KuppingerCole Report

LEADERSHIP COMPASS

By Martin Kuppinger, Richard Hill

September 07, 2021

Identity as a Service (IDaaS) - IGA

An emerging market, IDaaS IGA, is characterized mainly 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

By **Richard Hill**
rh@kuppingercole.com

Content

1 Introduction / Executive Summary

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 Highlights

- This Leadership Compass evaluates over 40% more IDaaS IGA product vendors over the previous years.
- The IDaaS IGA market is growing, and although maturing it continues to evolve.
- IGA is essential to business as a strategic approach to ensure overall IT security and regulatory compliance.
- The level of identity and access intelligence has become a key differentiator between IGA product solutions.
- Automation is a key trend in IGA to reduce management workload by automating tasks and providing process workflows.
- Leading IGA vendors are increasingly focusing on supporting interoperability with other products and services through the provision of secure APIs.
- The Overall Leaders are (in alphabetical order) EmpowerID, IBM, Microsoft, One Identity, SailPoint, Saviynt, Simeio.
- The Product Leaders (in alphabetical order) are EmpowerID, IBM, Ilantus, Microsoft, One Identity, SailPoint, Saviynt, Simeio.

- The Innovation Leaders (in alphabetical order) are Accenture, Avatier, EmpowerID, IBM, Microsoft, SailPoint, Saviynt, Simeio.
- Leading vendors in innovation and market (a.k.a. the "Big Ones") in the IGA market are (in alphabetical order) IBM, Microsoft, SailPoint, Saviynt, Simeio.

1.2 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 significant growth 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 different markets, and therefore their abilities to support IDaaS use-cases vary. IDaaS vendors backgrounds includes:

1. Access Management vendors that offered broader IAM capabilities required for large IAM implementations that extend these functions to support emerging cloud and consumer access use-cases.

2. IGA (Identity Governance and Administration) vendors that traditionally offered support for identity lifecycle management and access governance on-premises but could not extend these capabilities to applications in the cloud, or support access management beyond basic authentication and authorization.

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

The IDaaS market combines Access Management functions with IGA and Access Governance capabilities--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:

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.

3. **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.

Capability	Description
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 criterion in any tool's 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 only be based on the information provided in a KuppingerCole Compass. The 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 ratings. The Overall rating provides a combined view of the ratings for

- Product
- Innovation
- Market
- Overall Leaders are (in alphabetical order):

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.

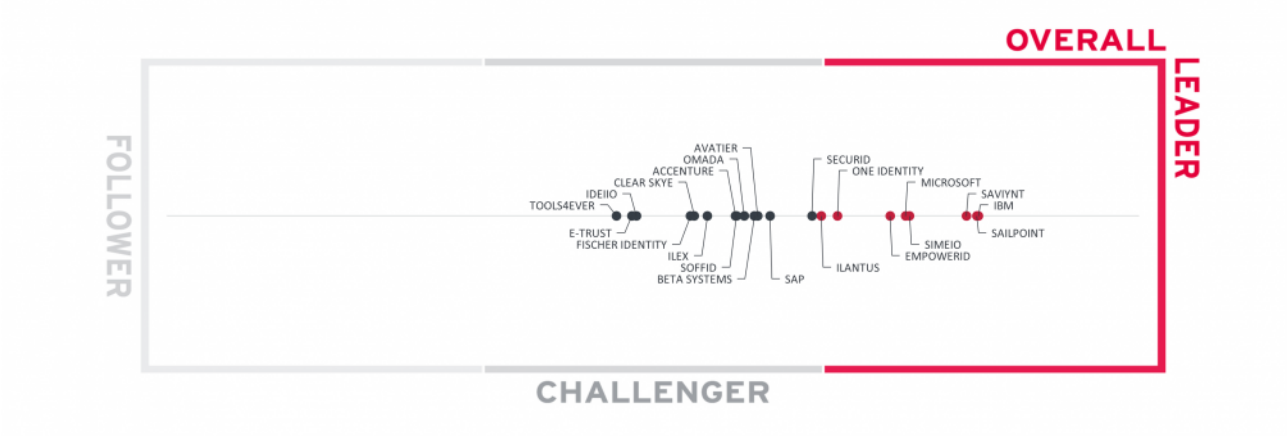


Figure 2: The Overall Leadership rating for the IDaaS IGA market segment

In this rating, we see both SailPoint and IBM ahead of the other vendors. IBM benefits from its overall market position and global ecosystem, while SailPoint's fully-featured offering is targetingthe large enterprise-market. Very closely following the top leaders, we see Saviynt, which also delivers a feature-rich solution. We also see Simeio and Microsoft head-to-head, with Simeio offering a position in both Product and Innovation Leadership. At the same time, Microsoft demonstrates a more significant overall market position and global ecosystem. EmpowerID is a vendor that has achieved a Leader position in both Product and Innovation Leadership closely behind Microsoft. Finally, One Identity and Ilantus holds a position as a Product Leader, with slightly less Market presence and therefore appears near the bottom border of the Overall Leader category.

Following these vendors, we find a group of challengers in the Overall Leadership rating, which includes (in alphabetical order) Accenture, Avatier, Beta Systems, Clear Skye, E-Trust, Fischer Identity, ideiio, Ilex, Omada, SecurID, SAP, Soffid, Tools4Ever. All deliver interesting yet very different solutions in the IDaaS IGA space. For example, SAP focus on the Access Governance capabilities with somewhat baseline Identity Provisioning, or Ilex giving full feature parity between the on-premises and SaaS solutions, while others provide rather full-fledged solutions. Tools4ever primarily targets medium-sized businesses and the mid-market and thus does not deliver the same breadth in integration and Access Governance capabilities as others do. E-TRUST, based in Brazil, provides an intriguing alternative but, e.g., yet lacks a global ecosystem. Accenture Memority 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
- Ilantus
- Microsoft

- One Identity
- SailPoint
- Saviynt
- Simeio

2.2 Product Leadership

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

Figure 3: Product Leaders in the IDaaS IGA market segment

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services.

Here, SailPoint, IBM, and Saviynt are head-to-head, all providing a leading set of IGA capabilities that is feature-rich. Following them, we find EmpowerID and Simeio, both ahead of One Identity, Microsoft, and Ilantus, all offering a very good set of IGA capabilities.

In the Challenger section, we see a tightly packed group of IDaaS IGA solutions (in alphabetical order) Accenture, Avatier, Beta Systems, Clear Skye, Fischer Identity, Ilex, Omada, SecurID, SAP, Soffid, Tools4Ever. Further Challengers include (again in alphabetical order) E-TRUST, ideiio, and Tools4ever. While Tools4ever targets the mid-market -- with a very good feature set for these groups 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):

- EmpowerID
- IBM
- Ilantus
- Microsoft
- One Identity
- SailPoint
- Saviynt
- Simeio

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 and other cutting-edge features, while maintaining compatibility with previous versions.

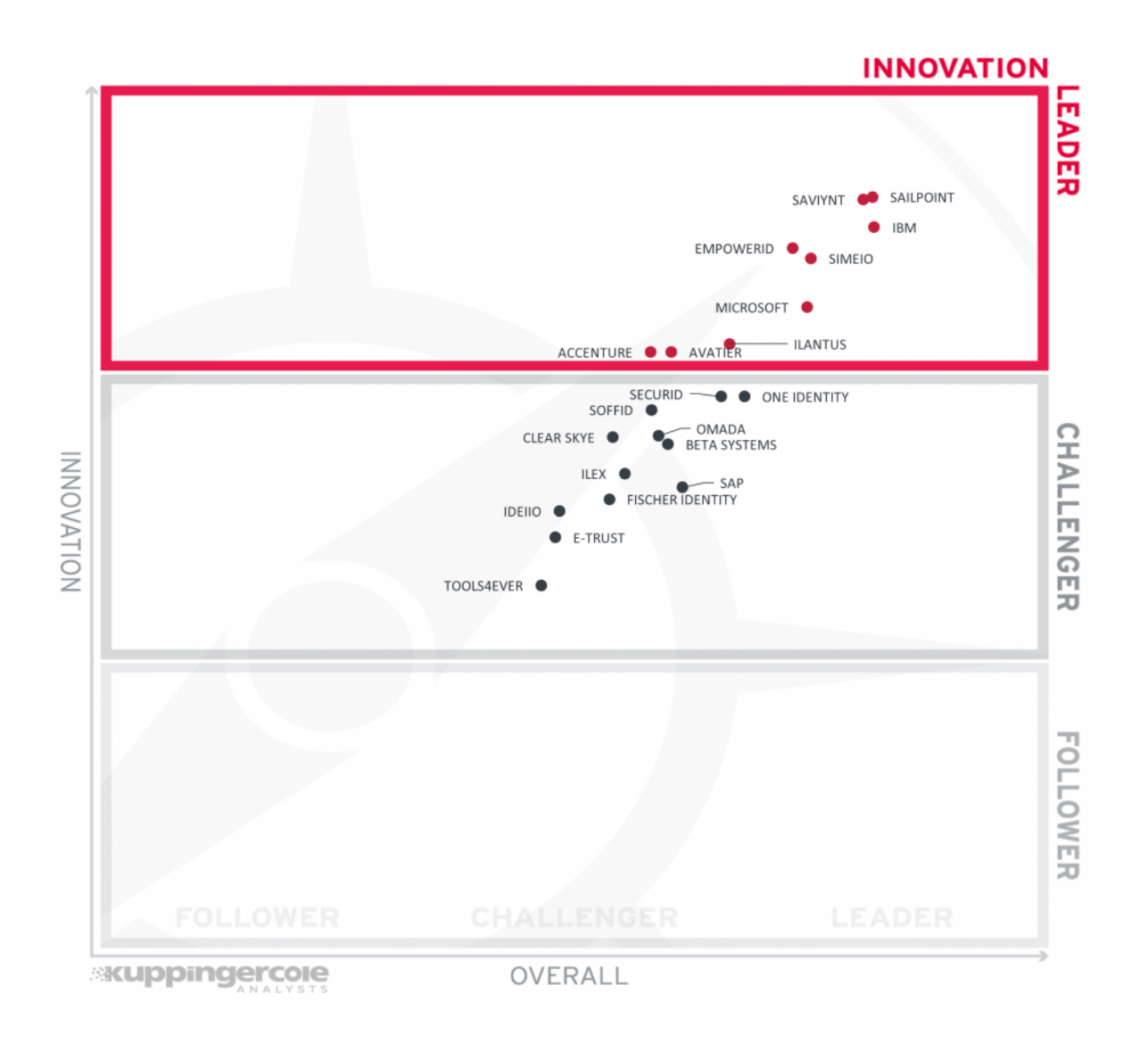


Figure 4: Innovation Leaders in the IDaaS IGA market segment

In this segment, we SailPoint and Saviynt being in lead head-to-head. Both SailPoint and Saviynt offer a robust IGA feature set complemented by new capabilities. Nearby, IBM completes the top grouping of leaders. Next are EmpowerID and Simeio, closely grouped, with both having a number of strong capabilities in certain areas. Finally, other vendors (in alphabetical order) in the Leader's segment include Microsoft, followed by Avatier, and Accenture near the bottom border. All these vendors provide a good level of innovative features around IGA and are constantly innovating their offerings.

The other vendors amongst the Challengers in Innovation Leadership include (in alphabetical order) Beta Systems, Clear Skye, E-Trust, Fischer Identity, ideiio, Ilantus, Ilex, Omada, One Identity, SecurID, SAP, Soffid, Tools4Ever.

Innovation Leaders (in alphabetical order):

- Accenture
- Avatier
- EmpowerID
- IBM
- Microsoft
- SailPoint
- Saviynt
- Simeio

2.4 Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, 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 prominent players in front, with IBM being ahead of Microsoft and SailPoint. Saviynt, Simeio, SAP, and One Identity also count amongst the Leaders.

The Challenger section for Market Leadership is very crowded, with SecurID, EmpowerID, Ilantus grouped near the top border. The remaining vendors are occupying the center of the Challenger section, which includes (in alphabetical order) Accenture, Avatier, Beta Systems, Clear Skye, E-Trust, Fischer Identity, ideiio, Ilex, Omada, SAP, Soffid, and Tools4Ever.

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
- Microsoft
- One Identity
- SailPoint
- SAP
- Saviynt
- Simeio

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.

All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

In this matrix, we find IBM, Microsoft, and SailPoint in the upper right area, with Leadership positions in both Product Leadership and Market Leadership. Saviynt, Simeio, and One Identity are placed slightly below the line while prominent players with a strong go-to-market. We expect these vendors to evolve their IGA capabilities gradually.

In the top middlebox, we see SAP as a Market Leader but missing the level of product capabilities as the Market Champions.

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 Ilantus and EmpowerID. All show a strong potential if they further grow their global ecosystem and their customer base -- many of these vendors currently are limited to specific geographies.

In the middle section, we find the remaining vendors. Each made it into the Challenger rating in Product Leadership and Market Leadership, which includes (in alphabetical order) Accenture, Avatier, Beta Systems, Clear Skye, E-Trust, Fischer Identity, ideiio, Ilex, Omada, SecurID, Soffid, Tools4Ever. These are intriguing alternatives to the other vendors, with specific strengths that make them particularly 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. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

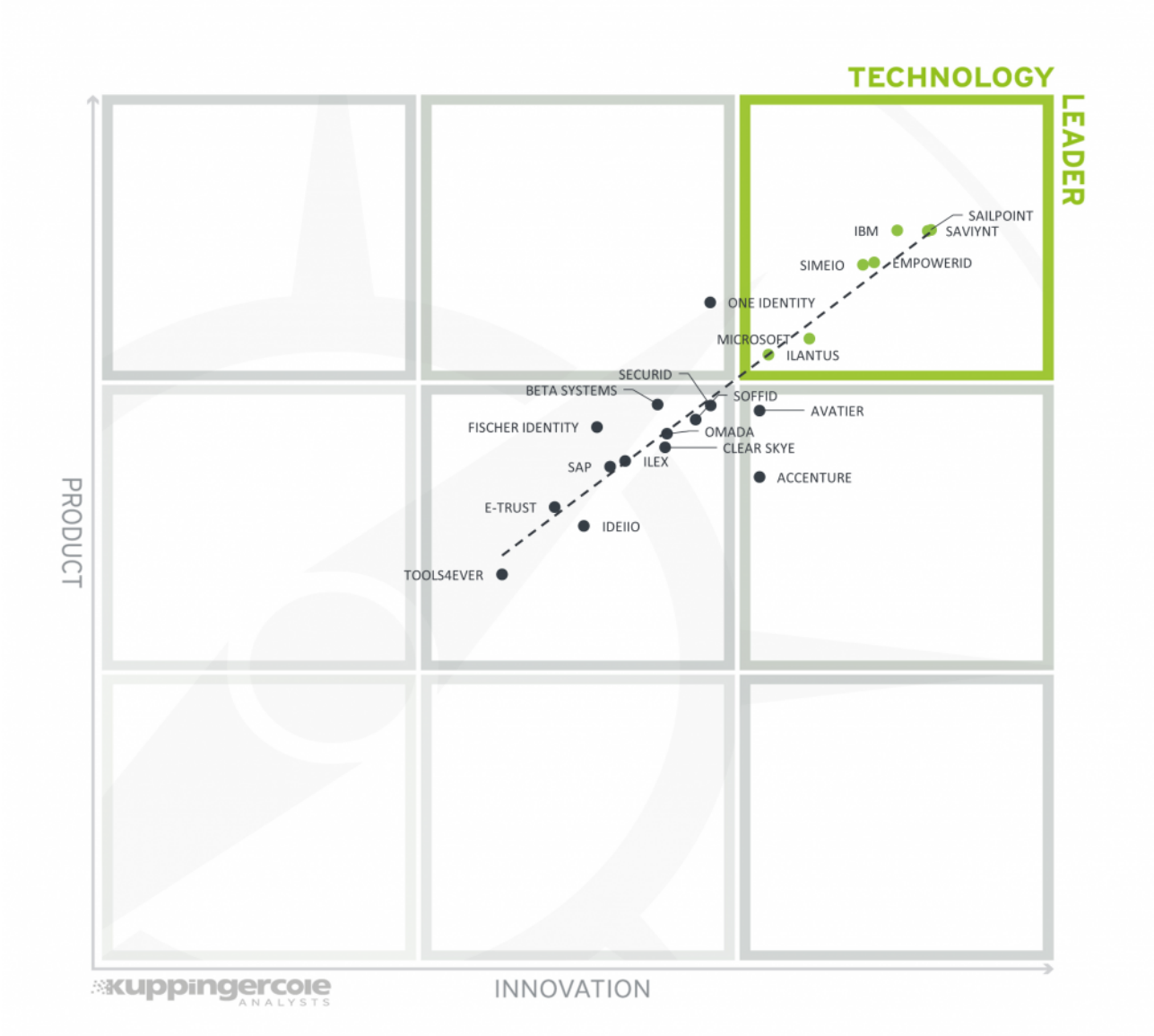


Figure 7: The Product/Innovation Matrix

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 - EmpowerID, IBM, Ilantus, Microsoft, SailPoint, Saviynt, and Simeio as Technology Leaders, with the SailPoint, Saviynt, and IBM being 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.

One Identity, 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 Avatier and Accenture being close to entering the Technology Leaders box.

Finally, we find (in alphabetical order) Beta Systems, Clear Skye, E-Trust, Fischer Identity, ideiio, Ilex, Omada, SecurID, SAP, Soffid, and Tools4Ever in the middle section, 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.

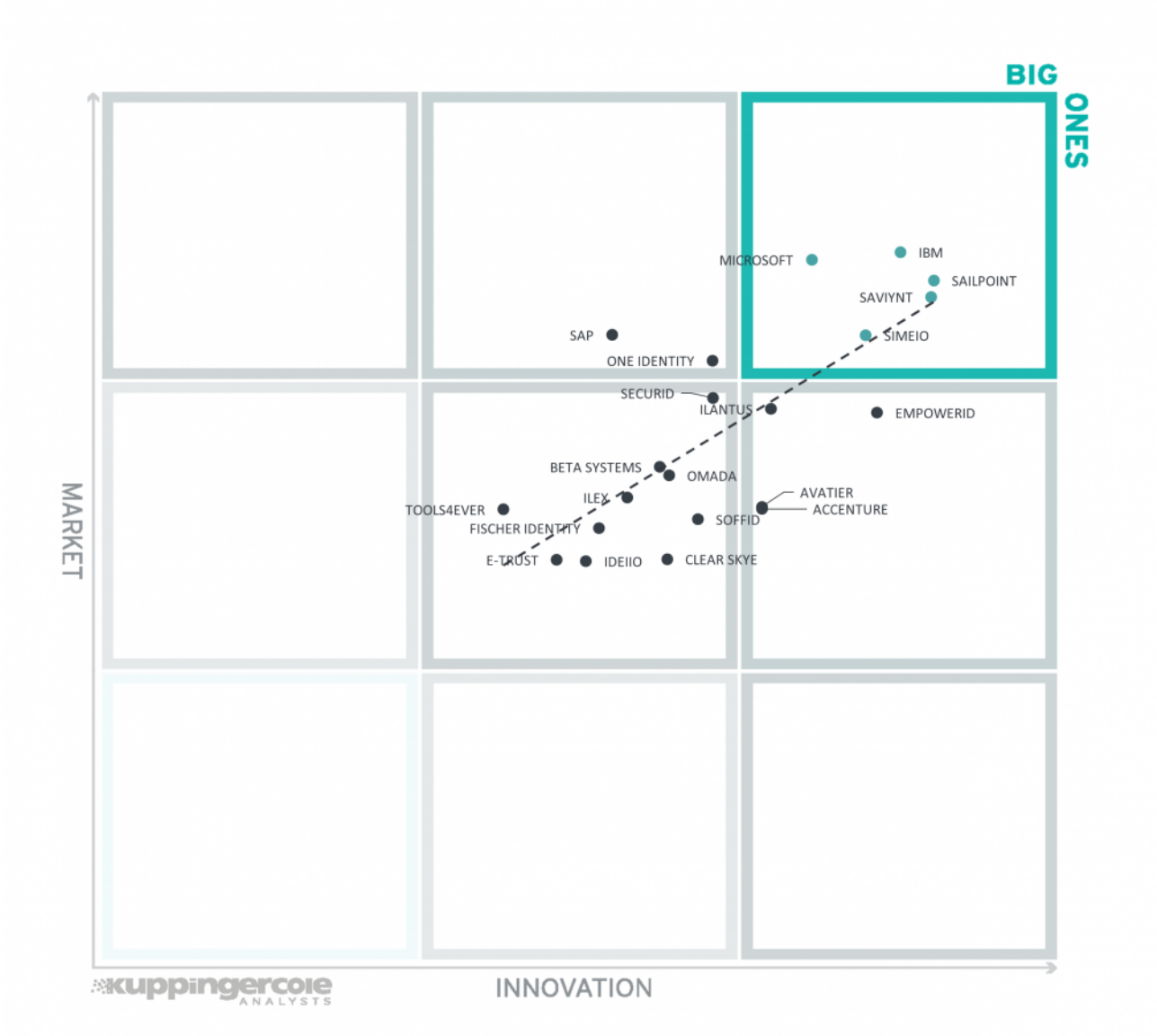


Figure 8: The Innovation/Market Matrix

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

Finally, the Big Ones such as IBM, Microsoft, SailPoint, Saviynt, and Simeio are in the top-right box, with other prominent players in the IT market such as One Identity and SAP being placed left of these.

Below the Big Ones, we find innovative yet not as big vendors, including EmpowerID, Ilantus, Avatier, and Accenture.

In the box to the middle, we find the remaining vendors such as (in alphabetical order) Beta Systems, Clear Skye, E-Trust, Fischer Identity, ideiio, Ilex, Omada, SecurID, Soffid, and Tools4Ever.

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

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

Product	Security	Functionality	Interoperability	Usability	Deployment
Accenture Security Memority	●	●	●	●	●
Avatier Identity AnyWhere	●	●	●	●	●
Beta Systems GARANCYaas	●	●	●	●	●
Clear Skye IGA	●	●	●	●	●
E-Trust HORACIUS IAM SaaS	●	●	●	●	●
EmpowerID	●	●	●	●	●
Fischer Identity as a Service, Managed Identity Services	●	●	●	●	●
IBM Security Verify	●	●	●	●	●
ideiio	●	●	●	●	●
Ilantus Compact Identity	●	●	●	●	●
ILEX IAMaaS	●	●	●	●	●
Microsoft Azure Active Directory	●	●	●	●	●
Omada Identity Cloud	●	●	●	●	●
One Identity Manager	●	●	●	●	●
SailPoint Identity Platform	●	●	●	●	●
SAP Cloud Identity Access Governance	●	●	●	●	●
Saviynt Enterprise IGA	●	●	●	●	●
SecurID Governance & Lifecycle Cloud	●	●	●	●	●
Simeio Identity Orchestrator	●	●	●	●	●
Soffid IAM	●	●	●	●	●
Tools4ever HelloID	●	●	●	●	●
Legend		● critical	● weak	● neutral	● positive ● strong positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Accenture Security	positive	weak	strong positive	neutral
Avatier	positive	neutral	positive	neutral
Beta Systems	positive	neutral	positive	neutral
Clear Skye	positive	weak	neutral	neutral
E-Trust	neutral	weak	neutral	neutral
EmpowerID	strong positive	positive	positive	positive
Fischer International Identity	neutral	weak	positive	neutral
IBM	strong positive	strong positive	strong positive	strong positive
ideiio	neutral	weak	neutral	neutral
Ilantus Technologies	positive	positive	positive	positive
ILEX International	positive	neutral	positive	neutral
Microsoft	positive	strong positive	strong positive	strong positive
Omada	positive	neutral	neutral	positive
One Identity	positive	neutral	positive	strong positive
SailPoint	strong positive	positive	strong positive	strong positive
SAP	positive	positive	strong positive	strong positive
Saviynt	strong positive	strong positive	positive	strong positive
SecurID	positive	neutral	strong positive	strong positive
Simeio Solutions	strong positive	strong positive	positive	positive
Soffid	positive	weak	neutral	positive
Tools4ever	neutral	neutral	positive	neutral
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

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

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 categories:

- User Lifecycle Management
  Management of user accounts and access entitlements across a multitude of IT systems providing the mechanisms for creation, modification and deletion of users and associated account information across the target systems and applications through the Joiners, Movers and Leavers (JML) process.
- Identity Provisioning
  Provisioning identities and access entitlements to target systems. This involves creating and managing accounts in such connected target systems and associating the accounts with groups, roles, and other administrative entities to enable entitlements and authorizations in the target systems in an automated way. This includes connectors to target systems, links to identity repositories, or a reconciliation engine for identifying unauthorized changes in the target system, as examples.
- Access Governance
  The solutions ability to implement controls to govern access management which includes access warehouses, access request management, access review, access certification, role management, and SoD (Segregation of Duties) controls.
- Access Intelligence & Risk
  Providing a level of access and risk intelligence using analytics, AI/ML, role discovery or mining, assistance in incident analysis and remediation, risk-based analysis of identity events, user activity monitoring, or support for container-based microservice-related deployment model as examples.
- Workflows
  The level of workflow support for decision-making processes or event execution such as access request and approval processes, role lifecycle management, or assigned risk scores that invoke relevant access workflows and can be configured to the specific customer's demand without coding.
- Architecture

This category looks at architecture such as modern, modular architectures based on microservices, multi-tenant public cloud services, or level of API support, for example. This also affects deployment, given that container-based deployments provide good flexibility, as well as the ability to interoperate with other solutions via APIs, SDKs, and standard protocols as some examples.

- IDaaS Deployment
  This reflects the IDaaS deployment characteristics such as supported data centers (DC) throughout the world, multi-tenancy, failover capabilities, DC capacity, performance monitoring, IDaaS DC security certifications, or time to deploy the on-premises components.

- Technology Integrations
  This reflects the level of technology integration support to other solutions and extension of capabilities such as ITSM, SIEM, DAG, GRC, UAM, or other COTs tools. Also considered is the solution's ability to reach back to on-premises resources and legacy systems.

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 Security

Accenture Memority is provided by a unit within Accenture delivering an IDaaS solution. Memority started as an independent software vendor and has become part of that larger group three years ago. Accenture Memority is an IDaaS solution that supports both IDaaS IGA and IDaaS AM (Access Management) use cases. It supports all major feature areas, from Identity Lifecycle Management and Access Governance capabilities to Access Management, Single Sign-On to cloud services, and Adaptive Authentication.

Over time Accenture Memority has increased its capabilities and now comes with a broad range of features and good standards support. In IGA, while providing a range of connectors to systems out-of-the-box, the differentiation to other vendors stems from advanced capabilities such as the elaborated delegation management models supported, from the integrated capabilities for privacy and consent handling, and Identity Relationship Management features. Identity repositories storage is fully integrated into the Memority solution without options to integrate with other third-party popular directories servers, databases, or virtual directories solutions. Good support for attribute mapping and synchronization between source to target systems is given, and SCIM for identity provisioning/de-provisioning is also provided. Integrations to ITSM solutions are limited to ServiceNow and not provided out-the-box but must be configured.

Accenture Memority UI allows for highly customized dashboards when requested. User self-service includes a service catalog with a shopping cart-based end-user search, an access request, and approval workflows which can be configured to orchestrate self-service access and registration validation process with step-by-step information filling process, for example. IGA related reporting capabilities are given, such as analytics trend analysis, attestation, delegated access, or privileged access as some examples, although missing reports for major compliance frameworks OOB. Baseline Access Governance capabilities are given but lack advanced features such as role discovery, advanced intelligence anomaly, or outlier detection through AI/ML. Good support for auditing and forensic capabilities to aid security incident analysis in which administrators can query audit trails with its self BI feature. Memority supports integration with SIEM solutions that integrate with Syslog, AWS S3 (ex. Splunk, Micro Focus ArcSight), AWS SQS (ex. Splunk), or FTP.

Accenture Memority has a modular architecture that allows flexibility to adapt to a wide range of customer use cases. The architecture provides for selecting distinct capabilities that are required but also for adding new capabilities quickly. This is supported by the strong focus Accenture Memority has put on delivering a consistent and comprehensive API layer as part of its solution. Thus, digital services can build on that platform and consume central Identity Services. Both REST-based APIs to all Memority functionality and OAuth/OIDC for application federation use cases are supported, although legacy application support using SOAP APIs is missing. For DevOps, only Android and iOS SDKs are provided for integrating Memority Mobile SSO authentication.

Accenture Memority customers are primarily mid-market, and enterprise organizations focused in the EMEA/Benelux region. As part of Accenture Security and with EU-based data centers and a range of datacenter certifications available, Memority is an interesting alternative to other vendors in the IDaaS

market, specifically the ones requiring customization for industry-specific use cases with the support of the Accenture group. Because Memority is part of Accenture and the overall good set of baselines IDaaS IGA capabilities, we see good potential for Memority to improve its role in the market.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●○○

accenture

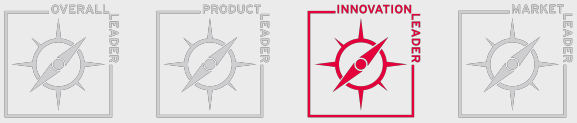
Strengths

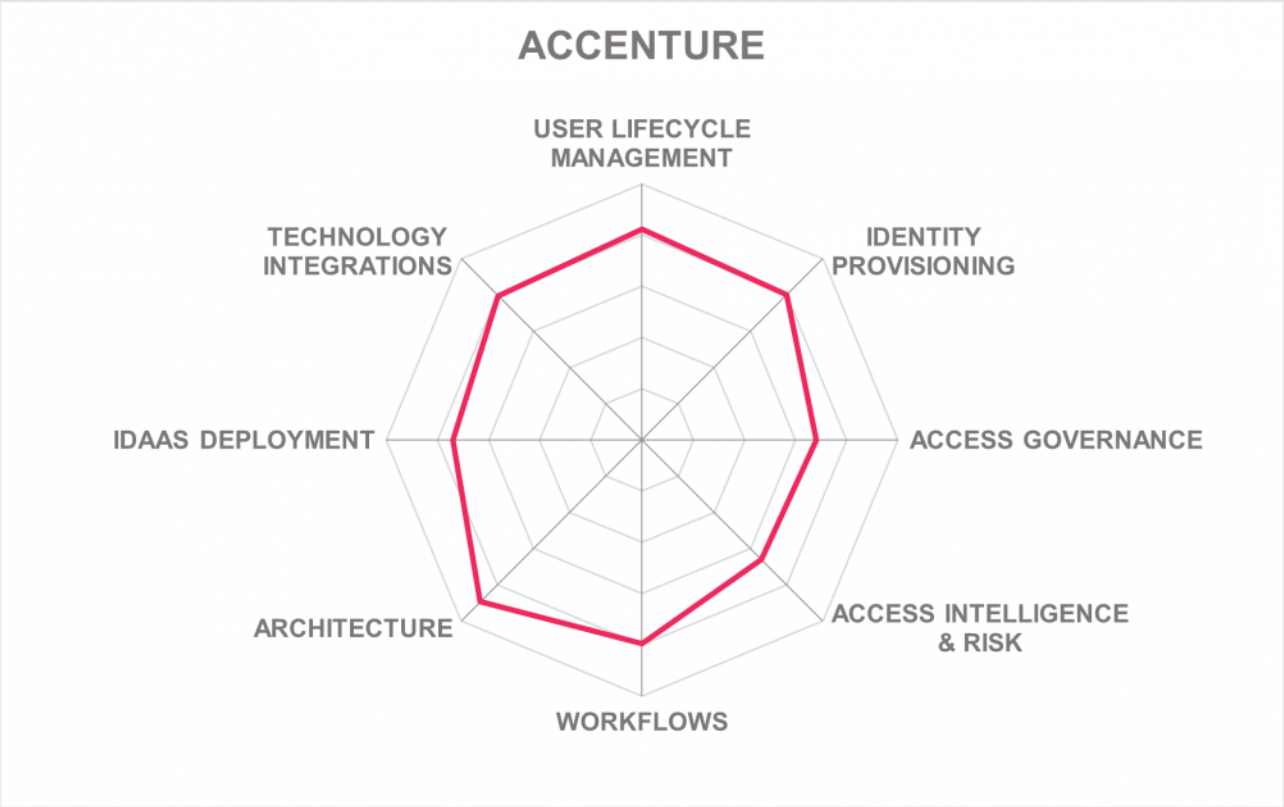
- User lifecycle management
- Modern architecture and API support
- Full IDaaS solution, with on-premise deployments supported as well
- Good user self-service and mobile support
- IGA related reporting capabilities
- Part of Accenture Security, providing global scale
- Proven scalability
- Support for IoT use cases and manufacturing environments

Challenges

- Still low number of customers, but a number of large customers with global deployments
- Lack of visibility in the market
- Access Governance capabilities only a baseline level
- Missing SOAP API support for legacy apps
- Limited SDKs for DevOps support
- Some limitation with OOB integrations to other third-part solutions

Leader in




ACCENTURE
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.2 Avatier

Avatier, based in California (US), is one of the few IGA vendors that have exhibited innovative changes to adapt to evolving market demands in the recent past. From a vendor that focused primarily on providing intelligent user interfaces while lacking the underlying depth of capabilities, Avatier has evolved into a vendor offering comprehensive IGA capabilities with its Identity-as-a-Container platform creating unique market differentiation. Based on Container architecture, Avatier's Identity Anywhere provides a fully containerized IGA platform to solve the deployment and scalability issues of traditional IGA. Avatier SaaS offers subscriptions to hosted or non-hosted functionality such as Password Management, Single Sign-On (SSO), Group Self-Service, Lifecycle Management, and Access Governance.

Identity Anywhere comprises several modules providing a range of IGA functionality. Lifecycle Management is its primary Identity Provisioning component and Group Automation/Self-Service, Workflow Manager, and Identity Analyzer supporting the Access Governance capabilities. Avatier supports SPML and SCIM for identity provisioning/de-provisioning and has a broad set of provisioning connectors available for a wide range of on-premises and cloud systems. Policy management is well supported, with the exception of support for Dynamic Authorization Management (DAM) features.

Avatier delivers a solution with an impressive user interface that extends to mobile devices (IOS and Android) and chat channels such as Skype Slack, Microsoft Teams, Microsoft Outlook, or Facebook Messenger, to name a few. While Avatier has a good breadth of governance features, depth of functionalities could challenge advanced governance requirements of complex IAM deployments. However, the focus on simplifying user interfaces offers a great abstraction of governance features for business users who are commonly unacquainted with technical details. Although Avatier offers a good drill-down of governance details, it currently does not provide a single pane dashboard, although it's on the roadmap. Also provided are well-thought-out self-service capabilities using a shopping cart paradigm allowing users to request access to systems and allowing managers' ability to approve or reject requests via mobile or other communication channels. Real-time control of user behavior in accessing resources is available through audit reports and SSO logging functionality.

Identity Anywhere supports a container-based cloud service that uses a REST API agent on-premises to communicate with on-premises identity stores and on-premises applications. The Identity Anywhere platform is a single container that can support the most popular container platforms and while leveraging microservices for supplemental functionality. Both the Identity Anywhere Agent or container deployed on-premises can support a hybrid environment. Hardware and virtual appliances for on-premises deployment options are not available. SOAP, REST, SCIM, SAML, and OAuth API protocols are supported. SDKs for developers are also available. The majority of Identity Anywhere functionality is accessible via REST APIs as well as some functionality via CLI.

Avatier is a privately held company that focuses on mid-market to enterprise organizations with customers and partner ecosystems located primarily in North America with growth in other regions. Avatier continues to innovate with its user-centric approach to IGA, covering a wide range of governance use cases. Avatier

delivers a rich set of features and integrations to its customers, with a clear emphasis on interfacing to on-premise solutions, and good support, particularly for enterprise-class cloud services. Overall, Avatier's Identity Anywhere container-based platform is an improvement in the IDaaS IGA market.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●○○

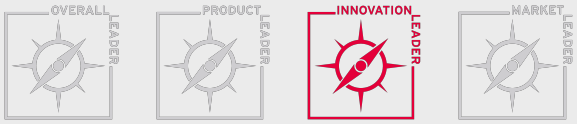
Strengths

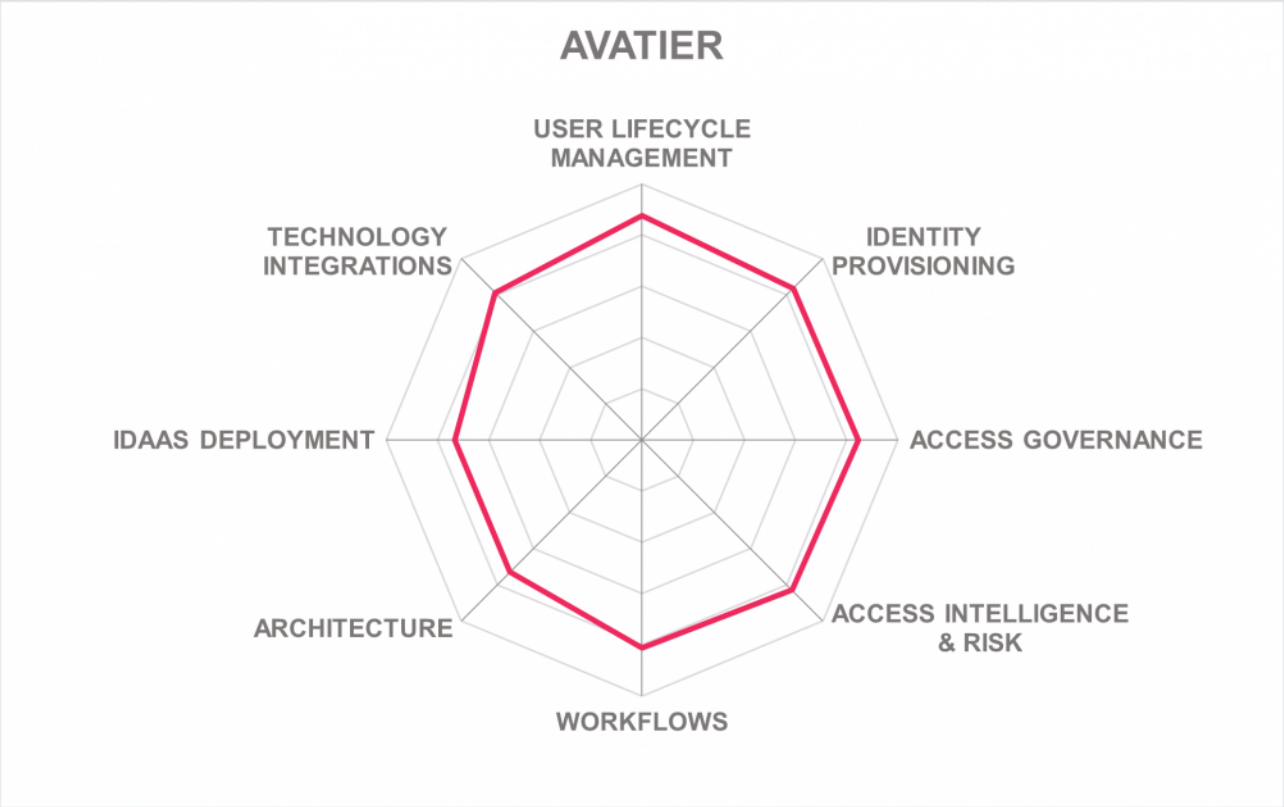
- Innovative, user-centric approach to IGA
- User lifecycle management
- Identity provisioning
- Flexible workflow automation capabilities
- Good reporting capabilities
- Technology integrations
- Workflows
- Access & risk intelligence
- Fully containerized IGA platform

Challenges

- A growing but limited partner ecosystem
- A limited footprint outside of North America
- Limited marketing visibility
- Missing DAM feature support for policies

Leader in




AVATIER
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.3 Beta Systems

Beta Systems, based in Germany, offers GARANCYaaS as a PaaS approach for its Garancy IAM solution. Beta Systems customers can design their IAM system based on a preconfigured standard engine managed by Beta Systems' cloud operation for an IAMaaS operated in the Cloud. Garancy IAM Suite consists of Identity Manager, User Center, Process Center, System Center, Recertification Center, Data Access Governance, Password Reset, and Access Intelligence Manager modules as a comprehensive IGA platform. While the Garancy Identity Manager enables identity administration and fulfillment, Recertification Center, User Center, Process Center, Access Intelligence, Password Synchronization, and Password Reset provide functionality for IGA.

Beta Systems is one of the few vendors offering connectors with full application integration, allowing applications to configure and request authorization decisions at runtime, enabling dynamic authorization management as an integrated feature within the base product. Garancy Process Center (PRC) allows customization of any governance workflow. Customization of attribute mapping between systems is supported through JavaScript. The built-in role management capability allows for the efficient and automated assignment of entitlements. Beta Systems also provides the Garancy Data Access Governance (DAG) module that manages user access entitlements and authorizations for unstructured data at a granular level. The DAG is a separate module but can be integrated with other Garancy modules to offer a complete IGA solution. Access intelligence is given, providing strong reporting and dashboarding capabilities. Reports for major compliance frameworks are available out-of-the-box are also supported. Integrations with ITSM tools include ServiceNow and BMC Helix ITSM.

GARANCYaaS supports a web-based administration UI that uses the Web Start technology for Java-based admin clients but is transitioning to a dedicated part of the Garancy Portal (System Center). With the introduction of the GARANCY 3 IAM Suite and GARANCYaaS, the entire web web-based administration UI and is on its near-term roadmap. Also, the Beta System GARANCYaaS near-term road map supports user self-service requests through a mobile or progressive web app designed for mobile user experience.

GARANCYaaS can be operated on Beta System's own data center service provider in its geographic DACH region and is compliant with German and European standards. Also, Beta Systems is a member of the AWS partner network to be operated in each preferred geographical cluster for international customers. Additionally, Beta Systems supports on-premises, cloud, and hybrid deployments and can deliver its solution as SaaS, virtual appliance, Docker container, or software deployed to a server. Future roadmap items include delivering a Docker container on Kubernetes and used for SaaS as well. For cloud delivery, full multi-tenancy is not supported. Almost all of the solution's functionality is accessible via SOAP or REST APIs, although SDKs are limited to the Java programming language. Also, no functionality is accessible via CLIs, and a developer portal is not available. Good support for self-service and administration authentication is given with more advanced MFA options.

Beta Systems is a mature and publicly list company. It serves primary mid to enterprise organizations with a market focus in the EMEA region and a somewhat small but growing and functional partner ecosystem.

GARANCYaaS, as a PaaS approach to IAM, offers a flexible approach to IAM in the cloud for organizations looking to deploy comprehensive and lightweight IGA capabilities.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ○ ○

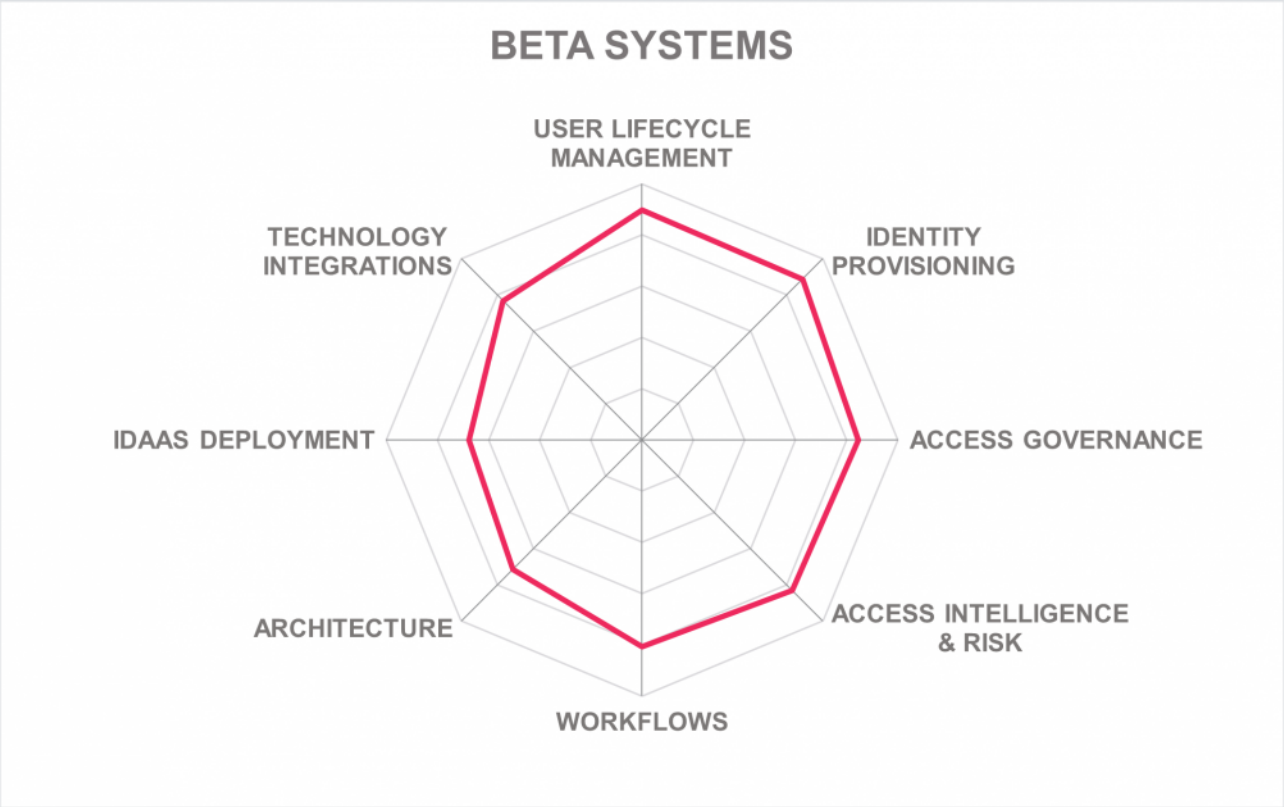
betasystems

Strengths

- User lifecycle management
- Identity provisioning
- Access governance
- Access & risk intelligence
- Self-service support
- Workflow customization flexibility
- Support for Dynamic Authorization Management
- Technology integrations
- Granular Data Access Governance

Challenges

- Primarily focused in the EMEA region
- Somewhat small but growing functional partner ecosystem
- Somewhat limited data centers delivering IDaaS services outside of the DACH region
- Somewhat fragmented admin UI technologies, although moving to a unified approach on the near-term roadmap
- Some DevOps support limitation


BETA SYSTEMS
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.4 Clear Skye

Founded in 2016, Clear Skye is a small privately-owned company headquartered in the San Francisco Bay area. The Clear Skye IGA solution is built on and exists within ServiceNow instead of delivering a separate IGA solution. From a technical architecture, all capabilities are provided on the NOW platform, leveraging standard capabilities of that platform such as the Service Portal, workflow and approval capabilities, and security features. Clear Skye enhances these by adding the IGA specific functionalities as a standard product offering.

Clear Skye support and synchronization with a good range of identity repositories. Any Identity can be implemented, and there are no limitations on the attributes or type of Identity that can be modeled. A modest range of OOB provisioning connectors to on-premises systems, although less support for OOB connectors to SaaS systems. Attribute values provisioned across target systems use Clear Skye workflows and connectors. Also, SCIM support for identity provisioning and de-provisioning is given. Since Clear Sky is integrated with ServiceNow, it can build on integrated ticketing and task management for manual fulfillment. IGA related workflows are well provided and flexible. Missing are some advanced access and risk intelligence features such as access modeling, anomaly detection, or various forms of outlier detections for identities, roles, or entitlements. Also missing are some SoD check capabilities. Although strong support for certification, recertification, and event-based micro certification support is given.

Clear Skye's user self-service capabilities support most access request management functionality and use a shopping cart-based approach to search, select and request access. Missing is the user's ability to manage aspects of their profile via the self-service interface. Most evaluated authentication methods can be used for self-service and admin portal access, although step-up authentication supported during administrative sessions is not given. Good IGA related reporting capabilities are available OOB, and custom reports can be created by end-users using low code platform abilities. Missing is support for major compliance frameworks are available OOB.

For cloud delivery, Clear Skye uses the customer's ServiceNow tenant pair since ServiceNow's data centers are arranged in pairs. Clear Skye builds on the ServiceNow MID Server for on-premises applications within organizations, which is the standard approach for connecting ServiceNow with other services running in corporate data centers. Most of Clear Skye IGA functionality is available via SOAP or REST APIs. However, less support is given via SDK and is limited to native JavaScript SDK for the Now platform. They provide integrations via JDBC, Microsoft PowerShell, REST APIs, SOAP, and CSV-based file sharing to connect to target systems such as Oracle databases, Microsoft AD, OpenLDAP, PeopleSoft, SAP, and others. Again, the number of pre-configured integrations is limited. Data centers delivering their IDaaS services are well supported in the North America, EMEA, and APAC regions.

Clear Skye IGA can help organizations with lower barrier IGA products or where existing IGA solutions are manual process intensive. Clear Skye IGA can also benefit customers who would like to leverage their existing ServiceNow investment complementing Clear Skye IGA. Clear Skye delivers a fair level of IGA capabilities out-of-the-box and extends these rapidly, benefiting from the ServiceNow platform capabilities.

However, customers must carefully check whether the available connectors are already sufficient.

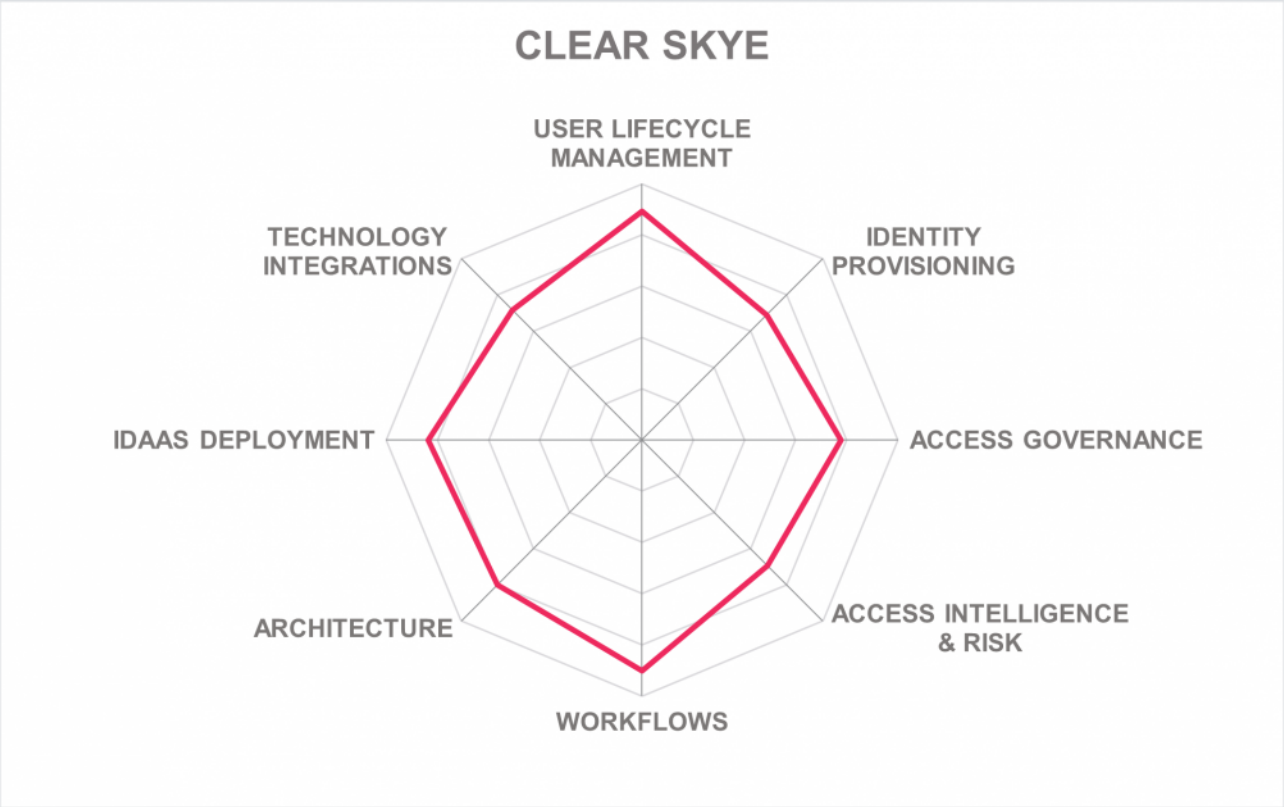
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●●
Deployment	●●●●○

Strengths

- User lifecycle management
- Access governance
- Flexible, adaptable workflows
- Focuses on automated, policy- and attribute-based assignment of entitlements
- Modern UI and dashboards
- IDaaS deployment model
- Fully integrated into the ServiceNow NOW platforms
- Rapid deployment and simple updates based on the ServiceNow platform features
- Full integration into ITSM for access requests and fulfillment

Challenges

- Some common features such as role management and SoD support still lacking
- Limited identity and risk intelligence
- Relatively few connectors to target systems, but well-thought-out integration approach to systems running on premises
- Limited language support
- Still a small vendor with small, but growing partner ecosystem


CLEAR SKYE
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.5 EmpowerID

Founded in 2005 and based in Ohio (US), it provides multiple products in a suite and offers EmpowerID as its IGA product. All services build on a common platform but are provided as distinct services within the IDaaS portfolio of EmpowerID and are one of the few vendors in the market delivering a comprehensive IAM Suite covering all areas of IAM. The EmpowerID Identity and Access Management product suite includes Identity Lifecycle Management, Advanced Identity Lifecycle Management, Group Management, Dynamic Group Management, Password Management, Multi-factor Authentication, Risk Management, Advanced Risk Management, Access Recertification, Role Mining, Policy-Based Access Control (PBAC), Azure Identity Manager, Azure RBAC Manager, Virtual Directory (LDAP), Core Services: RBAC/ABAC/PBAC authorization, Workflow Engine, Audit & Reporting, and Identity Warehouse.

For the traditional IGA model, EmpowerID is built on an identity warehouse, which is an inventory of an organization's systems. EmpowerID provides a good set of out-of-the-box (OOB) connectors to identity repositories. OOB on-premises systems are extensive with deep SAP connector options. Connectors to SaaS systems are less extensive but include some of the more popular applications. For custom connectors, EmpowerID offers a SCIM 2.0 microservice connector framework that allows developers to build their plugin to a given system. For applications that are not or will not ever be SCIM compliant, EmpowerID offers a SCIM Virtual Directory for those systems, exposing them to Azure as SCIM.

EmpowerID access governance capabilities provide for common governance scenarios, including role management, access certification, auditing, and reporting. However, EmpowerID provides strong role governance features that support role design and SoD compliance. Access certification includes micro-certification and recertification triggers such as access risks, organizational changes, and SoD violations, although more advanced outlier or fraud indicators are not available as examples. Other advanced governance features such as identity analytics and access intelligence support risk-based analysis of identities, role mining, recertification recommendations, and various outlier detections. However, intelligence capabilities such as anomaly and outlier detection are not given. EmpowerID workflow customization offers great flexibility in governance policies and workflow management and provides strong out-of-the-box reporting options and support for major compliance frameworks.

EmpowerID supports a cloud-native SaaS offering. A hybrid environment is also supported with the EmpowerID Cloud Gateway residing on on-premises for connecting to on-premises systems. On-premises deployments are delivered as either a Docker container that can run on Windows or Linux servers or as traditional software deployed to a Windows Server for IT organizations that can't support container orchestrations platforms. For traditional software deployment, Microsoft platform support is required. All of the solution's functionality is exposed via SOAP and REST API primarily. SDKs support Java, .Net, C# and JavaScript programming languages. Other API protocols supported are SCIM, UMA, OData, WebHooks, WebSockets, and Kafka for stream processing. Support for these APIs and specifications such as OAuth and OpenID allow for easy extension of Access Governance features to cloud-based applications. EmpowerID's Workflow Studio IDE supports the creation of custom APIs, Microservices, Functions as Services that can be published and run as containers or on Azure as App Services or Functions.

EmpowerID offers a comprehensive solution with strong IGA and access management capabilities. EmpowerID customers primarily reside in North America and the EMEA regions targeting mid to enterprise-sized organizations. Its partner ecosystem can be considered small, with a concentrated focus in Europe. EmpowerID continues to modernize its platform for cloud-native containerized environments. Built on Microsoft technology, EmpowerID offers distinct integration and performance benefits for Microsoft-centric organizations. EmpowerID is a preferred choice for organizations looking for a comprehensive IDaaS IGA solution with integrated access management features.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

empowerID

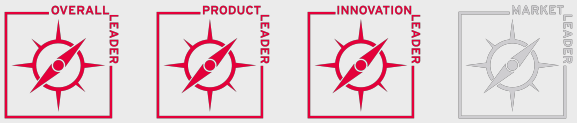
Strengths

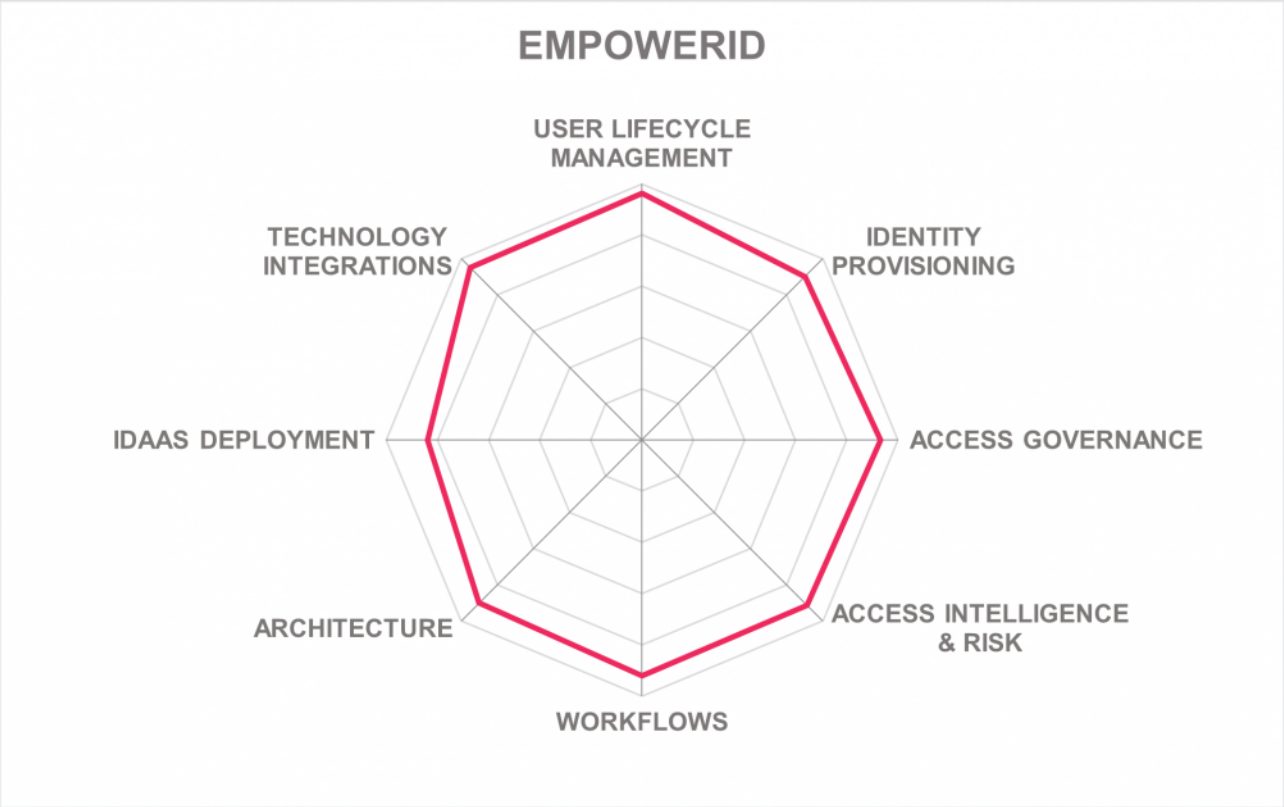
- User lifecycle management
- Identity provisioning
- Self-service and mobile support
- Access governance & review features
- Access & risk intelligence
- Strong workflow capabilities
- Technology integrations
- Modern and user-friendly UI
- Good API support

Challenges

- A small but selective partner ecosystem mostly concentrated across Europe
- Runs primarily on Microsoft platform for non-container deployments
- Missing some advanced IGA intelligence such as anomaly and outlier detection
- Missing more advanced recertification triggers for outliers
- Missing full multi-tenancy support for cloud delivery, although multi-tenancy on microservices is achieved through Kubernetes

Leader in




EMPOWERID
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.6 E-Trust

E-Trust is a privately held company founded in 1999 with its headquarters in Brazil. E-Trust started with a focus on information security. Later in 2006, E-Trust launched their Identity Access & Governance product Horacius. Horacius provides automated user provisioning and access governance capabilities that include access requests, recertification, account mapping, role & SoD management, and advanced features for workflows.

E-Trust offers Horacius Identity & Governance as a common platform for identity provisioning and access governance. The Horacius platform is growing over time to become a mature product offering a spectrum of IGA and specific access governance functionalities. Horacius can handle automated user provisioning, access reviews & attestations, orphan account monitoring, employee and third-party contract termination use cases, and provide auto-discovery capabilities to identify accounts, groups, and group memberships. Horacius supports a range of popular identity repositories and offers good breadth with some depth with out-of-the-box (OOB) connectors for on-premises systems, with less breadth regarding out-of-the-box connectors to SaaS systems. IGA policy management covers the majority of common use cases such as account termination, role modification, access exception approval, rights delegation, and SoD analysis and mitigation, as a few examples. However, policy authoring/editing and testing tools are neither OOB nor integration options to third-party policy tools or engines. Good support for OOB workflows that include registration, orphan account management, account request and review, and SoD, etc., are given. Access governance includes role discovery but missing advanced intelligence capabilities such as recommendations, and risk scoring, while access certification supports event-based micro certifications and triggers to recertify given a user's schedule, SoD violations, and organizational structure changes.

Basic but still modern UI layouts are given with a web interface that includes scorecard tiles for identities that are managed, active, as well as managed profiles or pending tasks. Graph widget can also show graphs over time for automatic access grants, revocation, or password resets, as some examples. Navigation through their functional screen is laid out in a user-friendly way. User self-service support with a shopping cart-based approach to search, select and request access. Horacius offers basic, mobile, and biometric authenticator options for user self-service and admin portal access.

E-Trust supports a single-tenant cloud on AWS, on-premises, and hybrid deployments. Horacius IGA is delivered as either a virtual appliance or a container-based that supports Docker and rkt (Rocket) container-based platforms, SaaS, or a managed service. Horacius provides REST and SOAP APIs to connect to third-party solutions for encapsulated identity requests, access functionality, and connecting to external AI, Analytics, or fraud services for additional functionality. SPML is currently supported. With E-Trust's latest release, a SCIM compatible connector using REST JSON is given as well as SCIM compliant integrations with popular applications such as Azure SCIM API, Slack SCIM API, Facebook Workplace SCIM API, and others. No SDKs, CLI, or developer portal for DevOps support are available at this time. ITSM related integration supports both HP OpenView and JIRA third-party solutions.

E-Trust is continuing to gain good momentum over the last few years. E-Trust customers are primarily

medium to mid-market, although making inroads into some enterprise-level businesses within the Latin America region. E-Trust shows a particular strength regarding workflows and is a good fit for organizations with average IGA requirements to satisfy the most common identity lifecycle administration use-cases with customers focused on the Latin American region.

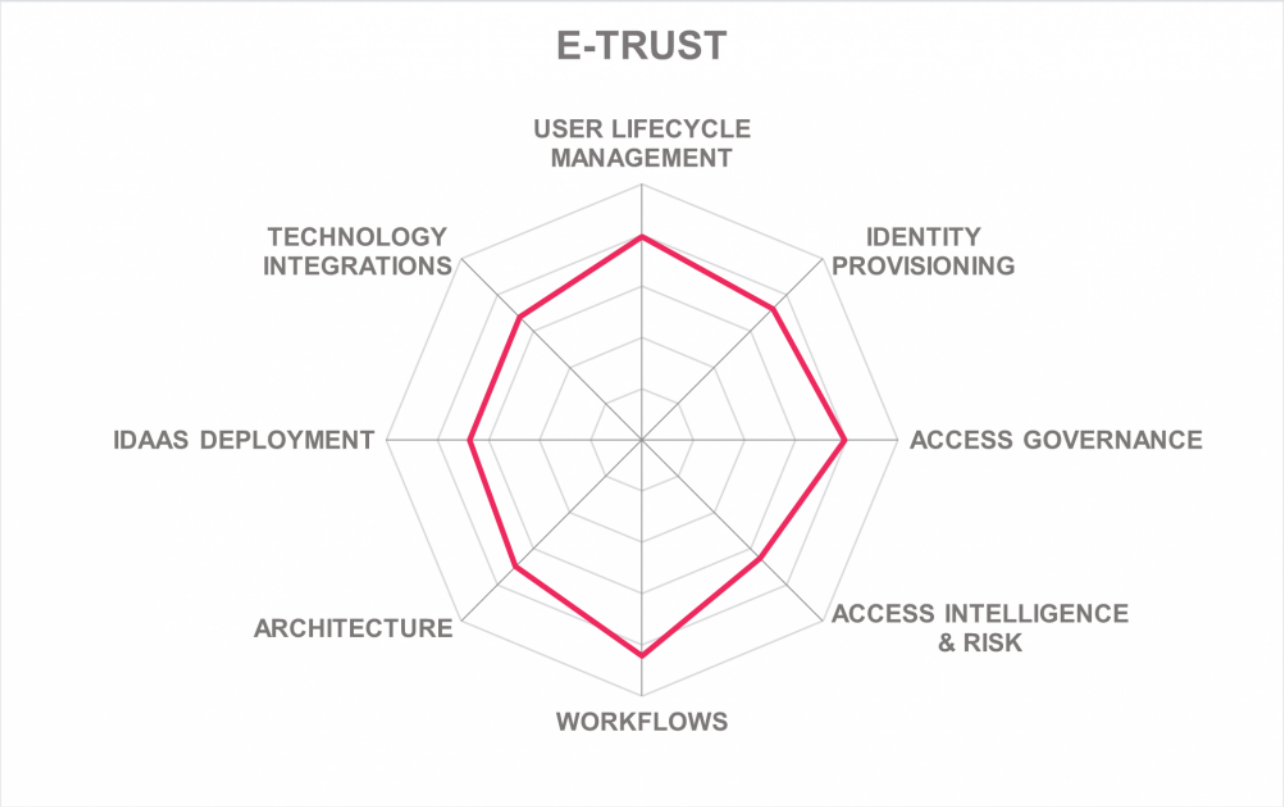
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●○○

Strengths

- User lifecycle management
- IGA policy management
- ITSM and other integrations
- Centralized governance UI
- Reporting
- Provides REST & SOAP APIs to almost all functionality and services
- SCIM connectors & SCIM compliant integrations with popular applications

Challenges

- Small partner ecosystem concentrated in South America
- Based on premises solutions, single-tenant SaaS deployment
- Somewhat limited OOB identity & access intelligence
- Some limitations of OOB connectors to SaaS systems
- Limited DevOps support for SDKs and access to functionality via CLIs


E-TRUST
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.7 Fischer International Identity

Fischer Identity is a vendor that is different from all other traditional Identity Management vendors. The company from the very beginning focused on SaaS delivery models for IAM as a primary 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 has given Fischer a head-start for SaaS deployments, including full multi-tenancy support.

Fischer Identity supports the most popular identity repositories with synchronization of user attributes across heterogeneous IT environments. Strong support for out-of-the-box (OOB) provisioning connectors to on-premises systems is given, with fewer OOB connectors to SaaS systems. Strong workflow support and automated identity lifecycle management are also available. Both access and event-based micro certification are provided with recertification triggers based on schedules, organization changes, outliers, or custom triggers. Good IGA policy management supports RBAC and ABAC-based authorization, allowing identity attributes to be used within access policies. Moderate SoD capabilities are included, but more advanced SoD risk analysis across roles or SoD checks embedded in role creation and user provisioning processes are unavailable. ITSM integration options include ServiceNow and Cherwell.

The Fischer product gives support to IGA related reports that are available out-of-the-box (OOB), such as access risks, accounts, analytics trend analysis, SoD, as an example. Still, it does not come with OOB reports for major compliance frameworks like HIPAA, CCPA, NIST SP 800-53, PCS DSS, or SOX. Fischer Identity SaaS user self-service UI is more modern than its on-premises admin UI. However, the consolidation of UIs is on the near-term roadmap. Fischer Identity suite does not support a native dashboard. It provides customers with structured queries for data to feed their existing analytics engines, although Fischer Identity will use Tableau for dashboarding in the future. Fischer's analytics and access intelligence are built into its reporting capabilities.

Fischer Identity has a SaaS-ready design approach that can support a hybrid environment. Their SaaS delivery model is supported by several CSPs and partners, including Wipro as a global partner. Supported data centers (DCs) delivering IDaaS services are primarily focused in North America with a minor presence in the APAC/ANZ region. The solution can also be delivered as a Docker container or as software deployed to a server. Its Global Identity Gateway provides a communication channel between the customer's premises and the cloud data center for on-premises support. Fischer has a good strategy for integration, supporting both an ETL-based approach and a comprehensive set of APIs with some functionality available via SOAP and REST APIs, although access via CLIs is not. SDKs and a developer portal are not available. Support for SPML is available, although support for SCIM is not.

Overall, Fischer provides an interesting approach to IDaaS IGA, supporting both on-premise and SaaS deployments. For organizations focused in the North American region looking for straightforward customization while avoiding coding overhead, Fischer Identity IDaaS IGA offers a comprehensive IGA suite suitable for customers across most industry verticals, particularly education.

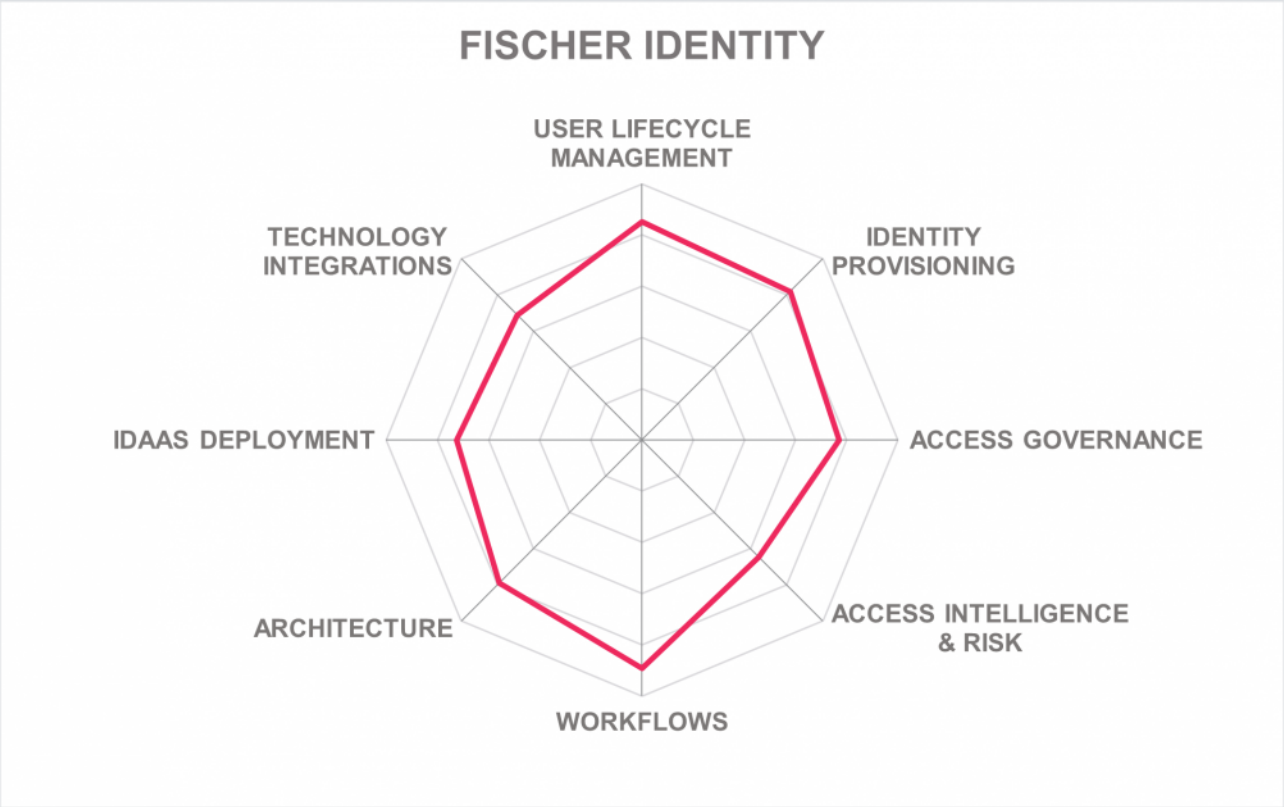
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●○○

Strengths

- User lifecycle management
- Identity provisioning
- Access governance
- Strong workflow support
- User self-service
- IGA policy management
- Strong multi-tenancy support, suitable for managed IGA service providers
- Cost effective delivering fair value

Challenges

- Customer base is primarily in the North America region
- Relatively small but growing partner ecosystem
- Somewhat limited access & risk intelligence
- Missing SCIM support
- DCs delivering IDaaS services are focused in North America


FISCHER IDENTITY
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.8 IBM

IBM has been evolving its IGA product line over the years. For years, IBM Security/Tivoli Identity Manager (ISIM/ITIM) had been one of the more mature products in the market, which preceded Security Identity Governance & Intelligence (ISIGI). At the time, IBM has integrated Identity Provisioning capabilities of ISIM with the Access Governance capabilities of the IDEAS platform acquired from CrossIdeas some years back into ISIGI and added additional features to enhance these. More recently, IBM Security Verify Governance (VG), previously IBM Security Identity Governance and Intelligence (includes IBM Security Identity Manager), and IBM Security Verify SaaS is IBM's current IGA offerings. Through these product iterations over the years, IBM has remained one of the largest and preferred IGA vendors for large-sized complex IGA deployment.

IBM Security Verify Governance is offered as a single comprehensive solution (Enterprise Edition) and separately as modules. The Lifecycle Module provides applications and users onboarding, automated account provisioning and password management, access request with role & attribute-based access control, and audit & reporting. It also supports a well-selected set of identity repositories connections. SCIM support is given for identity provisioning/de-provisioning. Java and JavaScript languages are available to support attribute mapping expressions. A good set of out-of-the-box (OOB) provisioning connectors are available to both on-premises and SaaS systems. The Compliance Module gives good support to access reviews and certification campaigns, and event-based micro certifications. Policy management is well supported, except for Dynamic Authorization Management (DAM) features. Also included are automated access revocation fulfillment, least privilege policy configuration and validation, segregation of duties configuration and validation, and compliance reporting. The Role Optimization Module provides role model design, role mining/discovery, simulation capabilities, and role lifecycle management capabilities.

IBM Security provides a good and functional UI, although with a slightly dated look & feel. A Quick insights dashboard provides a consolidated view of governance risk indicators and suggested action recommendations to take. A good user self-service is also given with a shopping cart-based approach to searching, selecting, and requesting access to applications and services or access roles and privileged access. Interfaces to tools holding business process descriptions as a starting point for role/access management and support for advanced analytical functions/business intelligence features regarding Access Intelligence are not given. User self-service is also available via a mobile phone app. A good set of user self-service and administrative authenticator options are given that include passwordless authenticators such as QR code, FIDO2, and FIDO2 U2F. Verify Governance also provides a built-in repository for admin users and allows external user repositories as well. QRadar is required to support reports for major compliance frameworks.

Between IBM Security Verify Governance and SaaS, all deployment models and most delivery options are available, including SaaS, virtual appliance, software deployed to a server. A managed service of Verify Governance is available by IBM security services and through IBM business partners. A container-based delivery option is not offered for Verify Governance, although the Verify SaaS identity analytics solution can be delivered as a Docker container. VG's functionality is available via REST APIs, SOAP, and WebSockets.

Less access to functionality via CLIs is given. The solution's capabilities are available via SDKs, which supports some of the most popular programming languages, including Android, iOS, Java, C/C++Python, and JavaScript.

Overall, IBM Security Verify Governance continues to move its long line of mature IGA offerings in a positive direction with some significant updates. It counts amongst the products that have seen the most substantial evolution over the years, making it a very competitive and interesting offering in the IGA market. IBM also benefits from its own strong professional services and excellent partner ecosystem, plus easy integration within the overall IBM Security product portfolio.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

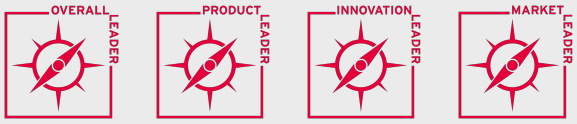
Strengths

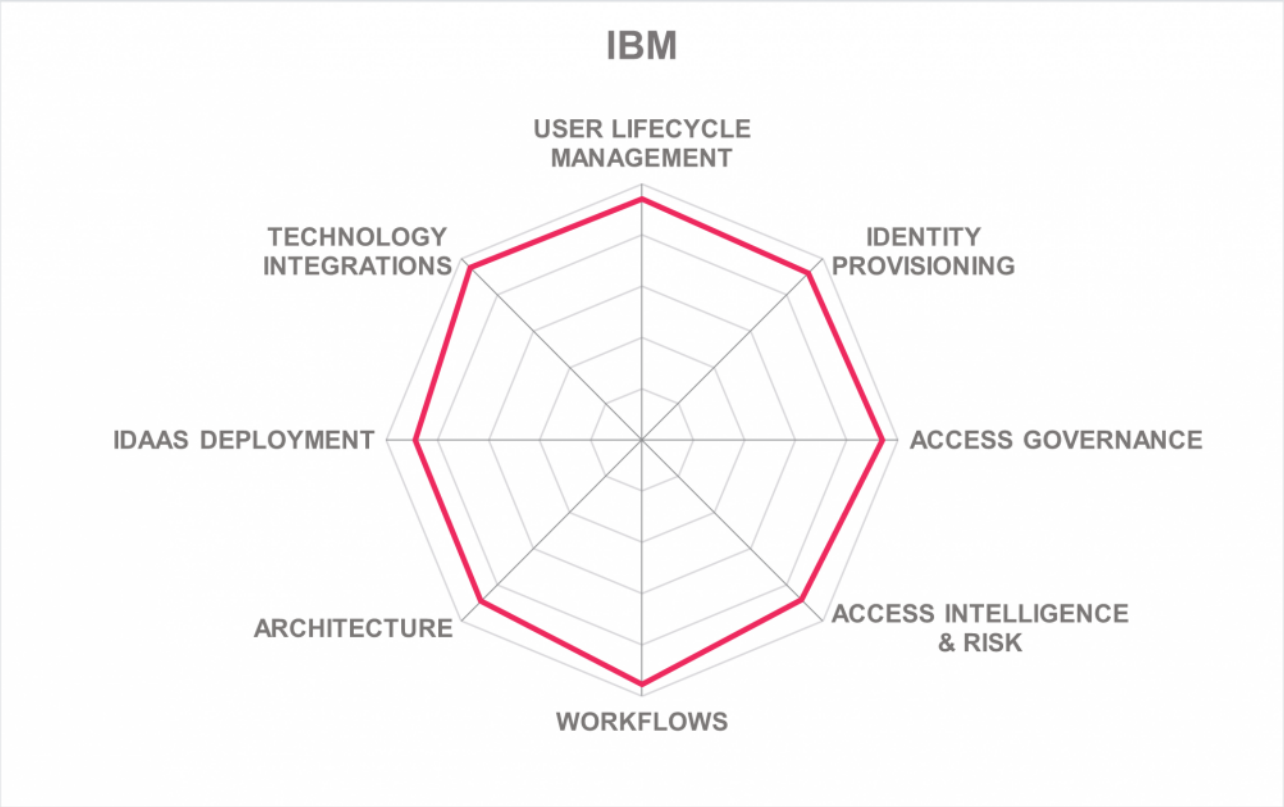
- User lifecycle management
- Identity provisioning
- User self-service and mobile support
- Good access governance and review
- Strong access and risk intelligence
- Flexible workflow capabilities
- Functional and useful UI and dashboard
- Good technology integration support
- Easy integration with IBM Security portfolio
- Strong partner ecosystem and professional services

Challenges

- The user interface has been redesigned in recent releases but still has limited flexibility to customize
- Missing DAM feature support for policies
- Limited reports for major compliance frameworks without QRadar support
- Container-based delivery options are limited

Leader in




IBM
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.9 ideiio

ideiio is a reasonably new vendor in the IGA space; spun out from ProofID - an IAM professional services provider and system integrator based in Manchester, UK, and Colorado Springs, US - ideiio builds upon the pre-existing and mature ProofID IGA product. ideiio has a particular strength in managing external users and B2B/supply chain. The ideiio IGA solution consists of three licensing models: connect, lifecycle and ideiio. ideiio connect links HR and other external sources to IT. ideiio lifecycle includes ideiio connect, ideiio self-service, ideiio people, ideiio partner, and ideiio govern modules. ideiio is designed and developed to meet the IGA requirements primarily of mid-market organizations and has achieved notable success in B2B implementations and the higher education industry.

ideiio supports a wide range of directories servers, databases, or virtual directories used as identity repositories. Out-of-the-box provisioning connectors for both on-premises and SaaS systems are well selected but limited in the range of options. User access self-service includes access and approval workflows with a shopping cart-based approach. Good IGA policy management is available with a built-in policy authoring/editing tool. However, a policy testing tool and integration options for external third-party policy management are not given. Access certification includes event-based micro certifications and scheduled recertification triggers. OOB integrations with ITSM solutions are not available, although currently on its short-term roadmap. With the exception of anomaly detection, missing are advanced IGA related intelligence such as anomaly or outlier types of detection.

ideiio web UI is modern and stylish with basic but functional layouts. Simple graphics for campaign progress overview are available, for example. Unique within the UI is an employee directory providing access to company employees and their contact details. Authenticator options to user self-service and administrative portals are limited and instead, rely on third-party integrations IDPs such as Okta and PingFederate. Good, but basic IGA related OOB reporting includes accounts, attestation, group, privileged access, roles, user access, SoD, and access request & approvers. The more advanced risk or analytics trend analysis type of report is not given. Also missing are OOB reports for major compliance frameworks.

With the options to be deployed in the public cloud (AWS) for IDaaS IGA, ideiio offers the flexibility to be deployed in a private cloud or on-premises environment in a multi-tenant fashion based on the customer's deployment preferences. Other deployment options include on-premises or a hybrid model in which ideiio bridge resides on-premises and management aspects of the solution from the cloud. A hosted managed service is also available through ideiio's partner ProofID. ideiio provides a REST API for identity lifecycle management and most of ideiio Core functionality and configuration. SCIM 1.1 & 2 are also supported, although SOAP and SPML are not. SDKs are available for both Java and PHP programming languages and an SDK to build custom connectors. A developer portal is currently on its near-term roadmap.

ideiio presents a viable alternative to several prevalent IDaaS IGA vendors for SMBs to meet their distinct IGA requirements as well as becoming an established IGA vendor for mid-market to enterprise organizations, although having some areas of improvement to meet some advanced enterprise-level requirements.

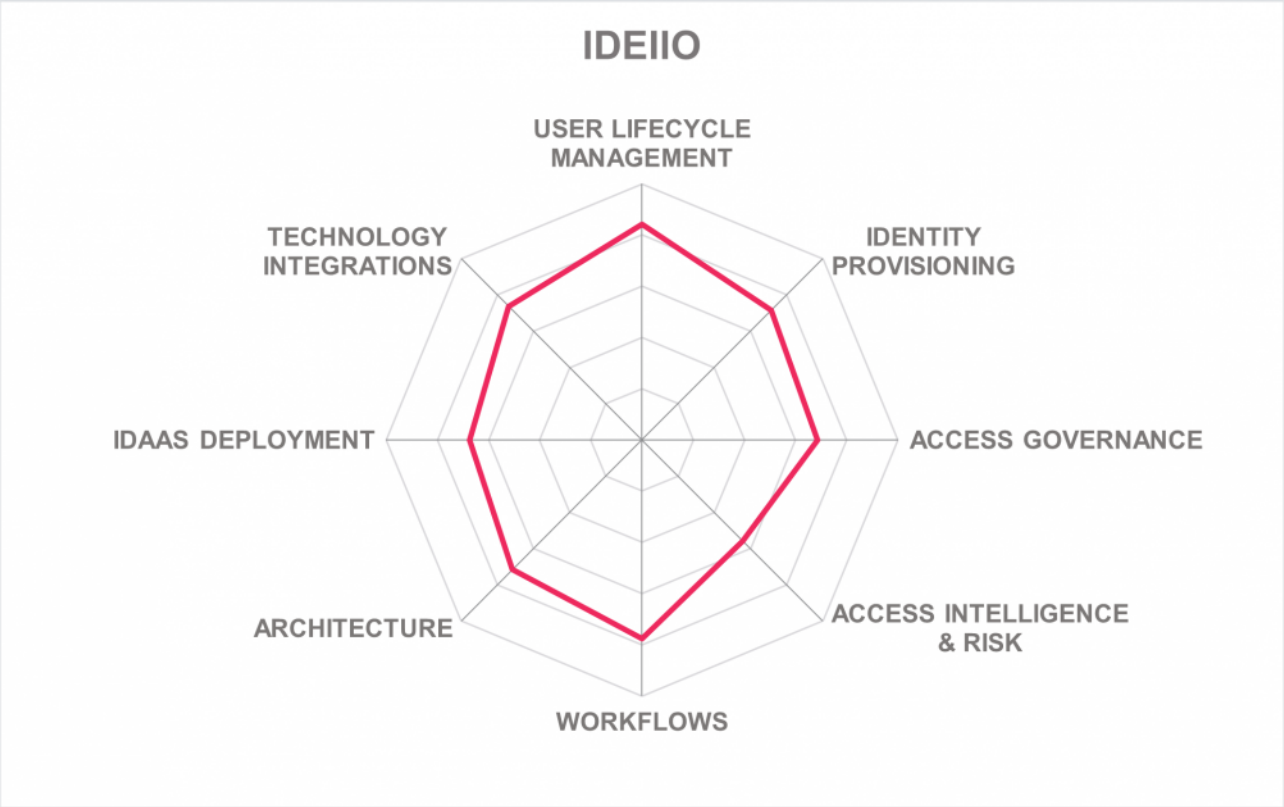
Security	● ● ● ● ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ○ ○

Strengths

- A focused approach to IGA for addressing mid-market IGA requirements
- User lifecycle management
- Workflows
- Policy management
- User self-service support
- Unique employee directory lookup
- Delegated administration support for B2B use cases
- Years of IAM systems integration experience

Challenges

- Limited technology integrations and partner ecosystem, although growing in Europe
- Limited access & risk intelligent capabilities
- Limited user and admin authenticators without third party IDP integrations
- Missing OOB ITSM integrations, although currently on its short-term roadmap


IDEIIO
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.10 Ilantus Technologies

Ilantus, which started as a system integrator, has grown to provide offerings targeted at multiple customer types. Compact Identity offers a risk-aware, Zero-trust framework that provides a fully integrated solution on a single platform. Its multiple services can deliver IGA, Access Management, PAM, and CIAM capabilities from a single codebase that can meet more complex Access Management and IGA requirements market.

In 2018, Ilantus merged all of its product offerings into one single platform. For identity lifecycle management, Ilantus supports a wide range of identity repositories types and good facilitation of the joiner/mover/leaver processes. Also available is synchronizing user attributes across heterogeneous IT environments, attribute mapping from source to target properties, and customizing mapping rules with workflow capabilities for data mapping. JavaScript can be used for mapping expressions. Strong out-of-the-box (OOB) support for both on-premises and SaaS applications is available. When running the solution as-a-service, an on-premises provisioning agent can be installed. The workflow capabilities are flexible and support different registration workflows and access request and approval workflows with additional workflows. For Access Governance, Ilantus delivers good access review support, including multi-level campaigns and other access intelligence capabilities. In addition, Robotic process automation (RPA) capabilities are integrated with SSO and user lifecycle management connectors. Integration with ITSM solutions includes ServiceNow, BMC Helix ITSM, Remedy, and Zendesk.

Compact Identity provides a modern UI that has a simple, easy-to-understand layout that is user-friendly. Ilantus gives good user self-service capabilities with a service catalog shopping cart-based approach, password management, workflows, and even some advanced features such as support for access requests through chatbots or messaging platforms. The Access Management features of the Compact Identity platform provides a strong set of authenticator options for both user and administrators, including BlockID and Cognitive ID options amongst others. Major compliance framework reports are available OOB and strong IGA and AG-related reporting that includes access risk, analytics trends, access related to roles, privileged, SoD, to name a few.

Ilantus supports on-premises, public & private cloud, and hybrid deployment models, which can be delivered as SaaS, virtual appliance, container-based, software deployed to a server, or a managed service. Support for container-based platforms includes Docker, Red Hat, and SUSE. The product is available for IaaS installation on AWS and Azure platforms. A majority of features and capabilities are available via REST APIs. Other API protocols such as SOAP, WebHooks, WebSockets, OData are also supported. CLIs arguments are available for all of the bulk import operations, and SDK support for a wide range of programming languages are available, as well as a developer portal.

Ilantus is a privately held company headquartered in Chicago, IL. Ilantus customers are primarily mid-market in North America, followed by the EMEA and APAC regions, and support a good partner ecosystem. Ilantus Compact Identity offers both Access Management and stronger IGA Access Governance capabilities that should make Ilantus a good candidate for evaluation.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

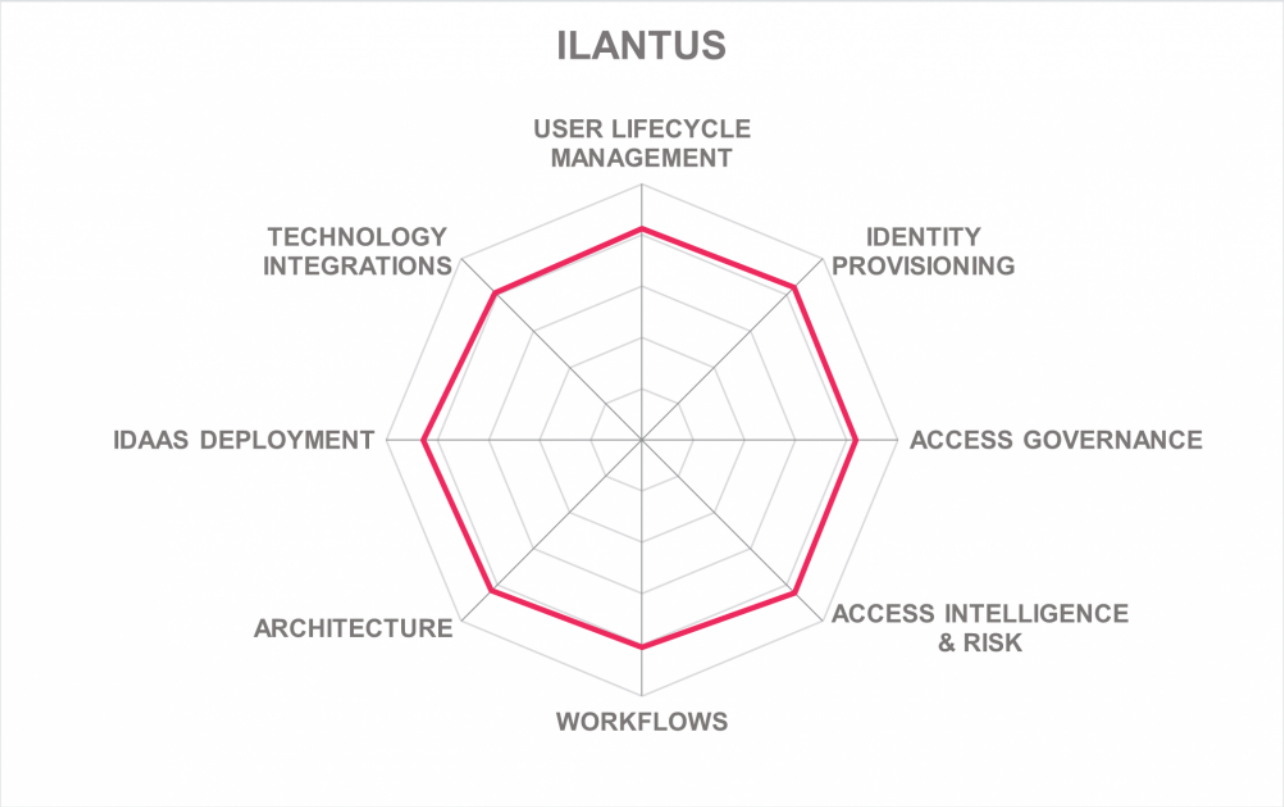
Strengths

- User lifecycle management
- Identity provisioning
- User self-service capabilities
- Access & risk intelligence
- Flexibility for customization including policy and workflow customizations
- Intuitive and user-friendly UI
- Good IDaaS deployment and delivery options

Challenges

- Customer presence is still primarily focused on the US, followed by EMEA and APAC countries
- Customer focus is predominately mid-market, with some growth at the enterprise level
- Backed by private funding with an aggressive growth strategy

Leader in


ILANTUS
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.11 ILEX International

ILEX, a French vendor, offers Meibo Identity Management as its primary Identity Governance and Administration platform, aimed at allowing customers the flexibility to develop their controls for identity lifecycle management. ILEX IAMaaS consists of Meibo People Pack (MPP) and Sign&go. MPP, a pre-packaged version of Meibo Identity Management, primarily focuses on the IGA requirements of SMB organizations that prefer an out-of-the-box solution. Sign&go Global SSO is Ilex's access management solution. While Meibo People Pack (MPP) has a strong Identity and Entitlement Management focus with many IGA features, it is not considered a pure IGA solution. Sign&go provides many Access Management options and, together with MPP, provides the IGA solution evaluated in this report.

Ilex MPP provides identity lifecycle management that supports identity repositories for managing the identities, identity attributes, access entitlements, and other identity-related information. MPP also supports the synchronization of user attributes across heterogeneous IT environments and attribute mapping through its provisioning engine. Auto-discovery capabilities to identify accounts, groups, group memberships are also given. Good support for out-of-the-box (OOB) provisioning connectors to on-premises systems is available. Alternatively, moderate support is given to OOB SaaS connectors. Good workflow features are supported through MPP's workflow engine. Access certification capabilities are provided but lack event-based micro certification and recertification triggers such as access risks, SoD violations, related compensatory controls, or outliers. Also missing are identity and access analytics and intelligence capabilities. OOB ITSM integration includes ServiceNow and EasyVista.

Ilex MPP provides basic but modern user and administration UIs, although a good dashboard of the scope of access review. User self-service management includes basic access request and approval workflows using a shopping cart-based approach to search, select, and request privileged access, roles, and user-based access cloning. Strong authentication options are provided as part of the Sign&go Global SSO solution.

Ilex delivers its solution as SaaS, software deployed to a server for on-premises deployments or a managed service. No container-based options are available, although it's on the roadmap. Its IDaaS offering is relatively new. The SaaS option is hosted with a French cloud provider with both data and support services in France. Ilex does not support a multi-tenant approach within its data center (DC) deployments. Instead, it supports a "one client - one tenant" approach to provide a partition between the various clients of Ilex. Ilex DCs delivering IDaaS services are only available in the EMEA region. The solution is Java/J2E based, providing independence from the OS. Both SOAP and REST APIs allow access to most features, although administration features are not all available via API. Both SPML and SCIM are supported for identity provisioning and de-provisioning. SDK support includes Android, iOS, Java programming languages. A developer portal is not given, but administrative documentation can be accessed online.

Ilex has a good mid-market customer base and a small partner ecosystem, both primarily within the EMEA region with some growth in the APAC region. ILEX Meibo Identity Management can be both - a tool to build a custom IGA solution and an add-on to existing IGA deployments to enhance the overall flexibility. Both

Meibo People Pack (MPP) and Sign&go Global SSO together offer a complete IGA solution. Also, the Ilex SaaS offering is hosted in France, fully compliant with the GDPR and not subject to the American Patriot Act, making it a good alternative solution set to consider in their primary geographic region.

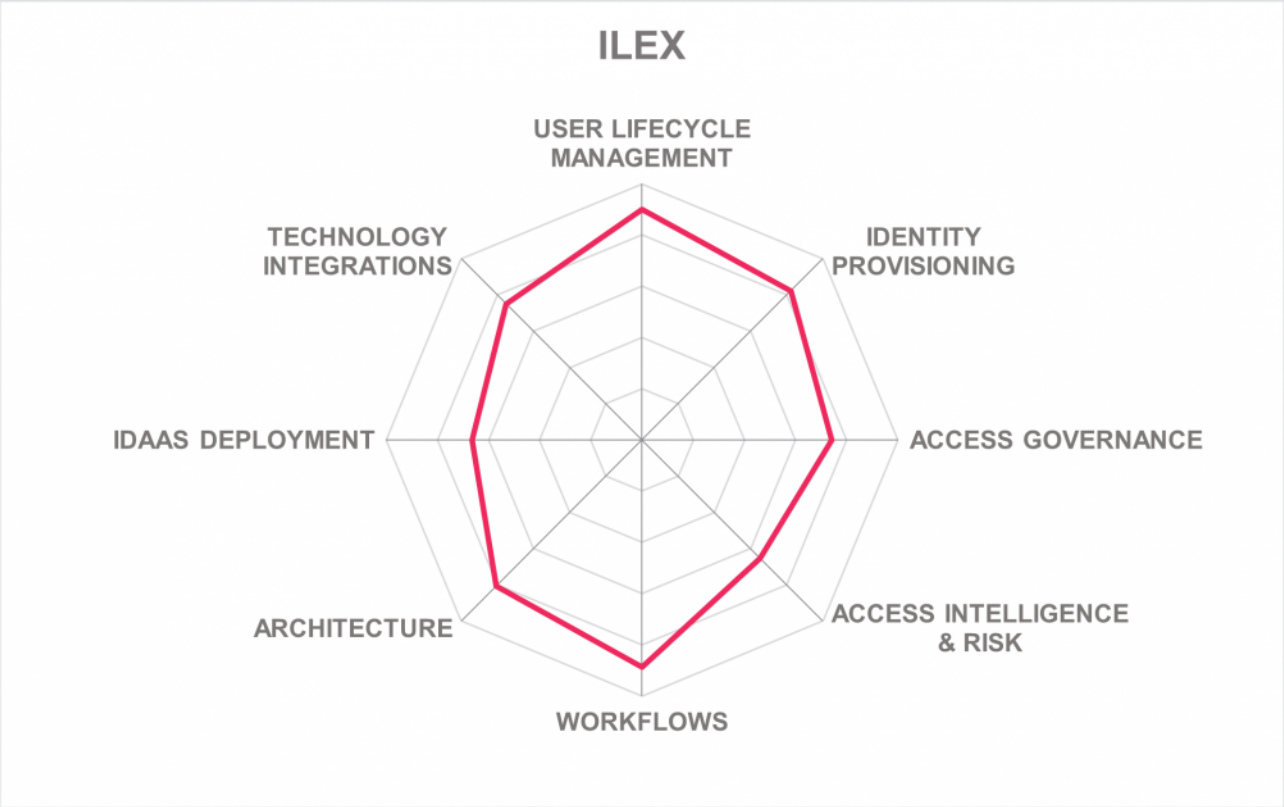
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●○○

Strengths

- User lifecycle management
- Identity provisioning
- Good policy management
- Flexible workflow capabilities
- MFA and adaptive authentication options
- User self-service and mobile support
- Technology integrations
- Pre-packaged solution reducing time to value

Challenges

- Customer and partner base are primarily limited to the EMEA region (France, Benelux, Switzerland and Morocco)
- More advance certification options missing
- Limited access & risk intelligence
- Limited dashboard capabilities
- Missing container-based deployment option, although on roadmap


ILEX
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.12 Microsoft

Microsoft offers Azure Active Directory (Azure AD) as its primary IDaaS platform. Azure AD Connect helps connect on-premises Active Directory (AD) to the cloud and provides 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.

Azure AD provides user lifecycle management support that can source from identity repositories types, emphasizing Microsoft AD and Azure AD. However, Azure AD can use directory data from other directories, databases, HR systems, including Workday, SAP SuccessFactors. Identity data can originate from and be provisioned to other directory and database services, including Oracle directory, Oracle databases, SAP, and many other systems. A wide range of identity types is support. Beyond employee, application, customer, organization, and government identities, machines (e.g., Device, IoT) are also supported. Synchronization of user attributes across heterogeneous IT environments includes HR systems, LDAP directories, databases, files, etc., into AD and Azure AD. From there, apply attributes to SaaS apps and other directories or databases. A good set of OOB on-premises provisioning connectors are given, emphasizing Microsoft-centric application, and an even larger set of OOB provisioning connectors to SaaS systems are available. SCIM for identity provisioning and de-provisioning support is available, and Azure AD provisioning also has an attribute mapping expression language similar to VBA. Bulk or batch importing for identity provisioning is supported through Microsoft Graph, a REST API, or MIM's PowerShell connector.

Policy management for rule-based decisions is available; however, limited in IGA related policies, although Azure AD provides an Azure ABAC integration, currently in preview. For Access Governance capabilities, access certification and recertification campaigns are supported but lack support for event-based micro certification and recertification triggers based on access risk, SoD violations, and related compensatory controls, for example. Also limited is its Segregation of Duties (SoD). For identity and risk intelligence, identity analytics, anomaly and identity outlier detection, and some recommendation capabilities are supported, but missing role mining, access modeling, entitlement, and role outlier detections as examples.

A user self-service UI is well supported with shopping cart-based abilities to search, select, and request access to applications and services. Good IGA related reporting option is available such as auditing and forensic capabilities to aid security incident analysis. Still, it has some minor limitation of JSON only report format, and the major compliance frameworks reporting OOB is limited to GDPR. Azure AD integrates with Azure Sentinel and other SIEM solutions, including ArcSight, Splunk, and SumoLogic. Dashboards of identities and access events are also given and can be customized. One of Azure AD's greatest strengths is its availability with data centers delivering its IDaaS service in each major region of the world. The Azure infrastructure is designed and managed to meet a wide range set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2.

With a large base of active users for third-party apps and active applications integrations makes 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. Overall, Microsoft has continued to increase its position in IDaaS IGA over time, with decreasing limitations. However, customers should be aware that the IGA capabilities are still growing and will continue to evolve. For now, customers should evaluate whether the solution is ready to deliver what they need.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●●

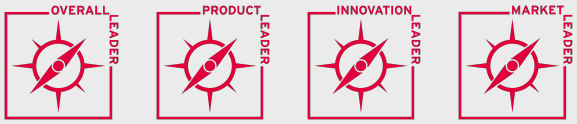
Strengths

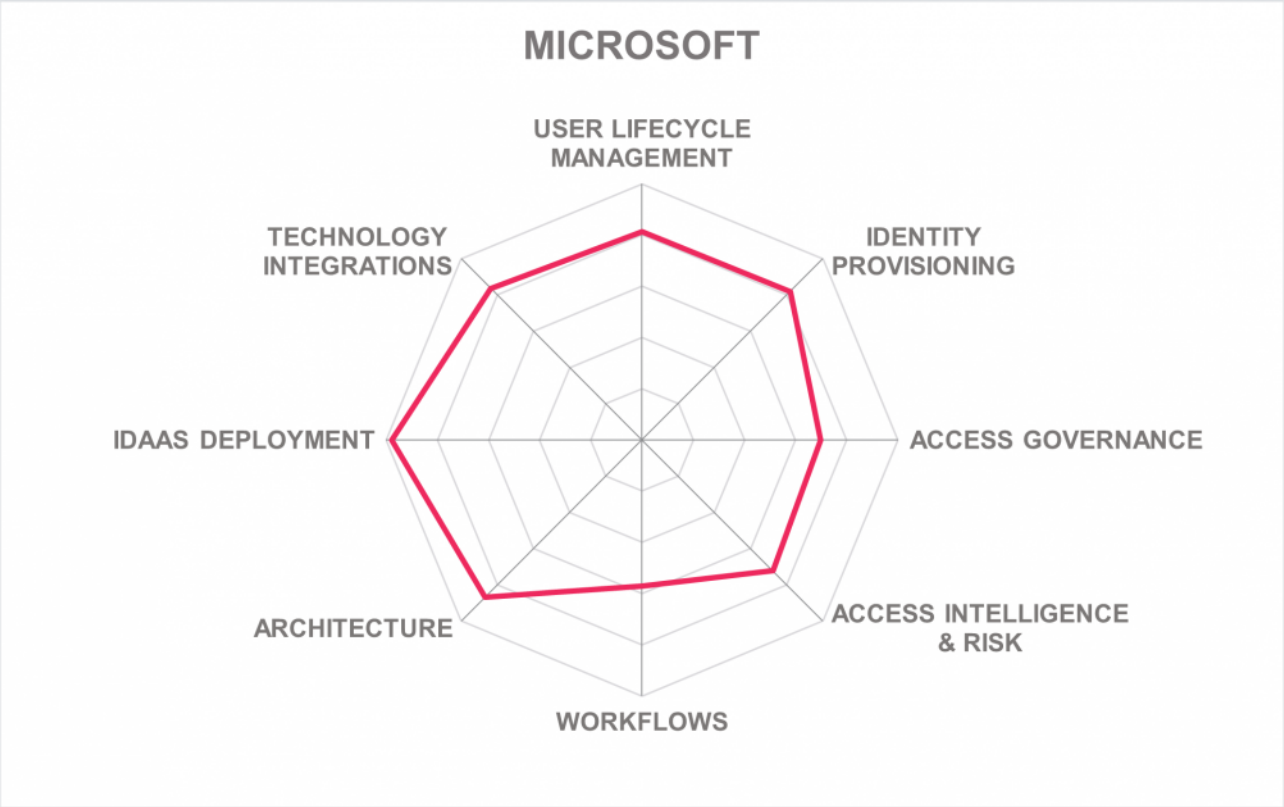
- User lifecycle management
- Identity provisioning
- Baseline access governance
- Strong IDaaS deployment model
- Technical integrations
- Tight integration with on premises Microsoft Active Directory
- Increasingly DevOps friendly with strong developer community support
- Large installed customer base
- Good support for popular SaaS integrations

Challenges

- Limited SoD support
- Limited IGA related policies
- Missing some advanced access & risk intelligence capabilities
- Limited workflow capabilities

Leader in




MICROSOFT
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.13 Omada

Omada, headquartered in Denmark, counts among the established providers of solutions for IGA. Omada provides Omada Identity Cloud for customers wanting a cloud-native SaaS solution - delivering a full range of IGA functionalities with feature parity to on-premises Omada Identity solution. Omada Identity components include an enterprise server portal and services for provisioning, data warehouse, and role & policy engine. Omada customers include organizations in the manufacturing, government, healthcare, finance, transportation, pharmaceutical, and utility market segments.

Omada's identity lifecycle management supports a wide range of different types of identity repositories, and replication to and from any source system directory or SQL database is possible. Synchronization of user attributes across heterogeneous IT environments can be accomplished through attribute mappings and synchronization rules/policies defined within the UI. SCIM support is given for identity provisioning, although SPML is not. A moderate range of OOB on-premises connectors is available, with a less but well-selected set of OOB provisioning connectors to SaaS applications. However, Omada's connectivity factory can configure and build connectivity to any system. Omada uses a semantic data model that gives flexibility in extending or redefining the entities needed to model an organization's IGA domain without developer support. Good IGA related policy management is available, as well as automated remediation of risks. Identity and access intelligence include access modeling, anomaly, entitlement, and role outlier detection capabilities. Omada's Control Policy feature includes automated compliance capabilities that can detect non-compliant situations that automatically react (e.g., terminate risky access, send alerts, trigger recertifications, etc.). Role mining is based on the Microsoft Power BI analytics platform. Out-of-the-box (OOB) ITSM integrations include ServiceNow, and the Omada Relayed Provisioning framework enables integration to ITSM tickets via API.

Omada's UI is modern, with many useful and detailed features. Omada offers good user access self-service capabilities, although more advanced features such as access requests through chatbots or messaging platforms are not given. For user self-service and admin portal access, a minimal set of authenticator options are provided natively. Instead, Omada Identity and Cloud rely on 3rd party IdP for authentication via SAML, and Open ID Connect is supported. Good IGA/AG-related reporting OOB includes access risks, analytics trend analysis, attestation, delegated and privileged access, SoD, and access request-related reports. Beyond delivering an IGA solution, Omada differentiates itself by offering support through standards, implementation methodology, and IGA educational courses. IdentityPROCESS+ provides a best practice framework OOB. IdentityPROJECT+ gives a customer the methodology to implement the solution in a short timeframe. Omada Academy offers classroom or E-learning and training to get up to speed on the solution.

Omada Identity Cloud is its cloud-native SaaS solution. Omada Identity Cloud is multi-tenant, and data is stored in per-customer instances. The data centers (DCs) delivering the Omada IDaaS services are located in the North American and EMEA regions using the Microsoft Azure infrastructure. Support for the APAC region is currently not available. Certifications for its DCs include ISO 27001, ISO 27701, SOC 1/2/3, NIST CSF, PCI DSS, and TISAX. For on-premises deployments, Omada Identity can be delivered as software

deployed to a server or container-based. Omada partners provide a managed service. Also, the solution uses Microsoft SQL Server components for ETL operations, reporting, and data analysis. The majority of Omada functionality is available via its OData (REST) and SOAP APIs. Access to functionality via CLI is not supported. A .NET and JavaScript SDKs are available for customizations. Also, a developer portal is available through the Omada Hub for customer DevOps and partners.

Omada is a privately held company that serves customers in mid to enterprise-sized organizations, primarily residing in the EMEA region, although growing in North America and the APAC region. Omada Identity and Identity Cloud is an attractive IGA solution for mid to enterprise customers that can benefit from Omada's process, project, and training support. With recent enhancements to its product capabilities, such as delivering an enterprise IGA solution as a cloud service, Omada remains a solid contender to traditional players in the IGA and Access Governance market segments.

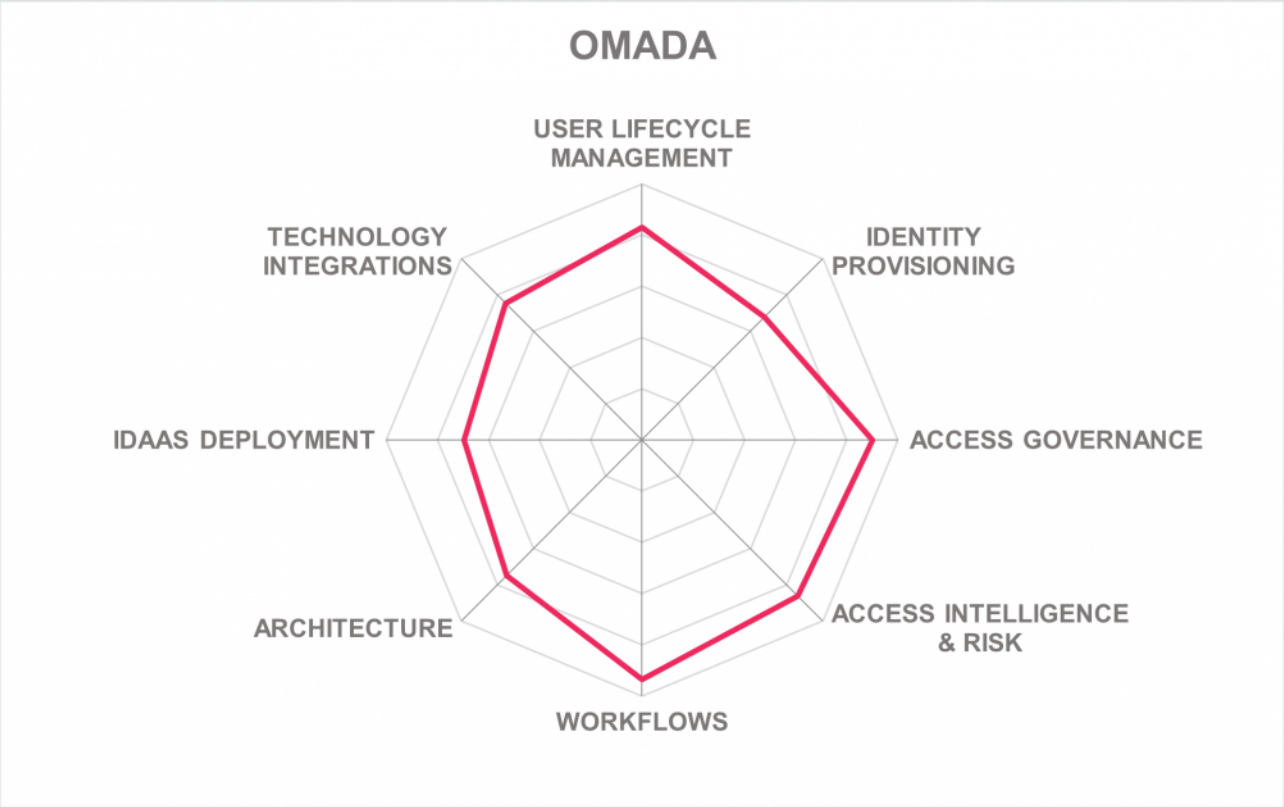
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●○○

Strengths

- User lifecycle management
- Access governance
- User self-service support
- Efficient approach for onboarding new applications
- Good identity and risk intelligence
- Mature solution with strong workflow and role management capability
- Policy management
- Good governance visibility
- Technology integrations
- IGA best practices process framework, implementation methodologies, and training

Challenges

- Good presence in Europe, although limited but growing global reach
- Moderate support of out-of-the-box connectors to on-premises and SaaS systems, although configurable template connectors are available for standard protocols
- Limited authentication options for user self-service and administrative access


OMADA
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.14 One Identity

One Identity, a Quest Software business established in 2004, and based in California, provides an identity-centric security strategy with a broad and integrated portfolio of identity management offerings developed with a cloud-first strategy. Core to One Identity's IGA portfolio is Identity Manager, which provide a single platform for governance and includes identity lifecycle, access request, access certification, auditing, privileged access governance, reporting, and data governance. Identity Manager's capabilities are delivered on-premises, hybrid, or cloud.

Identity Manager can support a wide range of governance use cases that include privileged access, device, microservice related (e.g., Containers, Kubernetes cluster/workload access), APIs, and RPAs. Identity data and life cycle management can connect to a wide range of different types of identity repositories that can synchronize, manage identities, identities' attributes, entitlements, and other identity-related information. However, its own identity repository only supports MS SQL and Azure SQL Managed Instance. Identity Manager shows strength in its data model and attribute mapping from source to target properties, C# and Visual Basic support for mapping expressions, as well as synchronization of user attributes across heterogeneous IT environments. Excellent support for out-of-the-box (OOB) on-premises and SaaS provisioning connectors to target systems. Both SCIM and SPML support is given for identity provisioning/de-provisioning. OOB ITSM integration includes ServiceNow. Besides offering a rich role framework to support complex role management requirements, One Identity also supports dynamic rule-based provisioning to applications with complex role structures.

One Identity provides a modern UI with some unique features, such as a department risk index heatmap that allows drill-downs to more details and 360 overviews of user access and the relationships between applications or even access violations. User self-service is good utilizing a shopping cart-based approach for access requests, features such as the ability to simulate the effect of changes to access entitlements or role definitions remain unique. Additionally, all access request management capabilities are available via mobile devices. Support is given for user self-service and administration authenticator giving several options. Additionally, Identity Manager provides an OAuth/Open ID Connect authentication module to integrate with access management products such as Okta, Ping, and Azure. Identity Manager includes analytics and intelligence base on risk from inheritance and risk from roles. This information is available on dashboard views in reports and indicators in access reviews, for example.

All components of Identity Manager can be deployed on-premise or a public or private cloud. A SaaS model is available in which all components are installed and run in the One Identity Cloud and delivered to the customer. A hybrid configuration requires some components on-premises and some in the cloud. The solution is delivered containerized using Docker, although traditional software deployed to a server is also supported as well as a managed service. Nearly all or solutions functionality is exposed via SOAP or REST APIs. The One Identity API Designer allows customers to create, record, compile and publish a REST-API. SDKs are given for both C/C++ and C# .NET programming languages. PoSH is supported too. Most functionality is accessible via CLI, and a Swagger page and SDK documentation are available as part of the product ISO.

One Identity is a privately held company with a large customer base predominantly in the EMEA region, followed by North America and expansion into the APAC and Latin America regions. It also maintains a good partner ecosystem proportionally in the same areas. Overall, One Identity continues to enhance the product's functional capabilities, establishing itself amongst the leaders in the market. One Identity remains a recommendation from us for evaluation in product selections.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

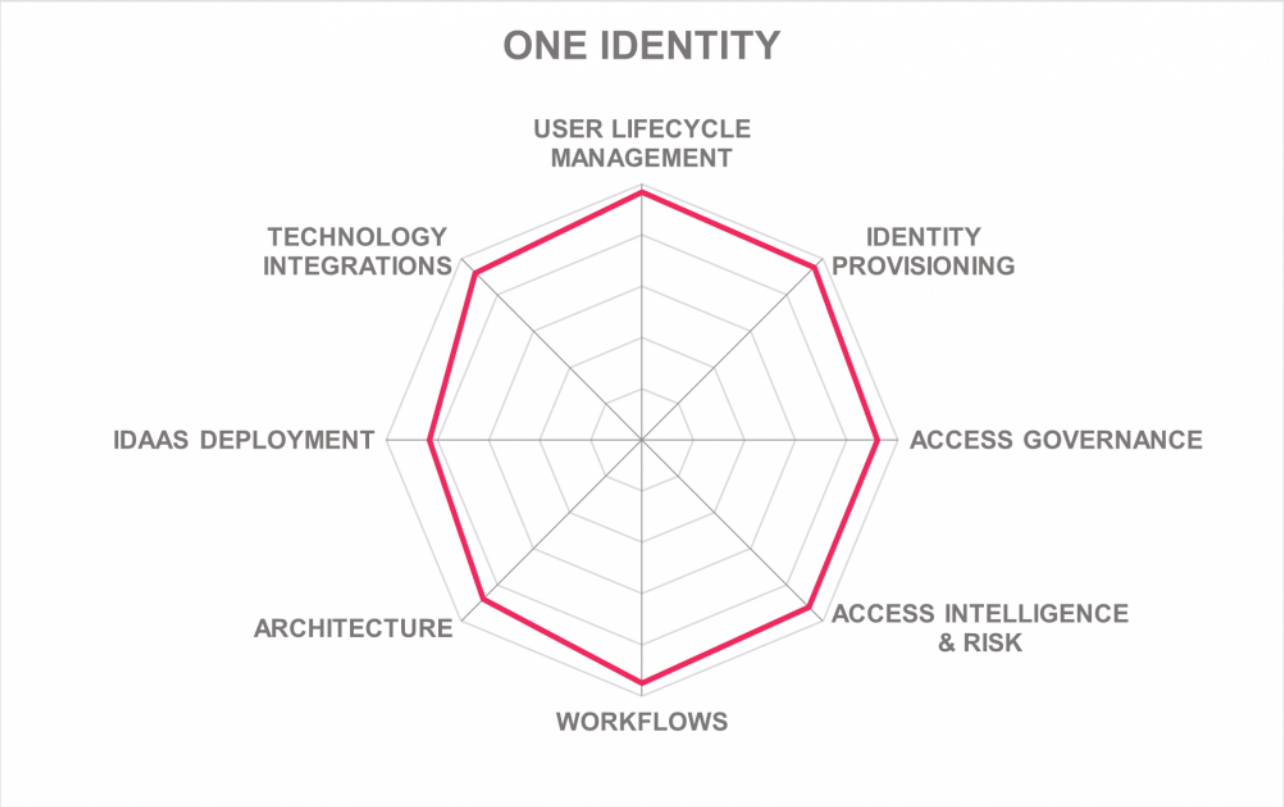
Strengths

- User lifecycle management
- Identity provisioning
- Access governance
- User self-service and mobile option
- Access & risk intelligence
- Workflows and automation
- Technology integrations
- Modern UI with some unique features
- Advanced role management with strong SoD support
- Strong sales and marketing execution

Challenges

- Cloud delivery does not support full multi-tenancy for all components
- Missing continuous monitoring of access compliance and User Activity Monitoring
- Missing access governance support for containers and container orchestration platforms such as Kubernetes

Leader in


ONE IDENTITY
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.15 SecurID

SecurID, an RSA business, is a provider of authentication, lifecycle management, and identity governance security solutions. SecurID Governance & Lifecycle was initially founded as Aveksa in 2004, Aveksa was later acquired by EMC/RSA in 2013. Dell then acquired EMC with RSA in 2016, and more recently, SecurID (RSA) emerged as an independent entity under Symphony Technology Group (STG) last September 2020. SecurID includes SecurID Access (Multi-factor Authentication, Access & SSO) and SecurID Governance & Lifecycle (G&L). SecurID Governance & Lifecycle is its IGA product delivering both Identity Lifecycle Management and Access Governance capabilities.

SecurID Governance & Lifecycle (G&L) offers core IGA capabilities, including automated access certifications, compliance audit reporting and analytics, SoD policy enforcement, rules, and policy management, role management and mining, and data access governance. The solution also automates the user administration process with password management, access requests, and automated provisioning capabilities. SecurID G&L provides a continuous and risk-based access assurance model that utilizes identity and access analytics. SecurID G&L also offers an integration with SecurID Access to deliver integrated access management capabilities for its customers. SecurID G&L shows specific strength in depth and breadth of out-of-the-box (OOB) connectors to both on-premises and SaaS systems. Also, integrations with ITSM tools include ServiceNow, Cherwell, and BMC Helix ITSM.

SecurID G&L offers a good, modern, and user-friendly UI. User access self-service is good, although missing more advanced OOB support for access requests through chatbots or messaging platforms (e.g., slack). However, a web services API toolkit is available for custom integrations. Both identity and access intelligence are visible through basic dashboard graphics and more extensive dashboards available on RSA Link. With SecurID Access, strong authentication options are given for self-service and administration access. A QR Code option is not available, although it's on the near-term roadmap. Passwordless authentication options include Yubico FIDO tokens and Fietian FIDO security keys. SecurID G&L also shows strong support for reporting and OOB reports for major compliance frameworks.

SecurID G&L can be deployed as a hardware appliance, virtual application, software-only, or bundled. It can also be delivered as a Docker container model. Additionally, a set of database views are available for customers requiring data access views. In addition to on-premises deployment options, SecurID offers feature parity between its on-premise functionality and its cloud-based offering. Cloud delivery is currently a single tenant model with some limited data centers delivering IDaaS services in the APAC and the EMEA regions. Also, the solution provides managed services and operational services as a part of SecurID G&L Cloud. In addition to the user interface, SecurID provides access to over half of its solution functionality via REST-based APIs. SDKs are only available for Java and JavaScript programming language with much less access to the functionality than their REST-based APIs. SPML and SCIM support is available for identity provisioning/de-provisioning. RSA Link also provides an interactive community portal for product, engineering, services, support, and other information.

SecurID security maintains a substantial global customer base in mid to enterprise-level organizations.

SecurID's dominance of GRC and authentication markets have helped SecurID cross and upsell SecurID G&L for IGA. Further, SecurID G&L takes a risk-based approach to Access Governance. SecurID G&L is a good choice for organizations with existing deployments of SecurID products and has primary IGA requirements for identity task automation, Access Governance, and identity & access intelligence while avoiding extensive customizations.

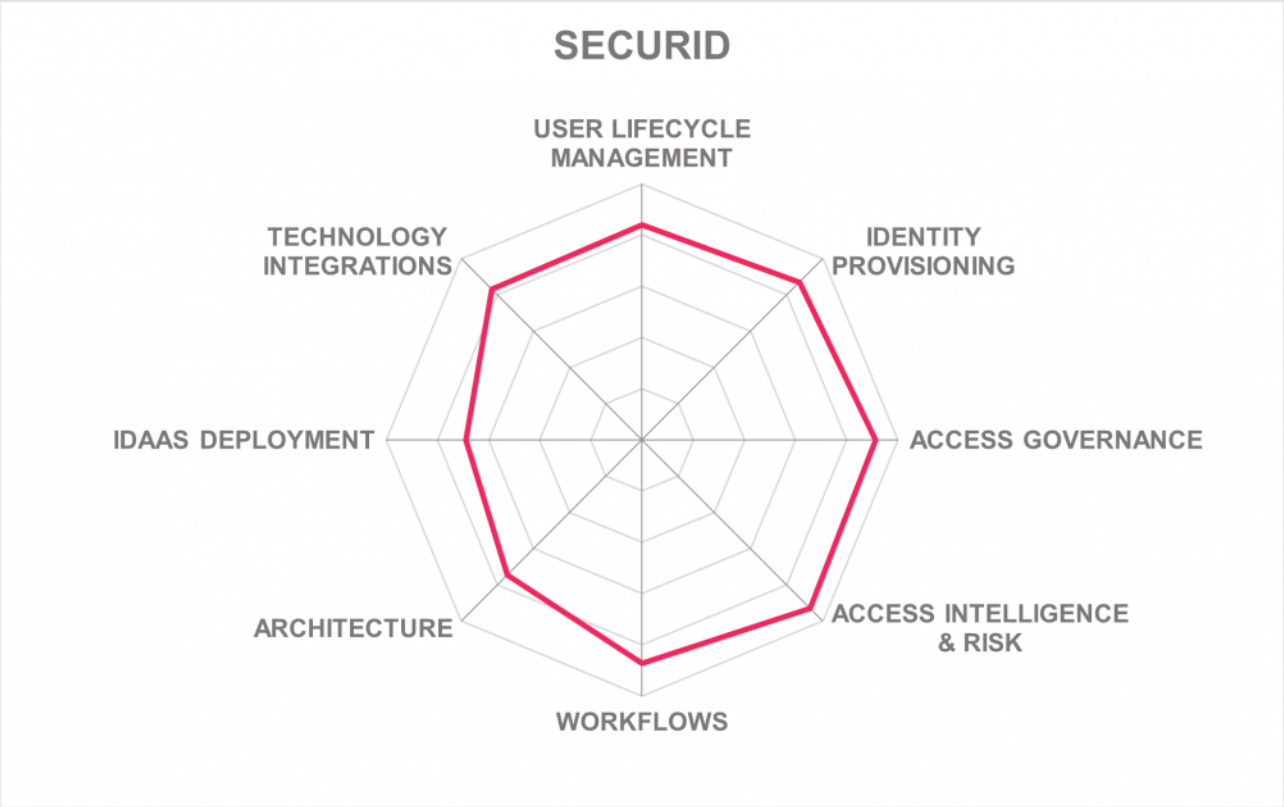
RSA SecurID®

Strengths

- User lifecycle management
- Identity provisioning
- OOB on-premise and SaaS connector support
- Risk-based Access Governance
- Identity & access intelligence capabilities
- User-friendly interfaces
- Strong partner ecosystem
- Useful user community portal
- Workflows
- Technology integrations

Challenges

- Cloud delivery is currently a single tenant model
- Limited Data Centers (DC) delivering IDaaS services in the APAC
- Some limitations on SDK programming language options and access to product functionality via the SDK
- The effects of acquisitions and spin-offs with EMC, Dell, and now STG left the product strategy unclear, although the recent business alignment of the SecurID product line may increase focus and investment moving forward


SECURID
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.16 SailPoint

Established in 2005 with headquarters in Austin, Texas, SailPoint started as a vendor specialized in Access Governance and made heavy investments in Identity Provisioning capabilities over the years. The recent acquisition of ERP Maestro will further provide visibility into SAP user access risks and accelerate its IGA capabilities. SailPoint Identity Platform is a single platform that adds AI-based capabilities to IGA and cloud governance via SaaS. The platform has a number of modules such as Compliance Manager focused on policy adherence and review of access, Lifecycle Manager for provisioning & access requests, and File Access Manager, which is fine-grained governance over file storage platforms, amongst other capabilities depending on the customer requirements. Recently added to the portfolio is the SailPoint Access Risk Management as a result of the ERP Maestro acquisition.

Strong support for identity data and life cycle management can connect to a wide range of different identity repositories. A definitive list of out-of-the-box (OOB) on-premises and SaaS connectors are also available. Attribute mapping from source to target properties includes workflows, customization of mapping rules, and synchronization of user attributes across heterogeneous IT environments. The solution also supports both SPML and SCIM for identity provisioning/de-provisioning. Beyond the core governance capabilities such as access certification, SoD, access request, provisioning, and password management, SailPoint's AI & ML investment enhances its core identity platform with access insights, recommendations, access modeling, and cloud governance capabilities. Access governance support for containers and container orchestration platforms such as Kubernetes is not available. Strong support for different identity types such as machine and Bot/RPAs is given. OOB integration with ITSM tools includes ServiceNow, BMC Helix ITSM, and Atlassian JIRA Service Desk.

The user interfaces are modern, well laid out, and user-friendly with some superior dashboard, graphics, and user identity & access detail drill-down capabilities. Administrators are provided a view of user identities and their history chain. Access certification comes with a good set of recommendations to base an access decision on and an auto-approve feature with an audit trail and explanation of why the access was given. Full reporting support is available, as well as OOB reports for major compliance frameworks. Other IGA and AG-related OOB reports also includes access risks, accounts, analytics trend analysis, SoD, stale data, role change, and role membership suggestions, to name a few.

SailPoint can support on-premises, SaaS, and managed service deployment models. The SailPoint Identity Platform can be delivered in the cloud as a Docker-based container or software deployed to a server. For cloud delivery, the product supports full multi-tenancy. All product functionality is exposed via SOAP and REST APIs, as well as the majority of the functionality is accessible via CLI. SDKs expose nearly all functionality and include the Java programming interface as well as JavaScript, Angular, and jQuery options. Also offered are a community-style portal for customers, developers, service partners, and employees with access to documentation, tutorials, examples to help with development, integrations, configuration, and deployments.

SailPoint has been a leading vendor in the IGA market, providing strong Access Governance capabilities. In

addition, SailPoint has built excellent support for identity and role lifecycle management as part of the IGA offering with an increased focus on identity and access intelligence. SailPoint's early recognition of Access Governance requirements in heavily regulated industries such as banking combined with strong marketing messaging and execution has led it to be one of the most evaluated IGA vendors for mid-to enterprise-sized organizations. SailPoint continues to enhance its provisioning, automation, and intelligence in a positive direction, making it a recommended consideration in any IGA evaluation.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

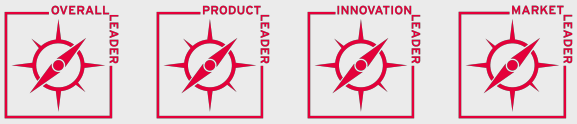
Strengths

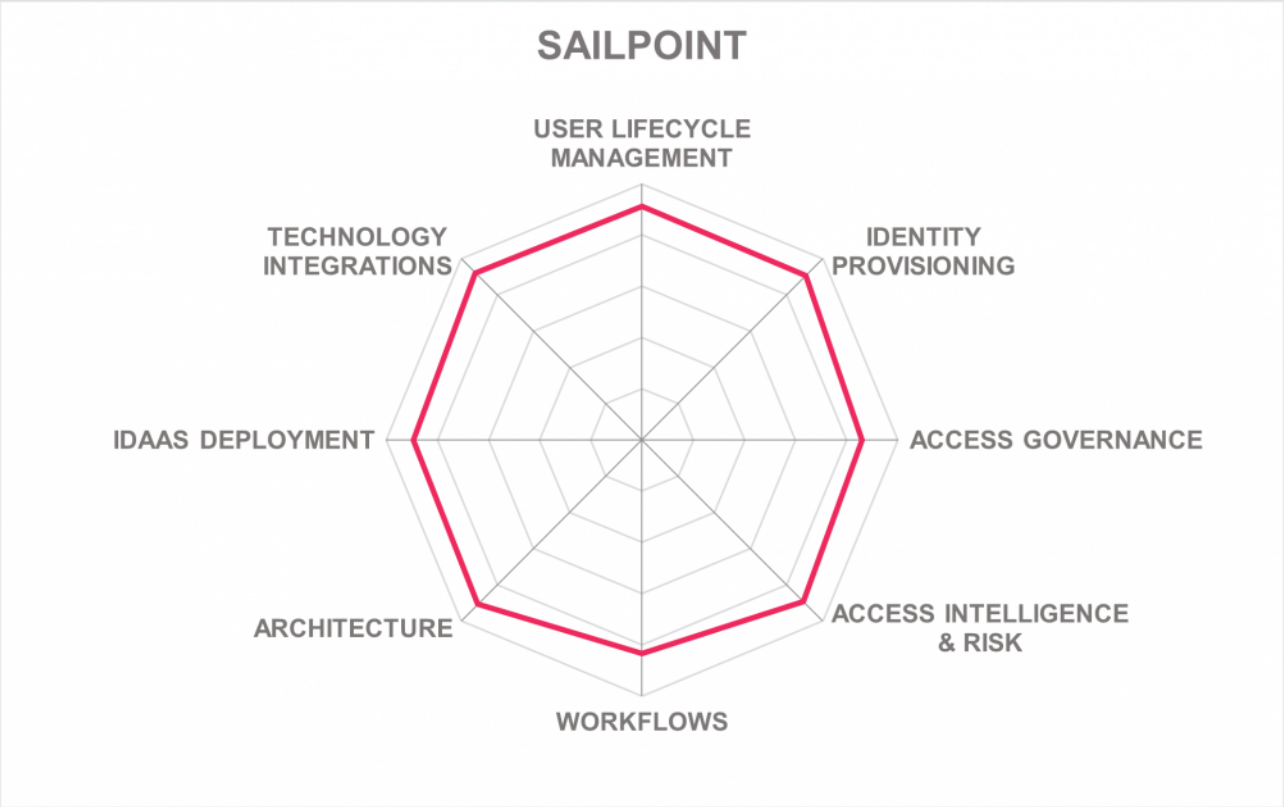
- User lifecycle management
- Identity provisioning
- Strong OOB on-premise and SaaS connector support
- Strong access & risk intelligence support
- User self-service support
- Access & review support with innovative features
- Modern, well thought out and user-friendly interfaces
- Workflows and automation
- Technology integrations
- Good IDaaS deployment and delivery options
- A large and effective channel partner network

Challenges

- Policies to define adaptive authentication and required authentication LoA to applications and services are not given
- Access governance support for containers and container orchestration platforms (e.g., Kubernetes) is not available
- Missing access governance support for containers and container orchestration platforms such as Kubernetes

Leader in




SAILPOINT
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.17 SAP

SAP Cloud Identity Access Governance is a pure-play IDaaS IGA solution. However, it focused primarily on the Access Governance part of IGA, including the assignment of entitlements. It provides baseline support for Identity Provisioning yet, which - in the SAP ecosystem - is also offered by either their Identity Manager or, with SAP-only focus, by SAP Access Control. For customers using SuccessFactors, HR events triggering provisioning to specific targets are already supported. The solution comes with certain interesting capabilities and plays an essential role in supporting the broader SAP ecosystem, i.e., the cloud-based applications such as Concur and SuccessFactors. This IDaaS IGA Leadership Compass evaluates the SAP Cloud Identity Access Governance, SAP Cloud Identity Authentication, SAP Cloud Identity Provisioning, SAP Identity Management, SAP Single Sign-on, SAP Dynamic Authorization Management together as its IDaaS offering.

SAP Cloud Identity Access Governance builds the bridge between the established SAP solutions in IGA and GRC to the new SaaS applications. For SAP customers, this also involves having an environment that commonly consists of 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. SAP gives limited support for out-of-the-box (OOB) provisioning connectors for on-premises systems and SaaS services other than some of the most popular applications. SCIM is supported for identity provisioning and de-provisioning. Automated workflow for provisioning/de-provisioning and auto-discovery capabilities to identify accounts, groups, group memberships is possible through role mining and analytics. Access Governance capabilities, including flexible workflows, support for automated assignment of entitlements based on roles, approval processes, and self-service functionalities, are available. OOB integrations to ITSM tools are available through SAP CPI, and APIs can be utilized for custom integrations.

Feature-wise, SAP Cloud Identity Access Governance is a strong offering for what it delivers. Strong policy management is available and includes an XACML policy integration that enables real-time SoD checking. The solutions also provide intelligence to the customer through outlier and anomaly detection, risk scoring, and recommendations. Good access certification, event-based micro certification, and triggers to initiate recertification are given. SAP Cloud Identity Access Governance comes with a modern UI and well-thought-out dashboards that provide immediate insight into the status and access risks. The product delivers good IGA related reporting and auditing capabilities, although support of out-of-the-box reports for major compliance frameworks is limited. Good support for user access self-service is given. Authenticator options to both user and admin portals are basic and missing FIDO and other biometric options.

SAP Cloud Identity supports a multi-tenant approach within its data center (DC) deployments, delivering IDaaS services in most regions. SAP Cloud Identity Access Governance (integration edition) is available for extending SAP Access Control for SaaS applications for hybrid deployments. Both SaaS and managed services are available as well. Less than half of the product's functionality is exposed via REST APIs, and SOAP APIs are not available to support legacy systems. Missing is CLI and SDK support, although a toolkit for integration connectors based on web services is given.

SAP maintains a significant customer base in North America and the EMEA regions. SAP Cloud Identity Governance is a stand-alone solution that is of specific interest for SAP customers, as well as those who need to extend the reach of SAP Access Control and SAP Identity Management. Overall, SAP provides a reasonably well-rounded set of IGA features, although primarily focused on SAP applications with open connectivity to third-party applications. Thus, customers must carefully evaluate whether this solution is the right fit. However, SAP Cloud Identity Access Governance will be a logical choice for all SAP customers, and SAP provides a well-thought-out roadmap for further evolution.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○

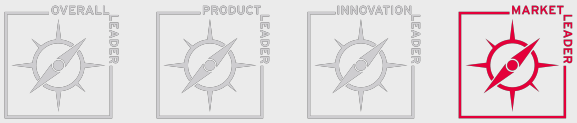
Strengths

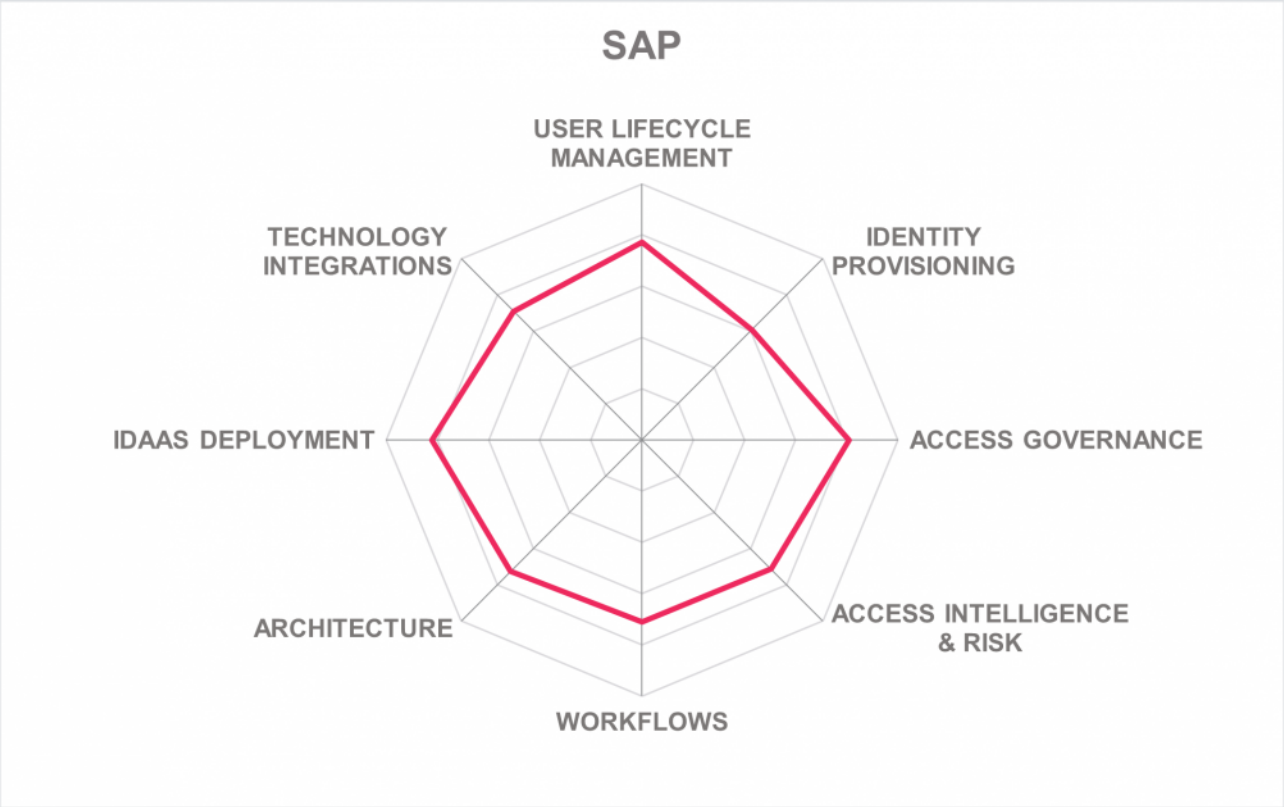
- User lifecycle management
- Access governance
- IDaaS deployments
- Useful and modern UI
- Workflow and automation support
- Access and risk intelligence
- Good support for SAP solutions
- Delivers continuous insight into the state of access entitlements
- Supports extended SoD controls, focused on high-risk business applications
- Preconfigured audit reporting

Challenges

- Baseline support for identity provisioning
- Limited connector support for OOB on-premises and SaaS systems with gaps particularly for non-SAP business applications
- Requires additional offerings for delivering a comprehensive IDaaS IGA solution
- Basic user self-service and admin authenticator options

Leader in




SAP
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.18 Saviynt

Founded in 2010 and based in California (US), Saviynt offers a platform - Enterprise Identity Cloud (EIC), made of five different Identity Governance products. Its three core products are Identity Governance and Administration, Privileged Access Management (PAM), and Application Access Governance (AAG). Other products include Third-Party Access Governance (TPAG), focused on third-party access, and Data Access Governance (DAG). EIC brings together all of these different aspects of identity comprehensively. Saviynt Enterprise IGA, built on the Saviynt EIC, is the IGA offering focused on in the Leadership Compass.

Saviynt offers a strong lineup of IGA, including cloud PAM, Application Access Governance, Third-Party Access Governance, and Data Access Governance through its EIC. Saviynt also offers ID Risk Exchange and the Saviynt Exchange products to their portfolio, a collaborative platform with their customers to exchange insights. Strong support for identity data and life cycle management can connect to a wide range of different identity repositories. Good support for attribute mapping from source to target properties can utilize JSON, JavaScript, and RegEx to construct attribute mapping expressions. Workflow management with a drag-and-drop feature is also given. Intelligence appears across a wide range of applications and infrastructure. Saviynt also offers granular Data Access Governance and cross-application SoD risk management capabilities. An impressive list of out-of-the-box (OOB) on-premises and SaaS connectors are available. Saviynt has also added a built-in connector RPA Bot that can deploy on-premises for a hybrid deployment. It can be used to onboard and convert disconnected applications to connected applications for automated reconciliation, provisioning, and account management. The solution also supports both SPML and SCIM for identity provisioning/de-provisioning.

The UI dashboard can be tailored from a simplified view for line managers to more detailed views for analysts and application owners displaying different aspects of access, activity, and vulnerability risk. Strong user self-service capabilities are given that include intelligent access request capabilities that allow more ways to request access. Using a custom browser-based plugin or native ServiceNow App, approvers/reviewers can collaborate using Slack or MS Teams, for example. Saviynt also provides a mobile application. A wide range of user and admin authenticator options are available natively and through third-party integrations with Okta, Ping, and OneLogin. Good IGA related audits and compliance reports are available, and support for major compliance frameworks is available OOB.

For cloud (private, public) deployments, Saviynt is a microservices-based SaaS, delivered as a mix of single tenancy services for security and multi-tenancy services for performance & scalability. For on-premise deployments, Saviynt provides Saviynt-in-a-box virtual appliance for easy deployment, container-based (Docker, Red Hat), or software deployed to server delivery models for customers not yet ready or can't move to the cloud. Nearly all of the product's functionality is exposed via REST APIs, although SOAP is not. Support for both Java and JavaScript-based SDK are provided, although with much less access to the product's functionality. CLI DevOps support is not available, although a developer portal is given that includes documentation, tutorials, and examples.

Saviynt is a privately held company backed by venture capital that is highly innovative and maintains an

aggressive growth strategy. Accelerated growth also has the potential of becoming de-focused by fast-growing feature sets and delivering to customers. Still, Saviynt has maintained a steady customer-focused trajectory over the years focused on large enterprise organizations with customer and partner ecosystems primarily located in North America with expansions into the EMEA and APAC regions. Forward-looking organizations needing an integrated risk-based approach to IGA across the range of on-premise and cloud-based applications should consider evaluating Saviynt.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

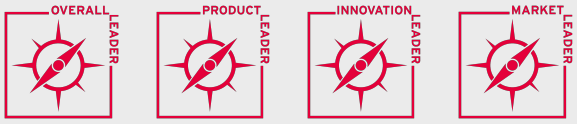
Strengths

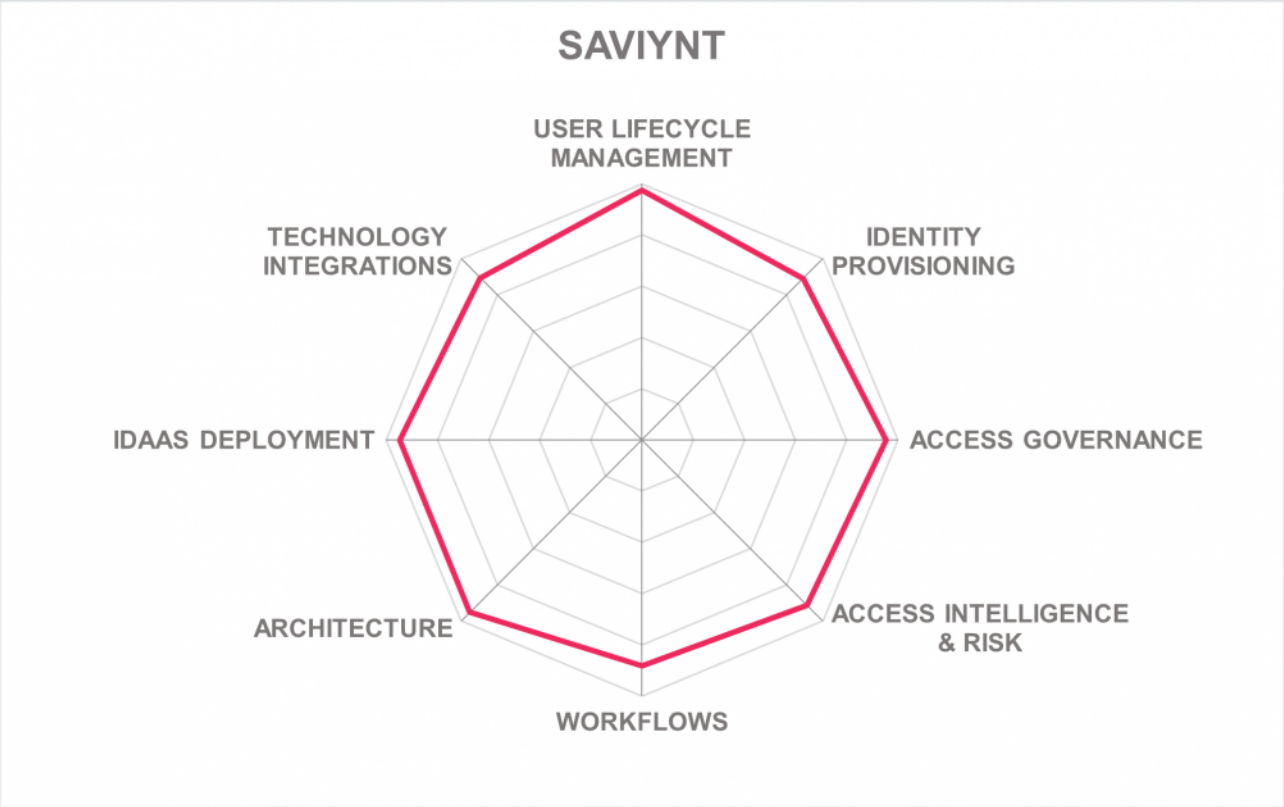
- User lifecycle management
- Identity provisioning
- Automated application on-boarding
- Built-in RPA for legacy applications
- Flexible policy and workflow management
- Well laid out and user-friendly UI
- Good use of intelligence throughout
- Mature DAG and SoD risk management
- Good IDaaS deployment and delivery options
- FedRAMP certified

Challenges

- VC-backed vendor with aggressive growth strategy
- Risk of de-focusing due to fast-growth in features
- Still limited but growing brand awareness in regions outside North America
- Some DevOps limitation such as available CLI, SDKs, and SOAP API

Leader in




SAVIYNT
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.19 Simeio Solutions

Based in Atlanta, Georgia (US), Simeio Solutions observed significant growth when shifting from its IAM system integration business into a full-fledged IDaaS service provider over the past few years. Simeio enters mainstream IAM business with Simeio Identity Orchestrator (IO), a single platform with multiple services. Simeio IO offers Access Management, PAM, and IGA together or individually on a subscription basis. Simeio IO IGA capabilities are evaluated here in this Leadership Compass.

Simeio IO's platform provides a fully integrated suite of IGA, AM, and PAM domains and providing 3rd party add-on capabilities via Splunk, BeyondTrust, and CyberArk integration as examples. Simeio offers a full range of identity repository support options and support for OOB on-premise and SaaS target system connectors. Good support for IGA related policies gives flexibility to entitlement models using attributes focused on roles and organizations. A good set of identity and access intelligence is shown through capabilities such as role discovery and mining, outlier, anomaly detection, and user risk level. Simeio IO features include a user onboarding invitation service, access request & approval, access certification, password management, delegated administration, and privileged check-out capabilities. Its mobile app interface provides the user the ability to conduct activities such as access request approvals and access certifications. Support for OOB ITSM tools integration includes ServiceNow, Remedy, and the Jira ITSM Module.

Simeio IO gives a modern, user-friendly web UI with useful dashboards for both user self-service and administration. Its mobile application also gives useful and innovative features such as Intelligent Identity with facial recognition and other identity validation information. Both basic and some more advanced authentication options are given to user self-service and administration portal access. Good out-of-the-box IGA related reports and reports for major compliance frameworks are also given.

The Simeio IO platform can be deployed on-premises, cloud, or hybrid environments. Although Simeio has a primary focus on providing a SaaS, it also offers a virtual appliance, software deployed to a server, and container-based options that can deploy on a standard orchestrator platform like Kubernetes or OpenShift for on-premises delivery. Although all of the solution's functionality is available via REST APIs, access to functionality is not offered via SOAP, CLI, nor are SDKs provided. Both SPML and SCIM interfaces are available for provisioning.

Simeio is a privately held company established in 2007 that supports mid-market organizations primarily in North America with a growing footprint in the EMEA and APAC regions. Simeio has significantly increased its platform and IGA capabilities over the last year - moving into a Product Leadership position. Also, Simeio combines its IAM development experience and systems integration expertise providing an alternative to several established vendors. Overall, Simeio offers good IGA capabilities as part of the Simeio Identity Orchestrator solution which should be considered by organizations primarily in the North American and EMEA regions.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

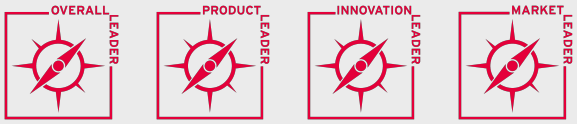
Strengths

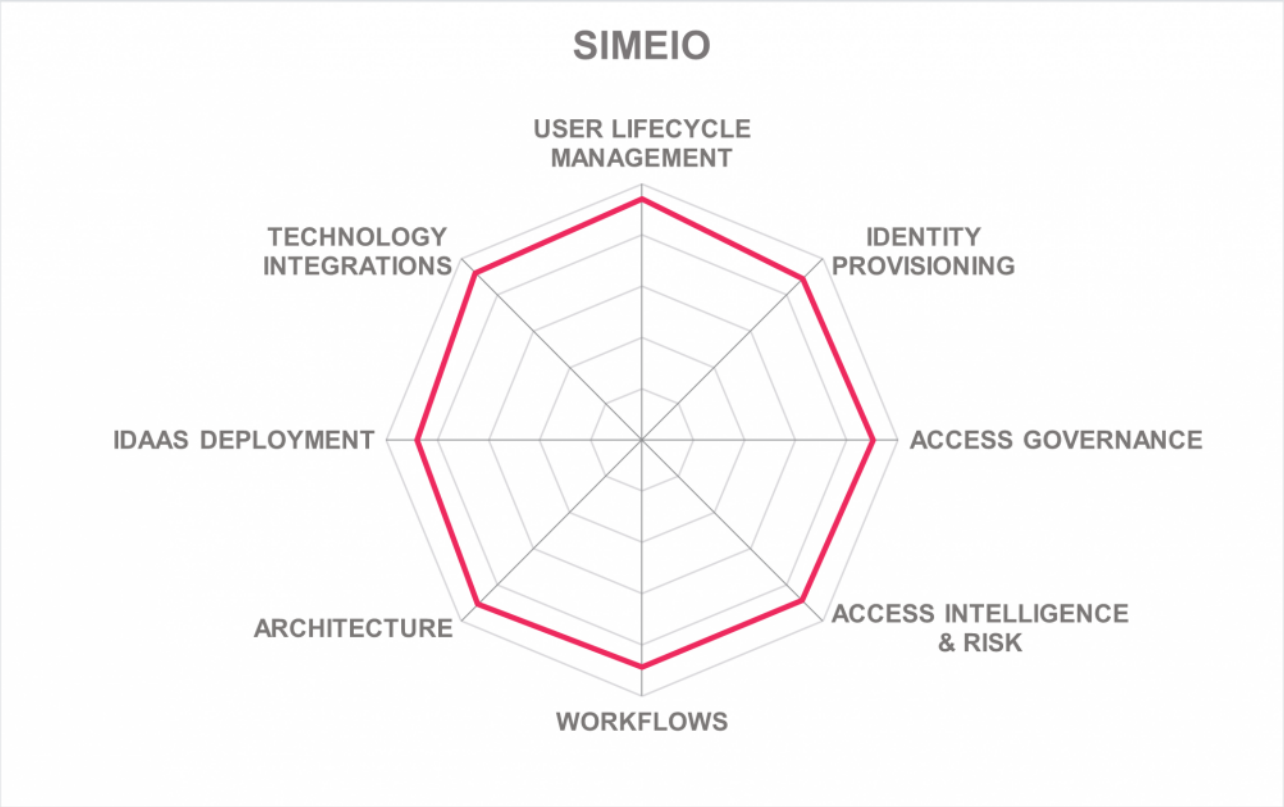
- User lifecycle management
- Identity provisioning
- Access Governance
- User self-service
- Access & risk intelligence
- Technology integrations
- Modern and user-friendly UI
- Workflow and automation
- IDaaS deployment
- Mobile application

Challenges

- Good ability to execute in North America, but limited system integrator partner network on a global scale
- Limited DevOps support (SOAP, CLIs, SDKs), although REST APIs are available
- The wide-spread reputation of primarily being only a global SI vendor, although beginning to fade

Leader in




SIMEIO
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.20 Soffid

Based in Spain and established in 2013, Soffid IAM is a single platform that provides an open-source Identity and Access Management (IAM) and Single Sign-On (SSO) solution. Soffid offers a subscription service to an enterprise edition of the software product and technical support service. Consulting and deployment services are also available through Soffid services. Soffid offers IGA related provisioning, access governance, and SSO capabilities of its Soffid IAM offering for this on-premise Leadership Compass report.

Soffid IAM supports a wide range of options for identity repositories types that can be used. A good set of out-of-the-box (OOB) provisioning connectors to popular on-premises systems. Less support is given to OOB connectors to SaaS applications. Good user self-service access request and approval capabilities are given using a shopping cart-based approach to search, select and request access, although more advanced support for access requests through chatbots and/or messaging platforms (e.g., slack) are available. Flexible attribute mapping tools and allows for the use of Bean Shell or Java mapping expressions within the product editor are given. Soffid IAM provides SSO and the capability to record sessions and keystrokes. Additional features include a workflow web editor and certification, and IGA related certification triggers capabilities, although event-based certification is not given. IGA related identity and access intelligence features are also given. OOB ITSM tool integration includes ServiceNow

Soffid has recently released a new version of its user and administrative interface to better engage customers with its UI. Soffid provides a useful dashboard with some analytics and intelligent features shown through status and risk indicators. Additionally, workflow diagram navigation and role mining capabilities are also available. Access to both user and administrative UI access supports a wide range of authenticator options, including full FIDO support. A good set of OOB IGA related reports is available, although OOB reports for major compliance frameworks are not.

Soffid IAM can support not only on-premises but also public & private cloud and hybrid deployment models. Hybrid solutions can be accomplished by mixing Kubernetes and software-based components. The solution can be delivered as a hardware appliance, container-based (Docker, Red Hat), and a managed service, although a virtual appliance option is not available. Soffid states that 100% of the solution's functionality is exposed via SOAP and REST APIs. SPML and SCIM is also supported. Only Java SDKs are available. Product customization requires Java programming skills, although a developer portal is available for DevOps documentation and tutorials.

Soffid IAM primarily serves medium to enterprise organizations with customers primarily in the EMEA region, expanding into Latin America. Soffid's partner ecosystem is relatively small and located in the customer's geographic locations. Soffid offers an alternative open-source solution to organizations with a reasonably well-balanced set of IAM and IGA capabilities.

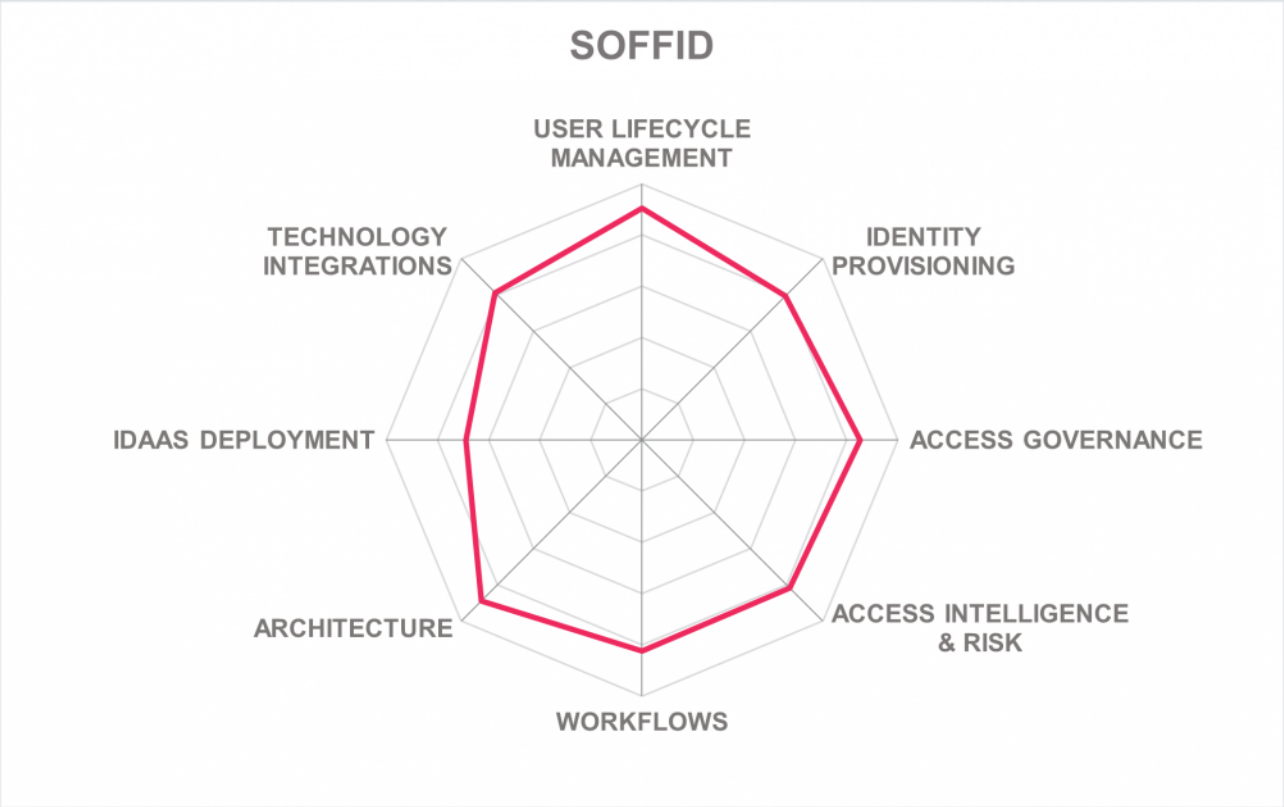
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●○○

Strengths

- User lifecycle management
- Identity provisioning
- Access governance
- Access & risk intelligence
- Workflows
- Good Architecture
- Technology integration
- All functionality exposed via APIs
- OOB workflow templates
- IGA related reports OOB

Challenges

- Small partner ecosystem
- Limited market presence outside Europe
- Some limitations on OOB provisioning connectors to SaaS systems
- Missing OOB reports for major compliance frameworks such as GDPR or SOX
- Limited SDK options


SOFFID
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

5.21 Tools4ever

Tools4ever is primarily focused on IAM requirements of the mid-market segment and is increasingly building on its portfolio to serve the complexities and needs of large organizations. Along with Identity & Access Manager as its actual primary offering for identity provisioning in the IAM market, Tools4ever offers HelloID as its newest IDaaS offering to serve the mid-market segment's most common Identity Management requirements. Its user provisioning, helpdesk self-service, access management, SSO, and MFA delivers its baseline IGA capabilities.

For user lifecycle management, HelloID support primarily Microsoft applications and technologies such as Microsoft AD and AAD, although Salesforce is also supported. Identity types are limed to employees, but not organization, customer, government, or machine identity types. Well-supported synchronization of user attributes across heterogeneous IT environments, and mapping functionality is also given. A good and diverse range of provisioning connectors to SaaS systems are available, although limited OOB on-premises connectors focused on Microsoft applications and SAP ERP. HelloID offers interfaces to various ITSM systems such as ServiceNow, TOPDesk, and Jira. HelloID itself can be integrated with the ITSM solution to provide the users UI.

Good user self-service access request and approval options are given for access governance, which includes requesting access to applications, roles, privileged access, and access cloning. Full functionality is provided for mobile devices user self-service requests. Support for user self-service password management is not given. IGA and AG-related reports available OOB are limited, and support for significant compliance frameworks available OOB is missing. Good IGA related policy management is offered, such as account termination, role modification, access exception approval, rights delegation, SoD analysis, and mitigation. Also, well-supported workflow options are given, although support for delegated registration workflows that allow partners, HR, etc., to register on user behalf is unavailable. Regarding access governance capabilities, limited access intelligence and certification capabilities are possible.

TOOLS4EVER HelloID is a single platform cloud service only with a local agent for on-premise management. Its cloud delivery supports separate data centers (DCs) for the USA and Europe, although DCs for the APAC region is not supported. The HelloID platform provides good API support for all of the solution's functionality using REST. SOAP APIs are not supported. SDKs are limited to SSO capabilities, and SAML and OpenID integration are possible. Data centers (DCs) delivering IDaaS services are located in North America and EMEA but missing DCs in the APAC region.

TOOLS4EVER customers range from medium to enterprise with a concentration of mid-market organizations located in North America and the EMEA region, as well as partner integrators. With offices in the U.S., The UK, France, Germany, and The Netherlands, TOOLS4EVER has a growing regional presence and makes a good choice for local SMB and mid-market organizations to make their shift to IDaaS. With a decent product roadmap and execution capability, we expect TOOLS4EVER to continue to progress in a positive direction to contend with the existing IDaaS players in the region.

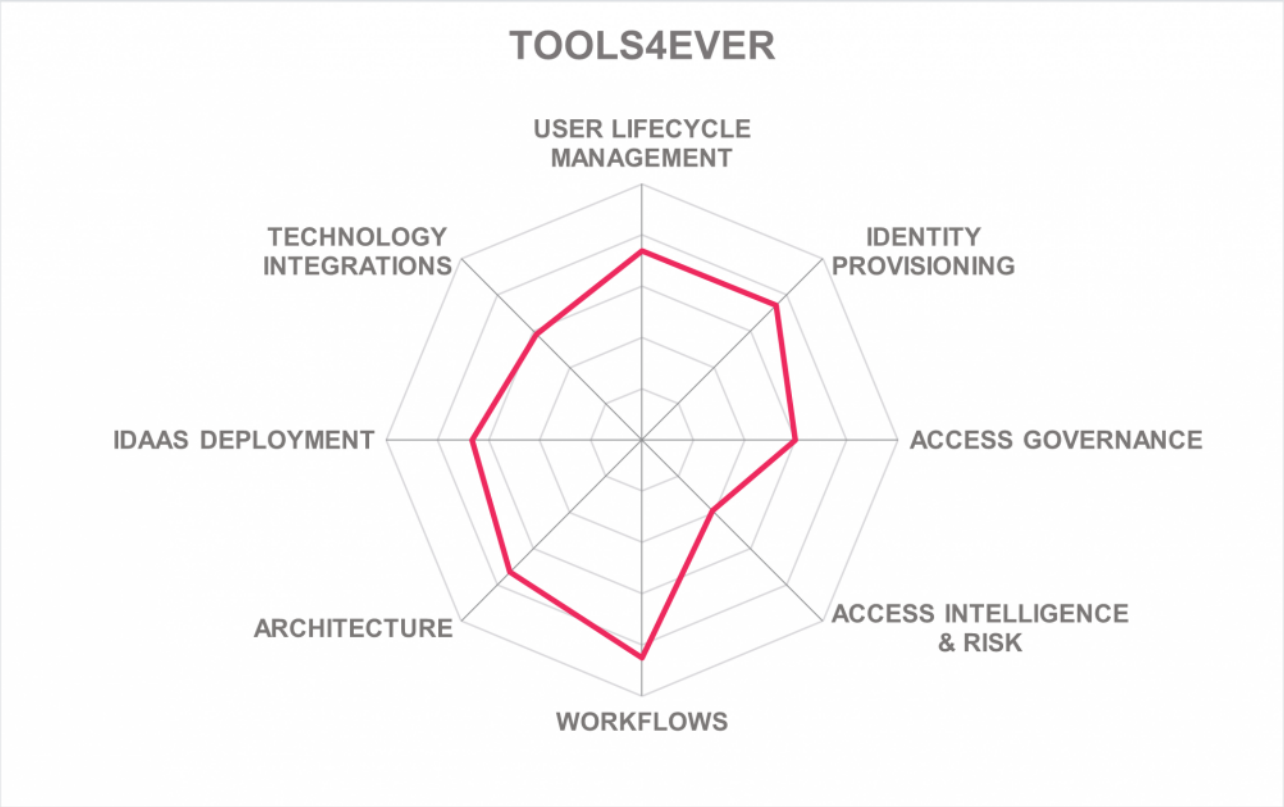
Security	●●●●○
Functionality	●●●○○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●○○

Strengths

- User lifecycle management
- Identity Provisioning for SaaS applications
- Baseline support for access governance
- Strong workflow capabilities
- Good user self-service support
- IGA related policy management
- Good understanding of mid-market IAM requirements
- Supports IDaaS-related regulations in the region
- Ease of deployment and initial configuration

Challenges

- Good Access Management capabilities for mid-market customers, but not leading-edge for large enterprise customers
- Limited set of OOB on-premises connectors
- Missing SOAP APIs for legacy applications
- Limited SDK support
- Limited access & risk intelligence
- Missing DC support for the APAC region


TOOLS4EVER
USER LIFECYCLE MANAGEMENT
IDENTITY PROVISIONING
ACCESS GOVERNANCE
ACCESS INTELLIGENCE & RISK
WORKFLOWS
ARCHITECTURE
IDAAS DEPLOYMENT
TECHNOLOGY INTEGRATIONS

6.1 Imprivata

Imprivata is a digital identity company focused primarily on healthcare. Imprivata Identity Governance is a healthcare-specific identity governance and compliance solution purpose-built to give clinicians and non-clinicians fast, secure, role-based access to critical healthcare and business systems and applications. Imprivata Identity Governance is an integrated component of the Imprivata identity and access management solution suite, which delivers end-to-end provisioning, seamless multifactor authentication, role-based access, ubiquitous single sign-on, and integrated governance and compliance to secure and manage digital identities across the healthcare ecosystem.

Imprivata Identity Governance helps healthcare organizations of all sizes to reduce IT costs by automating the identity management process; strengthening data security across the entire organization; and empowering care providers to deliver high-quality care with role-based, timely access to the right systems. The solution can be deployed on-premises or hosted in an Azure environment for greater flexibility and scalability.

Imprivata Professional Services has developed a streamlined approach for implementing Imprivata Identity Governance so customers can achieve ROI. The Imprivata Professional Services team has extensive experience with various EHR and clinical application provisioning processes along with the knowledge of integrating Imprivata Identity Governance with Imprivata OneSign and Imprivata Confirm ID. When the Imprivata Professional Services team is involved, customers achieve much higher rates of adoption and satisfaction with the solution without requiring a multi-year consulting service.

Founded in 2002, Imprivata is headquartered on the east coast of the U.S. Imprivata provides implementation services for Identity Governance themselves, with a small number of resellers and implementation partners in North America.

Why worth watching: Imprivata would be the preferred choice for healthcare organizations looking for vendors with the knowledge and expertise of managing industry-specific IAM challenges.

6.2 Kapstone

Founded in 2013 with headquarters on the east coast in the northeastern US, Kapstone released its Access Review product with Day Zero Application Onboarding and Attestation in 2016, and introduced Kapstone's Provisioning Gateway and Intelligent Identity products the following year. More recently, Kapstone added

both Autonomous IGA and Cloud Governance to its product portfolio. Today Kapstone's Autonomous IGA provides an innovative platform that focuses on three key capabilities - Automation, Intelligence, and Modularity.

Beyond core IGA capabilities, Kapstone Autonomous IGA gives some more advanced features that include service discovery, delegated administration, intelligent identity, application discovery and IGA application on-boarding, role discovery and automated access policies, IDaaS configuration management and analytics, as well as AWS, OCI governance. Kapstone also provides services to map IAM controls to such things as the NIST or HIPPA requirements as well as assessing an organizations security posture.

To further identify potential risks and threats, Kapstone gives the ability to aggregate risk information and threat intelligence through integrations. Information for risk scoring can be provided by third party on-premise and cloud SSO solutions like Oracle IDCS, OAM, Okta, Azure, SIEM, UEBA, or even CASB integrations as some examples. Risk analytics can be derived from entitlement analysis and peer review. Actions can be taken, depending on the risk analysis, to lock a user's account or trigger a security audit, for example.

Why worth watching: Kapstone's autonomous, intelligent, and flexible modular product architecture are some of its key differentiators in the IGA market.

6.3 Okta

Based in San Francisco, California (US), Okta offers a cloud identity platform targeted at the workforce and customer identity management. Okta's workforce identity solution caters to organization's access management requirements, including a universal directory service, SSO, MFA, identity lifecycle management, and API access management.

More recently, Okta introduced Identity Governance and Privileged Access as part of the Okta Identity Cloud offering. Okta's Identity Governance gives a cloud-first approach to identity governance and administration (IGA), leveraging its recent acquisition of atSpoke, which contributes tasks and workflow capabilities to Okta's IGA. Okta Identity Governance provides self-service access request and approval workflows, automatic provisioning of users, access reviews, certification, and governance reporting capabilities, along with the ability to utilize these features through modern standards like SCIM and API-based interfaces.

Why worth watching: Okta Identity Cloud continues to build out a more comprehensive solution by expanding its access management, identity governance, and privileged access use cases.

6.4 Pirean

Pirean is a medium-sized company founded in 2002 with offices in London and Sydney. Their company provides a Consumer and Workforce IDaaS platform with a focus on simplifying how IAM capabilities are delivered for their customers enterprise web and mobile applications.

Workforce Identity provides a diverse set of capabilities that offers a fully-featured end-to-end IAM solution. Workforce Identity supports both IAM and CIAM use cases on-premises and in the cloud. Pirean also goes beyond the traditional IAM feature set to securely connect mobile users as well as providing flexible integration and workflow options that allow for the orchestration of the platform's capabilities. Beyond Pirean's access management and adaptive authentication, IGA capabilities are given to allow the management of application access entitlements with their lifecycle policies and rules, as well as access certification, SOX, and SoD compliance and innovative user request features.

Why worth watching: With Pirean's focus on high assurance use case and its expanding capabilities into the IGA space, Pirean will be an interesting vendor to watch in the IGA market.

6.5 Systancia

Systancia offers an Access Management platform that includes multiple products within a suite to secure end user's digital workspace. The platform includes remote, privileged, virtual access, and IAM capabilities. Systancia is shifting its product portfolio from a traditional software product to a cloud service platform called Systancia Cloud in the near future. Systancia Cloud is a hybrid offering with Systancia Gateway for provisioning on-premises applications. Systancia Identity, formerly Avencis Hpliance, is its on-premise IGA offering.

Systancia Identity supports a set of well-selected identity repositories, such as Microsoft AD & AAD and Oracle DB. Out-of-the-box (OOB) provisioning connectors to on-premise systems are primarily limited to Microsoft products, Oracle DB, and other ODBC compliant databases. However, custom connectors can be made. Provisioning is automated and supports workflows. Systancia administrative UI is functional with a tab-based layout and less of a modern look and feel with UI dashboards that provide helpful graphs. A self-service UI allows users to request role or privileged access requests and management approvals using a workflow. Systancia products can be delivered as SaaS, virtual appliances, or software deployed to a server. When running the solution-as-a-service, both the Systancia Identity and Systancia Identity Provisioning servers must be installed on-premises. A hybrid cloud SaaS model only requires Systancia Identity Provisioning on-premise to connect to the cloud service.

Systancia is a privately held company established in 1998 with its headquarters in France. Systancia customers are focused on medium to mid-market organizations. Both customers and partner ecosystems reside almost solely in the EMEA, with some growth in other world regions. Overall, Systancia Identity provides basic IGA capabilities, focusing on Identity Lifecycle Management, automated provisioning, user self-service, and workflows.

Why worth watching: With an improved set of IGA capabilities and cloud offerings, Systancia can provide a good alternative to existing IGA vendors in the EMEA region.

6.6 Tuebora

Tuebora, based in California, offers Tuebora Governance as its primary IGA product. One of the earliest IGA vendors to leverage machine learning techniques for Identity Analytics and Access Governance, Tuebora offers its own Data Access Governance (DAG) and web access management (WAM) products as Tuebora DAG and SSO respectively. Tuebora combines Identity Provisioning and Access Governance with its machine learning and identity analytics platform to detect access risks based on real-time tracking of provisioning and user access behavior.

Founded in 2001 and headquartered in the San Francisco Bay area, Tuebora focuses on mid-market to enterprise access governance, risk, and compliance offerings. Tuebora's customer base is located in the EMEA, North America, and APC regions.

Why worth watching: Tuebora makes a good choice for organizations looking for risk-based IGA capabilities.

6.7 Usercube

Founded in 2009, Usercube is a French software company delivering an IAM solution based on the Microsoft technology platform with capabilities solely dedicated to IGA. Usercube's customer base is primarily focused on mid-market to enterprise organizations in the EMEA region.

Usercube is a single product provided for On-Premise and private cloud deployments. Usercube also uses Azure to host its solution and delivers a full multi-tenant, SaaS solution. Built on a container-based micro-service architecture, Usercube is capable of utilizing any system that supports communication with third parties through REST/JSON based APIs, web services, or data exchanges.

Usercube provides identity management, provisioning, governance, analytics, and reporting. Usercube can use all significant identity repositories and any LDAP compatible, SQL based, or API based directories. All identity types are also supported, including departments, work sites such as a meeting room, applications, or machine identity like IoT or RPA bots.

Why worth watching: Usercube has a well-balanced set of IGA capabilities as well as making good use of identity and access intelligence**.**

7 Related Research

Executive View: Accenture Memority - 80422

Executive View: Avatier Identity Management Suite (AIMS) - 71510

Executive View: Beta Systems Garancy IAM Suite - 71530

Executive View: Clear Skye IGA: IGA on the ServiceNow NOW platform

Executive View: EmpowerID - 70297

Executive View: IBM Cloud Identity - 79065

Executive View: ideiio - 80149

Executive View: Ilantus Compact Identity - 80177

Executive View: Microsoft Azure Active Directory - 80401

Executive View: Omada Identity Suite - 80506Executive View: One Identity Manager - 80310

Executive View: RSA SecurID® Access - 70323

Executive View: SailPoint Predictive Identity - 70323

Executive View: SAP Cloud Identity Access Governance - 80418

Executive View: Saviynt Security Manager for Enterprise IGA - 80325

Executive View: Simeio Identity Orchestrator - 80151

Leadership Compass: Identity Governance & Administration 2021 - 80516

Vendor Report: Fischer International - 70254

Vendor Report: Ilex Meibo and Meibo People Pack - 70356

Whitepaper: Why Modern Enterprise IAM Must Be Rearchitected: Build Your Case for Containerized IAM and IDaaS - 80044

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, 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, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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