continuous insight into the state of access entitlements	● Targeted at SAP business applications, no broad SaaS support
● Supports extended SoD controls, focused on high-risk business applications	● Requires additional tools for delivering a comprehensive IGA solution
● Preconfigured audit reporting	

Table 26: SAP's major strengths and challenges

For the latter applications, SAP Cloud Identity Access Governance factually builds the bridge between the established SAP solutions in IGA and GRC to the new SaaS applications. It allows leveraging role definitions, workflows, and SoD rules for cloud applications. For SAP customers, this also involves having an environment that commonly consists of both SAP Access Control and SAP Cloud Identity Access Governance, when using the whole range of SAP solutions from traditional on premises ERP to new, cloud-born offerings.

Feature-wise, SAP Cloud Identity Access Governance is a strong offering for what it delivers. It supports continuous analysis of entitlements across systems, delivering insight into the status and risks. This comes with monitoring of SoD controls and the ability to remediate risks. Access can be easily managed, based on configurable and also pre-defined rules.

Being a cloud-born solution, SAP Cloud Identity Access Governance comes with a modern UI and well-thought-out dashboards that provide immediate insight into status and access risks. Furthermore, the product provides pre-configured audit reporting, simplifying delivery of automation to the auditors. This is of specific relevance for business-critical applications, which are in the focus of the auditors.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 27: SAP's rating

SAP Cloud Identity Governance is a solution that is of specific interest for SAP customers that need to extend the reach of SAP Access Control and SAP Identity Manager to the new solutions, and which need to add more advanced Access Analytics. The solution is not well-suited yet to support more

heterogeneous, hybrid environments and has only limited Identity Provisioning capabilities. Thus, customers must carefully evaluate whether this solution is the right fit. However, for several customers, SAP Cloud Identity Access Governance will be a logical choice and SAP has a well-thought-out roadmap for further evolution.
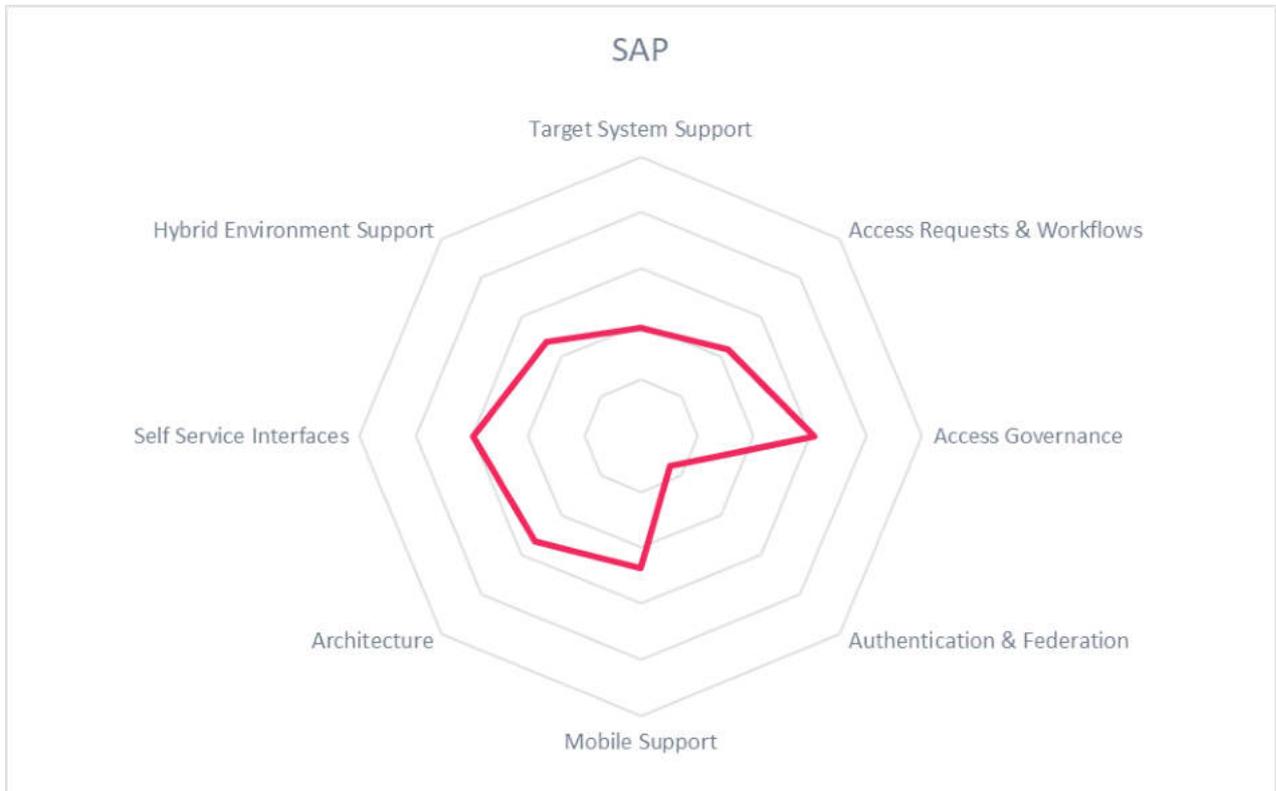
5.13 Saviynt Security Manager

Saviynt is a vendor that started with delivering Access Governance and Intelligence as a service. However, they also provide strong integration into applications on premises and Identity Provisioning capabilities. This makes Saviynt Security Manager an interesting alternative in the overall IGA market, but also a complementary offering to leading edge IDaaS Access Management solutions.

Strengths	Challenges
● Strong Access Governance and Intelligence feature set	● Interesting pricing model, but needs evaluation compared to traditional models
● Cloud-born solution	● Good partner ecosystem, but not equally strong across various regions
● Tight integration into a variety of enterprise-grade SaaS and on-premise services, delivering control of these environments	
● Integrates with some IDaaS Access Management services such as Okta, OneLogin, Azure Active Directory, and Ping Identity	

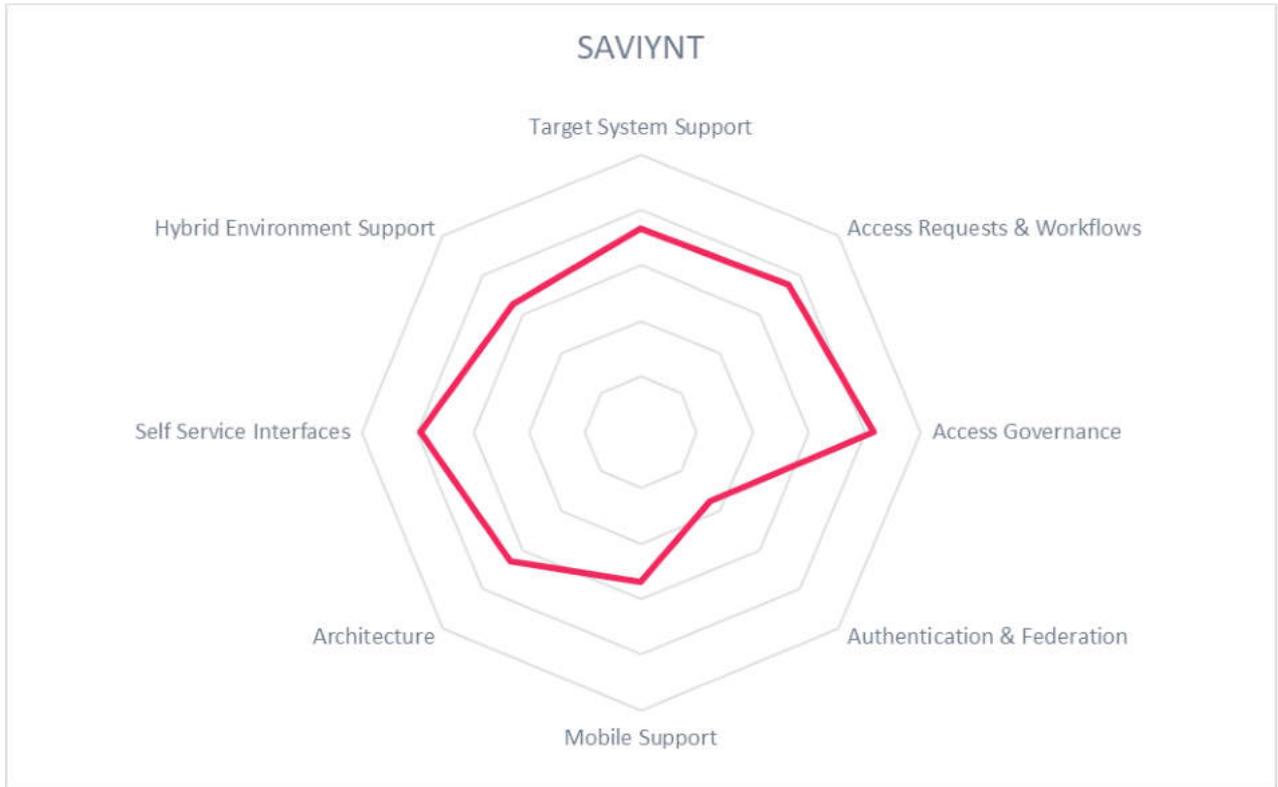Table 28: Saviynt's major strengths and challenges

Saviynt started as a vendor focusing on a gap many other solutions leave: Access Governance and Intelligence. This was a gap in all the initial IDaaS Access Management solutions, but also in other solutions including several IGA products in the market. From there, Saviynt successfully expanded the set of capabilities into full IGA support, plus additional capabilities around PAM (Privileged Access Management). They thus moved out of a niche, becoming a strong competitor in the overall IGA market.

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, AWS, Google Cloud Platform, and Alibaba Cloud, but also for enterprise applications such as Salesforce, Microsoft Office 365, Workday, SAP and the Oracle eBusiness Suite. They also provide Identity Provisioning capabilities to both cloud and on premises applications.

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

Table 29: Saviynt's rating

Saviynt has reached a state where it is not only a strong contender in the IDaaS IGA market, but also a challenger for the established on premises offerings in the IGA market. We recommend evaluating Saviynt when looking for IGA solutions, regardless of the deployment model, with the full support for on premises deployment provided by Saviynt as an option.

SAVIYNT

Radar chart with axes: Target System Support, Access Requests & Workflows, Access Governance, Authentication & Federation, Mobile Support, Architecture, Self Service Interfaces, Hybrid Environment Support

5.14 Simeio Access Governance Service

Simeo Solutions witnessed significant growth when shifting from its IAM system integration business into a full-fledged IDaaS service provider over the past years. Previously offering dedicated hosted services underpinned by other IAM vendor's products, Simeio enters mainstream IDaaS business with Simeio IDaaS. Simeio Access Governance Service is its primary IGA service, comprising of Directory Services, Identity Lifecycle Management, and Access Governance for a hybrid IT environment. Aside of that, Simeio IDaaS comes with strong Access Management capabilities.

Strengths	Challenges
● A wide range of SaaS integrations	● The wide-spread reputation of primarily being a global SI vendor than an IDaaS vendor
● Supports both IDaaS IGA and AM use cases	
● Good set of Identity Provisioning and Access Governance capabilities	● Part of code still underpins 3rd party software
● Flexible deployments and administration options across hosted service and full IDaaS	● Common deployment is per-tenant, not a turnkey solutions
● Good expertise with IAM systems integration, supporting all major legacy IAM solutions as target systems	

Table 30: Simeio's major strengths and challenges

Simeio IDaaS is hosted primarily in AWS, but also supports other IaaS platforms. It commonly uses an on-prem installation of Simeio Identity Interceptor for managing access across private domains and also to support legacy applications that prefer the use of agents deployed in the same environment. However, site-to-site VPNs are supported alternatively.

Identity Vault offers identity proofing service for critical B2C and G2C use-cases, particularly for banking and government organizations. By establishing trust in a user's identity through a score demonstrating the strength of assurance in the given identity. Providing broad authentication support, contextual authentication is offered as an add-on.

Simeio IDaaS comes with a strong support for Identity Provisioning and Access Governance, covering most of the common use cases. They provide good support for connecting back to on premises systems as well as broad support for SaaS target systems. Access Reviews, workflow support for request and approval, and a range of other capabilities are supported. Furthermore, Simeio integrates well with various other solutions in areas such as Threat Monitoring or Enterprise Mobility Management.

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

Table 31: Simeio's rating

As a lateral entrant in the IDaaS market, Simeio combines its IAM development experience and systems integration expertise to present a viable alternative to several established IDaaS vendors, particularly for

organizations that lack IAM knowledge and expertise internally and will require detailed guidance and support for transitioning existing on-prem access management to IDaaS.

SIMEIO SOLUTIONS

5.15 Tools4ever HelloID

Tools4ever is largely focused on IAM requirements of the mid-market segment and is increasingly building on its portfolio to serve the complexities and requirements of large organizations. Along with Identity & Access Manager as its primary offering for identity provisioning in the IAM market, Tools4ever offers HelloID Access Management as its IDaaS offering to serve the most common Access Management requirements of the mid-market segment plus delivering baseline IGA capabilities.

Strengths	Challenges
● Ease of deployment and initial configuration	● Good Access Management capabilities for mid-market customers, but not leading-edge for large enterprise customers
● HSM integration offers strong encryption and supports high assurance use-cases	● Limited set of IGA capabilities, including limited range of connectors
● Good understanding of mid-market IAM requirements	● Marketing is regionally aligned and ineffective, limiting international outreach and confining market growth
● Supports IDaaS-related regulations in the region	
● Lean solution for Identity Provisioning	
● Good baseline support for Access Governance	

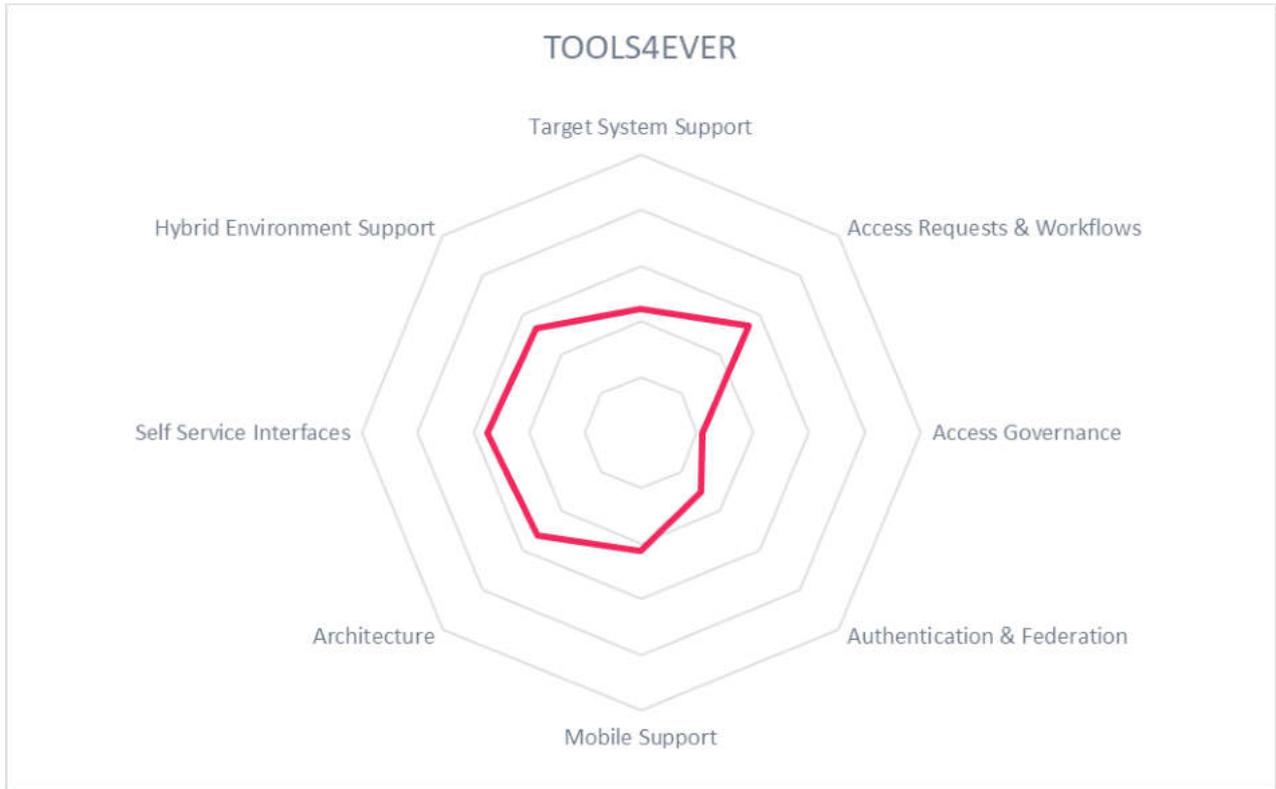Table 32: Tools4ever's major strengths and challenges

Launched recently as a standalone access management service, HelloID is hosted in Azure and Atlas data centres regionally and offers basic authentication and session management capabilities. HelloID delivers good baseline capabilities in IDaaS Access Management, while not being overly feature-rich. However, the capabilities provided are adequate to their mid-market customers, where they provide what commonly is needed.

Included in the base license, HelloID agent is the on-prem component that enables interfacing with local network resources such as on-prem AD or other applications. It supports capabilities such as deep Microsoft Active Directory integration and synchronization of users and groups to other systems.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 33: Tools4ever's rating

With a decent product roadmap and execution capability, we expect TOOLS4EVER to make some good progress over the next few years to be able to contend with the existing IDaaS players in the region. With offices in the U.S., The UK, France, Germany, and The Netherlands, TOOLS4EVER has a growing regional presence and make a good choice for local SMB and mid-market organizations to make their shift to IDaaS.

TOOLS4EVER

Target System Support

Access Requests & Workflows

Access Governance

Authentication & Federation

Mobile Support

Architecture

Self Service Interfaces

Hybrid Environment Support

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

6.1   AMI Praha

AMI Praha is a Czech software vendor and system integrator which offers a Microsoft Azure-based IDaaS IGA 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.Xx

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.

6.2   Cion Systems

Cion Systems is addressing the market more from the Active Directory management angle. They offer their solution as well in an as-a-service deployment model. Cion Systems might be best understood as a competitor to other companies being focused on the mid-market and SMBs, such as Tools4ever. Their capabilities are heavily centered around connecting to few systems from Microsoft Active Directory.

6.3   Hitachi

Hitachi ID Systems is a 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 IGA 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.

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.

6.4   iWelcome

Based in The Netherlands, iWelcome offers an IDaaS platform with B2B, B2E and CIAM variants. The B2E IDaaS provides user administration, identity lifecycle and request management, MFA, single sign-on, federation and basic provisioning capabilities. The B2B IDaaS offers white-labelling, extended metadata and marketing analytics and intelligence capabilities, in addition, the B2E feature set.

As one of the leaders in CIAM space, iWelcome offers a range of additional CIAM functions that include social identity integration, consent lifecycle management, KYC and progressive profiling.

Hosted across multiple data centres globally with 14 data centres in Europe and 2 each in the US and APAC, iWelcome's IDaaS platform delivers the range of access management capabilities with a strong focus on CIAM. Supporting most open identity standards for federation, iWelcome is designed to support a flexible data model with extensible metadata at the attribute level. Alongside support for Kantara UMA specifications, iWelcome also supports OAuth2 device flow for linking identity of the internet of things (IDoT). A large majority of its customer base is concentrated in Europe. iWelcome's B2B and B2E IDaaS services offer a good range of access management features but lack the required depth of functionalities to support complex IAM implementations. Its CIAM service presents a more complete option to support an organization's CIAM initiatives

6.5   iSM Secu-SyS

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.

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.

6.6   JumpCloud

JumpCloud is one of the single-service providers in the IDaaS market. They differ from other IDaaS services in their focus on a "directory as a service" offering. Instead of putting their emphasis on SSO capabilities or enhanced Identity Provisioning and Access Governance features, JumpCloud is essentially a directory service deployed from the cloud – the one directory to use when there is no directory service on premises.

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.

6.7   Omada

Omada is another of the established IAM players that offer their standard offerings in a MSP deployment 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.

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.

6.8 Open IAM

OpenIAM counts among the less known vendors in the IDaaS IGA 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.

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.

6.9 Oracle

Based in California, Oracle, the leading provider of database management and enterprise resource planning software, introduced Cloud Identity Services (IDCS) as its preliminary IDaaS service to deliver basic access management capabilities from the cloud. Targeted primarily at meeting the hybrid access management requirements of Oracle technology stack including Oracle E-Business Suite, Oracle PeopleSoft, and SAP, IDCS offers out-of-the-box configurations for a wide range of SaaS applications as well.

An integration with on-prem Oracle Access Management components might be necessary to realize advanced access management use-cases in a hybrid environment. IDCS offers MFA with one of the market's leading adaptive authentication capability that is powered by machine learning and applies a dynamic risk context to associate the appropriate access controls for a given level of risk. IDCS supports most open identity standards for SSO and federation. Oracle's API-first approach enables developers to build, secure and deploy mission-critical applications across a variety of platforms while streamlining the application development cycle. Available SDKs and drop-in widgets help developers build secure applications supporting DevOps in a developer-friendly manner.

Designed to complement existing enterprise solutions, IDCS supports multi-tenancy and integrates natively with Microsoft Active Directory and Azure, delivering seamless integration and control across both on-premises and cloud resources.

IDCS makes an ideal choice of IDaaS for organizations with existing investment in Oracle access management portfolio looking to extend the on-prem IAM controls beyond Oracle fusion middleware and business applications for the SaaS applications and even third-party PaaS. The significant presence of Oracle's technology infrastructure globally, combined with its industry-leading sales and a strong partner ecosystem makes IDCS the preferred choice for many customers worldwide, which, however, is changing faster than expected due to the increased adoption of open identity standards and easy integrations for Oracle technology stack offered by most IDaaS vendors.

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

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

7.1   Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the IDaaS IGA market. These products deliver most of the capabilities we expect from IDaaS IGA solutions. They are mature.

- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.

- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.

- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

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

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.

- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.

- Followers: This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

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

7.2   Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration

- Interoperability
- Usability

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

---

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

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

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

Interoperability can have several elements. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is related to interoperability and is measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status to ensure its importance is understood by both the vendor and the customer. As we move forward, simply providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

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

---

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

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

- Increased People Participation—Human participation in systems at any level is the highest area of cost and highest potential for breakdown for any IT endeavor.

- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will result in increased human participation in deploying and maintaining IT systems.

- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes and breakdowns. This will create openings for attack and failure.

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

7.3 Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

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

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

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

7.4   Rating scale for products and vendors

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

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

7.5 Inclusion and exclusion of vendors

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

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

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.

- Declined to participate: Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.

- Lack of information supply: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.

- Borderline classification: Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

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

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

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**