

# Identity Governance and Administration

Nitish Deshpande

November 21, 2022



**LEADERSHIP  
COMPASS**  
2022

The Identity Governance and Administration (IGA) market is continuing to evolve through more integrated Identity Lifecycle Management and Access Governance solutions that are now increasingly aided by intelligent features. This Leadership Compass will give an overview and insights into the IGA market, providing you a compass to help you find the products that can meet the criteria necessary for successful IGA deployments.

## Contents

Contents.....	2
Figures .....	3
Introduction / Executive Summary .....	4
Highlights.....	5
Market Segment .....	6
Delivery Models .....	12
Required Capabilities.....	13
Leadership .....	15
Overall Leadership.....	16
Product Leadership.....	17
Innovation Leadership.....	18
Market Leadership .....	21
Correlated View.....	23
The Market/Product Matrix.....	23
The Product/Innovation Matrix .....	24
The Innovation/Market Matrix.....	26
Products and Vendors at a Glance .....	27
Product/Vendor evaluation .....	30
Avatier – Avatier Identity Anywhere .....	32
Beta Systems – Garancy IAM Suite .....	35
Bravura Security – Bravura Security Fabric .....	38
Broadcom – Symantec IGA.....	41
ClearSkye – ClearSkye IGA.....	44
EmpowerID – EmpowerID IAM Suite .....	48
E-Trust – Horacius IAM.....	51
Evidian (Atos) – Evidian IGA, Evidian Analytics – IaaS Governance.....	53
Evolveum – MidPoint .....	56
IBM – IBM Security Verify .....	58

Micro Focus – NetIQ IGA Suite .....	61
Microsoft – Entra Identity Governance .....	64
Netwrix Corporation – Netwrix Usercube .....	67
Nexis GmbH – NEXIS 4.....	70
Omada – Omada Identity .....	72
One Identity – One Identity Manager .....	75
Oracle – Oracle Identity Governance .....	78
RSA– SecurID Governance and Lifecycle.....	81
SailPoint – SailPoint Identity Security Platform .....	84
SAP – SAP Access Control, SAP Access Governance .....	87
Saviynt – Enterprise Identity Cloud Platform .....	90
Simeio – Simeio IGA Managed Services.....	93
Soffid – Soffid IAM .....	96
Tools4ever – HelloID .....	98
ZertID – ZertID .....	100
Vendors to Watch.....	103
Methodology.....	106
Types of Leadership .....	106
Product rating .....	107
Vendor rating .....	108
Rating scale for products and vendors.....	109
Inclusion and exclusion of vendors .....	110
Related Research.....	111
Copyright.....	111

## Figures

Figure 1: Representation of core IGA functions by 'Identity Lifecycle Management' and 'Access Governance' categories.....	12
Figure 2: The Overall Leadership rating for the IGA market segment .....	16
Figure 3: Product Leaders in the IGA market segment .....	17
Figure 4: Innovation Leaders in the IGA market segment.....	19
Figure 5: Market Leaders in the IGA market segment.....	21
Figure 6: The Market/Product Matrix. ....	23

Figure 7: The Product/Innovation Matrix.....	25
Figure 8: The Innovation/Market Matrix. ....	26

## Introduction / Executive Summary

Identity Governance and Administration (IGA) combines the traditional User Access Provisioning (UAP) and Identity and Access Governance (IAG) markets. While many vendors today offer combined capabilities to qualify as IGA vendors, a few, especially the new entrants, provide either Identity Lifecycle Management (ILM) or Access Governance capabilities to cater to specific needs of the organizations.

The IGA vendors differ in the depth and breadth of functionalities offered and thus can be classified as either provisioning or governance focused. This KuppingerCole Leadership Compass provides an overview of the IGA market with notable vendors and their products or service offerings in the market.

From our interaction with organizations of varied IAM maturity across the industry verticals, we note that while some are still looking for an Identity Lifecycle Management solution with limited or no Access Governance capabilities, many others demand a strong Access Governance solution. The latter is mostly the case when organizations already have Identity Lifecycle Management in place or when their starting point is Access Governance. Some organizations are either looking at replacements of UAP and ILM or a IAG only solution. However, most of them want a comprehensive IGA solution, and this increasingly as-a-service. This development is the reason for combining IDaaS IGA and on-premises IGA into this one report. Following this Leadership Compass will be a separate report focussed on Access Governance/IAG, which is the only market where we, in the field, observe some companies looking for specialized governance solutions.

One of the adoption patterns we have observed in the market is a managed service achieving fulfilment through Identity Lifecycle Management, and Access Governance is run by and within the organization itself to retain absolute control over governance functions. There are several other adoption patterns witnessed in the market where customer's immediate requirements are limited to either Identity Lifecycle Management or Access Governance but do not demand an IGA solution. In most other cases where there is a need for both, IGA products are preferred over provisioning or governance 'only' solutions to achieve the desired mix of ILM and Access Governance capabilities such as for greenfield IAM implementations. It is important that organizations scope their IGA requirements well before starting to evaluate products that differ in the strength of functionalities making most of them better aligned for either provisioning or governance focused deployments.

Based on these adoption trends, changing customer priorities, and deployment patterns, we decided to center on Identity Governance and Administration holistically in this leadership compass to help security leaders identify relevant IAM market segments and subsequently shortlist the most appropriate technology vendors based on their immediate IAM priorities. In this Identity Governance and Administration Leadership Compass, the primary focus is on the vendors that offer both Identity Lifecycle Management and Access Governance

capabilities, either as a common product or separate but integrable product components to deliver capabilities across the IGA spectrum.

This IGA Leadership Compass will be followed by an upcoming Leadership Compass for Access Governance. LC IGA for SMBs (small and midsize businesses) that identifies and focuses on functional and operational IGA requirements of SMBs that are different in both objective and magnitude than large organizations. The other Leadership Compass on Access Governance will be a specialized version which will evaluate vendors based on core access governance capabilities. It will not include vendors who have strong ILM capabilities. A Market Compass (MC) on IAM solutions for mid-sized organizations is in development, while a leadership compass on Identity Fabrics replaces LC IAM Suites.

With these various LCs and MCs, we aim to provide CISOs and security leaders responsible for IAM the most practical and relevant information that they need to evaluate technology vendors based on the specific use-case requirements, whether these are IGA-driven, provisioning focused, governance focused, focused on comprehensive IAM suites or a combination of these.

## Highlights

- This Leadership Compass evaluates 25 IGA product vendors and over 12% new vendors compared to the previous year.
- The 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) Avatier, Broadcom, Bravura Security, EmpowerID, Evidian, IBM, Micro Focus, Microsoft, Netwrix Corporation, Omada, One Identity, Oracle, RSA, SAP, SailPoint, Saviynt, Simeio
- The Product Leaders (in alphabetical order) are Avatier, Beta Systems, Bravura Security, Broadcom, EmpowerID, Evidian (Atos), IBM, Micro Focus, Microsoft, Netwrix Corporation, Omada, One Identity, Oracle, RSA, SailPoint, Saviynt, Simeio, ZertID
- The Innovation Leaders (in alphabetical order) are Avatier, Bravura Security, Broadcom, EmpowerID, Evidian (Atos), IBM, Micro Focus, Microsoft, Netwrix Corporation, Omada, One Identity, Oracle, RSA, SAP, SailPoint, Saviynt, Simeio
- Leading vendors in innovation and market (a.k.a. the "Big Ones") in the IGA market are (in alphabetical order) Bravura Security, Broadcom, EmpowerID, Evidian, IBM, Micro Focus, Microsoft, Netwrix Corporation, One Identity, Oracle, RSA, SAP, SailPoint, and Saviynt,

## Market Segment

Identity Governance and Administration refers to the increasingly integrated Identity Lifecycle Management and Access Governance markets. Today, there still are some organizations either looking at replacements of UAP and ILM or IAG, but most are opting for a comprehensive IGA solution to tackle risks originating from inefficient access governance features.

Identity Lifecycle Management remains a core IAM requirement, but Access Governance is becoming a more sought-after capability for organizations requiring better visibility of identity administration and access entitlements across its IT infrastructure. Governance offers from simple reporting and dashboarding to other advanced capabilities that include AI and/or machine learning techniques enabling pattern recognition to deliver valuable intelligence for process optimization, role design, automated reviews and anomaly detection. IGA concerns the capabilities in IAM market that broadly deal with end-to-end identity life-cycle management, access entitlements, workflow and policy management, role management, access certification, SoD risk analysis, reporting and access intelligence and also Access Intelligence for business-related insights to support effective decision making and potentially enhance governance.

Identity Governance and Administration (IGA) products support the consolidation of identity information across multiple repositories and systems of record such as HR and ERP systems in an organization's IT environment. The identity information including user accounts, associated access entitlements and other identity attributes are collected from across the connected target systems for correlation and management of individual identities, user groups as well as roles through a centralized administration console.

The IGA products are primarily aimed at supporting the following activities in an organization:

- Automated provisioning and de-provisioning of user accounts across nominated target systems
- Synchronization of identity attributes and access entitlements related to user accounts and groups across the identity repositories
- Management of access entitlements and associated roles of users across the IT environment
- Configuration and enforcement of static as well as event-driven access policies for the accounts to access the IT systems and applications
- Allowing users to validate their access to systems and applications, reset the passwords and create new access requests using self-service options
- Verification and synchronization of user account passwords and other identity attributes from an authorized event and source across the identity repositories
- Reconciliation of access across the IT environment based on defined policies to ensure compliance and prevent SoD and other policy violations
- Supporting on-demand and event-driven user access certification campaigns to detect and mitigate access violations
- Auditing and reporting of access activities leading to critical information regarding service monitoring and optimization

Traditional IGA deployments in most organizations have been facing many challenges ranging from complex implementations and lengthy product upgrade cycles to maintenance of overly customized IGA product and a lack of support for emerging functional requirements. The disconnect between business and IT security functions is another big reason for failed IGA deployments. In many organizations, IT security is primarily driven by the need to meet regulatory compliance, resulting in an undesired shift of IGA priorities from administrative efficiency and better risk management to auditing and reporting. Security leaders focused on IAM must ensure they are able to demonstrate the success of IGA deployments early-on with initial deployment phases to build the credibility and gather necessary consensus required to support IGA initiatives among the IAM stakeholder community.

The IGA market has witnessed several trends over the last few years including a major shift in the product strategy and development roadmaps to provide in-built support for cloud applications. These advancements to support the cloud integrations are in two directions:

- 1) IGA vendors that have re-architected their products to offer an identity bridging capability to integrate with cloud providers using industry specifications. Some IGA vendors have partnered with specialty identity brokers to extend on-premises IGA capabilities to cloud applications. Such approaches are suitable for organizations with a decent on-premises IT footprint and requirements to support complex IGA scenarios for legacy on-premises applications.
- 2) IGA vendors that now offer a cloud IGA product that is cloud deployable with ready integrations with popular cloud applications as well as with standard on-premises applications. This approach is more suitable for organizations with a massive strategic focus on the move to cloud and looking at achieving the benefits of cloud IGA deployments such as shorter deployment cycles, faster upgrades and lower TCO in short term.

Increased adoption of cloud-based identity stores and directories such as Microsoft Azure Active Directory (AAD) has created additional pressure on IGA tools to support Out-of-the-Box (OOB) integrations with cloud services based on industry specifications such as SCIM. Many IGA vendors are already offering ready integrations with Unified Endpoint Management (UEM) tools to offer support for mobile devices in an attempt to enhance user experience (UX) which has become an important differentiating criterion for organizations to evaluate an IGA product. Most IGA vendors have undergone a significant re-engineering effort to enhance their user and administrative interfaces but offering mobile support for critical IGA functions such as access certifications and request approvals is not on the priority list for many organizations because of the expected due diligence required to be carried out to complete these tasks. Inaccurate access certifications and uncertain access request approvals resulting from the inability of users to conduct appropriate due diligence on mobile devices can be disastrous to an organization's overall security posture in the long term. Many IAM and security leaders are therefore advocating against offering mobile support for such critical IGA functions to the business.

IGA integration with other enterprise systems such as IT Service Management (ITSM) tools as well as Privileged Access Management (PAM) tools have also become a norm in the industry and more than 80% of the IGA vendors in the market today either offer OOB integration or utilize the available APIs for the required integration. The integration with ITSM



tools, particularly ServiceNow, is a popular approach for organizations wanting to consolidate IGA user functions (access requests, password management etc.) with other enterprise helpdesk functions under a common user interface (UI) or portal for IT related requests. ServiceNow APIs can be used to integrate with the IGA product in the background for request fulfilment on the target system.

Integration of IGA with PAM tools is another trend that we see picking up aggressively in certain industry verticals, particularly the ones that are heavily regulated. There are a few integration points observed, but the integration of IGA workflows for privileged access certification as well as role-based access of administrators to PAM system are amongst the ones delivering immediate credibility and business value to organization's IAM program.

There is an increased emphasis on integrating IGA tools with AI and Machine learning (ML) capabilities. Extending IGA tools functionality by integrating AI and ML can benefit by consuming the user's access activity such as authentication and authorization information across IT applications and systems to establish and continuously update user access patterns based on their role and peers' group. Similarly, DAG (Data Access Governance) tools can benefit from IGA integrations by consuming user identity and access entitlement information and in turn offer contextual information on device endpoint and data residing on the device and other sources to the IGA tools for better policy management.

Some IGA vendors have ramped up their efforts to align their product development roadmap with DevSecOps initiatives of organizations to support containerized deployments. With an increasing demand in the market for IAM Microservices delivery, a growing number of IGA functions will be grouped based on the functional objectives and usage patterns to be delivered as microservices.

At KuppingerCole, we have identified the following as core capabilities delivered by the IGA vendors, primarily grouped under two product categories: Identity Lifecycle Management and Access Governance.

#### Identity Lifecycle Management:

- **Identity Repository:** Identity repositories are a core component of an IGA deployment and provide a mechanism to manage the identities, identity attributes, access entitlements and other identity related information scattered across the IT environment. Management of access rights information and other entitlements across the identity repositories are captured and correlated as part of access entitlements management process to determine the user's access across the various systems. Often bundled as part of an IGA tool, identity repository offers a consolidated view of identity data. In case of disparate identity repositories, virtualization of identity information is achieved through virtual directories.
- **Identity Lifecycle Management:** Identity lifecycle management provides the mechanisms for creation, modification and deletion of user identity and associated account information across the target systems and applications. Often referred to as Joiners, Movers and Leavers (JML) process, identity lifecycle management offers inclusive support for all identity related events either through available connectors for automated provisioning/ de-provisioning or use of workflows for manual intervention.



Management of user accounts and access entitlements across a multitude of IT systems including cloud-based applications is an increasingly important requirement for identity lifecycle management capability of the IGA tools today.

- **Password Management:** Self-service password management allows for password resets and user account recovery in case of forgotten passwords on the target systems and applications. Password synchronization ensures that password changes are successfully propagated and committed across all required systems. Progressive IGA vendors offer risk-appropriate identity proofing mechanisms in case of forgotten passwords for account recovery actions, in addition to multiple form factors of user authentication for initiating password changes.
- **Access Request Management:** The self-service user interface for users to request access to IT assets such as applications, databases, and other resources. Access request management encompasses the entire process of delivering a user-friendly approach for requesting the access including searching for and selecting the desired resource from the available resource catalogue to browse the available hierarchy models available in the system and request access cloning. Shopping cart approach for searching and requesting access are becoming increasingly common to deliver better experience for users. Several vendors offer the flexibility of configuring workflows to allow for modification of access requests after the request submission and before actual fulfilment based on business process requirements.
- **Policy and Workflow Management:** Policy management offers the mechanism to deliver rule-based decision making based on pre-configured rules for identity lifecycle events such as account termination, role modification, exceptional approval, rights delegation, and SoD mitigation. The enforcement of policies is either triggered by lifecycle events or determined by associated workflows. Workflow management is concerned with defining the necessary actions to be undertaken in support of a successful event execution or decision-making process. This includes orchestration of tasks involved in the overall decision-making process to support the business requirements. Workflow management should allow for easy customizations to include common business scenarios such as approval delegations and escalations.
- **Role Management:** Role management delivers capabilities for managing access entitlements by grouping them based on relevant access patterns to improve administrative efficiency. The roles can be defined at several levels, most common being people, resource and application levels. The access patterns for logical grouping of entitlements can be derived with support of role mining capabilities of IGA tools delivered as part of role management. Role governance, a critical capability within broader Access Governance, encompasses basic role management as part of the overall role lifecycle management.

Access Governance:

- **Identity Analytics & AI/ML:** Identity analytics & AI/ML uses data analytic, and machine learning techniques to derive meaningful information out of the enormous logging and auditing information generated by the systems with an objective to enhance the overall efficiency of IGA processes in an organization. This includes recommendations for efficient use of roles, risk-based mitigation of access policy violations, automated access reviews, and even correlation of identity events across disparate systems to derive actionable intelligence. Identity analytics & AI/ML is fast

becoming an important vehicle to achieve visibility into the operational state of IGA processes by analyzing the operational data generated by IGA tools to evaluate process maturity and adherence to service quality standards as well as compliance mandates. Identity analytics can also feed user access information from authentication and authorization events to AI/ML tools for prototyping user access behavior patterns and detecting anomalous access.

- **Access Certification:** Another key capability to gain an organization-wide visibility in the state of access across the multitude of devices, systems and applications including access to cloud-based applications. Access certification allows process and role owners to initiate on-demand or periodic access reviews to manage attestations that users only have the access rights necessary to perform their job functions. Access certification campaigns facilitate faster and accurate reviews of access by highlighting policy violations and permission conflicts in users' access entitlements across multiple applications that are to be revoked or approved under listed exceptions. More commonly based on resource level or hierarchy requirements, access certification capabilities are increasingly becoming risk aware to include micro-certifications based on the risk of an identity lifecycle event. Unlike periodic access certifications, event based micro-certifications contribute significantly to continuous Access Governance capabilities of an organization.
- **Role Governance:** Role governance refers to the capability of having control of and visibility into a role's entire lifecycle, from its inception to decommission. In a typical role-based access control (RBAC) setting, role governance monitors and tracks the following key processes for governing the role lifecycle. IGA tools provide varied level of support for governing each of these role lifecycle events:
  - 1) Role Definition - Defining a role based on the business functions and logically grouping the access entitlements based on the approved prototypes
  - 2) Role Approval - The process of seeking consent of business, process or role owners including appropriate role analysis and tracking of approvals with associated workflows
  - 3) Role Creation - Monitoring and auditing of tasks involved in implementation of approved roles in production
  - 4) Role Assignment – Performing SoD and other policy checks to ensure role assignment is compliant
  - 5) Role Modification - Ensuring that changes made to existing roles are approved, tracked and do not introduce new risks
  - 6) Role Optimization - Using intelligence from identity analytics for identifying inefficient use of roles and approval processes and implement measures to optimize roles to improve the efficiency of user access administration.
- **SoD Controls Management:** Segregation of Duties (SoD) Controls Management refers to the controls that are important to identify, track, report and often mitigate SoD policy violations leading to substantial risks of internal fraud in an organization. These controls are essential to manage role-based authorizations across applications with complex authorization model. However, IGA controls provide more course-grained abilities to identify SoD risks than at a fine-grained entitlement level found in other complex homegrown applications, especially ERP solutions. Key controls that are offered as part of SoD controls management include cross-system SoD risk

analysis, compliant user provisioning, emergency access management, advanced role management, access certifications with SoD analysis, transaction monitoring and auditing and reporting.

- **Reporting and Dashboarding:** This refers to creation of valuable intelligence in formats that are easily ingestible by business functions for the purposes of enhancing governance and supporting decision making. Reporting is facilitated by in-built reports with provisions provided for customized reporting. Dashboarding is an important auditing control that allows for easy and business-friendly abstraction of metrics and data modelling to monitor effective operation of IGA processes. IGA vendors offer in-built templates for reporting with the ability to customize reporting to suite business's auditing and reporting objectives. Most vendors allow for IGA data export using specified industry formats into third-party reporting and analytics tools for advanced data modelling and business intelligence. For the purpose of evaluation of reporting and dashboarding capabilities of IGA vendors in this Leadership Compass, besides common reporting using in-built templates, we look at the ability of vendors to provide the breadth and flexibility of data model for customized reporting as well as the dashboarding capability to support complex and granular data metrics for easy interpretations.

Besides the core IGA capabilities described above, we also consider several operational factors in our evaluation of IGA vendors for this Leadership Compass. These operational criteria are:

- **User Experience (UX):** UX is an important aspect of IGA for security and IAM leaders trying to bridge the gap between the inconvenience of security controls and demand for enhanced user engagement through self-service options. Traditional IGA controls are overladen with several inefficiencies including poor design of user and admin interfaces that prevent easy understanding and completion of common IGA tasks. There is an increased need for organizations to ensure that IGA tools support their UX goals. Most vendors have significantly re-engineered their user interfaces to support better UX, a shopping cart paradigm for requesting access being the most common approach today. Many others are offering mobile support for common IGA tasks such as access requests, password resets and request approvals.
- **Automation support:** Automation of common IGA tasks has always been a priority for organizations to reduce the inaccuracy and administrative inefficiency encountered by manual completion of IGA tasks in the direction of making IGA operations leaner and achieve lower TCO. Most IGA tools provide support for automated provisioning and fulfilment leading to basic automation of IGA requirements. Some organizations have advanced requirements for automation such as automated access reviews and event-driven access certifications. While some vendors have started to support these capabilities, IAM leaders must ensure the right mix of manual and automated IGA processes to ensure the effectiveness of processes is preserved by continuously monitoring them against defined key performance indicators (KPIs).
- **Ease of deployment:** A lack of skillset combined with complexity of IGA deployments has led organizations to seek external help and actively engage IAM professional service providers to help with deployments. This can increase the overall TCO of IGA deployments by nearly three folds during the initial years of your IGA deployment. It is

important that IGA vendors allow for easy deployment approach for organizations to help manage with available internal resources. Besides underlying software design, IGA products should allow for easy customizations using common scripting languages as well as offer support for configuration and change management. This includes availability of features that help organizations reduce environment-based configurations such as support for DevSecOps and scripted deployments. We also evaluate ease of product upgrades along with the ease of configuring the product for operational requirements such as high availability, automated failover and disaster recovery.

- **Third-party Integrations:** IGA products are required to integrate with several other enterprise products and applications to deliver the expected business value. Most common integrations with IGA products as evidenced in the market are integrations with:
  - 1) IT Service Management (ITSM) tools, primarily ServiceNow, to essentially offer a common front-end for users to request access and other help-desk related tasks
  - 2) Unified Endpoint Management (UEM) tools to make IGA tasks accessible on mobile devices and even extending mobile Single Sign-On to IGA
  - 3) Privileged Access Management (PAM) tools to offer emergency access management for complex authorization model applications and for privileged Access Governance
  - 4) User Behavior Analytics (UBA) tools to help organizations establish a baseline of user behavior with feeds from identity analytics and detect anomalous behavior.
  - 5) Data Governance (DG) tools to extend standard IGA controls to data and information stored across multitude of systems including device endpoints, file shares, network mounts etc.

**Scalability and Performance:** With an increasing IT landscape for organizations, IGA deployments can easily go under stress to perform better in terms of process execution, target integration as well as overall scalability. IGA products are evaluated based on their ability to scale-up for accommodating an increase in the number of users, identity attributes, roles, managed targets and system connections. Many IGA tools have recently undergone significant product re-architecture to meet the scalability and performance needs of the organizations in a digital era.

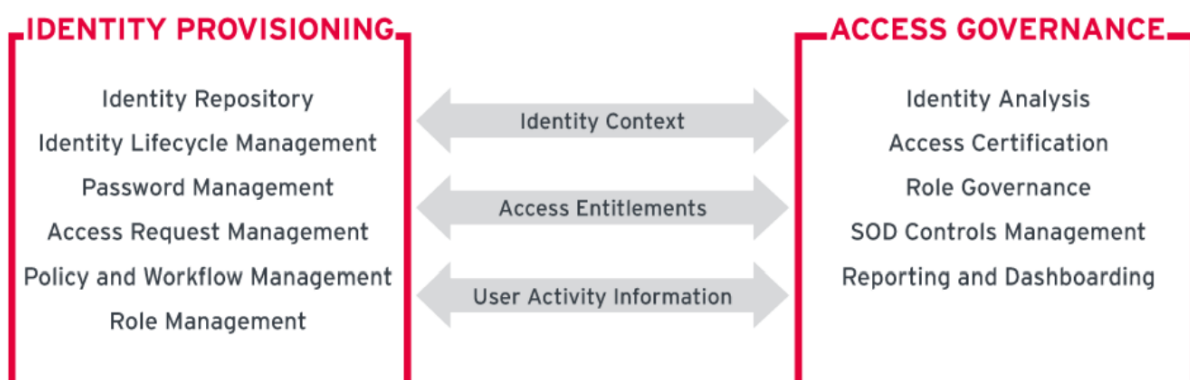


Figure 1: Representation of core IGA functions by 'Identity Lifecycle Management' and 'Access Governance' categories

## Delivery Models

This Leadership Compass is focused on products that are offered in on-premises deployable form, either at the customer's site or deployed and offered as a managed service by a Managed IAM Service Provider. We do not look at IDaaS (Identity as a Service) offerings in this Leadership Compass.

KuppingerCole has published separate Leadership Compass document on IDaaS, including IDaaS B2E, which are focused on IDaaS solutions supporting IGA for hybrid environments, delivered as a service.

## Required Capabilities

During our evaluation of IGA vendors for the purpose of representation in this Leadership Compass, we look at several evaluation criteria including but not limited to the following groups of capabilities:

- Target System Connectivity
- Access Review
- Access Risk Management
- User Interface and Mobile Support
- Access Request & Approval
- Access Intelligence
- Authentication
- Data Model

Each of the above group of capabilities requires one or more of the functions listed below to satisfy the criteria:

- Workflow support for request and approval processes
- Workflow support for role lifecycle management
- Tools that support graphical creation and customization of workflows and policies
- Centralized identity repository
- Access Intelligence capabilities
- Flexible role management with support for role governance
- Support for risk-aware, event-based access review certifications and targeted access review requests
- Support for SoD policies and continuous SoD controls monitoring
- Flexible customization of the UI to the specific demand of the customer organization
- Baseline connectivity to target systems and to Identity Lifecycle Management systems
- Cloud connectors, adding Access Governance support for common cloud services
- Customization of mapping rules between central identities and the accounts per target system
- Business-friendly user interface
- Strong and flexible delegation capabilities



In addition to the above functionalities, we also consider the depth of product's technical specifications for the purpose of evaluation in this Leadership Compass. These product specifications primarily include the following:

- **Connectivity:** The ability to connect to various sources of target systems, including direct connections, integration with existing Identity Lifecycle Management tools from various vendors, and integration to ITSM (IT Service Management) or Helpdesk ticketing tools. In general, we expect Access Governance solutions of today to not only read data from target systems but also initiate fulfilment and reconcile changes.
- **Heritage of connectors:** Having connectors as OEM components or provided by partners is not recommended and considered a risk for ongoing support and available know-how at the vendor.
- **SRM interfaces:** We expect that systems provide out-of-the-box integration to leading ITSM systems for manual fulfilment of provisioning requests.
- **SPML/SCIM support:** Support for SCIM (System for Cross-domain Identity Management) is preferred over traditional SPML (Service Provisioning Markup Language) for federated as well as on-prem provisioning. However, we evaluate support for both the standards depending on specific use-cases.
- **Deployment models:** Supporting multiple delivery options such as hard/soft appliances and optional MSP services gives customer a broader choice.
- **Customization:** Systems that require little or no coding and that support scripting or, if programming is required, SDKs or support for a range of programming languages, are preferred. We here also look for transport mechanisms between IT environments (e.g., development, test, and production), and the ability of keeping customizations unchanged after upgrades.
- **Mobile interfaces:** Secure apps providing mobile access to certain key capabilities of the product such as access request approvals etc.
- **Authentication mechanisms:** We expect IGA products to support basic authentication methods but use of multi-factor authentication methods to limit the risk of fraud using these systems is considered an advantage. Secure but simplified access for business users takes precedence.
- **Internal security model:** All systems are required to have a sufficiently strong and fine-grained internal security architecture.
- **High Availability:** We expect IGA products to provide built-in high-availability options or support for third-party HA components where required.
- **Ease of Deployment:** Complexity of product architecture and its relative burden on time to deploy as well as configuration and integration of basic services such as authentication, single sign-on, failover and disaster recovery should be minimal.
- **Multi-tenancy:** Given the increasing number of cloud deployments, but also specific requirements in multi-national and large organizations, support for multi-tenancy is highly recommended.
- **Shopping cart paradigm:** These approaches are popular for simplifying the access request management process by using shopping cart paradigms familiar to the users. Lately, there is an increasing trend towards integration to ITSM/ Service Desk solutions such as ServiceNow for access requests.
- **Standards:** Support for industry standards for direct provisioning including well known protocols like HTTP, Telnet, SSH, FTP etc.

Support for industry standards for federated provisioning, including OpenID Connect, OAuth and SCIM.

- **Analytical capabilities:** Analysis of identity and entitlement data to support capabilities like role management, access requests and policy management. Advanced analytical capabilities beyond reporting, using standard BI (Business Intelligence) technology or other advanced approaches, such as deep machine learning for automated reviews, are becoming increasingly important
- **Role and risk models:** Especially for the governance part of IGA products, what is becoming increasingly important is the quality and flexibility of role and risk models. These models not only need to be relevant but also need to have a strong conceptual background with sufficient flexibility to adapt to the customer's risk management priorities. It is important that organizations do not spend a lot of efforts in adapting their business processes to match the templates offered by the tool, rather have a tool that offers sufficient flexibility to adapt to their IGA requirements.
- **Data Governance:** Support for Data Governance, i.e., the ability to ensure access to data assets is controlled (roles, policies) and assist organizations with data compliance regulations.
- **Role/SoD concept:** Should be able to analyze enterprise as well as application roles for inherent SoD (Segregation of Duty) risks and continuously monitor for new SoD risks being introduced and offer remediation measures

All these technical specifications are subsequently evaluated for scoring each vendor on this Leadership Compass. The score arrived at following the evaluation of these technical specifications is added to our evaluation of the IGA products. We also look at specific USPs (Unique Selling Propositions) and innovative features of products in the overall evaluation which distinguish them from other offerings available in the market.

## Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership



## Overall Leadership

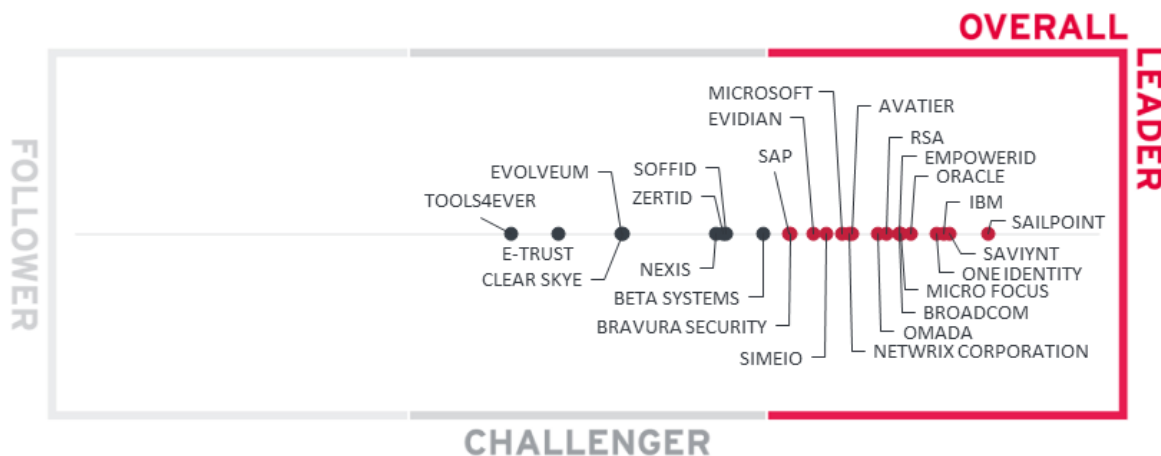


Figure 2: The Overall Leadership rating for the IGA market segment

When looking at the Leader segment in the Overall Leadership rating, we see a picture that is a typical representation of very mature markets, where a considerable number of vendors deliver feature-rich solutions. The market continues to remain crowded, with 25 vendors we chose to represent in our Leadership Compass rating with a few other vendors that did not meet our basic evaluation criteria, are new entrants into the market listed in the "vendors to watch" section or declined participation in this year's edition.

SailPoint retains its leadership position in the Overall Leadership evaluation of the IGA market. IBM, Saviynt and One Identity are close behind followed by Oracle, EmpowerID, Micro Focus, Broadcom, RSA. This group of vendors is made up of well-established players. We strongly recommend further, detailed analysis of the information provided in this document for choosing the vendors that are the best fit for your requirements.

Other vendors in the Overall Leaders segment for IGA include Avatier, Microsoft, Netwrix Corporation, Simeio, Evidian, Bravura Security and SAP. Omada has improved its capabilities to be now listed in the overall leader's section compared to being a challenger during last report. This group of vendors is a mix of established and emerging players, some being stronger in their market position, and others with a considerable push into the Overall Leader segment with their improved ratings for product, market, and innovation evaluation criteria.

The Challenger segment is less populated than the Leaders segment and features established vendors, vendors frequently being more regional-focused, and several niche vendors with fit-for-purpose IGA capabilities and preferred by many organizations over the established players. Leading in this segment are Beta Systems followed by Soffid, Nexis and ZertID. Evolveum and Clear Sky follow with some distance. Further vendors in this segment are E-Trust and Tools4ever. The Challenger segment shows vendors with good products with varying levels of IGA capabilities, market presence throughout the world, or other market niche focus.

Overall Leaders are (in alphabetical order):

- Avatier
- Broadcom
- Bravura Security
- EmpowerID
- Evidian
- IBM
- Micro Focus
- Microsoft
- Netwrix Corporation
- Omada
- One Identity
- Oracle
- RSA
- SAP
- SailPoint
- Saviynt
- Simeio

## 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 IGA market segment

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

As Identity Governance and Administration is constantly maturing, we find a number of vendors qualifying for the Leaders segment as well as a number of vendors adding IGA capabilities to their portfolio of product features. As vendors offer a wide variety of IGA capabilities and differ in how well they support these capabilities, it is important for organizations to perform a thorough analysis of their IGA requirements to align their priorities while evaluating an IGA solution.

Leading from the front in Product Leadership is SailPoint, closely followed by Saviynt, Oracle, EmpowerID, One Identity, Micro Focus, IBM, Omada. Broadcom, RSA, Simeio and Avatier comes later in the upper range of the Leader's segment, followed by a group of vendors including Bravura Security, Evidian, Beta Systems, Microsoft and Netwrix Corporation and ZertID all of which deliver leading-edge capabilities across the depth and breadth of IGA capability spectrum evaluated for the purpose of scoring the vendors in this Leadership Compass. IAM leaders must exercise appropriate caution while evaluating these vendors as subtle differences ignored in functionality evaluation of these products could translate into greater incompatibilities for business processes during implementation. Therefore, it is highly recommended that organizations spend considerable resources in properly scoping and prioritizing their IGA requirements prior to IGA product evaluation. Bravura Security with its strong IGA capabilities has moved from Challenger to the leader segment this year.

In the challenger's segment of product leadership are (in alphabetical order) Clear Skye, E-Trust, Evolveum, Nexis, SAP, Soffid and Tools4ever. All these vendors have interesting offerings but lack certain IGA capabilities that we expect to see, either in the depth or breadth of functionalities.

Product Leaders (in alphabetical order):

- |                    |                       |
|--------------------|-----------------------|
| • Avatier          | • Netwrix Corporation |
| • Beta Systems     | • Omada               |
| • Bravura Security | • One Identity        |
| • Broadcom         | • Oracle              |
| • EmpowerID        | • RSA                 |
| • Evidian (Atos)   | • SailPoint           |
| • IBM              | • Saviynt             |
| • Micro Focus      | • Simeio              |
| • Microsoft        | • ZertID              |
| •                  |                       |

## 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.

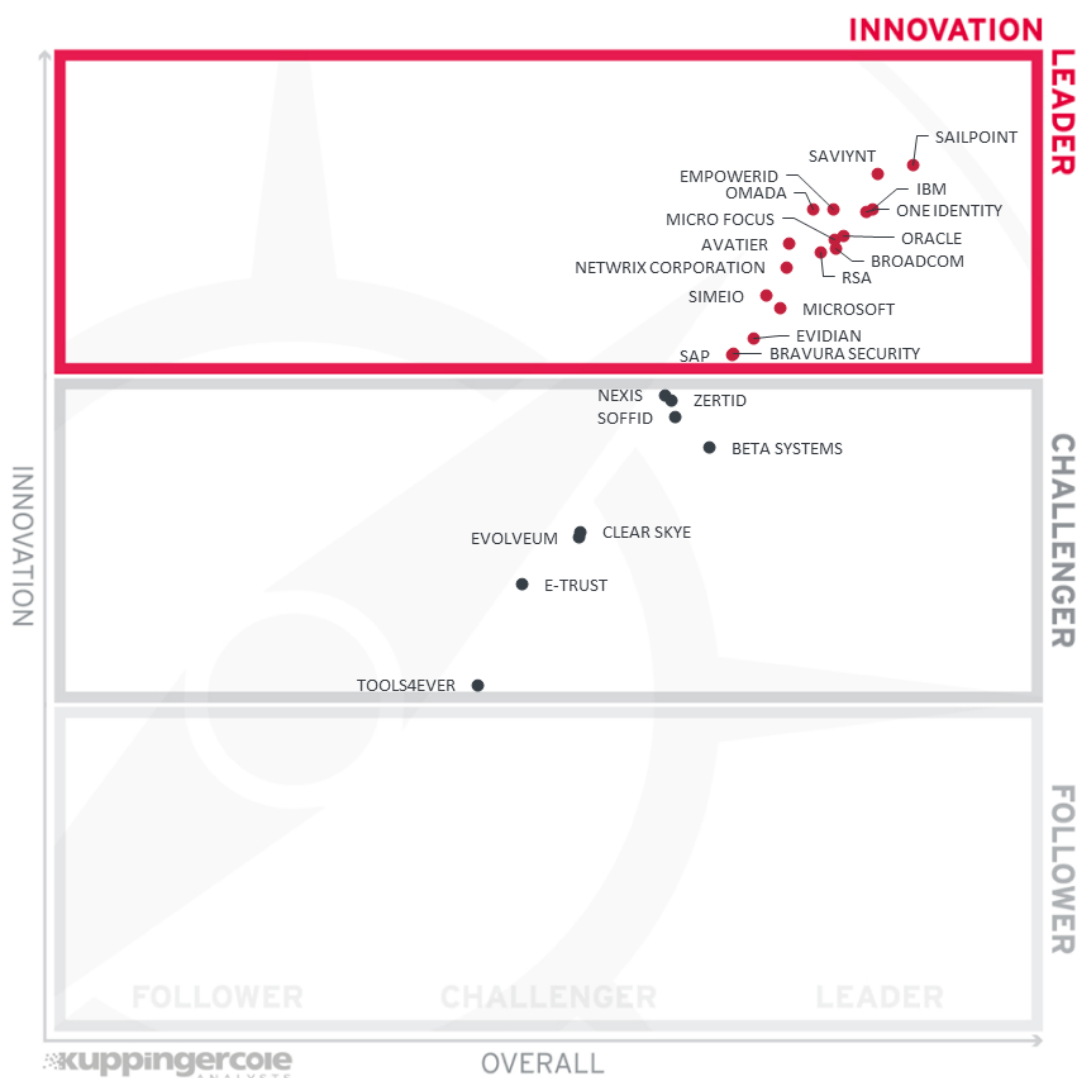


Figure 4: Innovation Leaders in the IGA market segment

We rated less than half of vendors as Innovation Leaders in the Identity Governance and Administration (IGA) market. Given the maturity of IGA solutions, the amount of innovation we see is somewhat limited. The vendors, however, continue to differentiate by innovating in several niche areas, from identity & access intelligence, modern UIs, containerized products, microservice architectures, and improved API layers to more specific areas such as improvements to access certification as examples, delivering better flexibility and automation. While ease of deployment remains an important capability for IGA products, desired levels of scalability and flexibility can considerably affect the ease of deployment for most large IGA deployments. Another innovation area is around simplifying and automating access review, specifically by applying predictive and other forms of analytics.

The graphic needs to be carefully read when looking at the Innovation capabilities, given that the x-axis indicates the Overall Leadership while the y-axis stands for Innovation. Thus, while

some vendors are closer to the upper-right edge, others being a little more left score slightly higher regarding their innovativeness.

SailPoint leads the Innovation Leadership evaluation followed by Saviynt. A group of vendors of IBM, EmpowerID, One Identity and Omada are followed by a distance. A group of vendors follows the leaders closely and are next on the chart (in alphabetical order) Avatier, Broacom, Micro Focus, Netwrix Corporation, Oracle and RSA continue to strengthen their IGA leadership position with constant innovation. Simeio and Microsoft appearing in the lower of the segment with Evidian, Bravura Security and SAP near the lower border of the segment. These vendors are making significant changes to their IGA product portfolio to be in line with other innovative vendors in the market. These vendors differ in many details when it comes to innovation and balancing it with overall product leadership. Therefore, a thorough vendor selection process is essential to pick the right vendor of all the IGA players that best fit the customer requirements.

About half of the players made it to the Innovation Challenger segment that includes SAP, Nexis, Soffid and Beta Systems Netwrix Usercubenear the upper border. Another group of vendors in the upper mid-section (in alphabetical order) are Accenture, Clear Skye, Evolveum and ZertID. All these vendors have also been able to demonstrate promising innovation in delivering specific IGA capabilities. Another group of vendors appears in the lower half of the Challenger segment: (in alphabetical order) E-Trust, ideiio, Tools4ever and Tuebora. Please refer to the vendor pages further down in the vendor's section of this report for more details.

Systancia has strong IGA capabilities but are ranked in the Follower segment due to lacking the breadth in innovative features we'd like to see from IGA vendors.

Innovation Leaders (in alphabetical order):

- Avatier
- Bravura Security
- Broadcom
- EmpowerID
- Evidian (Atos)
- IBM
- Micro Focus
- Microsoft
- Netwrix Corporation
- Omada
- One Identity
- Oracle
- RSA
- SAP
- SailPoint
- Saviynt
- Simeio

## 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 IGA market segment

The Market Leadership evaluation paints a different picture of vendors. With a group of leading, well-established IGA players, many others are new entrants or are rated low for several reasons, including limited market presence in certain geographies, limited industry focus, and a relatively smaller customer base.

With a strong market position, successful execution, and strengthened IGA product features SailPoint continues to lead the segment followed closely by IBM and One Identity with Microsoft and Broadcom at some distance. Closely following these vendors in the Market Leadership segment are (in alphabetical order) Beta Systems, Evidian, Micro Focus, Netwrix Corporation, Oracle, RSA, SAP and Saviynt. Bravura Security and EmpowerID appears near the bottom border. All vendors in this segment have several deep-rooted complex IGA deployments across multiple industries.

In the Challenger section, we find Simeio, Avatier, Omada and Soffid at the top section. While we count them amongst Market Leaders in other areas of the overall IGA market, their position in the IGA market is affected by several factors, including relatively lower global presence and a shortage of technology partners with their IGA product deployment as examples. Following this group (in alphabetical order) is Clear Skye, Evolveum, Nexis, Tools4ever and ZertID near the center. E-Trust appear in the lower half of the challenger segment with considerable gaps in the specific areas we evaluate for Market Leadership of IGA products, including the number of customers, average size of deployments, effectiveness of their partner ecosystem, etc.

Market Leaders (in alphabetical order):

- Beta Systems
- Bravura Security
- Broadcom
- EmpowerID
- Evidian
- IBM
- Micro Focus
- Microsoft
- Netwrix Corporation
- One Identity
- Oracle
- RSA
- SAP
- SailPoint
- Saviynt



## 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.

## 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 comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of "overperforming" in the market. 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 the upper right segment, we find the "Market Champions." Given that the IGA market is maturing fast, we find SailPoint, One Identity and IBM as market champions being positioned in the top right-hand box.

Close to this group of established IGA players, in the same box, are (in alphabetical order) Beta Systems, Broadcom, Evidian, Microsoft, Micro Focus, Netwrix Corporation, Oracle, RSA, Saviynt. Being positioned closer below the axis, Bravura Security and EmpowerID represents their inclination for stronger product leadership in comparison to the market leaders today.

SAP is positioned in the box to the left of market champions, depicting their stronger market success over the product strength.

In the middle right-hand box, we see the four vendors that deliver strong product capabilities for IGA but are not yet considered Market Champions. Simeio, Avatier, Omada and ZertID have a strong potential for improving their market position due to the stronger product capabilities that they are already delivering.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not Market Leaders as of yet. They also have moderate market success as compared to market champions. These vendors include (in alphabetical order) Clear Skye, E-Trust, Evolveum, Nexis, Soffid and Tools4ever.

## 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.

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

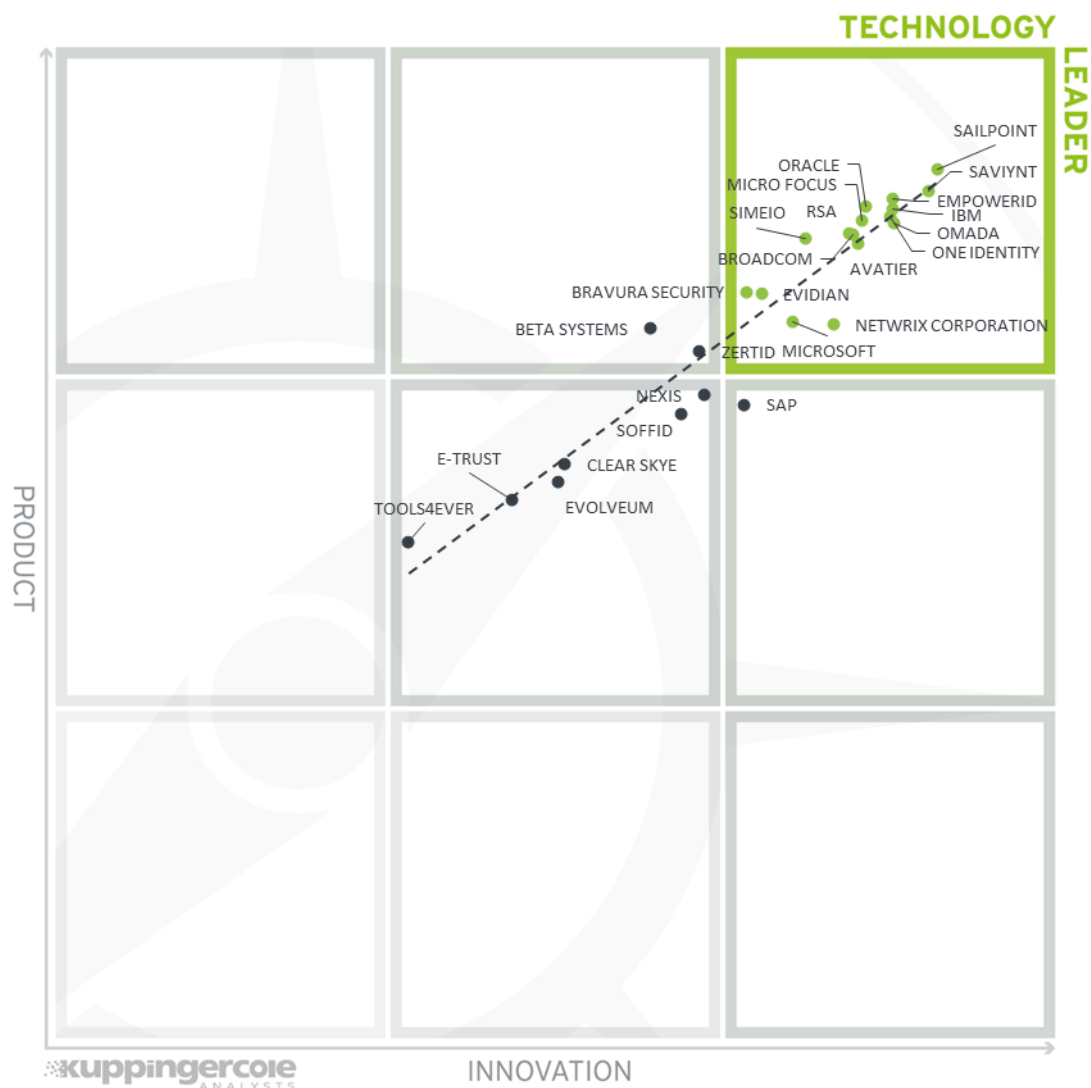


Figure 7: The Product/Innovation Matrix

Here, we see a good correlation between the product and innovation rating. Most vendors are placed close to the dotted line, indicating a healthy mix of product and innovation leadership in the market. Vendors below the line are more innovative. Vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Looking at the Technology Leaders segment, we find most of the leading vendors in the upper right corner, scattered throughout the box. The top-notch vendor is SailPoint, closely followed by Saviynt and EmpowerID and the remainder (in alphabetical order) Avatier, Bravura Security, Broadcom, Evidian, IBM, Micro Focus, Microsoft, Netwrix Corporation, One Identity, Oracle, Omada, RSA and Simeio - with most placing close to the axis depicting a good balance of product features and innovation.

In the top middlebox, we see Beta Systems and ZertID with slightly less innovation than the leaders in this section but still have a good product feature set.

In the center middlebox, we find (in alphabetical order) Clear Skye, E-Trust, Evolveum, Nexis, Soffid, and Tools4ever having less product and innovations than the Technology

Leaders. SAP appears just into the middle right box indicating slightly more innovation than product strength.

## 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 below the line are more innovative, vendors above the line are, compared to the current Market Leadership positioning, less innovative.

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.

In the upper right-hand corner box, we find the "Big Ones" in the IGA market. We see the large ones more on top, including (in alphabetical order) Broadcom, Evidian, IBM, Micro Focus, Microsoft, Netwrix Corporation, One Identity, Oracle, RSA, SAP, SailPoint, and Saviynt. Bravura Security and Empower ID is placed in the same box, more towards the bottom, indicating relatively lower market position as compared to the other established vendors.

Simeio, Avatier and Omada appear in the middle right box showing good innovation with slightly less market presence than the vendors in the "Big Ones" category.

In the middle top box, we find Beta Systems with a strong market position but not scoring for Innovation Leadership.

The segment in the middle of the chart contains the vendors rated as challengers both for market and innovation leadership, which includes (in alphabetical order) Clear Skye, E-Trust, Evolveum, Nexis, Soffid, Tools4ever and ZertID.

## Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Identity Governance and Administration 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	Deployment	Interoperability	Usability
<b>Avatier Identity Anywhere</b>	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
<b>Beta Systems Garancy IAM Suite</b>	Strong Positive	Positive	Positive	Positive	Strong Positive
<b>Bravura Security Fabric</b>	Strong Positive	Positive	Strong Positive	Positive	Positive
<b>Broadcom Symantec Identity Governance and Administration (IGA)</b>	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
<b>Clear Skye IGA</b>	Positive	Neutral	Positive	Neutral	Positive

<b>EmpowerID IAM Suite</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>E-Trust Horacius IAM</b>	Positive	Neutral	Positive	Neutral	Positive
<b>Evidian (Atos) IGA, Evidian Analytics</b>	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
<b>Evolveum MidPoint</b>	Positive	Positive	Positive	Positive	Positive
<b>IBM Security Verify</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>Micro Focus NetIQ IGA Suite</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>Microsoft Entra Identity Governance</b>	Strong Positive	Positive	Positive	Positive	Strong Positive
<b>Netwrix Usercube IGA</b>	Positive	Strong Positive	Positive	Positive	Strong Positive
<b>NEXIS 4</b>	Positive	Positive	Positive	Positive	Strong Positive
<b>Omada Identity Cloud, Omada Identity</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>One Identity Manager</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>Oracle Identity Governance Suite</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>RSA Governance &amp; Lifecycle</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>SailPoint Identity Security Platform</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>SAP Access Control &amp; Identity Access Governance</b>	Positive	Positive	Positive	Positive	Positive
<b>Saviynt Enterprise Identity Cloud Platform</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>Simeio IGA Managed Services</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>Soffid IAM</b>	Positive	Positive	Positive	Positive	Strong Positive
<b>Tools4ever HelloID</b>	Positive	Neutral	Neutral	Neutral	Positive
<b>ZertID</b>	Strong Positive	Positive	Positive	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
<b>Avatier</b>	Strong Positive	Neutral	Positive	Positive
<b>Beta Systems</b>	Neutral	Positive	Strong Positive	Strong Positive
<b>Bravura Security</b>	Neutral	Positive	Neutral	Strong Positive
<b>Broadcom</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>Clear Skye</b>	Neutral	Positive	Neutral	Neutral
<b>EmpowerID</b>	Strong Positive	Positive	Positive	Positive
<b>E-Trust</b>	Weak	Neutral	Neutral	Neutral
<b>Evidian (Atos)</b>	Positive	Positive	Positive	Strong Positive
<b>Evolveum</b>	Weak	Neutral	Weak	Strong Positive
<b>IBM</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>Micro Focus</b>	Strong Positive	Strong Positive	Strong Positive	Positive
<b>Microsoft</b>	Positive	Strong Positive	Strong Positive	Positive
<b>Netwrix Corporation</b>	Strong Positive	Strong Positive	Strong Positive	Positive
<b>Nexis</b>	Positive	Neutral	Neutral	Neutral
<b>Omada</b>	Strong Positive	Neutral	Neutral	Positive
<b>One Identity</b>	Strong Positive	Strong Positive	Positive	Strong Positive
<b>Oracle</b>	Strong Positive	Strong Positive	Strong Positive	Positive
<b>RSA</b>	Positive	Positive	Strong Positive	Strong Positive
<b>SailPoint</b>	Strong Positive	Strong Positive	Strong Positive	Strong Positive
<b>SAP</b>	Positive	Strong Positive	Strong Positive	Positive
<b>Saviynt</b>	Strong Positive	Positive	Positive	Strong Positive
<b>Simeio</b>	Positive	Positive	Positive	Positive
<b>Soffid</b>	Positive	Positive	Positive	Positive
<b>Tools4ever</b>	Critical	Positive	Positive	Neutral
<b>ZertID</b>	Positive	Neutral	Neutral	Positive

Table 2: Comparative overview of the ratings for vendors



## 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 Identity Governance and Administration (IGA) , we look at the following eight categories:

- **Identity Lifecycle Management:** The ability to provision and manage identities, access entitlements, and other identity-related information in the target systems over its lifecycle. Also, other capabilities considered, among others, is the ability to access identity stores, data modeling & mapping, as well as the ability to handle different identity types.
- **Target System Support:** Considered are the number of connectors and the breadth of target systems that the solution can connect to, including, e.g., directory services, business applications, mainframe systems, etc. Connector breadth also looks at support for standard cloud services. Connector depth further examines customization capabilities for connectors through connector toolkits and standards as examples and the connectors' abilities, especially when it comes to connecting to complex target systems such as SAP environments or mainframes.
- **Self-Service & Mobile Support:** User self-service interfaces and support for secure mobile access to selected IGA capabilities. Other capabilities include authenticator options, delegation of tasks and password reset.
- **Access & Review Support:** Integrated Access Governance capabilities that support activities such as the review and disposition of user access requests, certification definition & campaigns, and access remediation. Also looked at is Segregation of Duty (SoD) controls to identify, track, report, and mitigate SoD policy violations as part of integrated risk management capabilities, as well as role management and policy management capabilities.
- **Identity & Access Intelligence:** IGA intelligence that provides business-related insights supporting effective decision making and potentially enhancing governance. Advanced capabilities such as use of AI and/or machine learning techniques that enable pattern recognition for process optimization, role mining, role design, automated reviews, and anomaly detection are considered. Other capabilities can include the use of user access information from authentication and authorization events used for analyzing user access behavior patterns and detecting anomalous access.
- **Workflow & Automation:** Advanced workflow capabilities, including graphical workflow configuration, and the extent to which common IGA tasks can be automated.

- **Centralized Governance Visibility:** This is the extent to which the identities and their access under governance control can be viewed in a consolidated or single-pane view, such as in a dashboard format. Centralized access to reports and auditing support is typically also provided.
- **Architecture & Hybrid Environment:** This category represents the combination of architecture and hybrid environment support. In architecture, we look at the type of architecture and focus on modern, modular architectures based on microservices. This also affects deployment, given that container-based deployments provide good flexibility. Also evaluated is the solution's ability to support a hybrid environment for customers that anticipate or are currently taking an intermediate step towards migrating from on-premises to the cloud.

## Avatier – Avatier Identity Anywhere

Based in California (US), Avatier is one of the few IGA vendors that continues to exhibit innovative changes to adapt to evolving market demands in the recent past. From focusing 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. Avatier's Identity Anywhere provides a fully containerized IGA platform primarily to solve deployment and scalability issues of traditional IGA.

Identity Anywhere supports all core IGA functionalities. Lifecycle Management is its primary Identity Provisioning component and Group Automation/Self-Service, Workflow Manager, and Identity Analyzer supporting the Access Governance capabilities. SPML and SCIM is supported for identity provisioning/de-provisioning and the solution has a broad set of OOB provisioning connectors available for a wide range of on-premises and cloud systems. Avatier can develop and implement custom connectors based on requirements within two weeks' time. OOB integration is available to ServiceNow, Cherwell, BMC Helix ITSM and Atlassian Jira ServiceDesk. Solution has good support for a wide range of container-based platforms. SOAP, REST, SCIM, SAML, and OAuth API protocols are supported. Wide range of popular programming language SDKs for developers is also. The majority of Identity Anywhere functionality is accessible via REST APIs as well as some functionality via CLI.

Avatier provides a universal UI of Identity Anywhere across different devices such as mobile, web, extensions (slack, MS team, chatbots, MS Outlook). The solution allows frictionless authentication via MFA and FIDO. A very impressive list of authenticators for user self-service and admin access is available. Passwordless authentication is supported by leveraging existing integrated MFA providers. The identity lifecycle management UI is modest and can be configured only by the admin. Access approval/ rejection is controlled via a risk-based mechanism where the risk scoring matrix is configurable. Access review and certification campaigns in process have a good overview and can be downloaded and exported into CSV files.

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 that covers a wide range of governance use cases. Planned features include a full compliance control integration by regulatory framework and creation of user specific dashboards for audit, compliance, privacy and security. Overall, Avatier's Identity Anywhere container-based platform is an improvement in the IGA market. Organizations across the industry verticals seeking a solution to traditional IGA deployment challenges should consider Avatier's Identity Anywhere.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



## Strengths

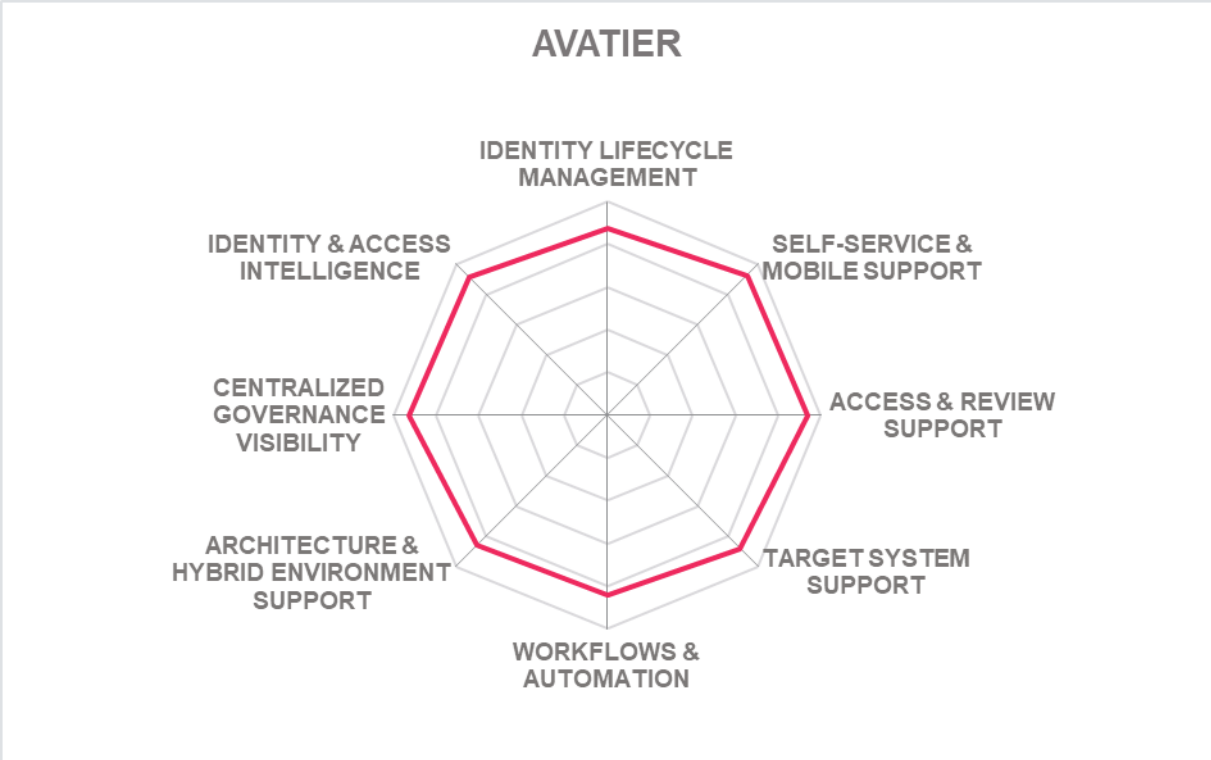
- Container based platform support
- Identity lifecycle management
- Strong target system support
- Wide range of OOB reports available for major compliance frameworks
- Good authenticator mechanism including passwordless authentication support
- Flexible policy and workflow management
- User friendly and modern UI

## Challenges

- Limited but growing presence and partner ecosystem outside North American market
- Multi tenancy not supported
- User dashboards are currently not customizable but planned for Q4 2022

Leader in





## Beta Systems – Garancy IAM Suite

Based in Germany, Beta Systems AG offers its Garancy IAM suite consisting of Identity Manager, User Center, Recertification Center, Systems Center, Data Access Governance, Process Center, Access intelligence Manager, Password Reset and Password Synchronization.

Garancy IAM suite supports on-premises as well as public and private cloud deployment, however, multi tenancy is not supported. The solution also supports hybrid installation with Garancy Identity Manager on-premises for identity administration and fulfillment, while IGA modules on cloud. The solution can be delivered as a service, virtual appliance, managed service and as a software deployed to the server. From 2022, support for container (Docker) based delivery is supported but hardware appliance delivery is missing. OOB integration to ITSM includes ServiceNow, Atlassian Jira ServiceDesk and BMC Helix ITSM. Garancy IAM's all functionalities are exposed via SOAP, REST, SCIM, LDAP and XML APIs while SDK support is limited to Java and JavaScript.

Garancy IAM supports a good variety of identity repositories. The solution specializes in bi-directional connectors and powerful hybrid cloud connectors via SCIM. The solution supports SCIM and SPML for identity provisioning and deprovisioning. It offers strong support for a wide range of OOB connectors for on-premises and SaaS systems. No functionality is accessible via CLI, and developer portal is not available either.

Good user self-service with wide range of authenticator options including passwordless for the admin as well and delegation of workflows are present. It has API based availability for micro services from this year, which allows orchestration for third party system. The solution supports reverting back changes after taking action, for example, deletion or reinstating of orphaned accounts. Strong support for wide range of IGA related OOB report types and reports for major compliance frameworks are available OOB.

Garancy IAM has admin and developer focused UI. The solution uses a browser interface with strong support for analytics for auditing and reporting purposes. From 2022 it has a new widget feature to illustrate affected objects and entities. The solution also supports strong B2B onboarding capabilities. Currently, the AI is in development for assignment of entitlements.

Beta Systems, founded in 1983, is a publicly listed company with a strong focus in the EMEA market. Its customers include mid-market and enterprise organizations with a relatively good share of small organizations. The partner ecosystem is limited outside EMEA with no plans soon to address these regions. Next features are focused on improving audit, a new SoD background validation service, and auto update of connectors with the target system.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive



## Strengths

- Good Workflow customization flexibility
- Strong user self-service support
- Impressive list of connectors for target system support
- Strong support for analytics
- Good set of capabilities for Identity life cycle management
- Support for Dynamic Authorization Management

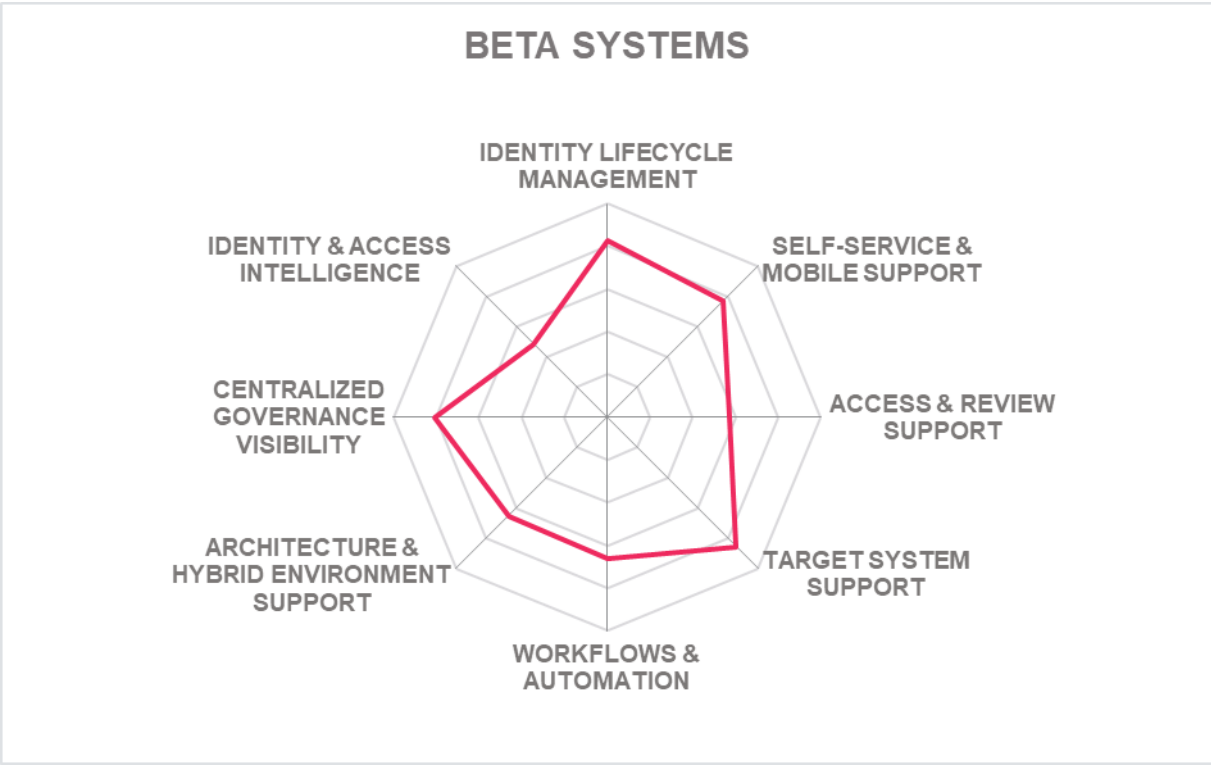
## Challenges

- Market presence focused in EMEA region
- Limited but growing partner ecosystem
- Limitation in devops and SDK support

Leader in







## Bravura Security – Bravura Security Fabric

Bravura Security, previously known as Hitachi ID, was recently acquired by the Volaris group. The Bravura Security Fabric supports identity lifecycle management automation, access governance, workflows, self-service identity, multi factor authentication, privileged access automation, decentralized credentials, and analytics. The common platform provides consistent UIs, database, connectors, and API throughout the other components in the Bravura Security Fabric. The current solution features self-service identity, federation and multi factor authentication, privileged access management, identity automation, privilege automation and decentralized credentials.

The solution supports all major deployment and delivery models including docker containerization. Virtual machines are utilized for core service hosting on EC2 platform. Bravura Security provides a single tenant solution. Bravura Security uses a multi-region architecture which supports hyper graining. All the functionalities of the solution are exposed via SOAP, REST APIs as well as CLIs, which are used for rich and complex secret management scenarios. SDK support is limited to 75% via Python.

Bravura Security Fabric supports all known identity repositories with the possibility to integrate with legacy solutions. The solution provides off-the-shelf universal connectors including support for SCIM, REST, and GraphQL. Strong support for OOB on-premises and SaaS connectors is offered. Good user self-service with a decent range of authenticators for access is present with good support for FIDO2. The solution supports secure sharing of credentials, as well as onboarding for privileged and Just-In-Time (JIT) identities.

Bravura Security is focused on Enterprise businesses with majority of presence in the North American market. The roadmap features include bringing AI and machine learning for identity classification, endpoint governance, anomaly detection, dynamic risk profiling, identity SOAR to the solution.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Positive



## Strengths

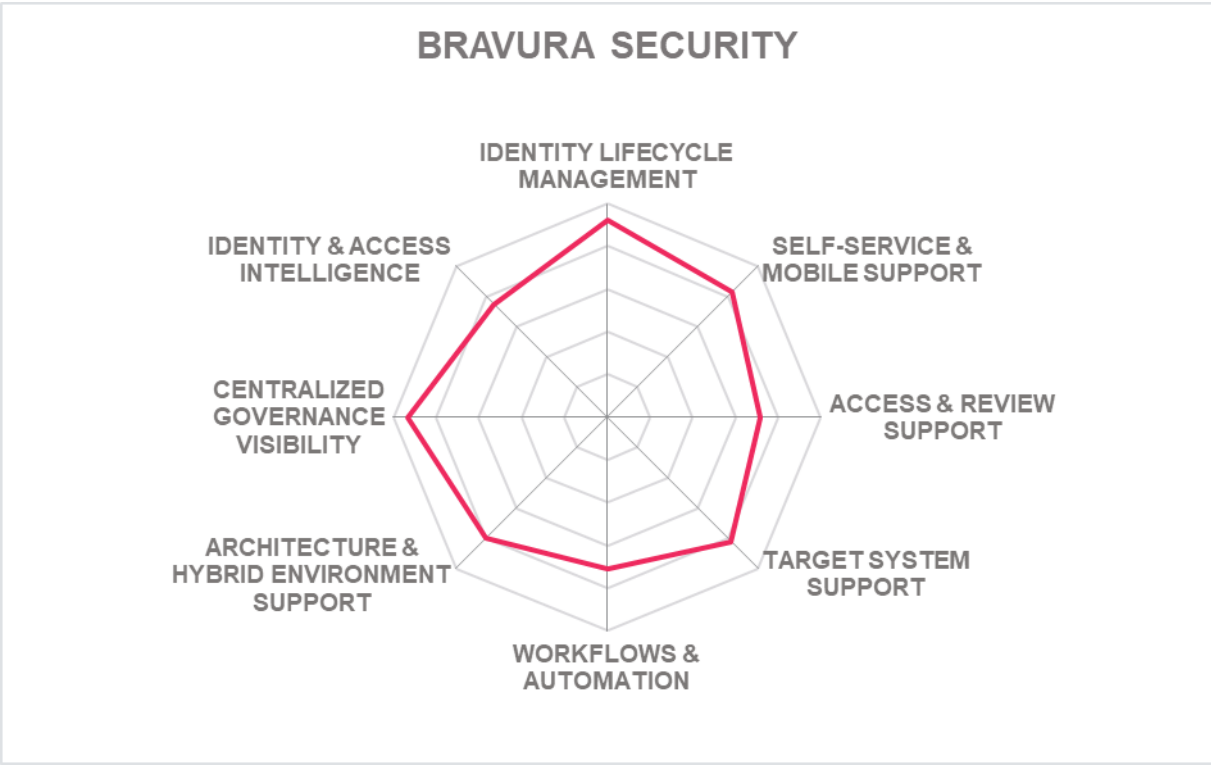
- Strong Identity Lifecycle management capabilities
- Good governance policies
- Good features for role and SoD management
- Strong support for access review and certification support
- Good support for user Self-service access
- Good deployment and delivery options
- Good support for reporting options and compliance framework support

## Challenges

- Limited presence outside North American market
- Limited set of authenticator options for admin but good FIDO2 support
- Quick approval processes missing, but planned in roadmap

Leader in





## Broadcom – Symantec IGA

Based in America, Broadcom is a manufacturer of semiconductor and infrastructure software products. It acquired CA Technologies in late 2018 and acquired the Symantec Enterprise business in late 2019. The former CA Security business is now part of the Symantec Enterprise Division of Broadcom. Broadcom's Symantec Enterprise portfolio includes Symantec Identity Governance and Administration (IGA), which consists of Identity Manager, Identity Governance, and the Identity Portal.

Symantec IGA is delivered as a virtual appliance or can be deployed to server as a software. The solution can be deployed on-premises, public or private cloud, hybrid, as well as offered as a license or subscription based. Around 75% of the functionalities of the solution are supported via SOAP, REST; SCIM, SCIM 2.0 or LDAP. SDKs are also offered, including Android, iOS, Java, C/C++, JavaScript, and AngularJS programming languages. The majority of the solution is delivered via SDK.

The solution strongly supports all known identity repositories. The products, fully capable of operating in silos, offer a strong line-up of IGA capabilities, including user access certification, SoD, entitlement clean-up, role discovery, automated workflows and policy management, access certification. Also offered are an access risk analyzer & simulator that can estimate a user's risk score based on the change in the context of an access request along with SoD check at shopping cart. Symantec IGA's UI is modern and user-friendly, making it productive for users, given its helpful context advice tools. All the functions are available on the home page. A customizable form for creating identities based on the requirements is provided. Certification campaign history is available via the consultation feature.

Symantec provides an entitlement catalog and shopping cart approach to usability. Strong support for out-of-the-box provisioning/de-provisioning is given for on-premises and SaaS applications. Customized connectors can be developed based on requirements.

Broadcom has a global presence in the medium to enterprise market segment, mostly in North America. It brings with it a large set of integration partners. Support for all known languages is provided 24x7. The product has potential to grow in terms of deployment options and has a roadmap for integrating AI/ML for access requests and provisioning, social account linking/importing, enhanced preference/personalization management, progressive profiling, Terms of Service (ToS) Management and auditing.

---

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive

---



### Strengths

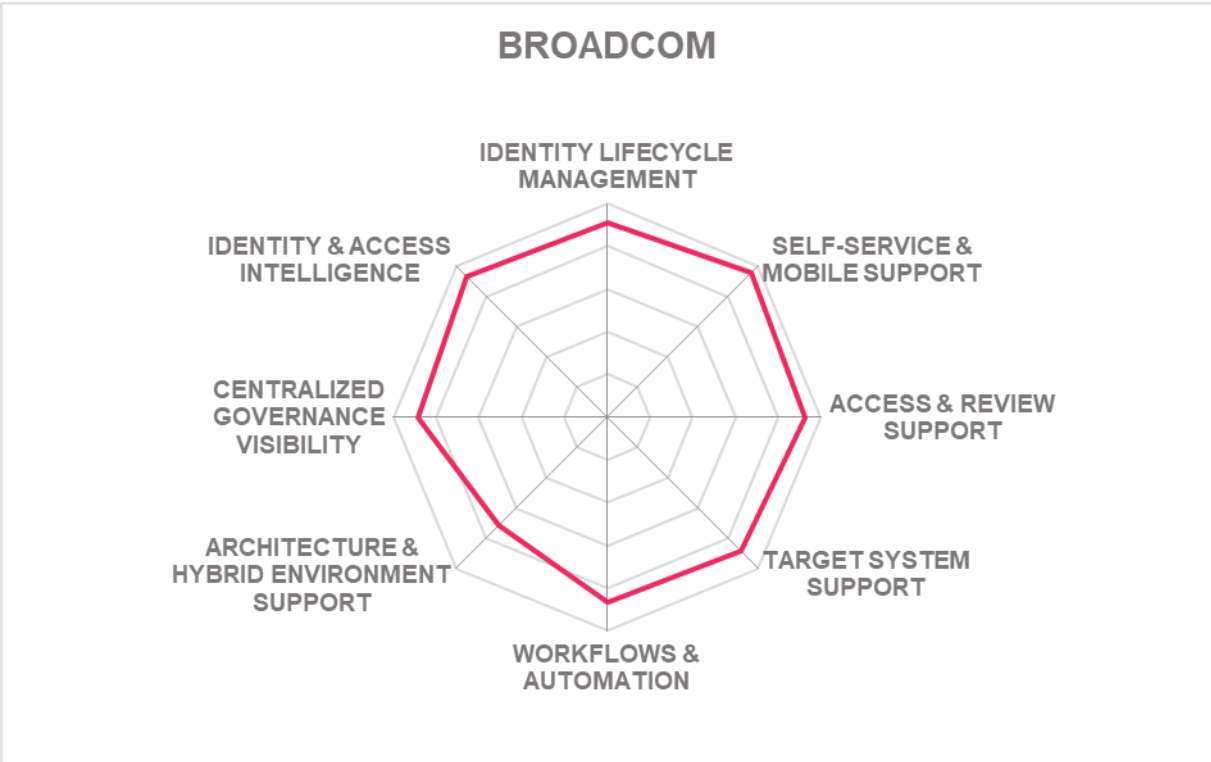
- Broad range of authenticators for user self-service and admin access
- Good capabilities for Identity lifecycle management
- Strong Policy management capabilities
- Workflow management
- Strong UI for Mobile
- Dashboard for analytics and reporting

### Challenges

- Limited product delivery option
- Limited support for OOB major compliance frameworks
- Limited product delivery options

Leader in







## ClearSkye – ClearSkye IGA

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 solely within ServiceNow. Customers install the application directly from the ServiceNow application store. Clear Skye IGA capabilities include Identity Lifecycle, Entitlement Management, Access Requests, Audit, Policy Management, Certifications (access reviews), Identity Analytics, and Workflows.

Being a native ServiceNow application, Clear Skye IGA utilizes the customers Now Platform database for managing accounts, access entitlements, and any other identity related information. The solution supports all known identities, and additional identity types can be configured. Attribute mapping from source to target is supported with each connector having defined capabilities. SCIM and SCIMv2 are supported for identity provisioning and deprovisioning. Since Clear Skye is a ServiceNow solution, OOB integration to other ITSM tools is missing. Clear Skye offers a moderate, but increasing, list of OOB provisioning connectors for both on-premises and SaaS systems although the ServiceNow Integration Hub can be leveraged as part of the IGA connectivity framework providing dozens of additional integrations.

Clear Skye IGA is delivered as a native ServiceNow as-a-service or can take advantage of ServiceNow's on-premises. ServiceNow customers benefit from the re-use of their existing ServiceNow investment in that Clear Skye IGA uses a customers' existing ServiceNow infrastructure with no additional components to procure or license. License-based and subscription-based deployment are also available. Clear Skye IGA uses the ServiceNow integration options for connecting to third party systems; both cloud and on-prem IGA connectors are available. For on-premises systems, the ServiceNow MID server is used. This is a standard Now platform component that is also available as a Docker container as of the San Diego platform release. Some services, such as Reporting, Database Services, and Security model are shared services on the Now Platform. Multi-tenancy is not supported. The product's functionalities are exposed via REST APIs. A majority of the functionalities of the solution are available via JavaScript SDK. Being on the Now Platform, the solution takes advantage of the native SDK which is exposed as JavaScript. Bidirectional integration is supported with connectors that populate the IGA Identity Warehouse as well as provisioning of access to target systems.

Clear Skye IGA uses the standard ServiceNow Service Portal as the interface to request access whereas an end user portal focuses on IGA for workers and supervisors. For requesting items, a standard ServiceNow experience is available via the ServiceNow catalog. The product has good integration of ServiceNow and functionalities for fulfilling the requests. It uses a good model for SoD checks and peer group analysis before forwarding the request to the system. Clear Skye IGA has a good user self-service model and uses a shopping cart paradigm. Visual workflows to see access request status are possible.

Clear Skye has good access review capabilities, with many access review templates provided out of the box and the ability to define additional access review capabilities. Access Review. Access Reviews are performed directly in the ServiceNow Service Portal.

Clear Skye supports delegation of recertifications for a specific period. For auditing purposes, Clear Skye has good analytics graphs. It has a relatively complicated delegation model. Clear Skye has a strong reporting tool. The technology uses a no-code approach. It has a strong workflow configuration engine as it uses ServiceNow's low code flow as a strategic workflow modelling tool. The product has a mature workflow designer model and customization of rules, flows and correlations is available.

Clear Skye IGA helps organizations that require lower barrier of entry IGA products or where existing IGA solutions are manual process intensive. The software benefits customers interested in leveraging their existing ServiceNow investment. Clear Skye mainly supports mid-market companies with considerable support given to medium and enterprise businesses. Market presence is almost equal in North America and EMEA, with growth being shown in APAC. Clear Skye has a good partner ecosystem across the globe, which includes Accenture, Ernst & Young, KPMG, and other companies.

<b>Security</b>	Positive
<b>Functionality</b>	Neutral
<b>Deployment</b>	Positive
<b>Interoperability</b>	Neutral
<b>Usability</b>	Positive

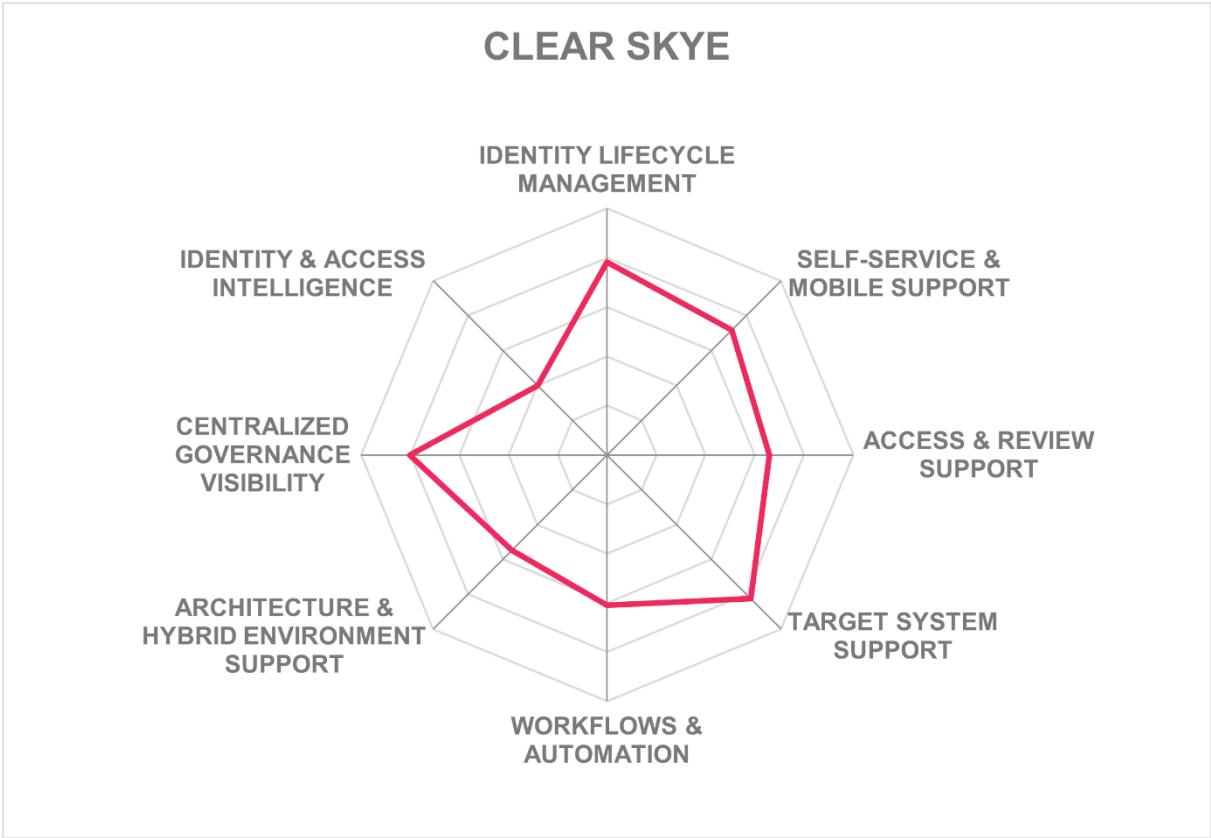


### Strengths

- Good breadth and depth of features for Identity and life cycle management
- Good capabilities supporting Access request and review
- Strong identity analytics
- Strong support for workflow and automation
- Built on ServiceNow
- Excellent connectors to target systems

### Challenges

- Limited authenticator options for user self-service and admin access
- Missing OOB support for major compliance framework reports
- Some OOB provisioning connectors for on-premise and SaaS systems is missing



## EmpowerID – EmpowerID IAM Suite

Founded in 2005 and based in Ohio (US), EmpowerID provides multiple products in a suite and offers EmpowerID IAM Suite as its IGA product. It includes Identity Lifecycle Management, Advanced Lifecycle Management, Group Management, Dynamic Group Management, Password Management, Role Mining, Access Recertification, Risk Management, Advanced Risk Management, Policy-Based Access Control, Azure RBAC Management, Azure Identity Management.

For the traditional IGA model, EmpowerID is built on an identity warehouse, which is an inventory of an organization's systems. It supports all known identity repositories for managing identities. Attribute mapping can be configured through the provided web user interface. In addition, custom attribute mapping logic can be configured through the provided workflow developer studio. SCIM and SCIM 2.0 is supported for identity provisioning deprivation, however SPML is missing. 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. It offers a strong custom connector model to create SCIM compliant connectors. Strong orphan account management workflow is given. EmpowerID provides strong role governance features that support role design and SoD compliance. It uses a polyarchal model for access where it leverages RBAC policies and location codes for giving appropriate access to people on same positions. 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 are provided.

Empower ID supports the majority of governance use cases. It can be deployed on premises, public cloud, private cloud, and hybrid. On premises deployment includes docker and Red Hat container-based platforms. It can also be delivered as a managed service, can be deployed to the server, SaaS or via a virtual appliance. Multi-tenancy is not supported. All the functionalities of the solution are exposed via SOAP, REST, SCIM and LDAP APIs while CLI support is marginally given. All the functionalities of the solution are available via java, .NET, C# and JavaScript SDKs.

Overall, 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 on 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 IGA solution with integrated access management features.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



## Strengths

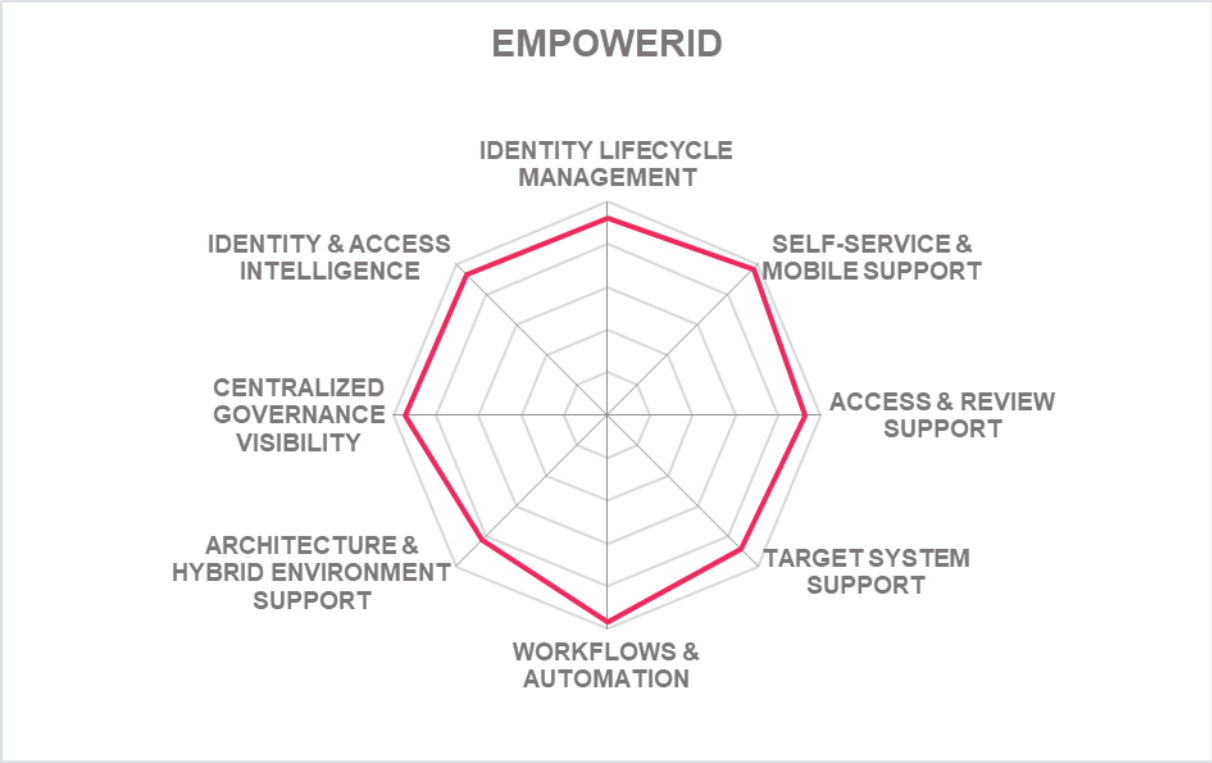
- Strong Identity life cycle management capabilities
- Excellent support for user self-service and mobile support
- Policy based access management
- Good set of Identity and access intelligence features
- Strong API support
- Strong set of workflow and automation capabilities
- Good support for user access review

## Challenges

- Comparatively weak partner ecosystem
- Some connectors missing for SaaS systems
- Anomaly and identity outlier detection is missing

Leader in





## E-Trust – Horacius IAM

E-Trust was founded in 1999 with headquartered in Brazil with an initial focus on information security. Later in 2006, E-Trust launched their Identity Access & Governance product Horacius. Horacius provides user provisioning and access governance capabilities that include access request, recertification, account mapping, and role & SoD management, with more advanced features such as workflows and identity analytics.

Horacius IAM supports identity provisioning and access governance. It is capable of handling automated user provisioning, access reviews & attestations, orphan account monitoring, or employee and third-party contract termination use cases, as well as providing auto-discovery capabilities to identify accounts, groups, group memberships. The solution supports some major identity repositories; however, depth is missing. OOB integration to ITSM tools is given for ServiceNow, Atlassian Jira Servicedesk, GLPI and any other that support WS REST or SOAP. A good range of OOB provisioning connectors for on-premises systems are present, however support for SaaS systems is limited. SCIM and SPML are supported for identity provisioning/ deprovisioning. Custom connectors can be made using a low code approach. IGA policy management covers most common use cases such as account termination, role modification, access exception approval, rights delegation, and SoD analysis and mitigation as a few examples, although policy authoring/editing and testing tools, OOB or integration options to third-party policy tools or engine are not available. 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 is missing advance intelligence capabilities such as recommendations, risk scoring, anomaly or outlier detection, while access certification supports event-based micro certifications and triggers to recertify given a user's schedule, SoD violations, and organizational structure changes.

Horacius IAM has a good UI, especially for workflows. The solution has a good pricing structure which includes full support. The UI for the user is customizable. The home page is defined with good tile graphs for admin and manager. Customization of business rules can be done easily. Reporting has a slightly outdated UI however, detailed reporting of access rights for auditing is available. The solution has good authentication options for user self-service and admin access which supports biometrics, MFA and SAML mobile token.

E-Trust offers all major deployment models for Horacius IAM. It can be delivered as-a-service, container (Docker, Redhat, Almalinux), as a managed service or can be deployed as a software to the server. Full multi tenancy using Amazon Web Service (AWS) is supported for cloud delivery. Most of the functions of the solution are exposed via SOAP, REST, SCIM APIs while only limited functionalities are given via CLI. SDK support is limited to Java, PHP and MS PowerShell. Developer portal is missing.

E-Trust has continued 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 mainly in Brazil. E-Trust is a good fit for organizations with average access governance requirements to satisfy the most common identity lifecycle administration use-cases with customer-focused in the Latin American region.



<b>Security</b>	Positive
<b>Functionality</b>	Neutral
<b>Deployment</b>	Positive
<b>Interoperability</b>	Neutral
<b>Usability</b>	Positive

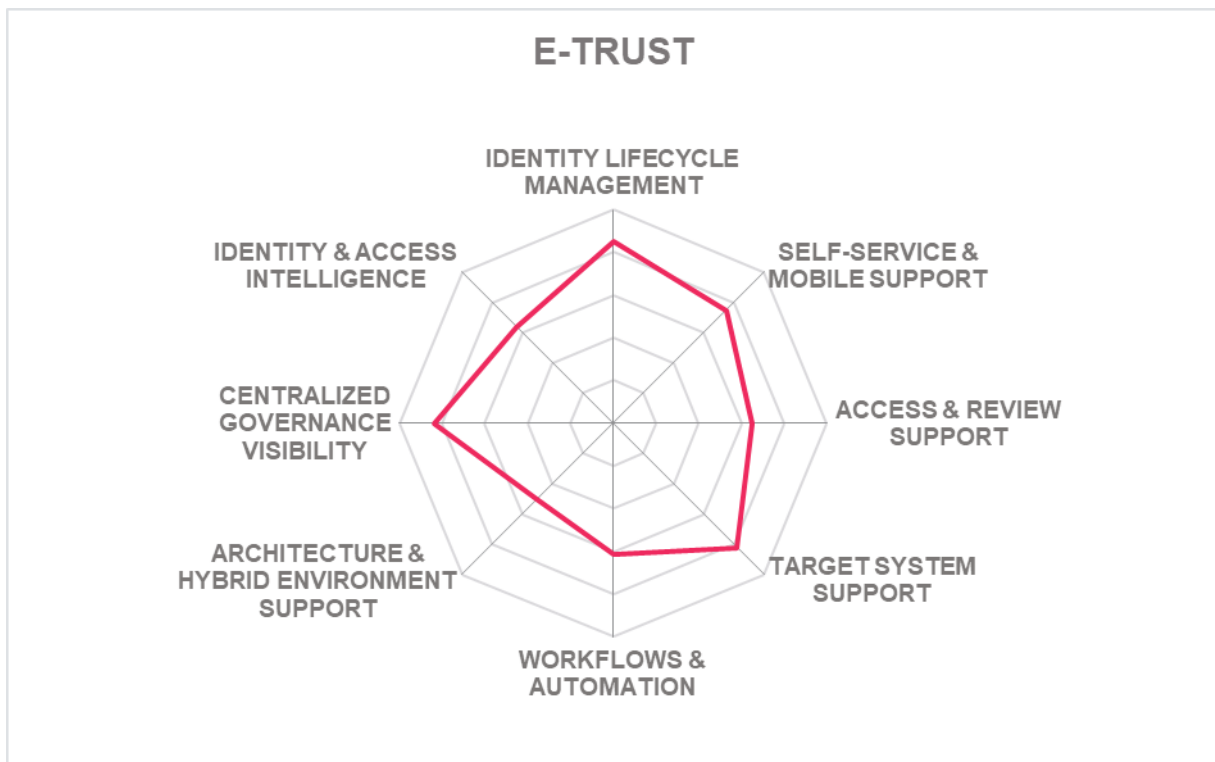


### Strengths

- Very good support for on-premises target system
- Strong Policy management capabilities in place
- Strong capabilities for Identity lifecycle management
- Relatively good support for user self-service access
- Strong set of features for supporting workflow and automations

### Challenges

- Market presence currently limited to Brazil
- Developer portal is missing
- Some limitations of OOB connectors to SaaS systems



## Evidian (Atos) – Evidian IGA, Evidian Analytics – IdaaS Governance

Based in France and since 2015, Evidian has been a dedicated division for digital security service line at Atos. Evidian is an established IAM business and has more than 900 customers with over 5 million users within the Finances Services, Manufacturing, Retail, Transport, Telecom, Media, Utilities, and Public Health sectors. Both Evidian Identity Governance and Administration (IGA) and Evidian Analytics and Intelligence (A&I) are evaluated together as its overall IGA solution in this Leadership Compass.

Evidian offers multiple products in a suite. Their product, Evidian Identity Governance and Administration (IGA), offers basic Access Governance in addition to strong on-premises identity lifecycle management capabilities. Support for identity repositories is limited to Oracle Directory Server (ODSEE), Microsoft AD LDS and 389 DS. Synchronization of attributes across heterogeneous IT environments is available. SPML and SCIM is supported for identity provisioning. OOB integration to ITSM tools includes ServiceNow, JIRA and EasyVista. Support for additional ITSM tools can be expanded using the provided SDK. Strong support for OOB provisioning connectors for on-premises systems is provided however, connector support for SaaS is limited. Evidian Analytics and Intelligence (A&I) is a separate product offering however it meets the increasing requirements of advanced Access Governance. It uses TIBCO JasperSoft for its reporting capabilities, giving Evidian the ability to provide good A&I dashboard capabilities. Evidian IGA ingests the components derived from the former Atos DirX portfolio.

Evidian supports deployment of all major models. The solution is delivered as a SaaS, Container (Docker), container orchestration system, managed service or as a software deployed to the server. The solution can also be installed on a virtual machine. Docker virtual appliance for synchronization stream from external sources like CSV, LDAP, SQL or WebService via SCIM is mandatory to run the solution as-a-service. Most of the functionalities of the solution are exposed via SOAP, REST, SCIM and LDAP APIs. Installation, imports/exports, and reports generation is available via the exposed CLIs. SDK for Java, .Net, JavaScript are available however Android and iOS SDKs are no longer available.

Evidian has a modern UI with customizable dashboards and pre-configured applications (e.g: salesforce). It has good user self-service support with clear instructions to the users for configuring applications. Risk level of scores for recertifications can be defined. SSO settings using SAML for exporting in XAML format and configuration of SSO settings are available. Reporting and analytics have a modern layout with the possibility to edit filters when defining.

Evidian customers and partner ecosystem are primarily focused in the EMEA region serving mid-market to enterprise-sized organizations. Roadmap for 2022 includes analytics and IDaaS governance features. Overall, Evidian delivers good provisioning capabilities with moderate Access Governance, making an interesting alternative to the leading IGA vendors in specific industry verticals, particularly healthcare. With a regional but strong partner ecosystem across Europe, ATOS acquisition is likely to help Evidian gain access to large customers and enter new geographies.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive



## Strengths

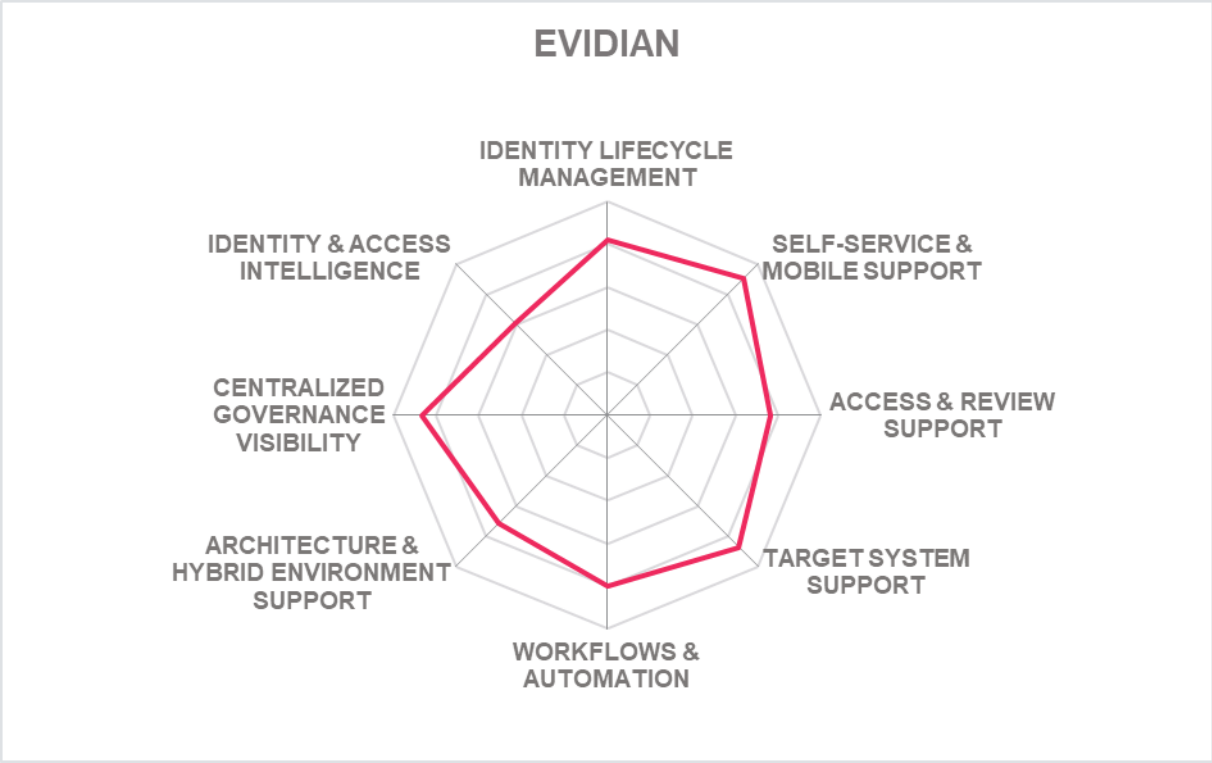
- Strong Identity and lifecycle management
- Impressive list of authenticators for user self-service and admin access as well as mobile support
- Good set of features for reporting and analytics
- Strong Policy management features
- Good capabilities for workflow and automation
- Strong OOB target on-premises system connectors support

## Challenges

- Limited presence and partner ecosystem outside EMEA
- Limited access intelligence capabilities without the Evidian Analytics and Intelligence offering
- Missing some OOB target connector support for SaaS systems

Leader in





## Evolveum – MidPoint

Evolveum is an Open Source IAM vendor based in Slovakia. Their MidPoint product is provided as an open source but needs a subscription for professional services. MidPoint is delivered as a single platform that focuses on IGA data protection and organizational management use cases.

MidPoint supports any identity repository as long as the connectors exist. As for LDAP access, only standard LDAPv3 features are supported. Except for AD access, where also some AD-specific features are supported. SCIM is supported for identity provisioning however SPML is no longer the preferred option. OOB integration to ITSM tools is not available but can be integrated by creating a necessary connector. A moderate amount of OOB provisioning connectors is given for on-premises systems however only a few OOB connectors to popular cloud systems are given. Attribute mapping between connected systems can be scripted using Groovy, JavaScript (ECMAScript), and Python programming languages. Policies for RBAC and organizational structure are also available that can be used for SoD use cases, for example. Evolveum deliberately removed its workflow engine in favor of a workflow-less approval process that is entirely driven by policies. For instance, for approval, policy rules are applied to roles, then the approval engine will compute the approval process.

Evolveum primarily focuses MidPoint as an on-premises deployment solution as a standalone server that can be downloaded and run as a Docker image, however hybrid or cloud deployment is also supported. Another option allows a more customizable open-source style using Apache Maven as a build system allowing for customization. Private cloud deployment is also available. Almost all of MidPoint's functionality is exposed via REST and SCIM APIs only. Roughly half of the solution's capabilities are available via CLIs. Only a Java and Python SDK is given.

MidPoint has a good UI with functional and configurable dashboards and widgets. Requesting roles is given via a shopping cart paradigm and the solution displays the status of the access request. Good workflow in place for approval of requests and the solution also supports bulk approval. SoD policies can be configured. Reporting capabilities are available based on native report mechanism, although missing support for major compliance frameworks OOB. Noticeably, MidPoint is missing more advanced identity and access intelligence capabilities. Role catalog model is on par with shopping cart paradigm in terms of execution. Updated UI is a strong improvement from the previous version and focuses on low code approach for end users.

Evolveum customers are primarily focused in the EMEA region with North America coming in as the second most important region. Evolveum's customer deployments include medium to enterprise companies and universities. MidPoint provides good on-premises DevOps options and hopes to move towards a hybrid or a full cloud environment in the future. Overall Evolveum MidPoint continues to improve and may be of interest to organizations with general IGA and solely on-premises requirements. Evolveum has plans to further enhance and work on identity analytics, role mining and a next gen user self-service support.

---

<b>Security</b>	Positive
<b>Functionality</b>	Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Positive

---

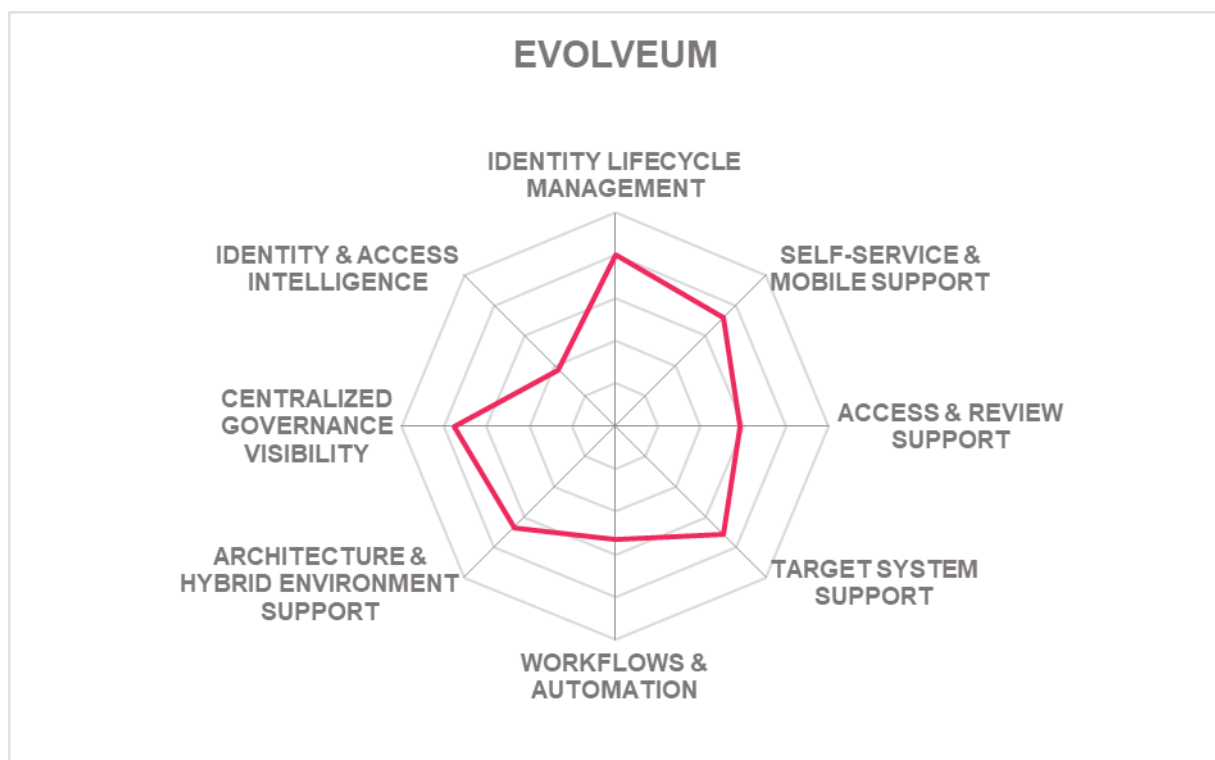


### Strengths

- Open-Source solution, provided at no (license) cost
- Strong list of connectors to on-premises systems
- Good Policy management
- Good support for access review
- Good support given for DevOps
- Strong features related to identity analytics and UI in the roadmap

### Challenges

- Missing OOB reports for major compliance frameworks
- Limited authenticator options for user self-service and admin access but using OpenID and SAML, all known authenticator options can be supported
- Limited but growing partner ecosystem outside EMEA



## IBM – IBM Security Verify

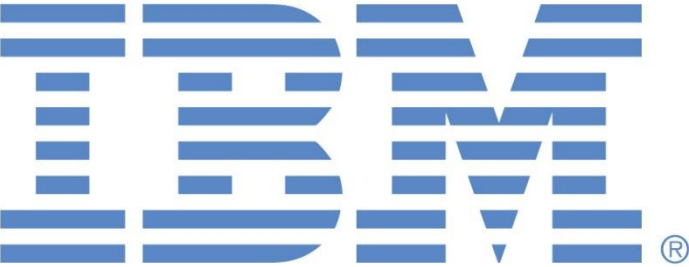
IBM, through its IBM Security Verify product, remains one of the largest IGA vendors for large-sized complex IGA deployment. IBM has integrated Identity Provisioning capabilities of ISIM with Access Governance capabilities of IDEAS platform acquired from CrossIdeas some years back into ISIGI and evolved the platform over the years. More recently, IBM Security Verify Governance (ISVG), previously IBM Security Identity Governance and Intelligence (includes IBM Security Identity Manager), and IBM Security Verify SaaS are IBM's current IGA offerings.

IBM Security Verify supports all known major deployment models and is delivered as-a-service, Container (Red Hat), software deployed to the server or as a virtual appliance. Managed service is also supported using verify governance which is provided by IBM Security services. The solution supports full multi tenancy. More than 60 percent of the functionalities of the solution are available via SOAP, REST, SCIM and LDAP APIs. Less than 10 percent access to functionality via CLIs is given. SDKs for Android, iOS, Java, JavaScript, .NET and Python are only supported in Verify Governance offering however almost all the solutions are available via the listed SDKs.

IBM Security Verify supports all known servers, databases or virtual directories which can be used as identity repositories. SCIM is supported for identity provisioning/ deprovisioning however a customer adapter is required for SPML. OOB integration to ITSM tools is limited to ServiceNow. Verify Service Desk is a ServiceNow plugin published in ServiceNow store. It supports access request and manual fulfillment tickets management. 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. Identity lifecycle management covers all aspects from onboarding to off boarding and uses AI and machine learning to analyze parameters of user and requested access.

IBM Security provides a modern UI with all required functionalities in the dashboard. 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. Good user self-service is given with a strong list of authenticator options for access including passwordless authenticators such as QR code, FIDO2, and FIDO2 U2F. Access request and access review is supported by a risk level is shown in terms of entitlements. Configurable OOB policies based on best practice in place for the analytics model.

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.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Deployment</b>	Strong Positive	
<b>Interoperability</b>	Strong Positive	
<b>Usability</b>	Strong Positive	

## Strengths

- Strong Identity lifecycle management features
- Strong partner ecosystem and professional services
- Impressive list of connectors for target system support for SaaS and on-premise systems
- Good workflow capabilities
- Very strong reporting and auditing capabilities
- Policy management
- Good support provided for user self-service and support

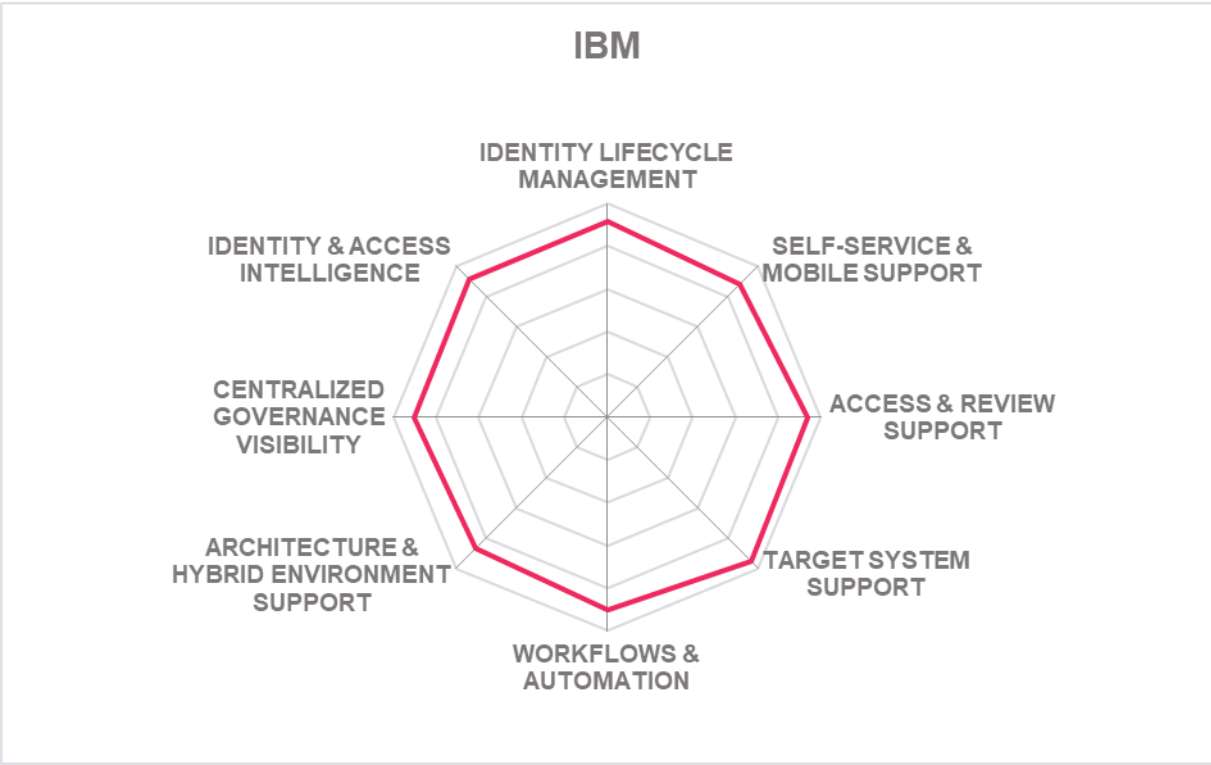
## Challenges

- Missing OOB reports for major compliance frameworks
- Relatively low presence outside North America
- Container-based delivery options are limited to Red Hat

Leader in







## Micro Focus – NetIQ IGA Suite

Based in UK, Micro Focus offers an Identity and Access Management Platform as a set of solutions that include Identity Governance and Administration, Access Management, Advanced Authentication, Data Security, Privileged Access Management and Security Information and Event Management. Identity Manager aimed primarily at Identity Provisioning and lifecycle management, and Identity Governance for Access Governance, Identity Intelligence, and Identity Tracking to deliver a wide range of IGA capabilities.

Micro Focus Net IQ Identity Manager is a robust product for automated Identity Provisioning with mature and comprehensive capabilities for identity lifecycle management and fulfillment. All known directories, servers, databases, or virtual directories can be used as identity repositories to manage identities. Any type of identity is supported with defined schema as well as an extensible schema to allow the customer to define any type of object class and attributes. SPML and SCIM is supported for identity provisioning and deprovisioning. Its flexible approach for workflow and policy management based on the designer tool is still widely unmatched in the industry, allowing for efficient and easy management of complex environments. IGA can integrate with Atlassian JIRA and Cherwell via REST. Other ITSM systems can be integrated via REST, SCIM. Very strong support for OOB provisioning connectors for on-premises and SaaS systems. It supports an event-driven, bi-directional provisioning model which allows organizations to process identity lifecycle events as they happen. Integrated role mining, adaptive access certification, and risk-based analytics are distinct and improved governance features.

NetIQ IGA Suite has a decent, modern UI which uses analytics to compare identities when preparing roles. Micro Focus also offers a wide range of IGA related reporting capabilities, including support for major compliance frameworks. It has strong analytics for reporting however the graphics are slightly outdated. The solution also supports behavioural analytics. Identity provisioning is done based on risk scores which are all real time and are dependent on users' behaviours and other attributes. Strong user self-service is given with many user and administrator authenticator options available.

Micro Focus supports on-premises, public or private cloud, and SaaS and Hybrid SaaS or Cloud deployment models. The solution can also be delivered as a managed service, can be deployed to the server, container orchestration systems or container-based platforms (Docker, Red Hat, Rancher Labs, Pivotal, Mesosphere, SUSE). Full multi tenancy is supported. All the functionalities of the solution are exposed via REST, SOAP; SCIM and LDAP APIs as well as managed using CLI. SDKs for a wide number of programming languages is available however Android and iOS are missing. Developer documentation and samples are provided through a community portal.

Micro Focus is a well-established company with a customer base predominantly focused on mid to enterprise-level organizations located in North America and EMEA regions. Micro Focus Net IQ Identity Manager, Governance, and Intelligence products offer a good range of IGA capabilities from flexible workflow and policy management to enhanced analytics-driven user activity reporting. Micro Focus continues to improve towards a more modern and flexible product with more innovative features for advanced analytics using AI and ML on its roadmap. Overall, Identity Manager and Governance products from Micro Focus remain

leading-edge products in the IGA market space with its broad, mature, and evolving functionality with a good partner ecosystem on a global scale.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



### Strengths

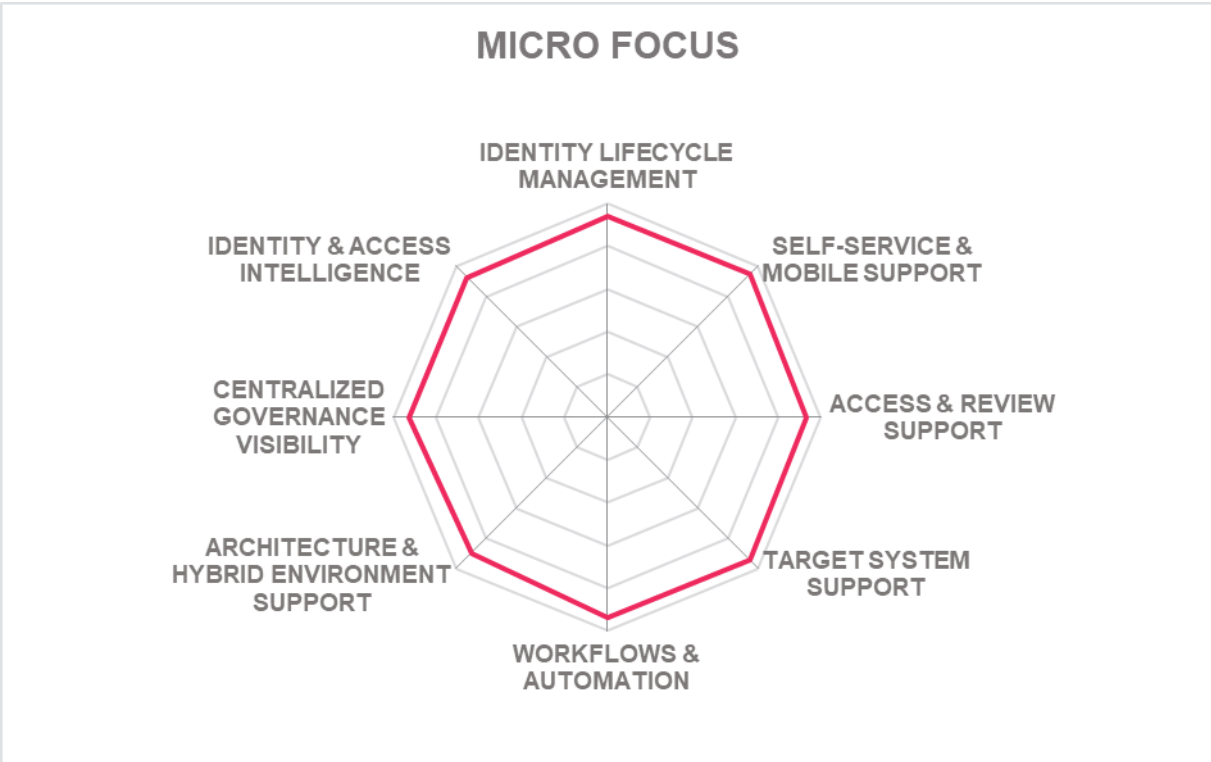
- Strong identity life cycle management features
- Strong target system support for on premise and SaaS
- Strong list of authenticators for user self-service and admin access
- Good access review capabilities
- Strong support for IGA analytics and access intelligence capabilities
- Good workflow and automation capabilities
- Broad range of features supported via its strong policy management
- Strong global customer base and partner ecosystem

### Challenges

- Missing popular SDKs for Android and iOS
- Relatively outdated UI

Leader in





## Microsoft – Entra Identity Governance

Microsoft Entra Identity Governance is a SaaS offering which covers governance for all applications and reduces dependability of ADMS, ADDS and ADFS. The solution supports automated workflows for identity lifecycle management of users and guests. Entitlement management supports review and granting of access through defined policies. The solution also incorporates AI for recommending roles and entitlements based on attributes and similar roles.

The solution supports a strong set of databases and virtual directories with the possibility of importing directory data from other directory databases and HR systems. It supports all types of identities. Microsoft Entra Identity Governance can be delivered as a SaaS or as a managed service with deployment possible on public cloud, hybrid model or as a subscription-based service. The majority of the functionalities of the solution are exposed via REST and SCIM APIs. The solution supports the majority of the SDKs including iOS, Android, Java, .NET, and Python.

SCIM is widely supported for identity provisioning. Good range of OOB SaaS connectors. Support for OOB on-premises connectors is limited due to the nature of the delivery and deployment of the product. OOB integration to ITSM tools for SSO and privileged access includes ServiceNow and Atlassian Jira Service Desk. Privileged access also supports Just-In-Time (JIT). There is a good set of authenticators for user self-service and admin access, however, FIDO support is missing. Portals for managing identities and resetting passwords are available via a web browser and render well on desktop and mobile platforms.

Strong policies in place for attribute-based access. Solution supports provisioning analysis and policy for user activity monitoring supported. Policy in place for supporting elevation of PAM. Solution does not use AI/ML in place for supporting workflows related to recommending access rights based on comparison of employees or other similar functions.

Microsoft Entra Identity Governance provides support to major parts of the world and with strong growth estimated in the following year based on the information provided regarding the number of additional employees that will be added to work on this product.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive



# Microsoft

## Strengths

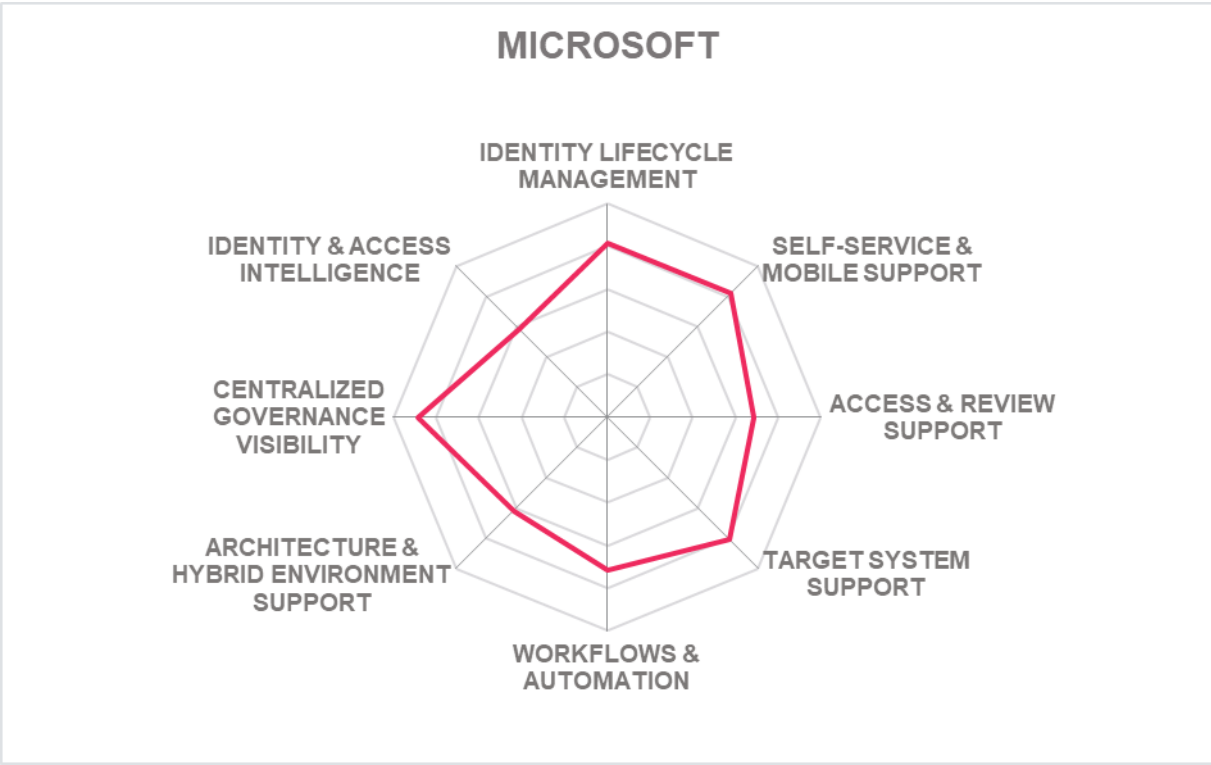
- Strong external user governance features that offer end to end lifecycle management for guest users and other external collaborators
- Strong list of OOB connectors for SaaS system
- User self-service support for managing and requestion access
- Excellent Access recertification and access review capabilities
- Strong global partner ecosystem
- Strong access governance capabilities
- Modern and user-friendly UI

## Challenges

- Support for OOB reports for major compliance frameworks limited to GDPR
- Solution does not make use of AI/ML for any functions
- Event based micro certification is missing

Leader in





## Netwrix Corporation – Netwrix Usercube

Founded in 2009, Netwrix Usercube is a French software company that was acquired by Netwrix in August 2022. It delivers an IAM solution based on the Microsoft technology platform with capabilities solely dedicated to IGA. The customer base is primarily focused on mid-market to enterprise organizations in the EMEA region and now through Netwrix benefits a worldwide network of distributors and partners. Netwrix, with its portfolio of security products for Data Governance, Privileged Access Management and Password Management will develop an integrated security offering with Netwrix Usercube.

Netwrix Usercube provides identity management, provisioning, governance, analytics, and reporting. Netwrix Usercube has strong support for 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. SPML and SCIM is supported for identity provisioning/ deprovisioning. The product has a strong support for OOB provisioning connectors for SaaS however support for on-premises is limited to Microsoft Azure AD, O365, ServiceNow, Workday, Google Apps, SAP/HANA, and Salesforce. Netwrix Usercube provides out of the box connectors for Service Now, EasyVista, Matrix 42 and many projects have covered Jira, Zendesk with custom connectors. The product provides generic ITSM connectors to speed up the integration with any ITSM. Netwrix Usercube also provides a fast and easy PowerShell scripting connector to synchronize/provision any identity with any target system. Netwrix Usercube is offered as a single software available for SaaS and as a subscription based on-premises delivery on all major deployment models. Docker container and Kubernetes is also available. For cloud, full multi tenancy is supported. The solution has all its functionalities exposed via REST API. CLI functionalities are also available but only for on-premises deployment. Developer portal is given, and the SDKs are integrated via REST API.

Netwrix Usercube has a modern UI with a dynamic and configurable dashboard. It supports configurable attributes along with user activity monitoring. Risk based SoD violations are available before giving access, delegating access or certification. Good user self-service and admin access with a wide range of authenticator options as well as passwordless authentication is available. Netwrix Usercube RoleEngine computes who is entitled to which access and automatically grant entitlements. The product has good reporting features.

Netwrix Usercube offers its services for small to enterprise businesses with majority of its customers based in North America. The partner ecosystem is globally very strong and growing. Service support is limited to English and French, however, a 24x7 support service is available. The recent update includes launch of Netwrix Usercube v6 which supports rapid IGA deployment allowing companies to run IGA from scratch within one month. Further updates include a feature for role mining based on the usage of the application. Overall Netwrix Usercube is emerging as a strong alternative due to its well-balanced set of IGA capabilities, as well as making good use of identity and access intelligence.



<b>Security</b>	Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive

**netwrix**

## Strengths

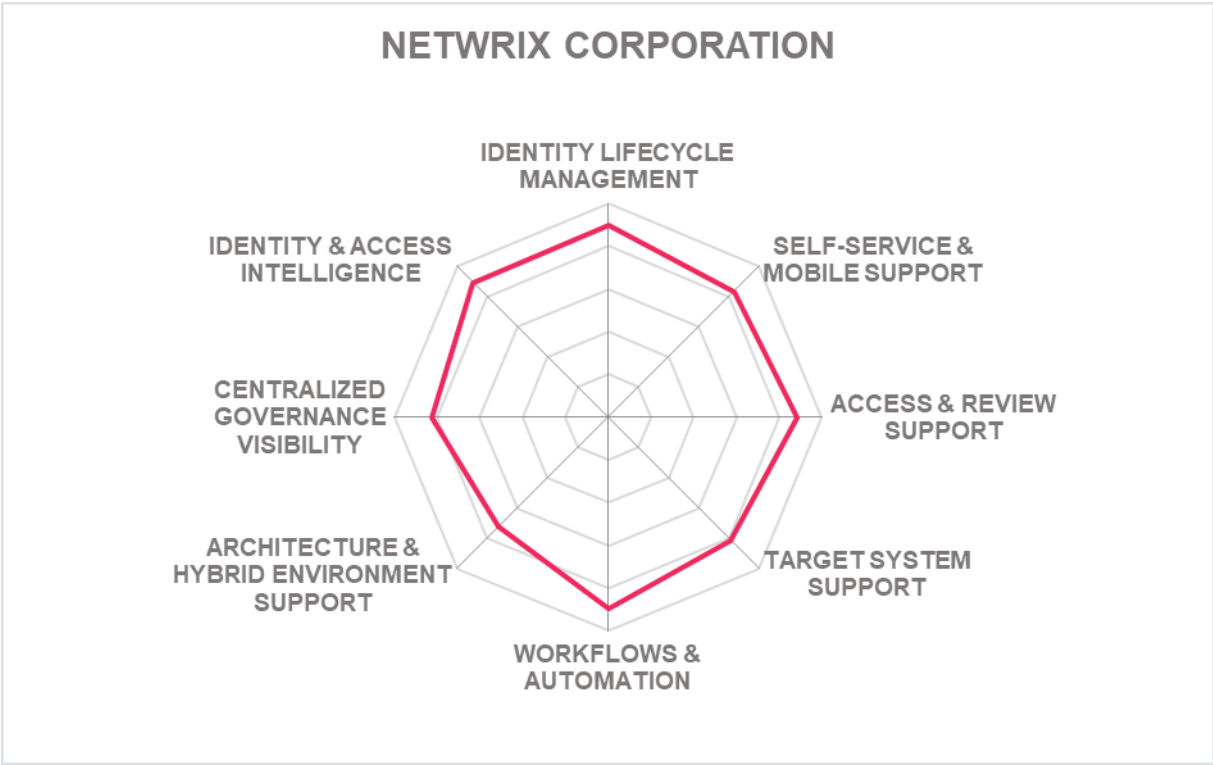
- Very good capabilities supporting identity and lifecycle management
- Good policy management features
- Strong support for OOB provisioning connectors for on-premises systems
- Ease of deployment
- Impressive real time access review and certifications
- Good workflow and automation capabilities
- Powerful risk-based access governance

## Challenges

- Limited OOB connectors for SaaS systems
- Missing OOB reports for major compliance frameworks
- Quick approval processes are missing

Leader in





## Nexis GmbH – NEXIS 4

Based in Regensburg, Germany, Nexis started with NEXIS Controle, first released in 2014, which builds upon a plug-and-play approach to access governance and role lifecycle management as its core focus. Since then, Nexis has made some significant improvements on the core products, now called NEXIS 4. The NEXIS 4 feature set includes access governance, analytics and modeling engine, a fully configurable UI, workflows, policy management, as well as other interesting integration options.

NEXIS 4 supports all major deployment models with its focus mainly shifting towards cloud. It can be delivered as SaaS (e.g., on Azure, AWS), hardware or appliance, managed service or container based (docker). The solution supports partial multi tenancy where the analytical interface for working with data is multi-tenant whereas the logging, reporting and configuration in the admin interface is single tenant. The necessary functionalities are exposed via SOAP, REST and SCIM APIs. A Java API and a JavaScript API is also supported. SDK for Java is available however a developer portal is missing.

The product supports all known identity repositories. Connections to a wide variety of identity repositories are given, although out-of-the-box (OOB) connectors to on-premises systems are limited to some Microsoft products such as Microsoft AD, SQL (MSSQL, Oracle SQL, PostgreSQL, DB2), SAP, LDAP, and database connectors while connectors to SaaS systems are limited only to Microsoft Azure AD, Microsoft O365, JIRA and Service Now. However, OOB connectors to most major IAM solutions exist, such as SailPoint IIQ, One Identity Manager, Microfocus Net IQ, Microsoft Identity Manager, Beta Systems Garancy. The solution can support custom connectors using plugins that are based on a comprehensive API and are written in Java. Integrations with third-party ITSM tools such as Remedy and ServiceNow are supported while Cherwell is also added since 2022. NEXIS 4 supports SoD checks, risk intelligence and simulating models for anomaly of entitlement structures, role outlier detection and role optimization simulations as well as real time SoD violation checks.

NEXIS 4 provides a user-friendly and fully configurable UI design that supports 150+ corporate identity settings and a WYSIWYG UI component editor. End-user request services are stakeholder-centric, and dashboards use a card-based interaction to display specific target information and buttons to trigger an action. The dashboards are customizable and fully compatible with existing IAM solutions. No coding is required at any stage, for example, for configuring workflows.

NEXIS 4 is a comprehensive solution for access privilege scans, risk analysis, visual (re-)modelling of entitlement structures, and access governance processes. It has limited global presence with its focus mainly in the EMEA region with relatively low partner ecosystem. Support is limited to English and German languages; however, documentation is available in all known major languages. Nexis has a planned deployment for further expanding AI and ML mechanisms for administrative tasks, a recommendation engine on all analytical aspects of IAG data and access concept management.

<b>Security</b>	Positive
<b>Functionality</b>	Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive

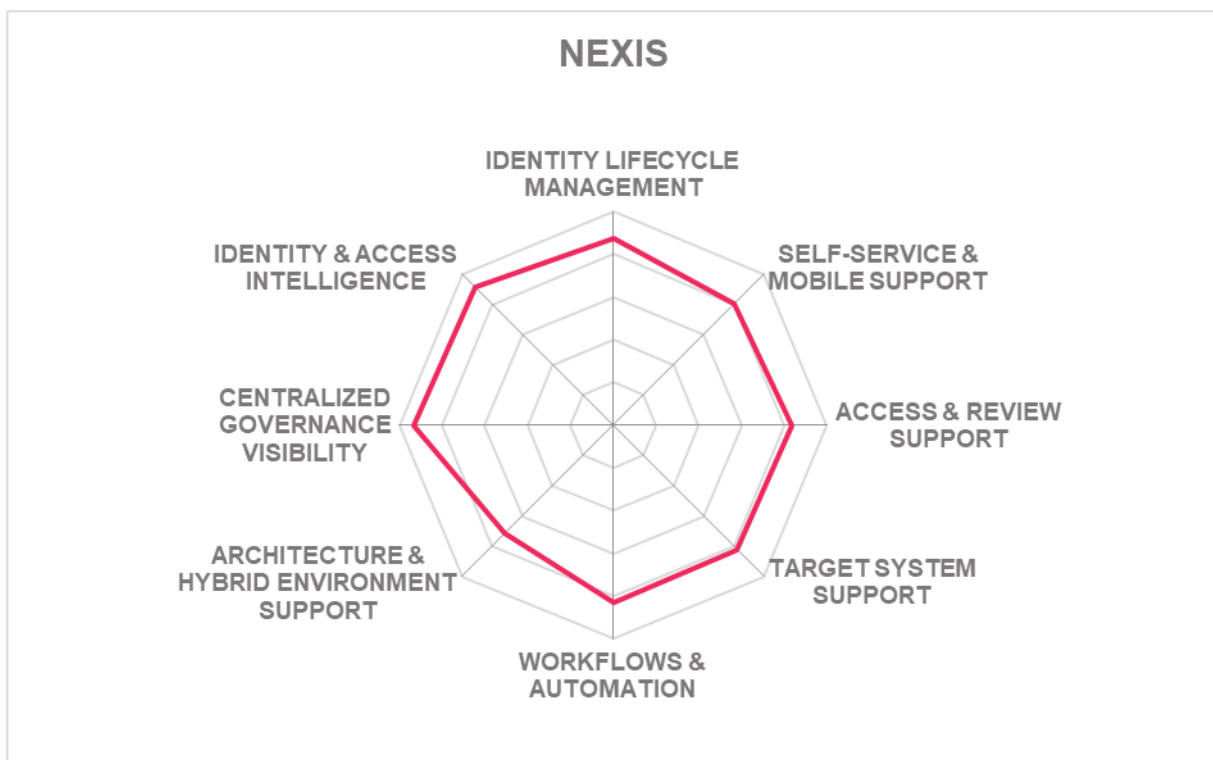


## Strengths

- Strong identity and access analytics and modeling capabilities.
- Follows a zero-code approach throughout the solution
- Strong features for workflow management and configuration
- Good capabilities for SOD management
- Strong support provided for access review and certifications
- Supports the majority of access governance use-cases

## Challenges

- Limited market presence outside EMEA
- Limited breadth of OOB connectors for SaaS systems but support for major connectors is available
- Limited user and admin authenticator options
- Missing OOB major compliance frameworks



## Omada – Omada Identity

Omada, headquartered in Denmark, counts among the established providers of solutions for IGA. Omada provides Omada Identity as an on-premises solution and Omada Identity Cloud for customers wanting a cloud-native SaaS solution - both delivering a full range of IGA functionalities with feature parity between the delivery models. The accelerator package allows customers to be operational within 12 weeks. Omada components include an enterprise server portal and services for provisioning, data warehouse, and role & policy engine.

Omada has a broad set of configurable connectors for SaaS and on premises. It supports a connector community for peers to share, generate and install connectivity packages. The deployment is easy into relevant tenants. All the functionalities of the solution are exposed via SOAP, REST APIs. SDK support is limited to .NET and JavaScript. A customer portal is available through the Omada Hub for customers and partners. The solution supports a good range of identity repositories and replication to and from any SQL database. SCIM is supported for identity provisioning including support for SCIM 2.0. Omada's Identity lifecycle management allows moving of identities as per context, association or roles including review of access right. Access review for all identities including external identities is available.

Omada Identity's UI is modern with good features for user self-service, including the Omada Identity Cloud Management Portal, which enables SaaS customers to fully manage the back end of the solution including performing upgrades, creating and editing environments, and more, without requiring assistance from Omada support. Strong set of authenticators are available for users and admins along with support for passwordless authentication. It offers good UI for self-service for access request, delegate access from tablets and mobile phones, as well. The solution uses AI for recommending access-request based on peers via a thorough analysis. Policies in place for assignment using automation. Good IGA/AG-related reporting OOB includes access risks, analytics trend analysis, attestation, delegated and privileged access, SoD, and access request-related reports

Omada is focused on medium to enterprise sector customers. Most of its presence is based in EMEA with no presence in APAC or Latin America. Omada provides support 24x7, but it is currently restricted to English, German, Russian, Ukrainian, and Danish. Recent updates include a ServiceNow app for access request management, and roadmap items feature a new reporting platform and integration with EiPaas solutions to increase target system connectivity.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



## Strengths

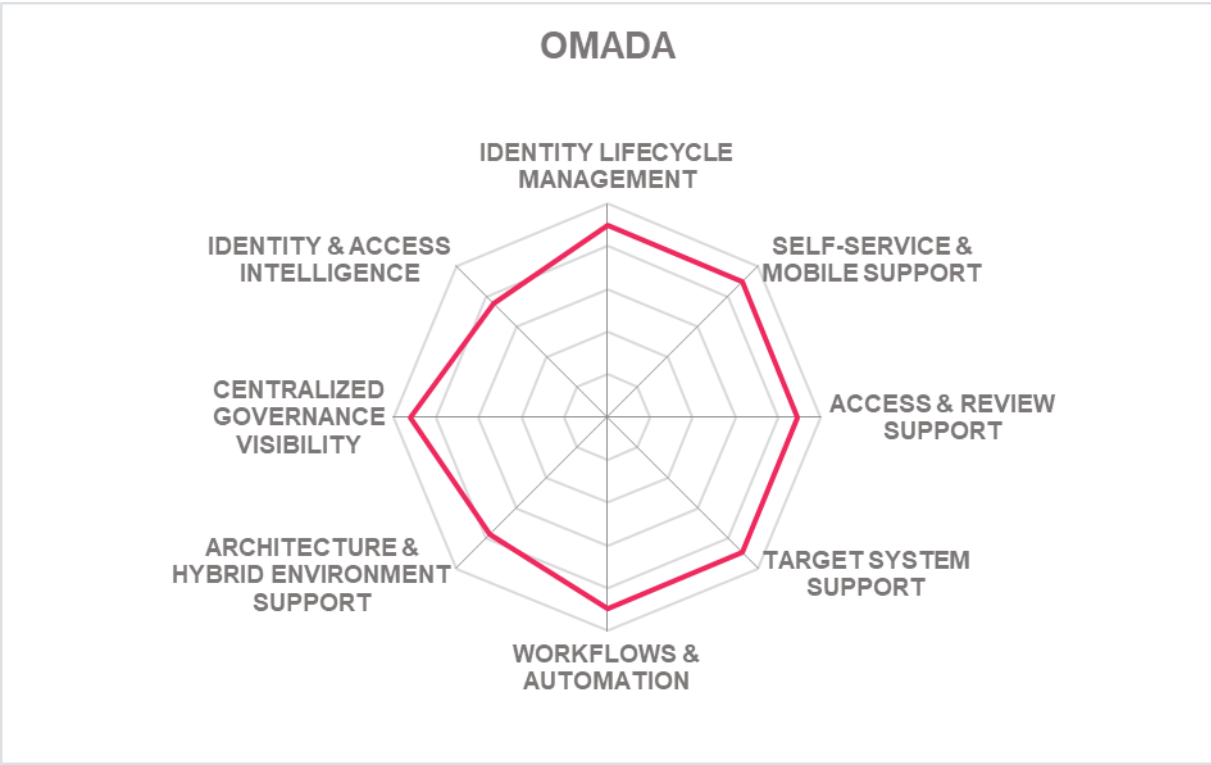
- Unique configurable connector community
- Strong identity Lifecycle management capabilities
- Good support for user self-service
- Strong features supporting identity and access Intelligence
- Good workflow and automation capabilities
- Strong Policy Management
- Advanced analytics for reporting
- Improved authenticator options for user self-service and admin access

## Challenges

- Limited presence outside EMEA and North American market
- Major OOB compliance frameworks missing however solution in place to support all relevant frameworks
- Some OOB connectors to on-premises systems are missing

Leader in





## One Identity – One Identity Manager

Based in California, One Identity provides an identity-centric security strategy with a broad and integrated portfolio of identity management offerings developed with a cloud-first strategy. One Identity's Identity Manager provides a single platform for governance and includes identity lifecycle, access request, access certification, auditing, privileged access governance, reporting, and data governance.

One Identity Manager supports a wide range of repositories as authoritative systems for managing identity lifecycle however, its own identity repository only supports MS SQL and Azure SQL Managed Instance. Schema extensions for adding new identity types over existing identities is available. SCIM is supported for identity provisioning and accelerating application onboarding. OOB integration to ITSM tools is limited to ServiceNow. Connectors to ITSM can consume data and grab ServiceNow catalog which is the product's unique capability. Integration of other ITSM tools is available based on customer requirements. Strong support for OOB provisioning connectors to on-premises and SaaS systems is available. Configurable policies for governing automated provisioning are supported along with Just-In-Time provisioning. The solution uses a strong AI for risk score system, peer group analysis, entitlement right sizing and future capabilities will include AI support for recertification requests, access requests. The risk dashboard is interactive and can show role and entitlement sprawl. The product has a strong architecture model which is flexible and supports cloud governance, data access governance, application governance, privileged governance and identities and entitlements.

One Identity Manager supports strong governance use cases including governance of devices, APIs and microservices in terms of versioning. The product supports on-premises, public and private cloud, and hybrid deployment. License based and subscription-based deployment is also supported. The solution is delivered as a service, Container (Docker), managed service or as a software deployed to the server. It can be delivered in hardware or virtual appliance by using a partner. Support for cloud multi-tenancy is not available. The solution has all its functionalities exposed via REST, SCIM, .NET and Posh APIs. SDK for .NET and JavaScript is available. Developer portal for publishing samples, examples and also on GitHub is available.

One Identity has a modern UI with a strong graphical representation of an identity and the associated roles and access. Access control is driven via RBAC policies. Additionally, all access request management capabilities are available via mobile devices. Moderate support is given for user self-service and administration authenticator options but does include FIDO2, mobile app, and biometric options. Support for passwordless authentication is not available. Real time risk awareness is provided to users when making access requests and approval. Reporting and auditing dashboard and UI has a relatively outdated feel.

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.



<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



## Strengths

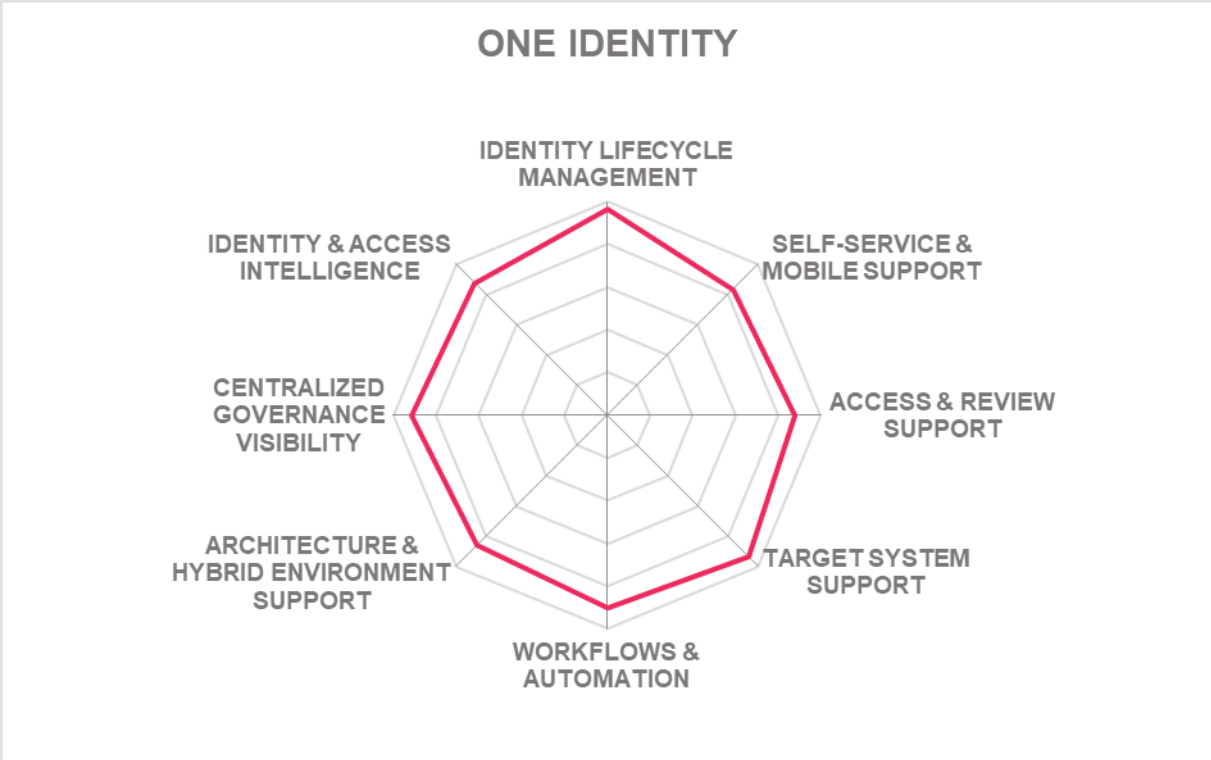
- Strong OOB target connector support for on-premises and SaaS systems
- Strong support for analytics and supported via machine learning
- Good features for workflow automations
- Very good features for access review and certifications
- Good features for management of access request
- Advanced policy management

## Challenges

- Missing OOB major compliance frameworks
- Moderate list of authenticator options for user and admin access
- Cloud multi-tenancy not supported

Leader in





## Oracle – Oracle Identity Governance

Oracle Identity Governance (OIG) Suite is the on-premises offering within Oracle's IAM portfolio. Oracle Identity Governance is Oracle's primary IGA offering that includes Oracle Identity Manager and Oracle Identity Analytics. Several IGA and particularly Access Governance capabilities have been significantly improved over the years, especially the integration of modules and the ease of its deployment. Oracle remains a preferred vendor for organizations with a substantial investment in Oracle Fusion Middleware and requires high flexibility for customizations to accommodate complex business processes.

Oracle's solution supports all known identity repositories and types of identities. Java/Groovy can be leveraged for mapping expressions. SCIM and SPML support for identity provisioning/ deprovisioning is available. Very impressive list of OOB provisioning connectors for SaaS and on-premises systems. Oracle supports developing custom connectors to integrate with non-standard/bespoke systems. Also, Oracle connector suite includes a flat file connector that can be leveraged for offline integration with non-standard systems. OOB ITSM integration is available for ServiceNow and BMC Helix ITSM. For Cherwell, Atlassian JIRA Service Desk, out of the box integrations is not given, however, customers/partners can extend the functionality and integrate these systems.

With options of deploying as software or containers, Oracle provides several deployment options on physical, virtual, private, or public clouds. This flexibility makes it easy for customers to have a scalable solution on heterogeneous clouds. The High availability and Disaster recovery options for maximum availability makes a huge difference to Governance customers. On-premises deployments can be delivered as a virtual appliance, container-based, software deployed to a server, as well as a managed service through Oracle advanced customer services and Oracle partners. Container based delivery supports all known platforms. Almost all functionality is exposed through APIs via SOAP or REST. REST is preferred over SOAP. LDAP is supported with integration with LDAP directories through LDAP connectors. SDKs for C/C++, .NET, Java and JavaScript is given.

Oracle Identity Governance Suite cuts across its competition through its enhanced UIs, recent pricing adjustments, enterprise-level design, support for modern architectural concepts, and an extensive partner network. Risk based access certification is available. It offers good analytics for access review campaigns, which can be exported as CSV. The analytics are AI and machine learning driven. User self-service support has a good UI with a customizable landing page. The solution uses a shopping cart paradigm and SoD violation checks are performed at checkout. Access request has recommendations feature which uses analytics to suggest access based on entitlement or attribute of the user.

Overall, Oracle Identity Governance Suite counts among the leading IGA products in the market. It provides a broad set of features focused on Identity Provisioning, Access Governance, and Intelligence, as well as good support for enterprise-level architectures, including external workflow systems. OIG makes an excellent choice for large IGA implementations requiring scalability and flexibility to support complex IAM scenarios.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive

**ORACLE®**

## Strengths

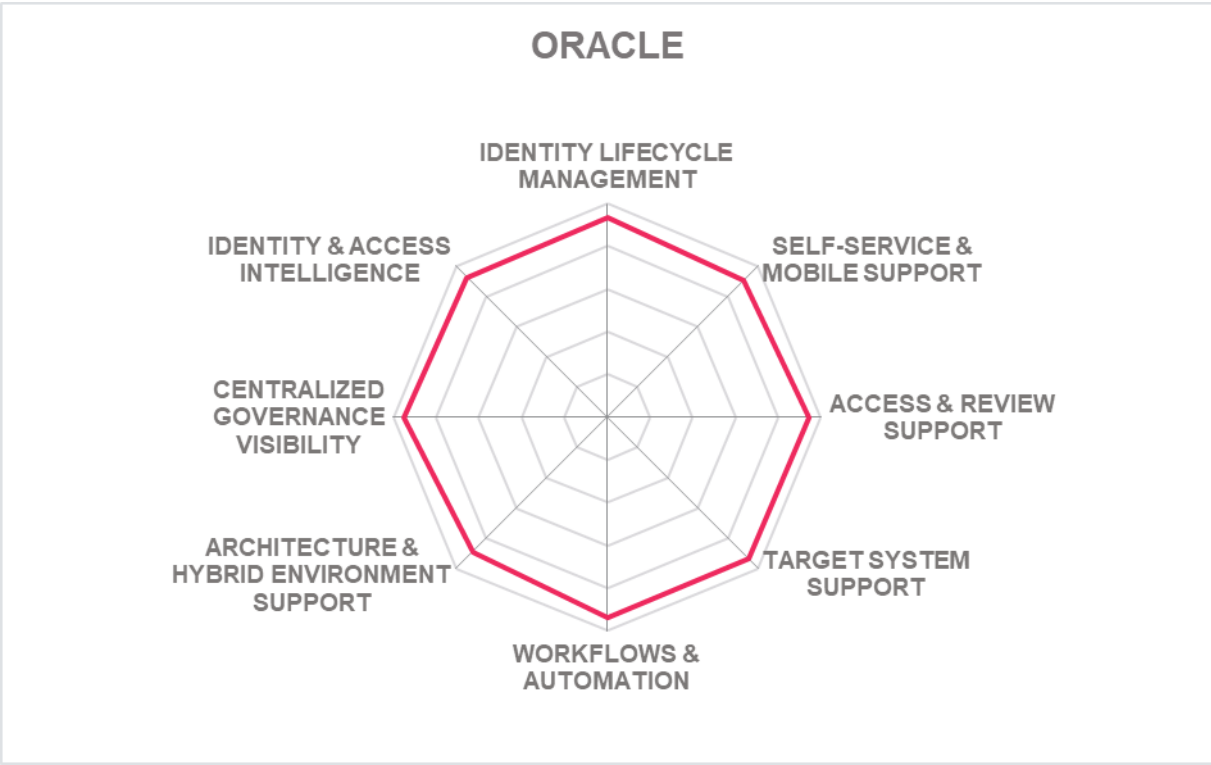
- Very strong identity and life cycle management
- Good support for user self-service and admin
- Strong list of authenticators for user self-service and admin access
- Strong IGA related reporting OOB
- Very good policy management
- Strong target system support for SaaS and on-premises systems
- Workflow and automation
- Powerful access governance capabilities
- Modern and user-friendly UI

## Challenges

- Some SDKs missing
- Oracle database is required

Leader in





## RSA– SecurID Governance and Lifecycle

RSA is a provider of authentication, lifecycle management, and identity governance security solutions. RSA 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, RSA emerged as an independent entity under Symphony Technology Group (STG) last September 2020. RSA has a complete identity offering available through ID Plus, and includes Access, Authentication, SSO and Governance & Lifecycle (G&L). RSA Governance & Lifecycle is its IGA product delivering both Identity Lifecycle Management and Access Governance capabilities.

RSA 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. G&L supports all known databases, servers, or virtual directories for identity repositories. Solution supports automated discovery of access, automated provisioning of birth rights, continuous risk-based access assurance approach including governance for entire identity lifecycle management. SPML and SCIM is supported for identity provisioning/ deprovisioning. Policy in place to do bulk importing of identities and bulk approval/ rejections based on SoD violations. OOB integration to ITSM tools is available for ServiceNow, Cherwell, BMC Helix ITSM and Jira. It supports a wide range of out-of-the-box (OOB) connectors to both on-premises and SaaS systems.

RSA has a modern UI with configurable dashboards based on CSS files. Product has the same UI for users, admin and any third-party identity. The solution adapts the functionalities based on the roles. Both identity and access intelligence are visible through basic dashboard graphics and more extensive dashboards available on the RSA Community. Strong authentication options are given for self-service and administration access. Passwordless authentication options include Yubico FIDO tokens and Fietian FIDO security keys. RSA G&L also shows strong support for reporting and OOB reports for major compliance frameworks. Risk analytics driven review of access requests based on priority and urgency of the requests is available. Dashboard in place for suggestion of orphan accounts and policy for alerting privileged access is also available.

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

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



## Strengths

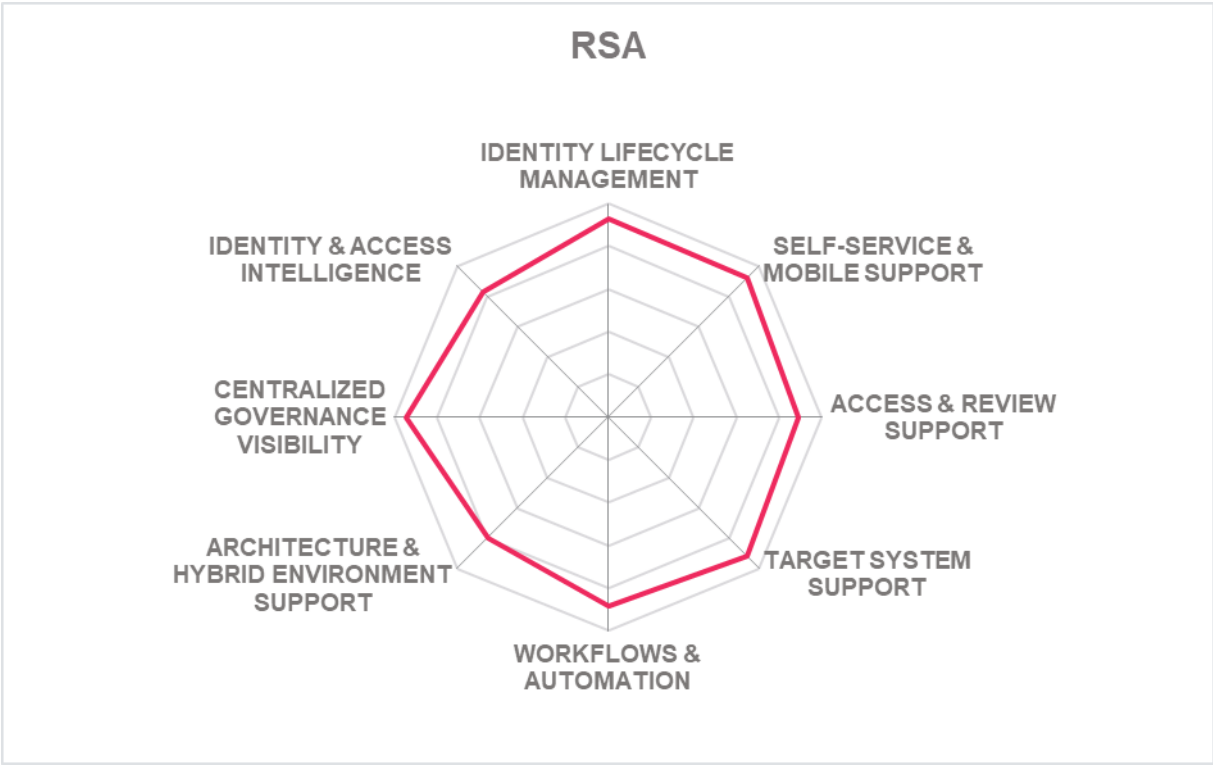
- Strong capabilities for identity lifecycle management
- Strong OOB on-premise and SaaS connector support
- Very good risk analytics-based access governance
- Strong global partner ecosystem
- Advanced identity & access intelligence capabilities supported
- Strong Policy management

## Challenges

- Cloud delivery is currently a single tenant model
- Some limitations on SDK programming language options and access to product functionality via the SDK
- Container based platform support limited to Docker

Leader in







## SailPoint – SailPoint Identity Security Platform

Based in Austin, Texas, SailPoint started as a vendor specialized in Access Governance and made heavy investments in Identity Provisioning capabilities over the years. SailPoint Identity Security Platform is a single platform that adds AI-based capabilities to IGA and cloud governance via SaaS deployment. 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.

The solution has strong support for identity and lifecycle management with all known identity repositories available. SailPoint supports mapping of SOD policies from SAP GRC to form a coherent SOD policy across the enterprise and has a dedicated mapping UI for attribute mapping. 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. OOB integration with ITSM tools includes ServiceNow, BMC Helix ITSM, and Atlassian JIRA Service Desk. Very strong support for OOB provisioning connectors for SaaS and on-premises systems with a dedicated list of options.

SailPoint Identity Security Platform supports public and private cloud deployment with full multi tenancy supported. On-premises deployment is also available. Along with SaaS, the solution can be delivered as a container (Docker, terraform), as a managed service or can be deployed as a software to the server. All product functionality is exposed via SOAP and REST APIs, as well as the majority of the functionality is accessible via CLI. SDKs for Java, Angular and JQuery is also given with the majority of the functionalities of the solution supported.

SailPoint has a modern UI with good authenticator options for user self-service and admin access. Provisioning of access and pre-defining of entitlements is dynamically driven by birth rights, roles. Access review and certifications is AI and machine learning driven. Cloud Access Manager supports dynamic visibility while making access reviews of the user on given clouds. Support for micro certifications is available. Reporting and auditing features are based on detailed timeline logs. Event triggers in place to initiate workflow operations which are customizable and configurable.

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, AI driven risk mitigation, and reporting capabilities in a positive direction, making it a recommended consideration in any IGA evaluation.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



## Strengths

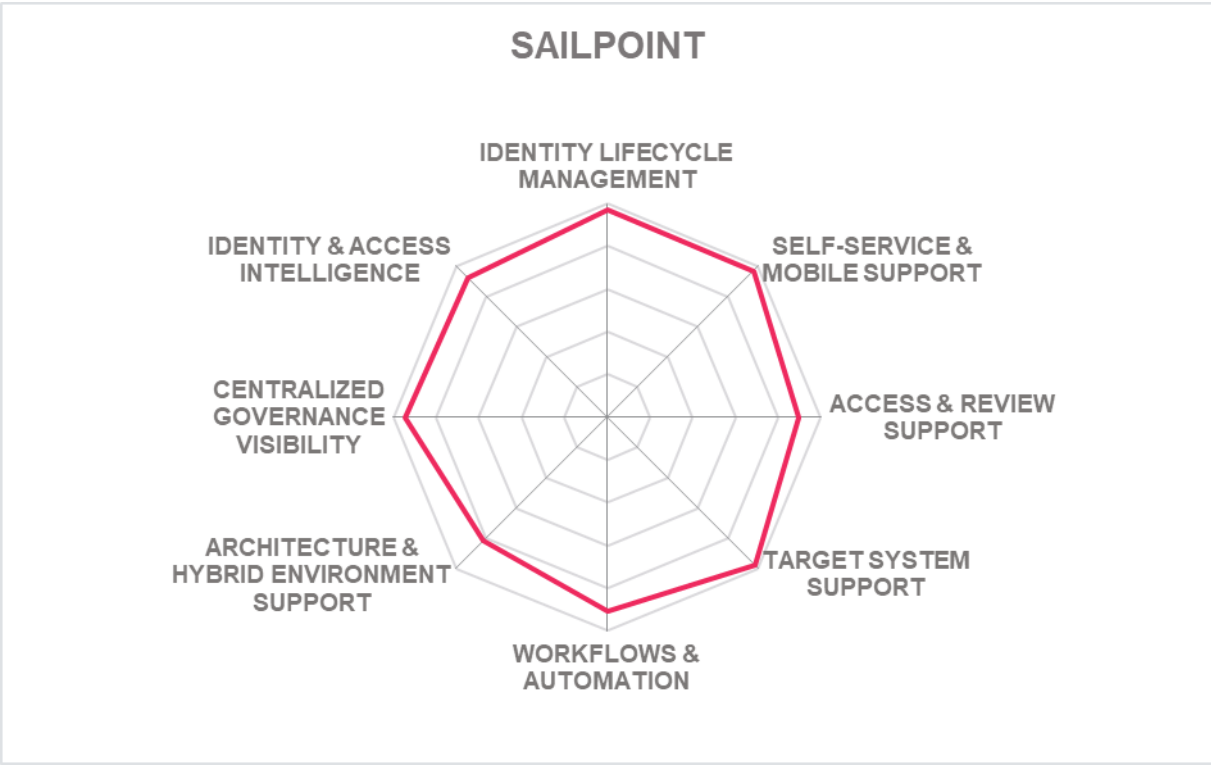
- Strong global partner ecosystem
- Strong support for all known governance use cases
- Excellent identity life cycle management
- Very good support for user self-service and admin access
- Strong auditing and reporting features
- Very good policy management
- Access review and certification is driven by AI/ Machine learning
- Workflow management

## Challenges

- SoD policy violation not available after addition of each item to shopping cart
- Missing access governance for container and container orchestration platforms
- Limited SDKs available

Leader in





## SAP – SAP Access Control, SAP Access Governance

SAP has an established IAM portfolio. Along with CIAM capabilities from the acquisition of Gigya a few years back, it shows its continued commitment to grow and compete in the mid to enterprise market. SAP offers SAP Access Control and SAP Identity Access Governance products as part of its IGA solution. Both of which are well-integrated with other SAP solutions such as SAP Business Suite to provide excellent Access Governance capabilities for SAP and a few other ERP applications.

SAP Identity Access Governance supports a good set of identity repositories including AD/Azure, LDAP, SAP HR, SAP IDM, SuccessFactors, as well as any SCIM supported repository natively with IGA solutions. SAP IDM is available for synchronization with any supported identity repositories. Solution supports all types of identities however specific features are not implemented for certain entities. Bulk processing and provisioning of identities is supported. OOB integration to popular third-party ITSM tools is not given, although a workflow interface does help extend capabilities. Good support is given for out-of-the-box (OOB) provisioning connectors for on-premises systems, but noticeably less support for SaaS. SCIM and SPML is supported for target system connectivity. Automated provisioning is supported and policy in place for RBAC when onboarding. Definition of business rules for birth right access is given. Just-In-Time (JIT) provisioning is supported with transaction definitions. Solution uses machine learning for flagging malicious transactions/anomalies and allows user to review the actions.

For SAP Identity Access Governance, the UI and dashboards are modern and customizable. Good support for access-request is given with a possibility of choosing between a one-step or two-step approval process. Business role definitions are automated with a strong UI for role visualization. The solution uses machine learning for clustering business roles. Authenticator options to both user and admin portals are strong, including FIDO supported by SAP Cloud Identity authentication. The appearance of reporting and analytics is relatively poor, with support for out-of-the-box reports for major compliance frameworks limited to SOX.

SAP Access Control is on-premises or in the cloud via Private Cloud Extended (PCE) option, with SAP Identity Access Governance as their fully multi-tenant cloud solution. SAP IAG is a multi-tenant SaaS solution whereas Access Control, IDM, Enterprise SSO are offered as private cloud editions and deployed like containerized solutions. Less than half of the product's functionality is exposed via REST APIs, and SOAP APIs are not available. 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, with comparatively lesser presence in APAC and Latin America. Overall, SAP provides a well-rounded set of IGA features. Despite the limitations mentioned, SAP Identity Management remains a contender in the IGA market and a preferred vendor for organizations with significant investments in SAP software.

<b>Security</b>	Positive
<b>Functionality</b>	Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Positive



## Strengths

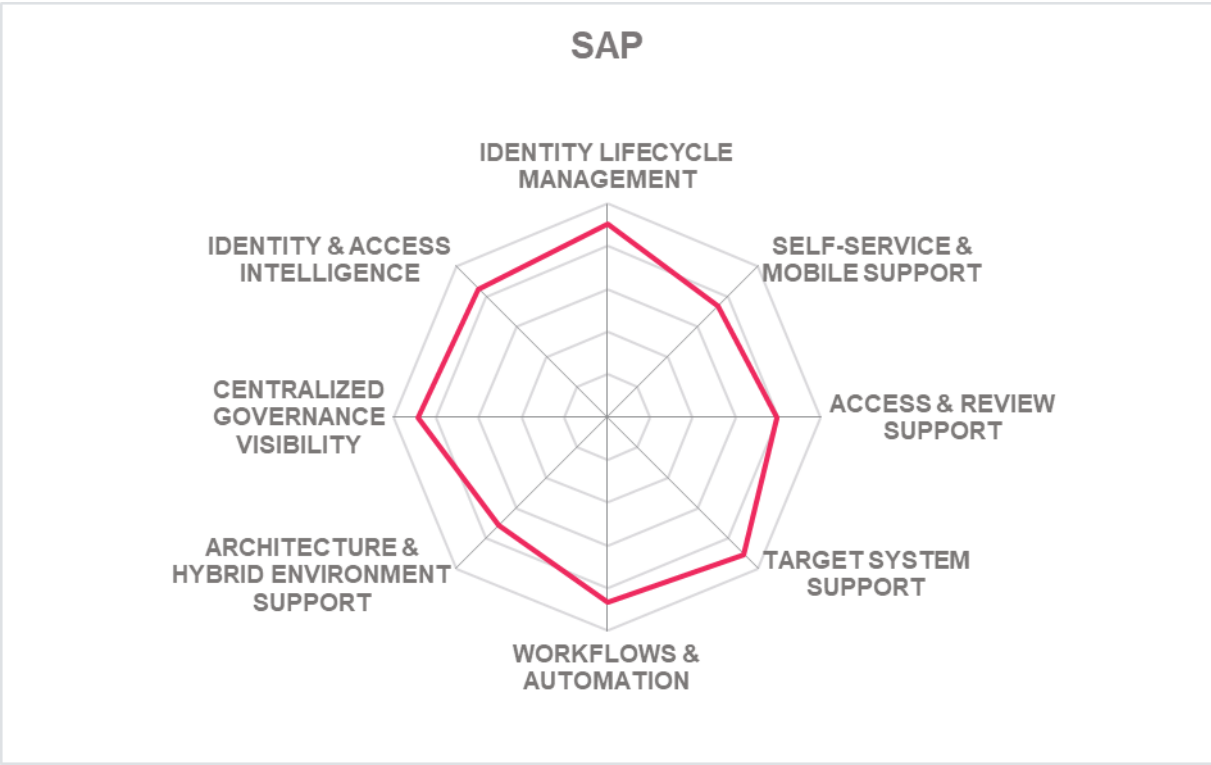
- Very strong policy management
- Very good access governance capabilities
- Strong capabilities for identity and lifecycle management
- Modern and user-friendly UI
- Good support for flexible workflow and automation
- Machine learning integration into various functions

## Challenges

- Limited support for governance use cases
- Strong connector support for on-premises systems, but some gaps particularly for non-SAP business applications and SaaS application
- Limited delivery options

Leader in





## Saviynt – Enterprise Identity Cloud Platform

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 and Administration (IGA), Privilege 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 EIC Platform is a cloud-based solution. 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 connecting to a wide range of identity repositories. SCIM and SPML is supported for identity provisioning/ deprovisioning. Saviynt integrates with ITSM tools such as ServiceNow, Remedy, Boomi, etc. for manual fulfillment of requests originated from Saviynt. Saviynt also provides extensibility using which any ITSM tool can be integrated through some customization via API. A very impressive list of OOB provisioning connectors for on-premises and SaaS systems is available. Saviynt has also added a built-in Identity RPA Bot that can deploy on-premises for a hybrid deployment. It can be used for rapid onboarding and convert disconnected applications to connected applications for automated reconciliation, provisioning, and account management.

Saviynt supports all known deployment models and can be delivered as-a-Service, Container based platform (Docker, Redhat, Unix/Linux, Windows systems). It can also be deployed as software to the server, as a managed service and virtual appliance. Saviynt provides a modular and ground-up microservices architecture for flexible deployment and scaling. It is built on a containerized model to automatically scale up and down based on the usage of a microservice. The majority of the functionalities are exposed via SOAP, REST, SCIM and LDAP APIs. SDKs for Java is available, but REST based APIs can consume most of the programming languages.

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. Persona based mini applications are visible and support is given for governing bots and external risks. Risk based SoD violations is shown and the risk weightage is configurable. The solution has an inbuilt hybrid SoD analysis model for discovering entitlements and suggesting roles. Access request/ approval is comprehensive with zero code approach for workflow configuration. The dashboard for reporting is well laid out.

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. Saviynt's roadmap features for the EIC includes zero trust model, identity proofing, advanced identity analytics and its existing IGA capabilities make it a recommended product.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



## Strengths

- Strong features for identity and access intelligence
- Very strong list of OOB provisioning connectors for target systems
- Access certifications driven by AI and machine learning
- Advanced features supported for policy and workflow management
- Strong SoD and role management

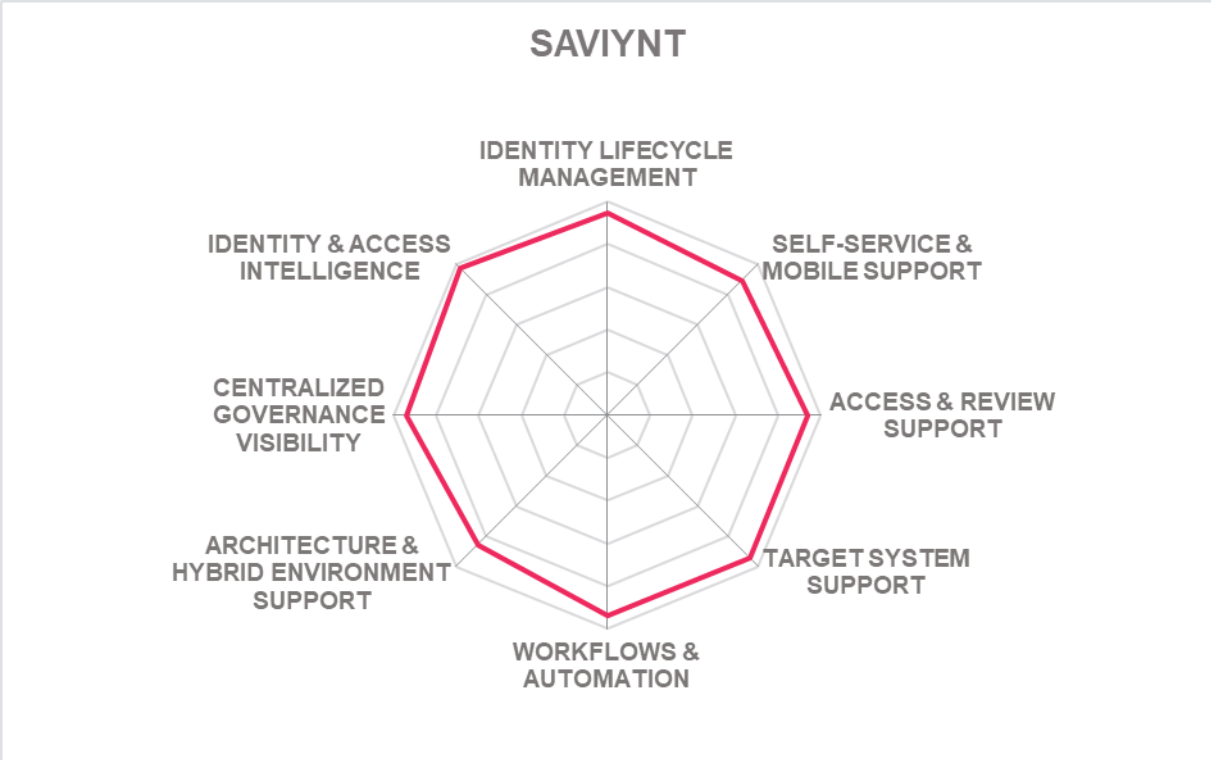
## Challenges

- Missing CLI functionality
- Limited SDK support
- Limited but growing presence outside North American market

Leader in







## Simeio – Simeio IGA Managed Services

Founded in 2007 and 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 IGA managed services includes orchestration platforms. The platform provides a simple and efficient solution for application on boarding to various different IAM technologies from IGA to Access Management and PAM from one Simeio IO Platform.

Simeio offers a full range of identity repository support options and a strong support for OOB on-premises and SaaS target system connectors. SCIM and SPML is supported for identity provisioning and deprovisioning. Simeio offers a platform with a fully integrated suite of IGA, AM, and PAM domains as well as providing add-on capabilities via certified integrations with commercial solutions like BeyondTrust and CyberArk as examples. OOB integration to ITSM tools ServiceNow, Cherwell, BMC Helix ITSM, Atlassian Jira Service Desk and Remedy is given. Simeio IO OOTB connector facilitate on pulling the ticketing status using the ITSM integration to the downstream systems. Other strong features include offline certification capability to the certifiers, dynamic workflows, business partner/ delegated management console and business partner user onboarding.

Simeio IGA Managed Services supports all known types of deployment models including containerised deployment. Simeio primarily focuses 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. Almost all capabilities of the solution are exposed via REST, SCIM and LDAP APIs. Access to functionality is not offered via CLI, nor are any SDKs provided.

Simeio IGA Managed Services has a modern web UI with useful dashboards for both user self-service and administration. Good workflow capabilities for requesting access. The product requires CSV files for defining entitlements. It has good user self-service there the forms can be previewed and edited in real time. Progress details of application on boarding can be visualised. Access review is available for application on boarding. It has a strong orchestration model for identity unification, governance, automation, monitoring and reporting. Simeio IGA Managed Services provides OOB support for all known reports for major compliance frameworks. Strong list of authenticators is provided for user self-service and admin access.

Simeio is a privately held company that mainly supports mid-market organizations, primarily in North America with a growing footprint in the EMEA starting with the UK. 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 innovation capabilities in RPA and bots and good IGA capabilities as part of the Simeio IGA Managed Services solution which should be considered by organizations primarily in the North American and EMEA regions.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



## Strengths

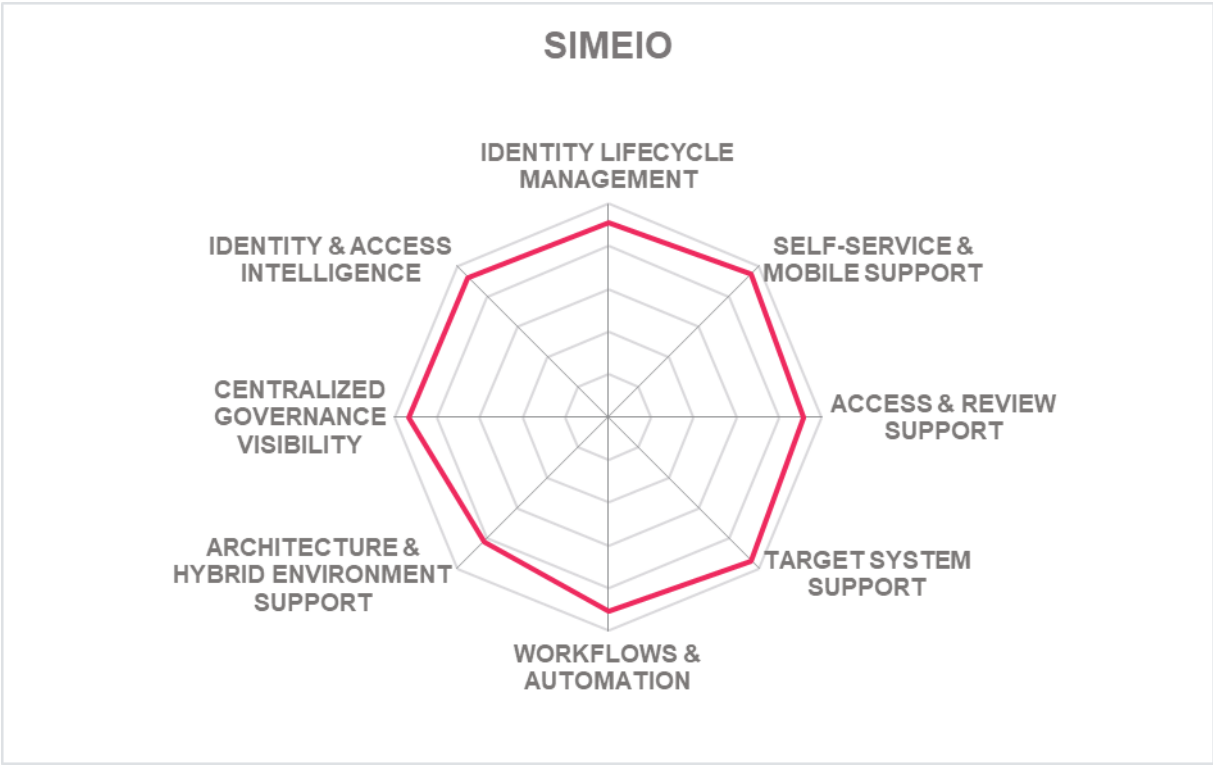
- Strong identity life cycle management capabilities
- Strong target support for on premise and SaaS systems
- Very good list of authenticators for user self-service and admin access
- Good Policy management
- Impressive workflow and automation capabilities
- Identity and access intelligence capability
- Very good access governance capabilities

## Challenges

- Strong customer base however relatively low partner ecosystem
- Limited presence in EMEA market
- CLI and SDK support is missing

Leader in





## Soffid – Soffid IAM

Based in Spain and established in 2013, Soffid IAM provides a converged IAM Platform that brings Access Management (AM), Single Sign-On (SSO), Identity Governance (IGA), Identity Risk & Compliance (IRC) and Privileged Account Management (PAM) in one comprehensive platform. Soffid offers a subscription service to an enterprise edition of the software product. Technical support service is provided only to the enterprise edition. 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-premises Leadership Compass report.

Soffid IAM not only supports on-premises deployment but also full multi tenancy for private & public cloud deployment. From 2022, the solution can now be delivered on a virtual appliance. Other options for delivery include as a service, hardware appliance, server deployment and container-based platforms (docker and red hat). Delivery as a managed service is planned for release in Q3 2022. Soffid states solution's 100% functionalities are exposed via SOAP, REST, SCIM and LDAP APIs and the functionalities are available via SDKs.

Soffid IAM supports a wide range of identity repositories with additional support for integrating into legacy directory solutions of customers. Support for generating identities which do not exist is available. Wide range of OOB provisioning on-premises and SaaS connectors is supported. The solution uses a smart engine to fetch and post information from target systems. OOB integration to ITSM includes ServiceNow and Atlassian JIRA service desk.

Soffid IAM has an engaging UI. The solution supports easy attribute mapping but also supports an online editor for complex scripts. Soffid IAM has a useful dashboard which displays information such as status of requests, analytics, and risk analysis matrix to compare the risk level before providing access. The solution supports a wide range of authenticator options including approval or rejection of permissions via email or OTP. The approval model is connected to a web interface which supports a configurable web workflow editor. A good set of OOB IGA related reports is available, although OOB reports for major compliance frameworks are not.

Soffid IAM currently focuses on enterprise organizations but also serves small, medium organizations but with customers primarily in Latin America and growing in Europe, North America, and Middle East region. 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.

<b>Security</b>	Positive
<b>Functionality</b>	Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive

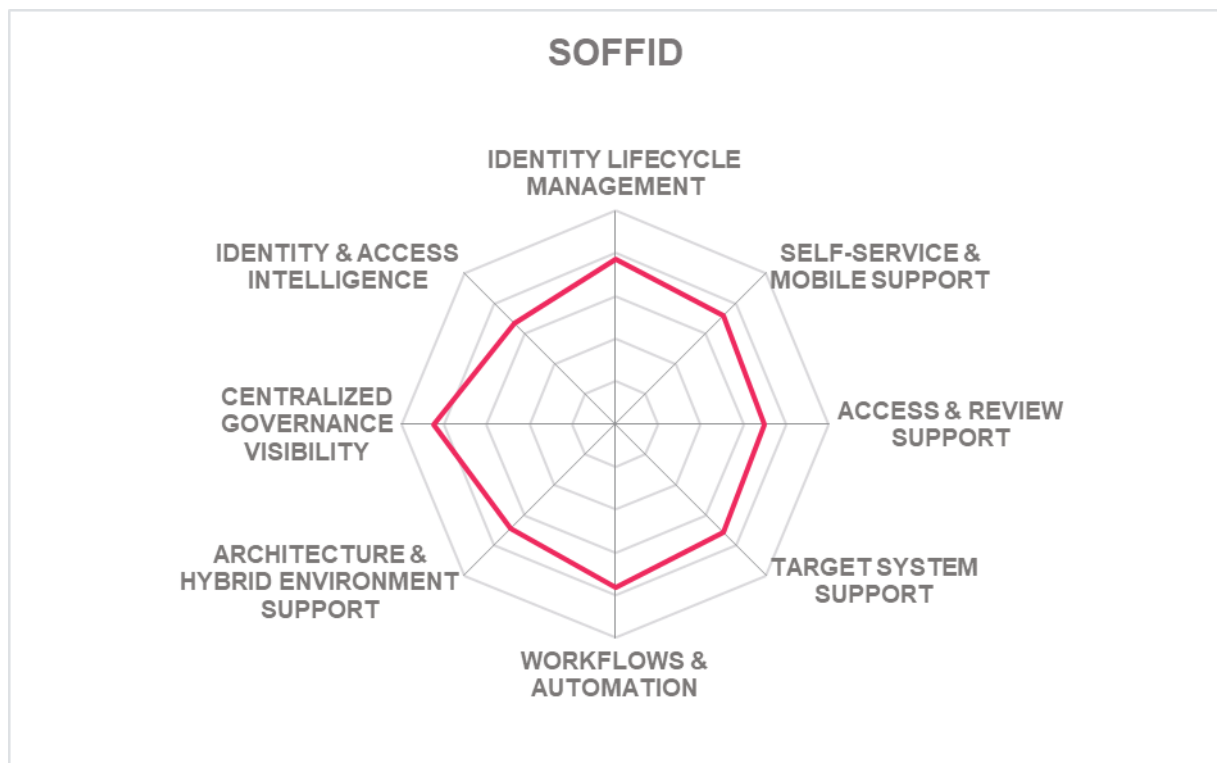


### Strengths

- Good IGA related policies for onboarding and offboarding
- Good support for IGA related reports
- OOB SaaS and on-premises target system support
- Wide range of user and admin authenticator options
- Good web workflow editor
- Good role mining engine

### Challenges

- Limited market presence and partner ecosystem in Europe
- No support for OOB reports for major compliance frameworks
- Event based micro certification is missing



## Tools4ever – HelloID

Tools4ever is a Dutch software company that started in the SMB market segment but has grown its portfolio to a level where it can also serve the IAM requirements of larger organizations. HelloID is a completely cloud-based solution with features focused on access management, provisioning, ABAC and service automation.

HelloID supports limited servers, databases or virtual directories which can be used as identity repositories. Currently it supports only Microsoft AD, Microsoft AAD and Google for this function. SPML and SCIM connectivity is supported for identity provisioning. The product has strong support for all known major OOB ITSM tools for integration including ServiceNow, JIRA, Cherwell, Helix, OTRS and Topdesk. Strong support for OOB provisioning connectors for SaaS systems with over 150 connectors on offer for on-premises and cloud systems. HelloID has a strong set of authenticator options for user self-service and admin access. Passwordless authentication is also available within the solution and support for FIDO2 tokens is also given. HelloID has strong capabilities of access recertifications, governance, policy management, access review.

The product is offered as a SaaS only solution with deployment on MS Azure public cloud. It is a complete cloud-based platform with on-premises agent provided for management of on-premises accounts. The majority of the functionalities of the solution are exposed via SOAP, REST and SCIM APIs. SDK support is currently not available, and a developer portal is also missing. The test portal and the technical support are provided in the subscription model.

HelloID has a modern UI with configurable dashboard based on the RBAC model. The tab-based layout provides a clear indication of applications on the homepage. The user self-service access request is well defined and has a transparent workflow. Definition of rules and entitlements is available, and the system recommends the identities who are qualified for the changes.

With a good product roadmap and execution capability, Tools4ever can make some good progress over the next few years to be able to contend with the existing IDaaS players in the region. Currently its customers are mainly based Europe and North America. It is a dominant market leader in the Netherlands.

<b>Security</b>	Positive
<b>Functionality</b>	Neutral
<b>Deployment</b>	Neutral
<b>Interoperability</b>	Neutral
<b>Usability</b>	Positive

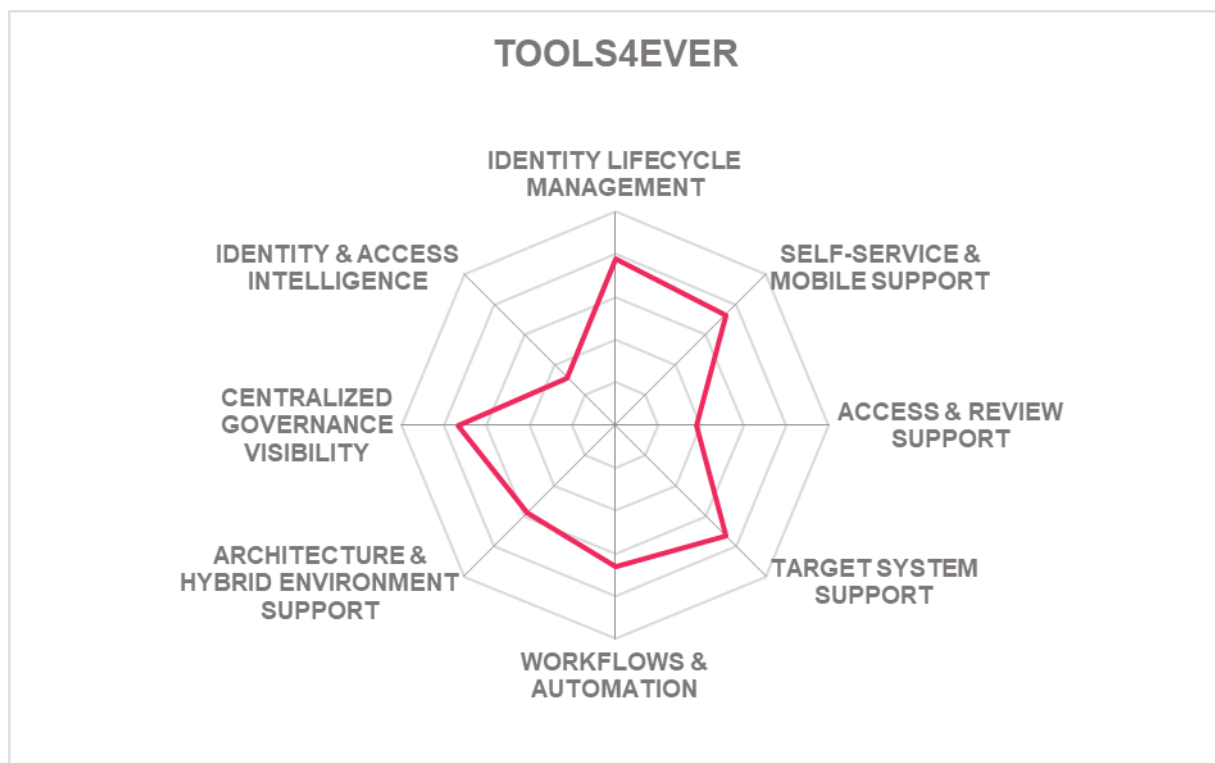


## Strengths

- Strong support for OOB IGA related reports
- Very good policy management
- Good features supported for workflow automations
- Modern and user-friendly UI
- Wide range of OOB provisioning connectors for SaaS systems
- Strong capabilities for identity provisioning

## Challenges

- Missing OOB major compliance frameworks
- Missing identity and risk-based analytics
- Missing support for OOB workflows





## ZertID – ZertID

Founded in 2021 and a spin-off of Sysintegra, ZertID provides an IGA solution that is built on top of the ServiceNow platform with rapid implementation ability. It has a strong UI capability with adaptation to ServiceNow portal design. The product integrates neatly with ServiceNow features such as the CMDB and Security Incident handling. By utilizing capabilities such as the data management, workflows of ServiceNow, and with full user interface integration into the ServiceNow portal, it is a lean and efficient solution for IGA. All areas of IGA, including provisioning of connectors to target systems, are supported with major capabilities in user lifecycle management, identity provisioning and access governance.

ZertID has strong workflow capabilities inheriting from ServiceNow. The solution supports real time role and attribute-based access controls. It supports a moderate level of identity repositories for managing identities. SPML and SCIM are supported for identity provisioning and deprovisioning. Native integration with ServiceNow is standard however, connectors are available for OOB integration to other ITSM systems. The solution further inherits the pre-built target system connectors from the ServiceNow integration Hub. New connectors can be rapidly implemented based on the requirements. The solution uses access intelligence for identification of orphaned accounts and then mitigating access related risks. Access intelligence features also provide recommendations for access based on reference identity which is selected by the users.

Cloud deployment of ZertID on ServiceNow is the preferred choice. On premise deployment of the solution is possible for the early few customers who started with on-premises ServiceNow infrastructure. This does not apply to the new customers and the vast majority who run ServiceNow from the cloud. Integrating with existing IGA solutions is currently not available out-of-the-box. It can also be delivered as a managed service or deployed as software to the server. However, deployment to server depends on customers having on-premises ServiceNow agreement. The majority of the solution's functionality is available via SOAP, REST, SCIM and LDAP APIs. SDKs and a developer portal are missing.

ZertID primarily supports mid-market businesses focused on the APAC region. Recent updates include an RPA capability for orchestrating access provisioning to third-party systems that are not electronically (API, Data Base etc) connected with ZertID. This capability uses ServiceNow's relatively new RPA engine. Further update includes a built-in PAM solution with IGA workflows providing deep level Privileged Access Governance (PAG). With its strong identity and lifecycle management capabilities and target system support, ZertID further plans to expand its list of pre-built connectors and incorporating the use of AI and machine learning showing its innovation roadmap.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive



## Strengths

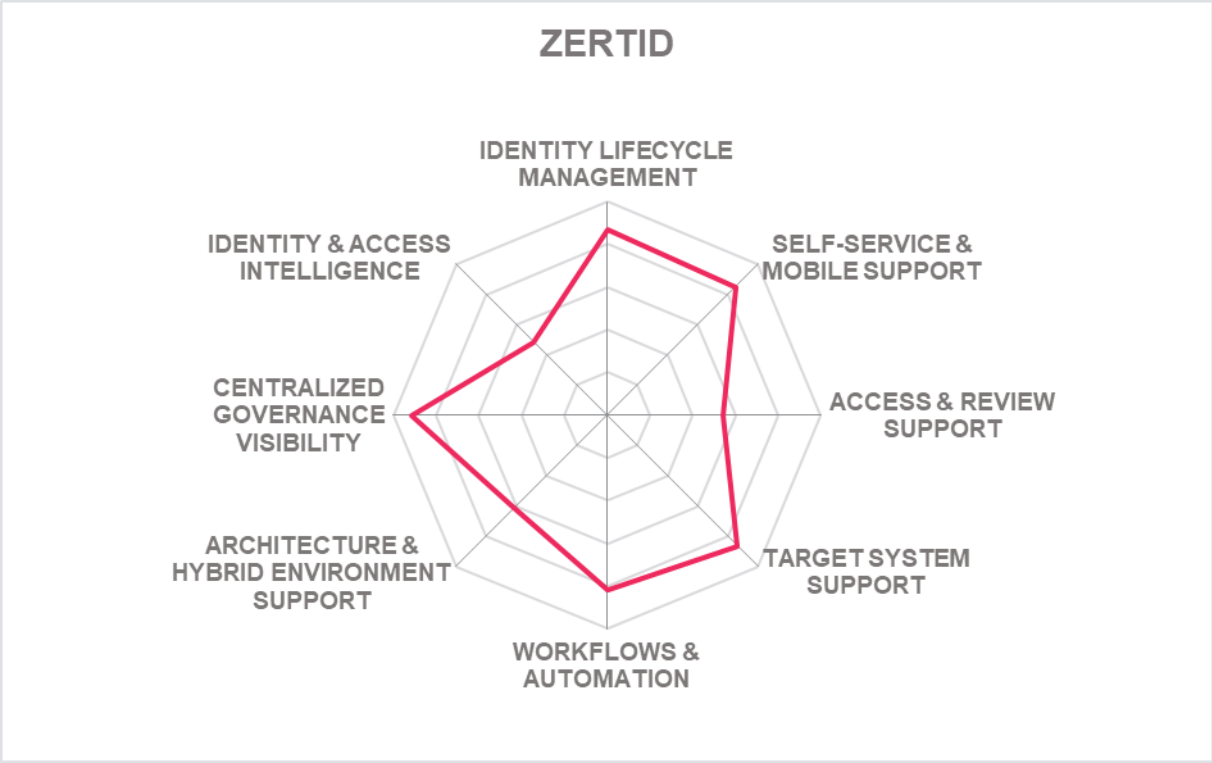
- Good Identity and lifecycle management
- Good set of connectors for common requirements of mid-market and medium-sized organizations
- Intelligent Access recommendations and use of AI/ML
- Persona-based user interface, integrated with the ServiceNow portal
- Easy deployment on top of ServiceNow
- Strong access governance capabilities
- Strong relationship of vendor to ServiceNow, being an Elite Partner

## Challenges

- Still a relatively small vendor with a limited global partner network
- Integration to existing IGA solution is not yet available out-of-the-box
- SDKs and developer portal are missing

Leader in





## Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment or may be a fast-growing startup that may be a strong competitor in the future.

**Fastpath** – Fastpath recently acquired ideiio to create a more complete IGA package by addressing the missing functionalities. They have a solution covering broad cross-system IGA plus in-depth access control/governance for SAP and other Line of Business Applications). It takes over the capabilities of ideiio of having a strong support to all known 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 including SCIM and SCIM 2.0 and LDAP support. Custom connectors can be made according to requirements. The product provides a REST API for identity lifecycle management and most of the core functionality and configuration. The solution supports transformation of connectors and can connect to external systems.

Their solution is designed and developed to achieve notable success in B2B implementations and the higher education industry. Currently its presence is in UK, Benelux, and USA and growing. Their roadmap includes improved identity and access reporting and role-based governance certifications and expansion of 3rd party integrations and advanced access governance and access intelligence capabilities.

**Why worth watching:** With the latest acquisition of ideiio by Fastpath, their solution offers a positive roadmap and growth in the IGA segment as well as being a strong vendor in the B2B implementations.

**Fischer Identity** - Fischer Identity offers Fischer Identity Suite comprising several modules available as a bundled offering to deliver a broad range of IGA capabilities. Besides standard identity lifecycle management and user administration capabilities, the Governance and Compliance module combined with the Role and Account Management component provides effective Access Governance.

**Why worth watching:** Fischer has some areas for improvement that are already on its near-term roadmap, Fischer offers a comprehensive IGA suite suitable for customers across most industry verticals, particularly education.

**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. Meibo People Pack (MPP), a pre-packaged version of Meibo Identity Management, is primarily focused on the IGA requirements of SMB organizations that prefer an out-of-the-box solutions. 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 Global SSO provides authentication options and, together with MPP, provides the IGA solution evaluated in this report.

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 overall flexibility. Both Meibo People Pack (MPP) and Sign&go Global SSO together offer a complete IGA solution.

**Why worth watching:** Ilex SaaS offering is hosted in France, fully compliant with the GDPR, and making it a good alternative solution set to consider in their primary geographic region.

**Imprivata** – 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. 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.

**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.

**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 organization's 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 Oracle IDCS, OAM, SIEM, UEBA, or even CASB integrations as examples. Risk analytics can be derived from entitlement analysis. Actions can be taken, depending on the risk analysis, to lock a user's account or trigger a security audit, as some examples.

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

**Pirean** – Founded in 2002, Pirean is a medium-sized company 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.

**Systancia** – Based in France, 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 Identity provides basic IGA capabilities, focusing on Identity Lifecycle Management, automated provisioning, user self-service, and workflows. Systancia is an access platform for users, privilege, internal, external, zero trust access and provides identity management and manages all entitlements and rights. It mainly supports customers in the medium to mid-market sector with most of them focused in the EMEA region. It has a good partner ecosystem in EMEA.

**Why worth watching:** Systancia has advanced features for access request and management with a very strong modelling of entitlement rules. entitlement model. Their solution will be an interesting choice for a solution that can quick results without any need of technical coding

**Tuebora** – Found in 2001 and based in San Francisco, California, Tuebora provides a self-driven identity and access management platform. Tuebora relies on AI and machine learning for Identity Analytics and Access Governance. It is powered by predictive analytics and

intelligence for its functioning of a self-driven IAM model. 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.

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

## Methodology

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

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

## Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders:** Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders:** Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.
- For every area, we distinguish between three levels of products:
- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also



mature and might be leading-edge when looking at specific use cases and customer requirements.

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

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

## Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Deployment
- Interoperability
- Usability

**Security** is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

**Functionality** is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

**Deployment** is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

**Interoperability** refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.



**Usability** is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

## Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

**Financial strength** even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are

venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

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

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

## Rating scale for products and vendors

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

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

## Inclusion and exclusion of vendors

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

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

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

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

We provide a quick overview about vendors not covered and their offerings in chapter ***Fehler! Verweisquelle konnte nicht gefunden werden.*** In that chapter, we also look at some other interesting offerings around the market and in related market segments.

## Related Research

[Link 1](#)[Link 2](#)[Link 3](#)

## Copyright

©2022 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks or registered trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

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

KuppingerCole, founded in 2004, is a global, 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](mailto:clients@kuppingercole.com).