

KuppingerCole Report

LEADERSHIP COMPASS

By **Martin Kuppinger, Richard Hill**
April 30, 2020

Identity Governance & Administration (IGA)

The Identity Governance and Administration (IGA) market is continuing to evolve through more integrated Identity Provisioning 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.



By **Martin Kuppinger**
mk@kuppingercole.com



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

Content

1 Introduction	4
1.1 Market Segment	5
1.2 Delivery models	14
1.3 Required capabilities	14
2 Leadership	18
3 Correlated View	26
3.1 The Market/Product Matrix	26
3.2 The Product/Innovation Matrix	28
3.3 The Innovation/Market Matrix	30
4 Products and Vendors at a glance	33
4.1 Ratings at a glance	33
5 Product/service evaluation	37
5.1 Avatier Identity AnyWhere	39
5.2 Beta Systems Garancy IAM Suite	42
5.3 Broadcom Symantec Identity Governance and Administration (IGA)	45
5.4 EmpowerID	48
5.5 E-Trust Horacius	51
5.6 Evidian IGA	54
5.7 Evolveum midPoint	57
5.8 Fischer International Identity Suite	60
5.9 Hitachi ID Identity Manager	63
5.10 IBM Security Identity Governance & Intelligence	66
5.11 Identity Automation RapidIdentity	69
5.12 Ilantus Compact Identity	72
5.13 Ilex Meibo People Pack (MPP)	75
5.14 Micro Focus Identity Manager Suite	78
5.15 One Identity Manager	81
5.16 Oracle Identity Governance	84

5.17 RSA SecurID Suite	87
5.18 SailPoint Predictive Identity Platform	91
5.19 SAP Access Control	94
5.20 Saviynt Security Manager	97
5.21 Simeio Identity Orchestrator	100
5.22 Soffid IAM	103
6 Vendors and Market Segments to watch	106
6.1 Accenture Memory	106
6.2 Atos	106
6.3 Clear Skye	107
6.4 ForgeRock	107
6.5 Ideiio	107
6.6 Imprivata	108
6.7 Nexis	108
6.8 Omada	109
6.9 Pirean	109
6.10 Singular ID	110
6.11 Tools4ever	110
6.12 Tuebora	110
6.13 Usercube	111
7 Related Research	112
Methodology	113
Content of Figures	119
Copyright	120

1 Introduction

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 Provisioning 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 Provisioning 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 Provisioning in place or when their starting point is Access Governance. One of the adoption patterns we have observed in the market is where fulfilment through Identity Provisioning is achieved via a managed service, 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 Provisioning 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 capabilities. This is generally true for greenfield IAM implementations that have a need for both Identity Provisioning and Access Governance capabilities. It is important that organizations scope their IGA requirements well before starting to evaluate IGA products that differ in the strength of IGA functionalities making most of them better aligned for either provisioning or governance focused deployments.

Based on the adoption trends, changing customer priorities and deployment patterns, we decided to create two distinct Leadership Compass documents to help security leaders identify relevant IAM market segments and subsequently shortlist most appropriate technology vendors based on their immediate IAM priorities:

- **LC Access Governance:** This Leadership Compass focuses primarily on Access Governance and Intelligence capabilities, with required integrations into own or third-party entitlements and/or account repositories. We look at complete IGA offerings here too if they have strong Access Governance & Intelligence capabilities.

- **LC Identity Governance and Administration:** In this Leadership Compass, the primary focus is on the vendors that offer both Identity Provisioning and Access Governance capabilities, either as a common product or separate but integrable product components to deliver capabilities across the IGA spectrum.

These two LCs are complemented by two other Leadership Compass documents – 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 is LC IAM Suites that focuses on comprehensive IAM suites and evaluates vendors for their completeness and functional depth of IAM portfolios to include core and even adjacent IAM capabilities such as Privilege Management, Enterprise SSO, Identity Federation, Web Access Management, API Gateways, Fraud Detection and Prevention etc. in addition to IGA as an integrated offering.

With these various LCs, 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.

1.1 Market Segment

Identity Governance and Administration refers to the increasingly integrated Identity Provisioning and Access Governance markets. Where Identity Provisioning focuses on tasks related to administering access fulfilment and entitlements throughout an identity life-cycle, Access Governance provides necessary (mostly self-service) tools for business to manage workflows and access entitlements, run reports, access certification campaigns and SOD checks. Access intelligence is the analytics layer over Identity Provisioning and Access Governance that offers business-related insights to support effective decision making and potentially enhance governance.

While Identity Provisioning remains a core IAM requirement, 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 moves beyond simple reporting and dashboarding to offer advanced capabilities that include 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. As IGA becomes an important security risk and management discipline directly impacting the security posture of any

organization, a lack of basic IGA capabilities can leave organizations exposed to risks originating from inefficient administration of identities and access entitlements, poor role management and lack of adequate auditing and reporting. These risks range from identity thefts to unapproved and unauthorized changes, access creeps, role bloating, delays in access fulfillment, orphan roles and accounts, SOD conflicts leading to occupational and other internal frauds. Several incidents in recent past have emphasized the need to have better IGA controls for organizations of all sizes, across all industry verticals.

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:

- a) 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.
- b) 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 Enterprise Mobility Management (EMM) 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 & Support Management (ITSSM) 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 ITSSM 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 also an increased emphasis on integrating IGA tools with User Behavior Analytics (UBA) and DAG (Data Access Governance) tools depending on the drivers and business value expected of such integrations. UBA tools can benefit from integration with IGA tools 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 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, more and more 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 Provisioning and Access Governance.

Identity Provisioning:

- **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:** Identity analytics uses data analytic 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 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 also feeds required user access information from authentication and authorization events to User Behavior Analytics (UBA) 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 its 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:** 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, especially ERP and other complex homegrown applications. 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 overlaid 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. Enterprise Mobility Management (EMM) 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 Access Governance (DAG) tools to extend standard IGA controls to data and information stored across multitude of systems including device endpoints, file shares, network mounts etc.

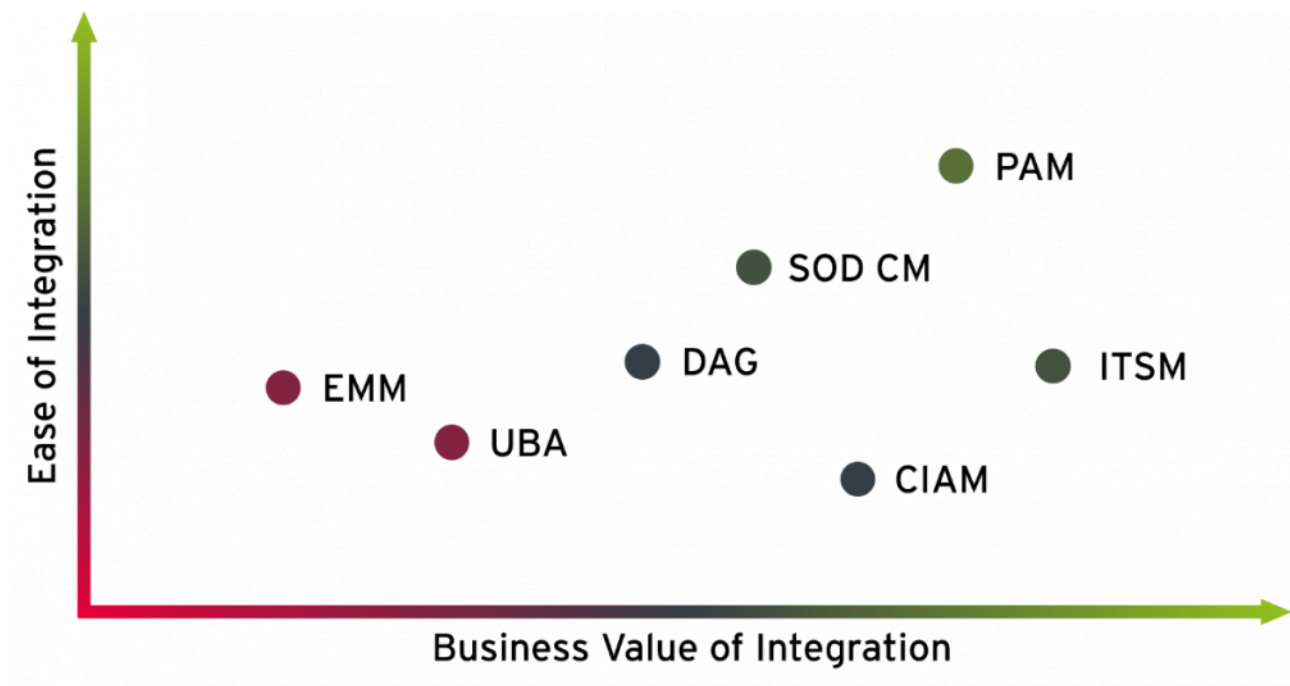


Figure 1: Business Value of Integration

Ease versus perceived business value of IGA integrations with enterprise systems

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 Provisioning' and 'Access Governance' categories.

1.2 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.

1.3 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 Request & Approval
- Access Review
- Access Intelligence
- Access Risk Management
- Authentication
- User Interface and Mobile Support
- 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 Provisioning 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 Provisioning 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 pretty popular for simplifying the access request management process by using shopping cart paradigms familiar to the users.
- **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.

- [EAG](#)/Data Governance

Support for Entitlement and Access Governance (EAG), i.e. the ability to also analyze entitlements at the level of underlying systems such as SAP, Windows file servers, etc.

- 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.

2 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



Figure 3: 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 mature markets, where a considerable number of vendors deliver feature-rich solutions. The market continues to remain crowded, with 22 vendors we chose to represent in our Leadership Compass rating with a few other vendors that did not meet our basic evaluation criteria listed in the “vendors to watch” section or which declined participation in this year’s edition, such as ForgeRock and Omada.

SailPoint retains its leadership position in the Overall Leadership evaluation of the IGA market closely followed by IBM. A group of vendors is following, including One Identity, Oracle, Micro Focus, Saviynt, EmpowerID, Broadcom, and RSA. This group of vendors is a mix of established and emerging players, some being stronger in their market position, and others in innovativeness. We

strongly recommend further, detailed analysis of the information provided in this document for choosing the vendors that are a best fit to your requirements.

Other vendors in the Overall Leaders segment for IGA include Hitachi ID and SAP – both find a considerable push into the Overall Leader segment with their improved ratings for market and innovation evaluation criteria.

The Challenger segment is as populated as the Leaders segment and features both established 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 Evidian, Beta Systems, and Avatier, closely followed by Ilantus. Fischer Identity, Soffid and Ilex follow with some distance. Further vendors in this segment are Simeio and Identity Automation. Near the bottom boarder of the Challenger segment is Evolveum and E-Trust, all good products with varying levels of IGA capabilities, market presence throughout the world or other market niche focus.

No vendors appear in the Follower segment.

Overall Leaders are (in alphabetical order):

- Broadcom
- EmpowerID
- Hitachi ID
- IBM
- Micro Focus
- One Identity
- Oracle
- RSA
- SailPoint
- SAP
- Saviynt

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, very closely followed by Saviynt and

IBM. EmpowerID takes a position in the upper range of the Leader's segment, followed by a group of vendors including Hitachi ID, Micro Focus, One Identity, and Oracle (in alphabetical order), 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. It is therefore highly recommended that organizations spend considerable resources in properly scoping and prioritizing their IGA requirements prior to IGA product evaluation. RSA Security and Broadcom are positioned next as leaders in the product leadership segment, trailing the others from a close distance in the completeness of product leadership qualities. Beta Systems appears near the bottom boarder of the Product Leadership segment.

In the challenger's segment of product leadership are (in alphabetical order) Avatier, E-Trust, Evidian, Evolveum, Fischer Identity, Identity Automation, Ilantus, Ilex, SAP, Simeio, and Soffid. All these vendors have interesting offerings but lack certain IGA capabilities that we expect to see, either in the depth or breadth of functionalities.

No vendors appear in the Follower segment.

Product Leaders (in alphabetical order):

- Broadcom
- Beta Systems
- EmpowerID
- Hitachi ID
- IBM
- Micro Focus
- One Identity
- Oracle
- RSA Security
- SailPoint
- Saviynt

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.

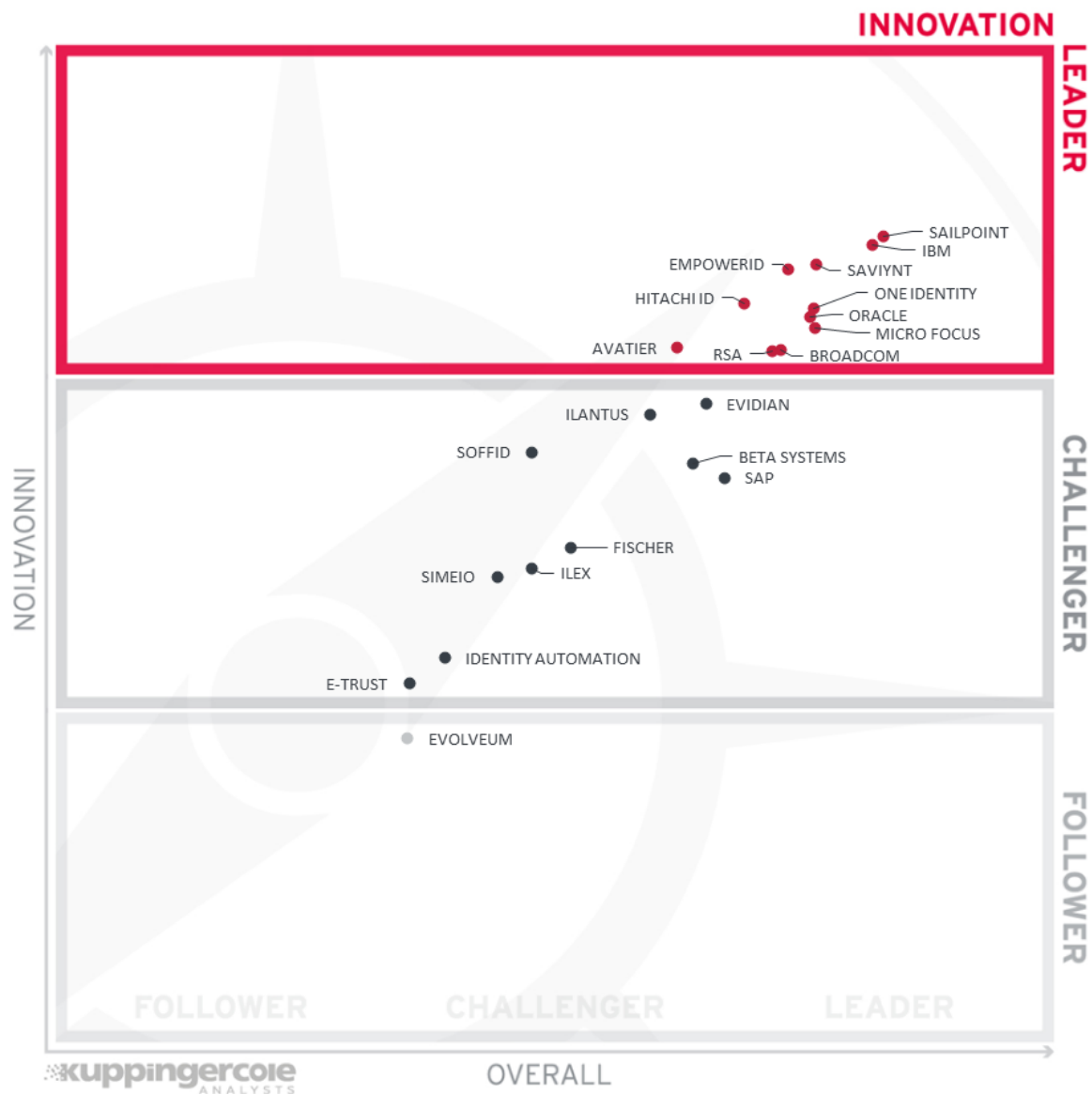


Figure 3: Innovation Leaders in the IGA market segment

We have rated several vendors as Innovation Leaders in the Identity Governance and Administration 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, and improved API layers to more specific areas such as improvements to access certification, 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 area of innovation 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 continues to lead the Innovation Leadership evaluation, very closely followed by IBM, Saviynt, and EmpowerID. Hitachi-ID, Micro Focus, One Identity, and Oracle (in alphabetical order) are next on the chart and continue to strengthen their IGA leadership position with constant innovation. Ranked next are Avatier, Broadcom, and RSA Security (in alphabetical order) that have made 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, and therefore a thorough vendor selection process is essential to pick the right vendor of all the IGA players that best fit the customer requirements.

Players that have made it to the Innovation Challenger segment (in alphabetical order) are Beta Systems, E-Trust, Evidian, Fischer Identity, Identity Automation, Ilantus, Ilex, SAP, Simeio, and Soffid. All these vendors have also been able to demonstrate promising innovation in delivering specific IGA capabilities. Please refer to the vendor pages further down in the vendor's section of this report for more details.

Evolveum is the only vendor in the Follower's segment, showing some specific innovations but lacking the breadth in innovative features we'd like to see from IGA vendors.

Innovation Leaders (in alphabetical order):

- Avatier
- Broadcom
- EmpowerID
- Hitachi ID
- IBM
- Micro Focus
- One Identity
- Oracle
- RSA Security
- SailPoint
- Saviynt

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 3: 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 relatively

smaller customer base.

With a strong market position, successful execution, and strengthened IGA product features, SailPoint and IBM are set to lead the Market Leadership evaluation from the front. Closely following these two vendors in the Market Leadership segment are (in alphabetical order) Broadcom, Micro Focus, One Identity, Oracle, and SAP – all of which have several deep-rooted complex IGA deployments across multiple industries. RSA is placed next in this segment, followed by Saviynt, EmpowerID, Evidian, and Beta Systems – all but SailPoint have a broader IAM portfolio, which helps them upsell IGA products to large customers.

In the Challenger section, we find Hitachi ID, and Avatier close to the Leader segment. 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 limited global presence, and a shortage of technology partners with their IGA product deployment being one of them. Following this group is Ilantus, with Fischer Identity and Ilex near the center. E-Trust, Evolveum, Identity Automation, and Simeio (in alphabetical order) appear close to the bottom boarder.

In the Follower segment, we find Soffid – 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):

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

3 Correlated View

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

3.1 The Market/Product Matrix

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



Figure 7: The Market/Product Matrix.

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership.

In this comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of “overperforming” in the market. It comes as no surprise that these are mainly the very large vendors, while vendors below the line are often innovative but focused on specific regions.

In the upper right segment, we find the “Market Champions”. Given that the IGA market is fast

maturing, we find SailPoint and IBM as market champions being positioned in the top right-hand box. Close to this group of long-established IGA players in the same box are Broadcom, Micro Focus, One Identity, Oracle, and RSA Security (in alphabetical order). Being positioned closer to the axis, SailPoint and IBM represent a slightly better balance of market vs product leadership.

EmpowerID and Saviynt are positioned under the axis representing their inclination for stronger product leadership in comparison to the market leadership today, and with Beta Systems just above the axis.

SAP and Evidian are 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 two vendors that delivers strong product capabilities for IGA but is not yet considered Market Champions. Hitachi ID has a strong potential for improving its 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 average market success as compared to market champions. These vendors include (in alphabetical order) Avatier, E-Trust, Evolveum, Fischer Identity, Identity Automation, Ilantus, Ilex International, and Simeio.

Finally, in the bottom middle box is the remaining vendor, Soffid, with less market visibility than product strength.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

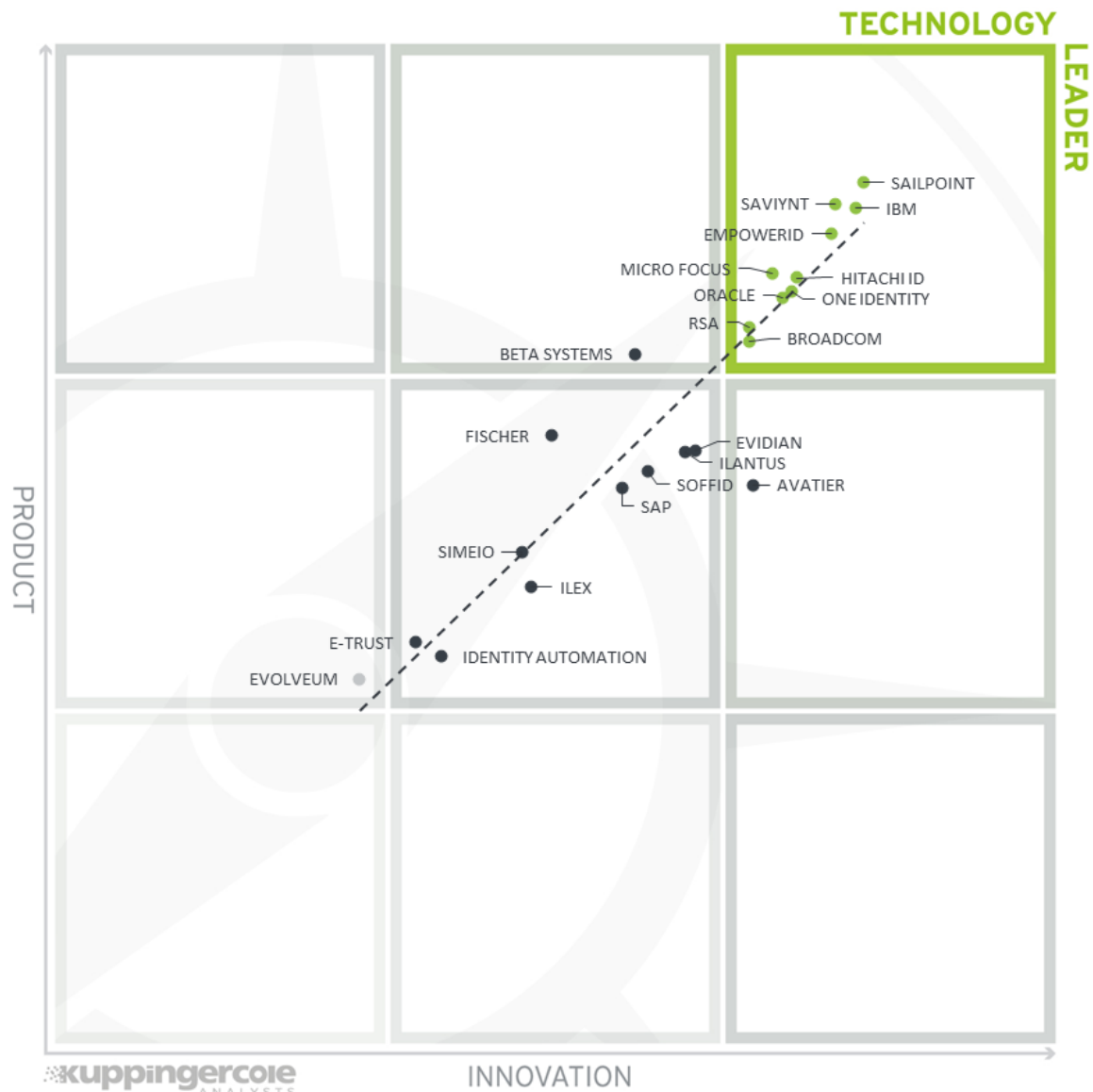


Figure 8: The Product/Innovation Matrix.

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

Here, we see a good correlation between the product and innovation rating, with most vendors being placed close to the dotted line indicating a healthy mix of product and innovation leadership in the market. 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 (in alphabetical order) IBM, EmpowerID, and Saviynt – with most placing close to the axis depicting a good balance of product features and innovation.

Micro Focus, Hitachi ID, One Identity, and Oracle are following. RSA Security and Broadcom are found more towards the bottom of the box.

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

The right middle box vendors show stronger innovation with less product strength which includes Avatier.

In the center middle box, we find (in alphabetical order), E-trust, Evidian, Fischer Identity, Ilantus, Ilex, Identity Automation, SAP, Simeio, and Soffid having less product and innovations than the Technology Leaders.

Lastly, to the left, we find Evolveum, just missing the Challenger level in innovation.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.



Figure 9: 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 compared to their relatively weaker position in the Innovation Leadership rating, while vendors below the line show, based on their ability to innovate, the biggest potential for improving their market position.

In the upper right-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, IBM, Micro Focus, One Identity, Oracle, RSA, and SailPoint. Saviynt and EmpowerID are placed in the same box, more towards the

bottom, indicating that they haven't yet reached the same market position as the established players.

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

In the box at the middle top, we find Evidian, Beta Systems, and SAP, all 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 leaderships, which includes Ilantus, Fischer Identity, Ilex, Identity Automation, Simeio, and E-Trust.

Only Soffid appears in the bottom middle box indicating innovation with lower market presence. Vendors appearing in the bottom box gave the least amount of innovation and market presence in this Leadership Compass product evaluations. However, these vendors have the potential to become more innovative, increase market presence or both.

Finally, Evolveum is placed in the left-most box to the bottom, indicating their relatively weak market position and gaps in innovativeness.

4 Products and Vendors at a glance

This section provides an overview of the various IGA products/services we have analyzed within this KuppingerCole Leadership Compass on Identity Governance and Administration. This overview goes into detail on the various aspects we include in our ratings, such as security, overall functionality, etc. It provides a more granular perspective, beyond the Leadership ratings such as Product Leadership, and allows identifying in which areas vendors and their offerings score stronger or weaker. Details on the rating categories and scale are listed in chapter 7.2 to 7.4.

4.1 Ratings at a glance

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

Product	Security	Functionality	Interoperability	Usability	Deployment
Avatier Identity AnyWhere	●	●	●	●	●
Beta Systems Garancy IAM Suite	●	●	●	●	●
Broadcom Symantec Identity Governance and Administration (IGA)	●	●	●	●	●
E-Trust Horacius	●	●	●	●	●
EmpowerID	●	●	●	●	●
Evidian IGA	●	●	●	●	●
Evolveum midPoint	●	●	●	●	●
Fischer International Identity Suite	●	●	●	●	●
Hitachi ID Identity Manager	●	●	●	●	●
IBM Security Identity Governance & Intelligence	●	●	●	●	●
Identity Automation RapidIdentity	●	●	●	●	●
Ilantus Compact Identity	●	●	●	●	●
Ilex Meibo People Pack (MPP)	●	●	●	●	●
Micro Focus Identity Manager Suite	●	●	●	●	●
One Identity Manager	●	●	●	●	●
Oracle Identity Governance	●	●	●	●	●
RSA SecurID Suite	●	●	●	●	●
SailPoint Predictive Identity Platform	●	●	●	●	●
SAP Access Control	●	●	●	●	●
Saviynt Security Manager	●	●	●	●	●
Simeio Identity Orchestrator	●	●	●	●	●
Soffid IAM	●	●	●	●	●
Legend	● critical ● weak ● neutral ● positive ● strongly positive				

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
Avatier	●	●	●	●
Beta Systems	●	●	●	●
Broadcom Inc.	●	●	●	●
E-Trust	●	●	●	●
EmpowerID	●	●	●	●
Evidian (was acquired by Atos)	●	●	●	●
Evolveum	●	●	●	●
Fischer International Identity	●	●	●	●
Hitachi ID Systems	●	●	●	●
IBM	●	●	●	●
Identity Automation	●	●	●	●
Ilantus Technologies	●	●	●	●
ILEX International	●	●	●	●
Micro Focus	●	●	●	●
One Identity	●	●	●	●
Oracle	●	●	●	●
RSA Security	●	●	●	●
SailPoint	●	●	●	●
SAP	●	●	●	●
Saviynt	●	●	●	●
Simeio Solutions	●	●	●	●
Soffid	●	●	●	●
Legend	● critical	● weak	● neutral	● positive
			● positive	● strongly positive

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

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

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

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

vendors with better ratings might fail and disappear from the market.

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

5 Product/service evaluation

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

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 IGA Leadership Compass, we look at the following six categories:

- **Identity Provisioning & Lifecycle**
The ability to provision identities, access entitlements, and other identity-related information in the target systems. 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.
- **Connectors Depth & Breath**
Considered is both the number of connectors and the breadth of target systems, including e.g., directory services, business applications, mainframe systems, etc., and the capabilities of connectors, especially when it comes to connecting to complex target systems such as SAP environments or mainframes. 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.
- **Self-Service & Mobile Support**
User self-service interfaces and support for secure mobile access to selected IGA capabilities.
- **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. Capabilities such as advanced capabilities

that use machine learning techniques that enable pattern recognition for process optimization, 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.
- **Authentication**
Support for strong and adaptive authentication for both administrators and end users accessing the service.

The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some vendor services may have gaps in certain areas, while are strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations of Fraud Reduction technologies.

5.1 Avatier Identity AnyWhere

Avatier, based in California (US), is one of the few IGA vendors that have demonstrated revolutionary changes to adapt to evolving market demands in the recent past. From a vendor that focused primarily on providing smart user interfaces while lacking on the underlying depth of capabilities, Avatier has evolved into a vendor offering comprehensive IGA capabilities with its Identity-as-a-Container platform creating unique market differentiation. Based on Docker architecture, Avatier's Identity Anywhere provides a fully containerized IGA platform primarily aimed at solving deployment and scalability issues of traditional IGA.

Identity Anywhere is a Docker container-based cloud service that uses a REST API agent on-premises to communicate with on-premises identity stores and on-premises applications. Hardware or virtual appliances for on-premises deployments are not available. SDKs for developers are given for SCIM, SAML, OAuth, Java, C/C++, and .NET programming languages. The majority of Identity Anywhere functionality is accessible via REST APIs.

Identity Anywhere is comprised of several modules catering to a broad spectrum of IGA functionalities, with Lifecycle Management being its primary Identity Provisioning component along with Group Automation/Self-Service, Workflow Manager, and Identity Analyzer supporting the Access Governance capabilities. Avatier supports both SPML and SCIM for identity provisioning/de-provisioning, and has a broad set of provisioning connectors available for a variety of systems, Avatier IMS offers good Identity Provisioning and fulfillment capabilities.

Avatier delivers a solution with an excellent user interface that extends to mobile devices and chat channels such as Skype Slack, Microsoft Teams, or Facebook Messenger to name a few. While Avatier has a good breadth of governance features, depth of functionalities could be a challenge to support advanced governance requirements of complex IAM deployments. A focus on simplification of user interfaces offers a great abstraction of governance features for business users who are commonly unacquainted with technical details.

Avatier customers and partner ecosystem are primarily in North America with growth in other regions. Overall, Avatier's Identity Anywhere container-based platform is positioned to disrupt the traditional IGA market and organizations across the industry verticals seeking a solution to traditional IGA deployment problems and should consider Avatier's Identity Anywhere.

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



Strengths

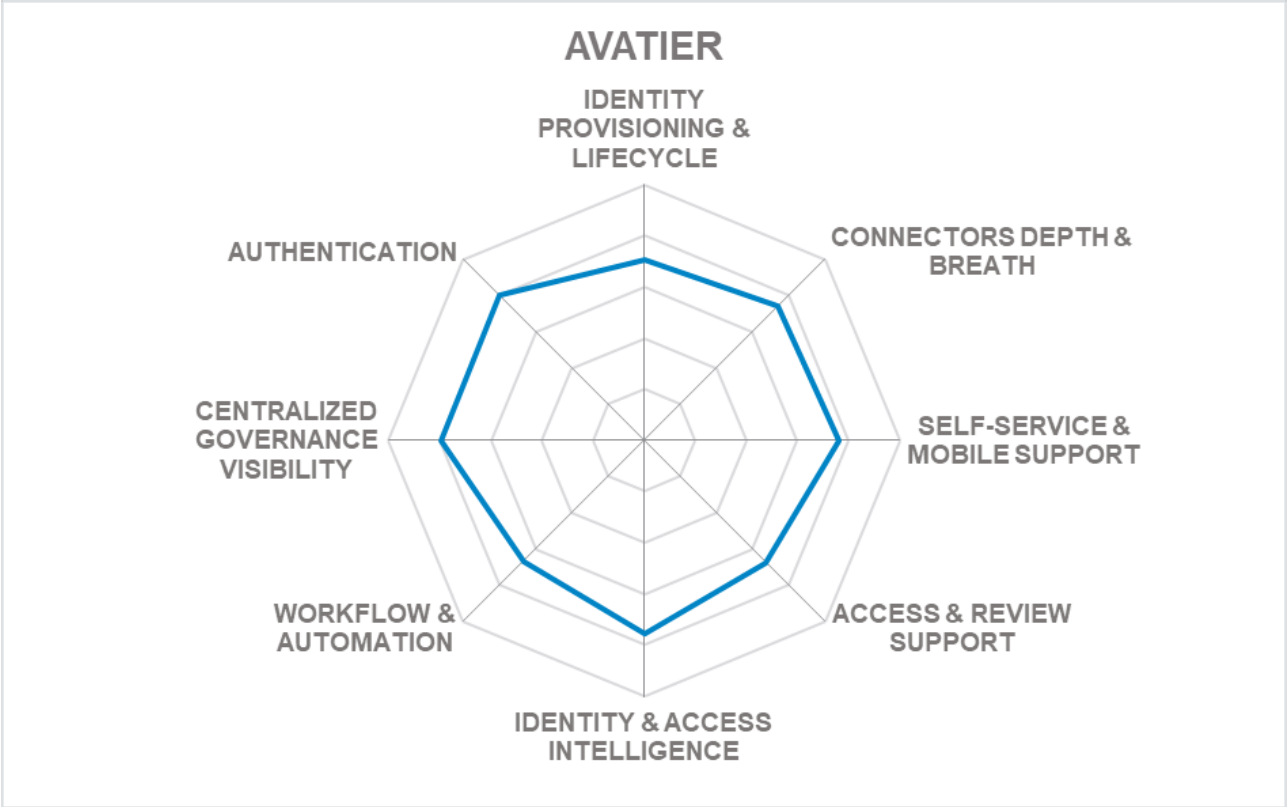
- Fully containerized IGA platform
- Innovative, user-centric approach to IGA
- Depth & breadth of OOB connectors to both on-premises and SaaS systems
- Strong authentication option support
- Flexible workflow automation capabilities
- Good reporting capabilities

Challenges

- A growing but limited partner ecosystem
- A limited footprint outside of North America
- Limited marketing visibility

Leader in





5.2 Beta Systems Garancy IAM Suite

Beta Systems, based in Germany, offers Garancy IAM Suite consisting of Identity Manager, User Center, Process Center, Recertification Center, Data Access Governance, Password Reset, and Access Intelligence Manager modules as a comprehensive IGA platform. While the Garancy Identity Manager enables identity administration and fulfillment, Recertification Center, User Center, Process Center, Access Intelligence, and Password Reset provides functionality for access governance.

Beta Systems is one of the few vendors offering connectors with full application integration, allowing applications to configure and request authorization decisions at runtime and therefore enabling dynamic authorization management as an integrated feature within the base product. Garancy Process Center enables customization of connectors for applications and non-standard target systems while offering a business-friendly approach to create and configure authorization workflows. The built-in role management capability allows for the efficient and automated assignment of entitlements. Beta Systems also provides the Garancy Data Access Governance module that manages user access entitlements and authorizations for unstructured data at a granular level. The DAG is a separate module but can be integrated with other Garancy modules to offer a complete IGA solution. Access intelligence is given, providing strong reporting and dashboarding capabilities, although basic support for SOD risk analysis and transaction monitoring.

Beta Systems supports on-premises, cloud and hybrid deployments and is capable of delivering its solution in the standards except for hardware appliances, and soon Docker with Kubernetes capabilities on the roadmap. Almost all of the functionality of the solution is accessible via SOAP or REST APIs, although SDKs are limited to the Java programming language. Support for self-service and administration authentication is limited to the most basic options with no support for more advanced MFA options.

Beta Systems' has a primary market focus in the EMEA region with a somewhat small but growing and functional partner ecosystem. Garancy IAM Suite offers a comprehensive and light-weight IGA capabilities for organizations looking to quickly deploy IGA for on-premises or cloud-based systems.



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

Strengths

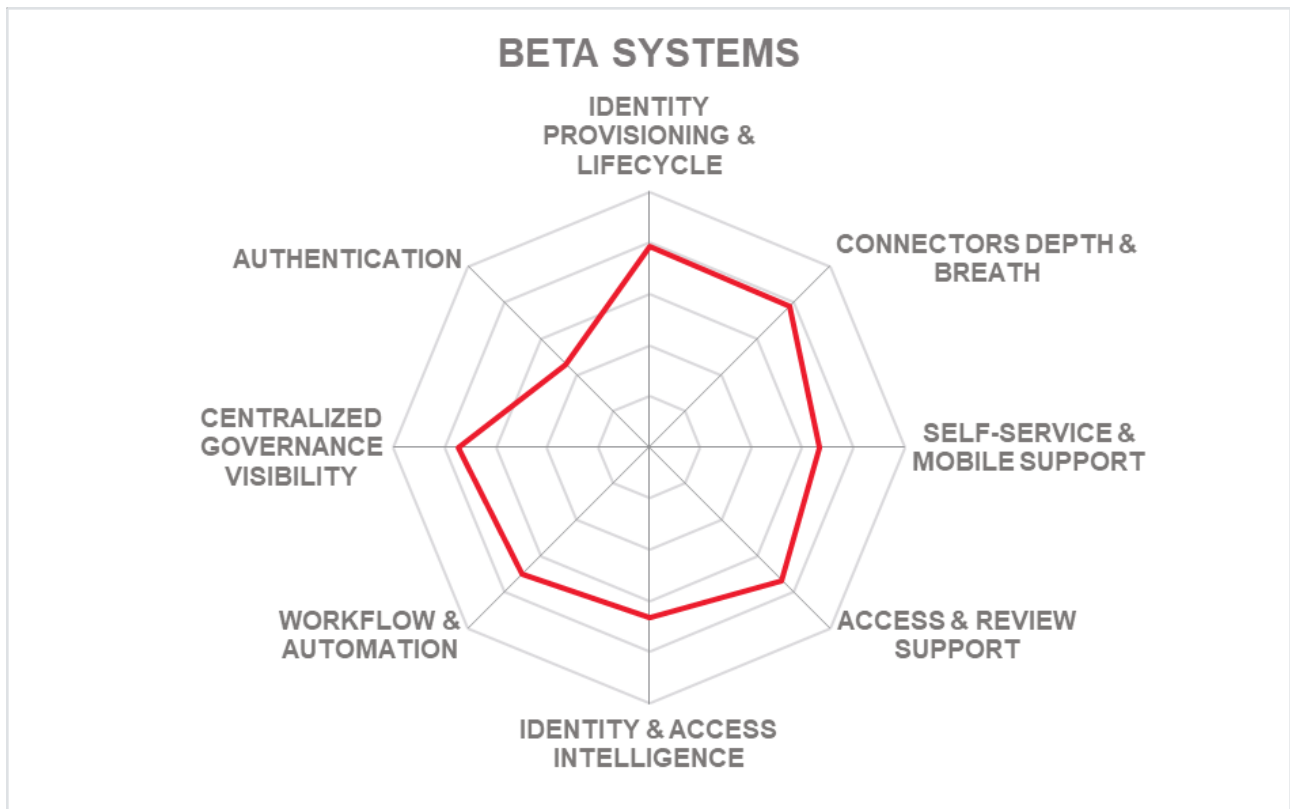
- Breadth of OOB connectors
- Ease and flexibility of workflow customization
- Support for Dynamic Authorization Management
- Supports granular Data Access Governance
- Dedicated support for mainframe environments

Challenges

- Primarily focused in the EMEA region
- Somewhat small but growing functional partner ecosystem
- Some room for improvement regarding OOB connector support for SaaS applications

Leader in





5.3 Broadcom Symantec Identity Governance and Administration (IGA)

Broadcom, an American manufacturer of semiconductor and infrastructure software products company, 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. Today, Broadcom Symantec IGA maintains a well-integrated platform providing the range of IGA features to be expected from an established market player.

With the Symantec portfolio of security products, Broadcom has several large deployments of Symantec IGA globally. The products, fully capable of operating in silos, offers a strong line-up of IGA capabilities including user access certification, SoD, entitlement clean-up, role discover, workflows and policy management, access certification and access risk analyzer & simulator that can estimate a user's risk score based on the change in context of an access request. Symantec IGA also offers an out-of-the-box connector to Privileged Access Manager for provisioning/de-provisioning PAM user accounts. Given the overall complexity of the product, deployment and configuration can be a challenge for customers looking for basic IGA.

Beyond on-premises deployments, Broadcom supports both cloud and hybrid scenarios through the use of virtual appliances, although software can still be deployed to the server as well. A managed service is also available. SaaS or container-based deployment options are not given. The majority of admin and end-user functionality is supported via SOAP and REST APIs, as well as support for SCIM 2.0. SDKs are also offered, but limited to the Java and C/C++ programming languages, although an AngularJS option is also given.

Strong support for out-of-the-box provisioning/de-provisioning is given for on-premises applications, although slightly less support for connectors to SaaS systems. Strong support is also given basic to advanced authentication options for both user self-service and administration access.

Overall, Broadcom's Symantec IGA solution is a mature and feature-rich product but may be more suitable for large complex IGA deployments. Broadcom has a global presence, but a relatively smaller number of specialized integration partners as compared to other global IAM suite vendors.



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

Strengths

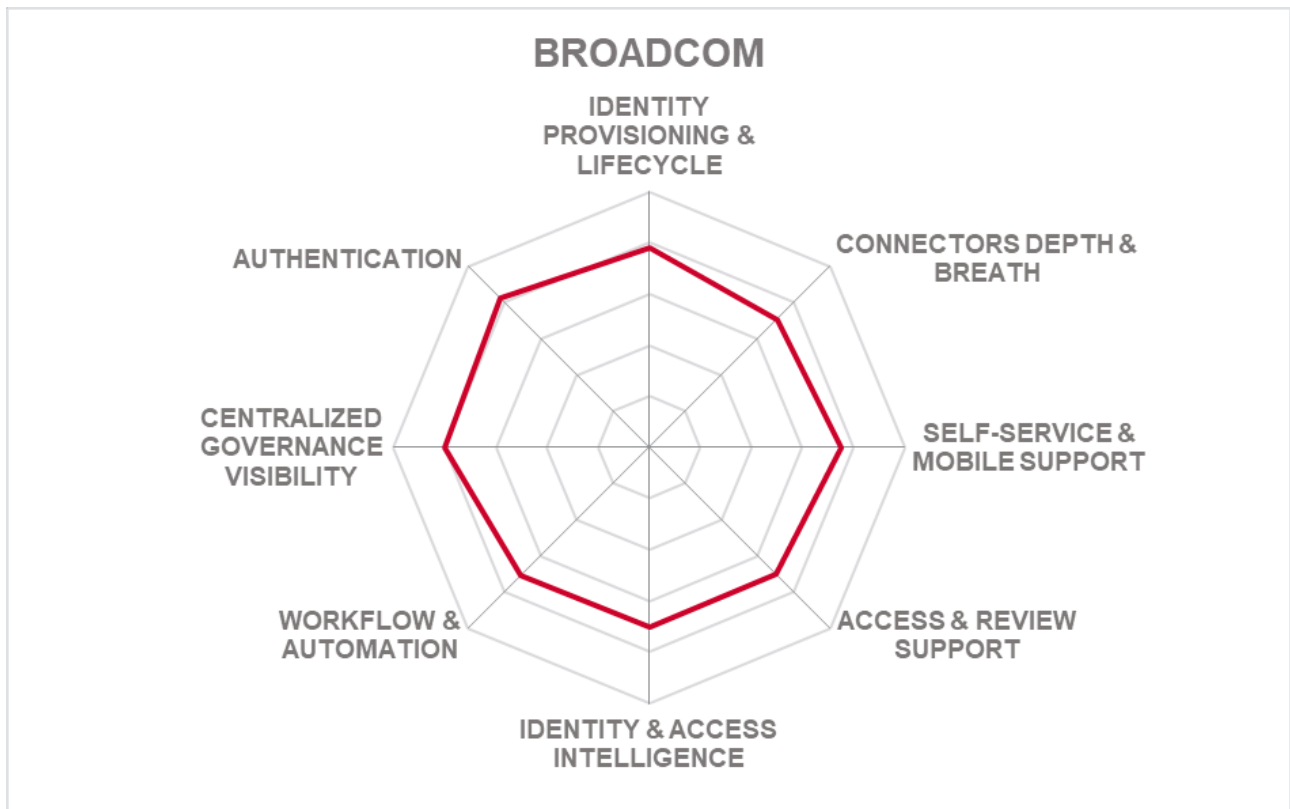
- Feature-rich solution that integrates well with all Symantec IGA components
- OOB support for a broad range of on-premises systems and cloud applications
- Modern, leading-edge UI
- Large global customer base
- Strong engineering and technical support

Challenges

- Customization is better than in past but could easily grow complex and expensive
- Relatively smaller technology partner ecosystem in comparison to other established IGA players
- Limited product delivery options

Leader in





5.4 EmpowerID

Founded in 2005 and based in Ohio (US), it provides multiple products in a suite and offers EmpowerID as its IGA product. EmpowerID supports medium to large companies primarily in North America and the EMEA regions with some growth in the APAC region. EmpowerID's partner ecosystem can be considered small, with a concentrated focus in Europe.

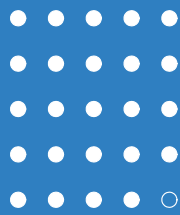
EmpowerID supports on-premises deployments as well as a subscription-based Cloud SaaS. The majority of the solution's functionality is exposed via SOAP and REST APIs. Support for these APIs and specifications such as OAuth and OpenID allow for easy extension of Access Governance features to cloud-based applications. Support for secure token service (STS) and integrated privileged access management capabilities offer unique advantages over its competitors.

For the traditional IGA model, EmpowerID is built on an identity warehouse, which is an inventory of an organization's systems. EmpowerID has both depth and breadth of out-of-the-box connectors to identity repositories, as well as on-premises and SaaS systems. For custom connectors, EmpowerID offers a SCIM 2.0 microservice connector framework that allows developers to use to build their own plugin to a given system.

EmpowerID meets most identity provisioning requirements. Access Governance capabilities are limited to common governance scenarios, including role management, access certification, auditing, and reporting. However, EmpowerID provides strong role governance features that support role design and SOD compliance. Advanced governance features such as identity analytics and access intelligence support risk-based analysis of identities, role mining, recertification recommendations, as well as various outlier detections. EmpowerID workflow customization offers great flexibility in policy and workflow management, as well as giving good out-of-the-box reporting options.

Overall, EmpowerID offers a comprehensive solution with strong IGA and access management capabilities. Built on Microsoft technology, EmpowerID offers distinct integration and performance benefits for Microsoft centric organizations. EmpowerID is a preferred choice for vendors in mid-to-large sized organizations looking for a comprehensive IGA solution with integrated access management features.

Security
Functionality
Interoperability
Usability
Deployment



empowerID

Strengths

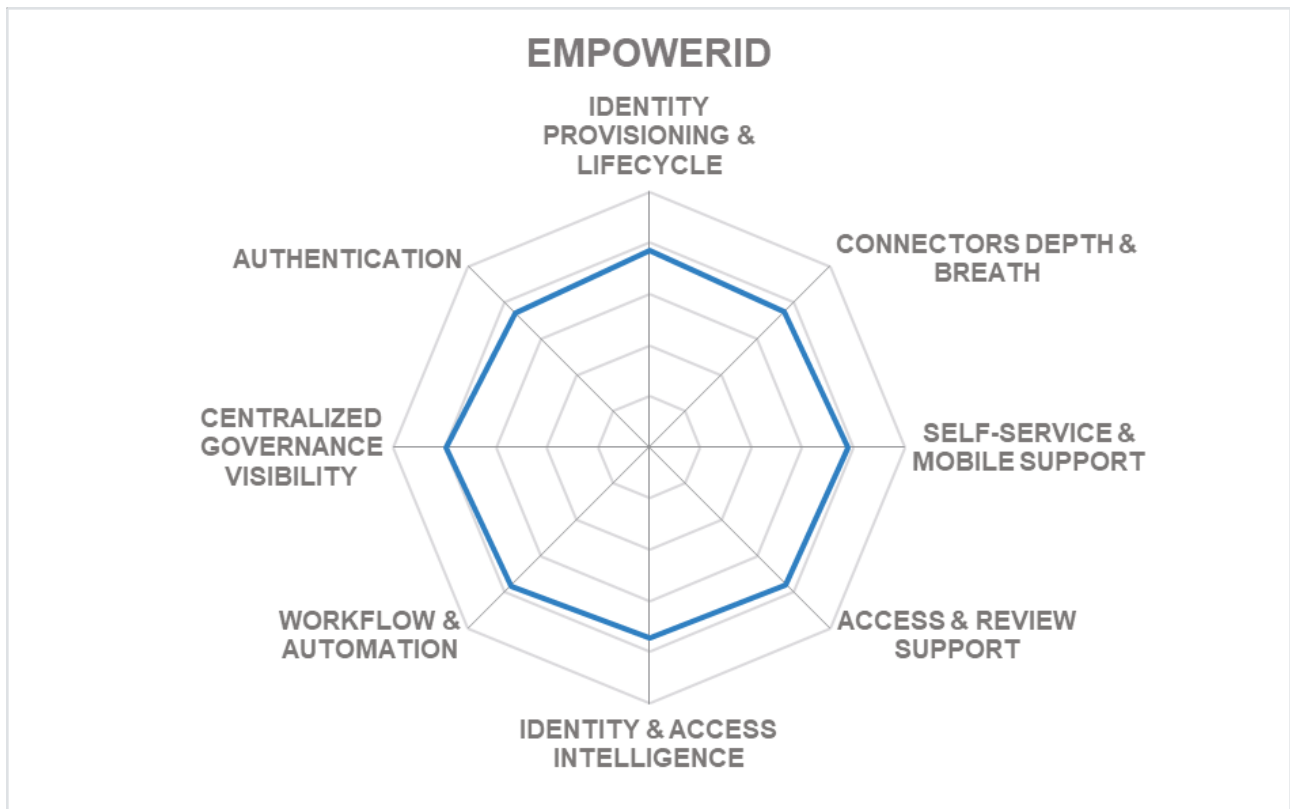
- Strong role management and access certification capabilities
- Easy and flexible policy and workflow management
- Strong Data Access Governance capabilities for windows environment
- Both depth & breadth of OOB connectors to systems
- Well thought out and modern UI

Challenges

- Runs primarily on Microsoft platform
- A small but selective partner ecosystem mostly concentrated across Europe
- Some limitation on more advanced authentication options for self-service and administration access

Leader in





5.5 E-Trust Horacius

E-Trust was founded in 1999 with headquarters in Brazil and having 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 includes access request, recertification, account mapping, role & SoD management, with more advanced features such as workflows and identity analytics.

E-Trust supports on-premises but can support cloud and hybrid deployments as well. Horacius IGA is delivered as either a virtual appliance, container-based, SaaS, or as a managed service.

E-Trust offers Horacius Identity & Governance as a common platform for identity provisioning and access governance. The Horacius platform has grown over time to be a mature product offering a spectrum of access governance functionalities. Horacius is capable of handling automated user provisioning, access reviews & attestations, orphan account monitoring, or employee and third-party contract termination use cases, to name a few. Currently, E-Trust only supports Microsoft AD & ADD, Oracle ODSEE, and Apache Directory Server identity repositories. Horacius offers good breadth with some depth with out-of-the-box connectors for on-premises systems, with less breadth regarding out-of-the-box connectors to SaaS systems. Horacius does provide REST and SOAP APIs to connect to third-party solutions for encapsulated identity requests, access functionality, as well as connecting to external AI, Analytics or fraud services for additional functionality.

Their web interface can include scorecard tiles for identities that are managed, active, as well as managed profiles or pending tasks. Graph widget can also show graphs over time for automatic access grants, revocation, or password resets as some examples. Navigation through their functional screen is laid out in a user-friendly way.

E-Trust has gained good momentum over the last few years. E-Trust customers are primarily small to mid-market, although making inroads into some enterprise-level businesses. 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 North and South American regions.

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

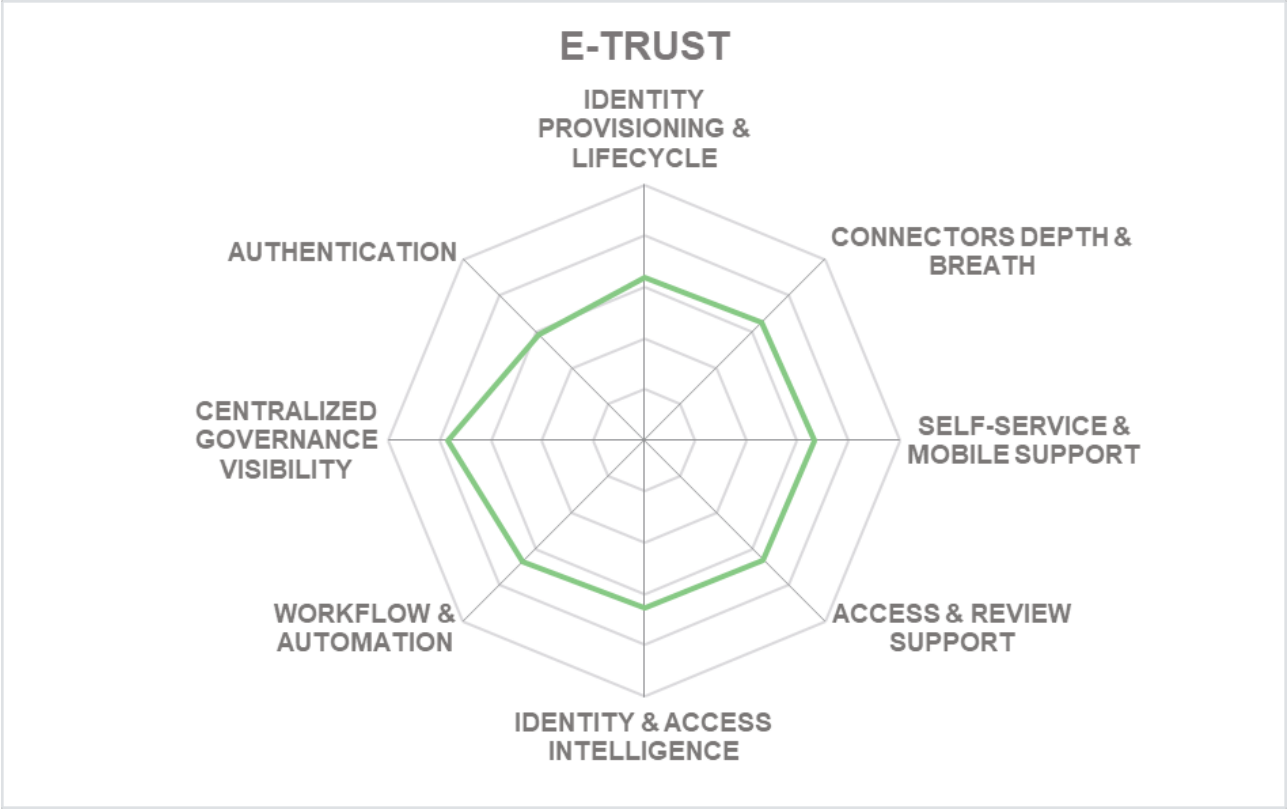


Strengths

- Connectors to on-premises systems
- Centralized governance UI
- Major compliance framework reporting
- Provides REST & SOAP APIs to functionality and services

Challenges

- Smaller partner ecosystem mostly concentrated in South America
- Limited support for some identity repositories
- Some limitations of OOB connectors to SaaS systems



5.6 Evidian IGA

Based in France, Evidian is a dedicated business branch of the ATOS group within their Cybersecurity division since 2015, which is one of the leading IT service providers in Europe. Evidian has been in the IAM business for many years 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.

Their product, Evidian Identity Governance and Administration (IGA) offers basic Access Governance in addition to mature Identity Provisioning capabilities. Currently, Evidian supports Microsoft AD LDS, Oracle Directory Server (ODSEE), and 389 DS types of identity repositories and a somewhat limited set of out-of-the-box connectors to SaaS systems. Evidian Analytics and Intelligence (A&I) was introduced in 2017 to meet the increasing requirements of advanced Access Governance. Evidian A&I 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. The solution goes beyond Identity Provisioning and Access Governance to offer an integrated approach to core IAM requirements. Evidian delivers an integrated IAM product which covers all major aspects of IGA. Besides the core provisioning capability, the product is tightly integrated with the SSO (Single Sign-On) and Access Management solutions offered by Evidian. While it supports risk-based access, continuous and event-based delta certification capabilities are currently not supported. Advanced role management, particularly role mining could be a challenge.

Evidian offers multiple products in a suite with partial functionality provided by third-party products. Both on-premises and cloud deployment models are supported, but software is only delivered as software deployed to a server, although the solution can be installed in a Virtual Machine. Evidian is also available as a managed service. Nearly all of the Evidian capabilities are exposed via SOAP or REST APIs. SDKs for Android and the Java programming language are also available.

Over the last few years, Evidian has made considerable progress in several areas including better integration across its IGA product components and reducing overall configuration complexity as well as improved look & feel of the UI and integrations into ITSM systems. In addition to basic SOD support, there is built-in support available for Dynamic Authorization Management.

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.

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



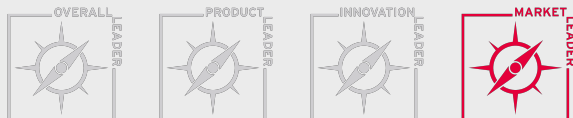
Strengths

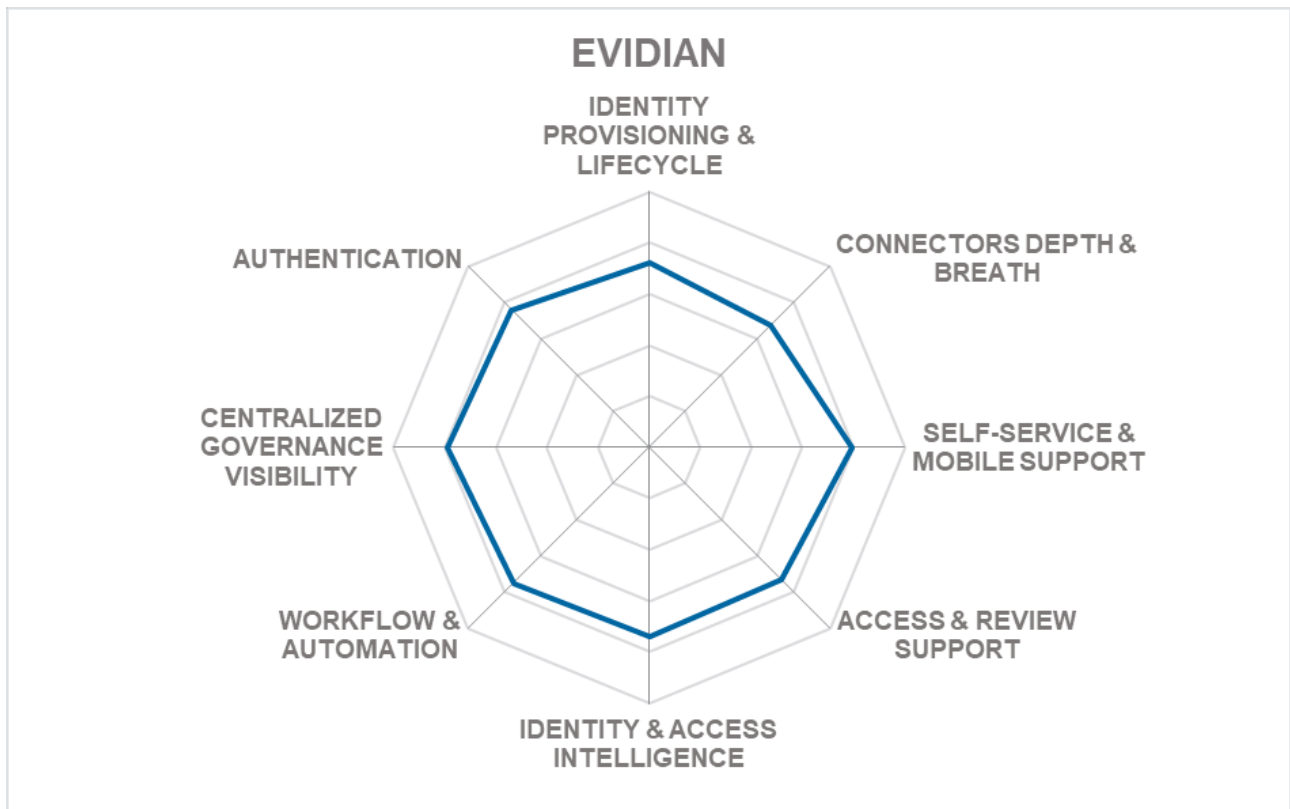
- Established and feature-rich product sets for Identity Provisioning and Access Governance
- Comprehensive suite offering includes access management capabilities
- ATOS acquisition helps to extend global network and reach to large customers
- Availability as multi-tenant cloud offering

Challenges

- Lack of advanced access certification capabilities
- Limited access intelligence capabilities without the Evidian Analytics and Intelligence offering
- Limited presence and partner ecosystem outside Europe

Leader in





5.7 Evolveum midPoint

Evolveum is an Open Source IAM vendor based in Slovakia. Their midPoint product is provided for free, but with a subscription for professional services available. The product has the same roots as the ForgeRock OpenIDM product but was forked away in development a while ago. While it has matured over the past years, midPoint still isn't leading-edge in all areas of Identity Provisioning but delivers on its promising potential.

MidPoint development is guided by customer requests and currently has a backlog of roadmap features to implement capabilities such as adding an external workflow engine, data provenance, data protection, and compliance reporting capabilities, to name a few.

Evolveum's midPoint governance features include delegated administration, deputies, role catalog. In addition to the other governance basics, midPoint also supports re-certification campaigns, basic role management lifecycle, and data protection. 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 recently 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.

When looking at the current version of the product, we observe a lack of compliance reporting out-of-the-box, although general-purpose reporting capabilities are available based on Jasper Reports. A shopping cart paradigm is available for requesting roles, users can choose from a role catalog. We would like to see more integration of the administrative interfaces and more flexibility in customization. On the other hand, we see a lot of strong capabilities and a number of interesting features on the roadmap.

Evolveum customers are primarily in the EMEA and North America regions, with small to mid-size companies and universities. Evolveum midPoint has the potential to improve its position in the market when the vendor successfully executes on its roadmap.

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

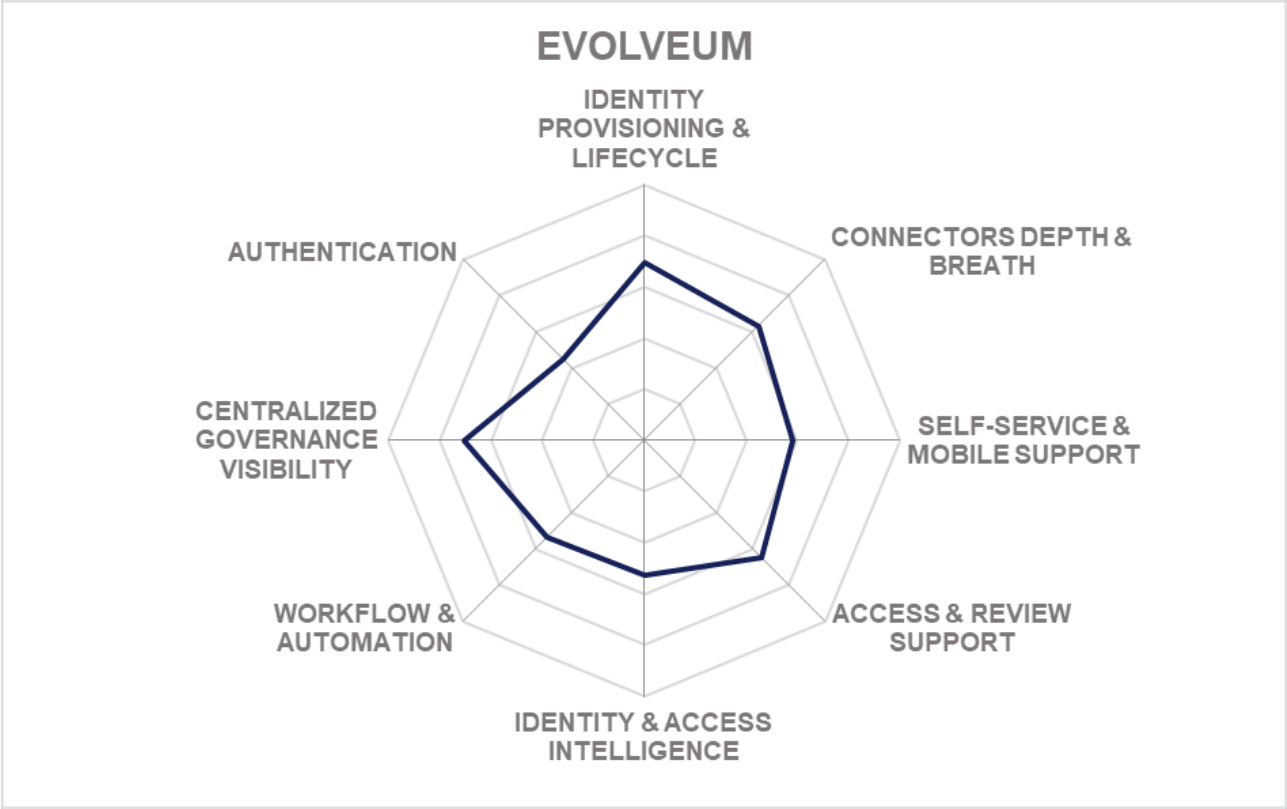


Strengths

- Open Source solution, provided at no (license) cost
- Connectors to on-premises systems
- Access review support
- Some innovative features on roadmap primarily focused on Access Governance

Challenges

- Small partner ecosystem
- Limited authentication options
- Limited connectors to SaaS systems
- Limited intelligence and analytics capabilities
- Missing compliance reporting (on roadmap)



5.8 Fischer International Identity Suite

Fischer Identity offers Fischer Identity Suite comprising of several modules available as a bundled offering to deliver a broad range of IGA capabilities. Besides standard provisioning and user administration capabilities, the Governance and Compliance module combined with Role and Account Management component provides effective Access Governance. The current architecture requiring only a gateway at the customer's site is optimal for supporting both on-premises and SaaS deployments. This approach gives Fischer's customers an easy head-start for cloud-based IGA deployment, having, for example, full multi-tenancy support as a logical design principle.

Although Fischer Identity supports on-premises deployments, it has a SaaS-ready design approach, with a focus on providing a broad set of features with standard configurations to avoid programming. Some functionality is available via SOAP or REST APIs, with SDKs for both Android and iOS for mobile development. Support for SCIM is not given.

Fischer Identity provides a breadth of out-of-the-box connectors to on-premises systems, but less support for out-of-the-box connectors to SaaS applications. Role management is adequate for Identity Provisioning but doesn't meet the Access Governance criteria of role mining and governance. Role mining is not supported and triggers to recertify a user due to SoD violations, and related compensatory controls are also not available. Good authentication options are given for self-service access, although more advanced authentication options are missing for administration access. Fischer supports RBAC as well as ABAC-based authorization allowing identity attributes to be used within access policies. Access intelligence capabilities are limited with basic and inflexible reporting used for analytics purposes.

Fischer customers range from mid-market to enterprise organizations primarily in North America and limited presence in the APAC region. Their partner ecosystem is still somewhat limited in size but growing and based on a few global, engaged partners. Overall, Fischer offers a comprehensive IGA suite suitable for customers across most industry verticals, particularly education.

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

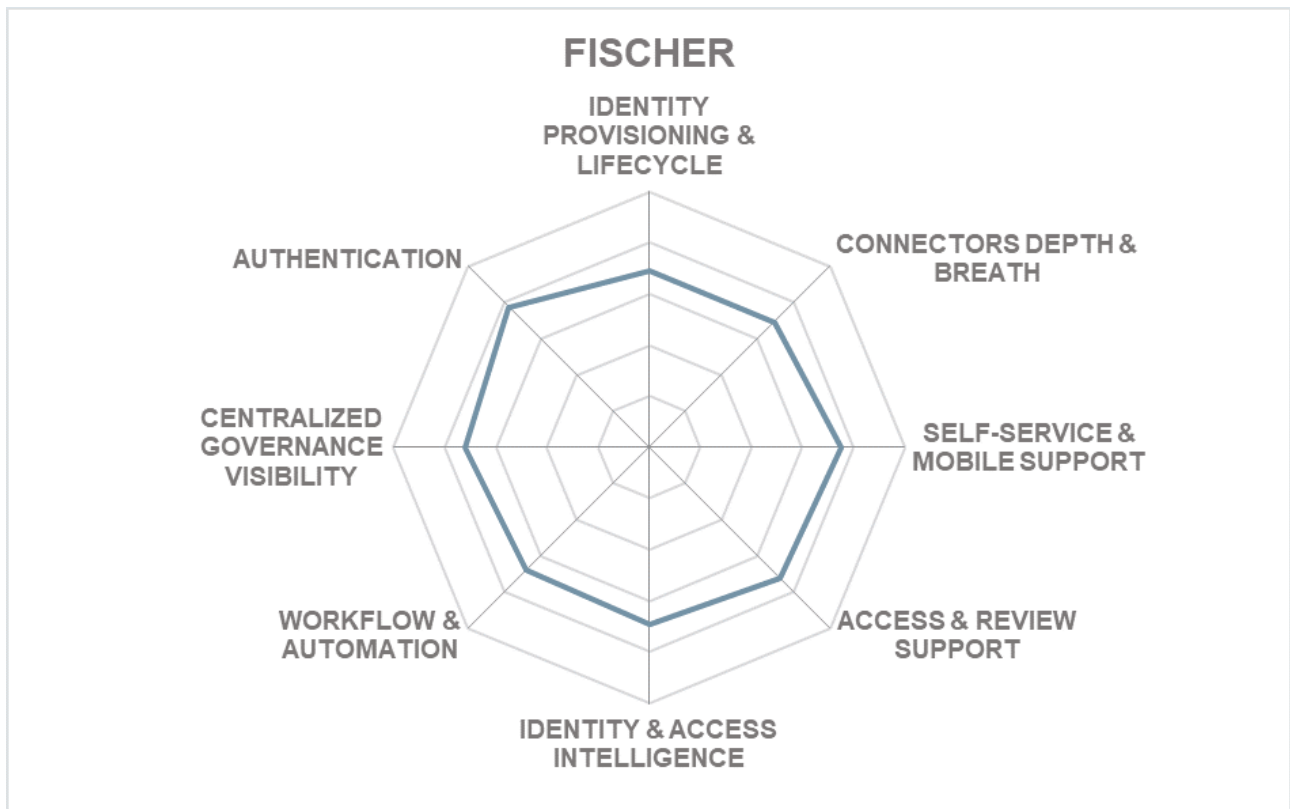


Strengths

- Offers comprehensive IGA capabilities
- Depth & breath of OOB on-premises connectors
- Easy to deploy and configure for common IGA scenarios
- Well-defined user interfaces for quick-start deployments
- Cost effective delivering fair value for money
- Strong multi-tenancy support, suitable for managed IGA service providers

Challenges

- Role management is basic with no support for role discovery and mining
- Limited access analytics and intelligence with somewhat rigid reporting
- Customer base is primarily in the North America region with a small but growing partner ecosystem



5.9 Hitachi ID Identity Manager

Hitachi ID provides a product named Identity Manager, which integrates Identity provisioning and Access Governance, including strong support for SOD (Segregation of Duties), access certification, and peer group mechanisms offering recommendations to requesters and highlighting unusual entitlements to reviewers. The product builds upon an open, flexible architecture that is also the foundation of other Hitachi ID IAM/PAM products. Hitachi ID provides a well-defined model for the segregation of code and customizations, allowing the retention of customizations when applying release changes.

The Hitachi ID Identity and Access Management Suite is designed as Identity and access management (IAM) middleware. Identity Manager includes, at no additional charge, the Hitachi ID Access Certifier, Hitachi ID Group Manager and Hitachi ID Org Manager (Delegated construction and maintenance of Orgchart data). Hitachi ID supports all major deployment and delivery models, although it has some required infrastructure and operational requirement dependencies on Windows Server. SOAP and APIs are available to access every part of the system, although access to product features via REST APIs is somewhat more limited. SDKs are available for all major programming languages. Support for SPML or SCIM for identity provisioning/de-provisioning is not given.

In general, the product provides a mature set of IGA features, delivering what customers typically need. It offers a wide range of provisioning connectors. Access Governance is moderately strong with flexible workflow and policy management capabilities, which can support complex governance use-cases. Analytic features include outlier detection, recommendation level indicators, as well as role mining. Access modeling and anomaly detection are not given. However, some intelligence capabilities can detect data quality issues, and corrections can trigger a recalculation of user entitlements and automatically generate access change requests. Strong support for reporting, as well as major compliance framework reporting, is available out-of-the-box. Another strength of Hitachi Identity Manager includes integrations with Microsoft SharePoint and Windows Explorer, allowing users to request access to resources from these environments directly. The product also supports group lifecycle management in which users can create new and manage existing groups through the system.

Hitachi ID's customers and partner ecosystem are primarily in North America, with a substantial footprint in the EMEA region as well as some presence in other parts of the world. Overall, Hitachi ID Management Suite is a balanced product with a scalable architecture and broad feature set, providing good flexibility. It thus is an interesting alternative to established products that should be evaluated when looking for robust IGA capabilities with leaner operations.

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



Strengths

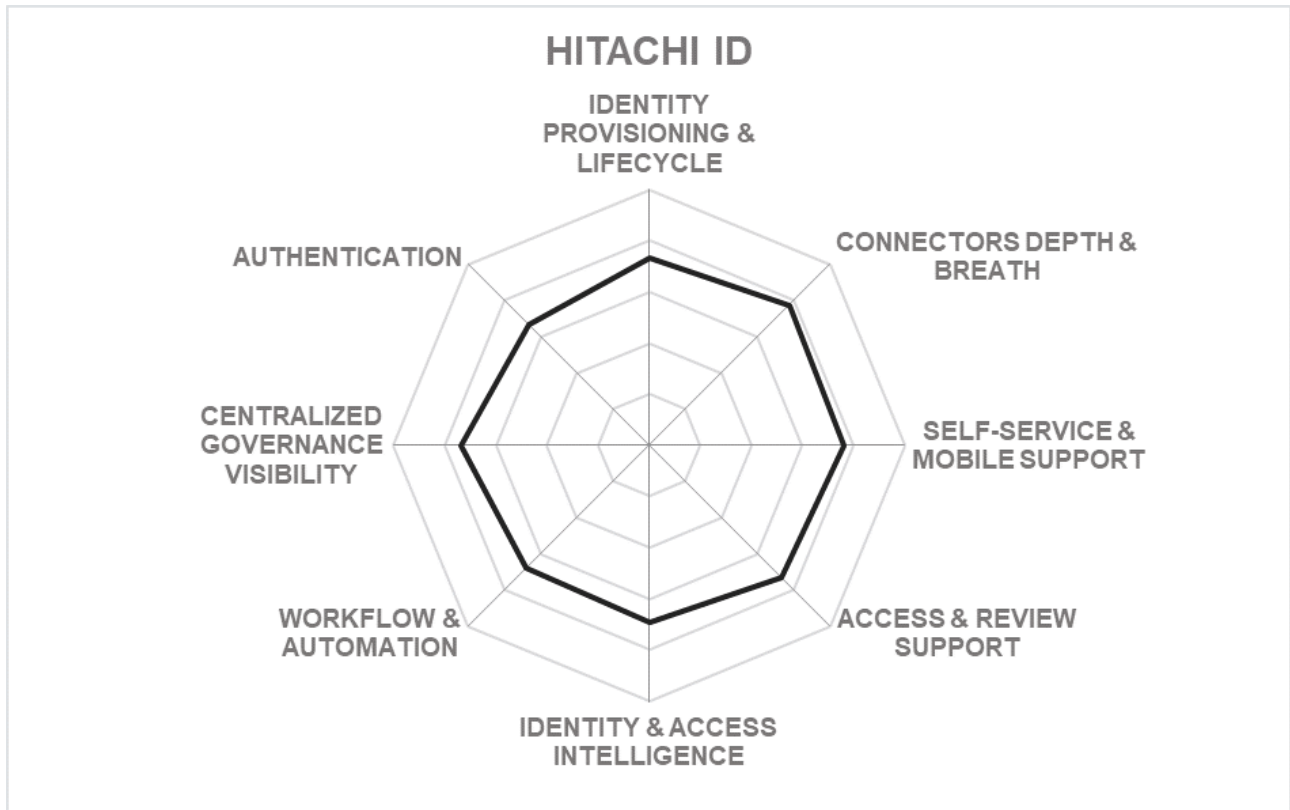
- Good analytics feedback mechanism
- Flexible workflow and policy management
- Excellent support for user groups management including SOD policies
- Reporting options and compliance framework support
- Deployment and delivery options
- SDKs for all major programming languages

Challenges

- Robust end-user interface that could be more user friendly
- Required dependencies on Microsoft platforms
- Limited footprint and partner ecosystem outside of North America

Leader in





5.10 IBM Security Identity Governance & Intelligence

IBM Security Identity Governance & Intelligence is the successor of IBM Security/Tivoli Identity Manager (ISIM/ITIM) and one of the more mature products in the market. IBM has integrated Identity Provisioning capabilities of ISIM with Access Governance capabilities of IDEAS platform acquired from CrossIdeas some years back into ISIGI and added additional features to enhance these. With several product iterations from Tivoli Identity Manager to ISIGI, IBM remains one of the largest and preferred IGA vendors for large-sized complex IGA deployments.

Almost all deployment models and most delivery options are available for ISIGI. More than half of ISIGI's functionality is available via REST APIs, although SOAP is not supported. SDKs for most popular programming languages are given except for C/C++ and .NET. SCIM support is given for identity provisioning/de-provisioning. Java and JavaScript languages are available to support attribute mapping expressions.

IBM Security Identity Governance & Intelligence builds on an established product supporting a broad range of different target systems with deep integration. IBM has dramatically improved the usability and user interface recently, providing a good and well-integrated product now. ISIGI also provides full Access Governance capabilities. Flexible workflows are given for role management, access request, identity data synchronization as well as account, entitlement provisioning/de-provisioning as well as access request workflow is supported. Limited supports are given for more advanced analytical functions/business intelligence features such as access intelligence, although good out-of-the-box access risk management and access risk analytics support is available.

Both depth and breadth for out-of-the-box provisioning connectors are given for on-premises systems, although slightly less support for some SaaS applications. Most major identity repositories are supported. Good support for self-service access authentication options are given, but more advanced authentication options are not available for administration access. Good out-of-the-box reporting capabilities are available, although reports for major compliance frameworks are not. Also, IBM provides out of box integration with other products in its broader security portfolio. This makes ISIGI a good fit for customers looking for a comprehensive package of overall Access Governance and security.

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

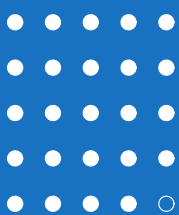
Security

Functionality

Interoperability

Usability

Deployment



Strengths

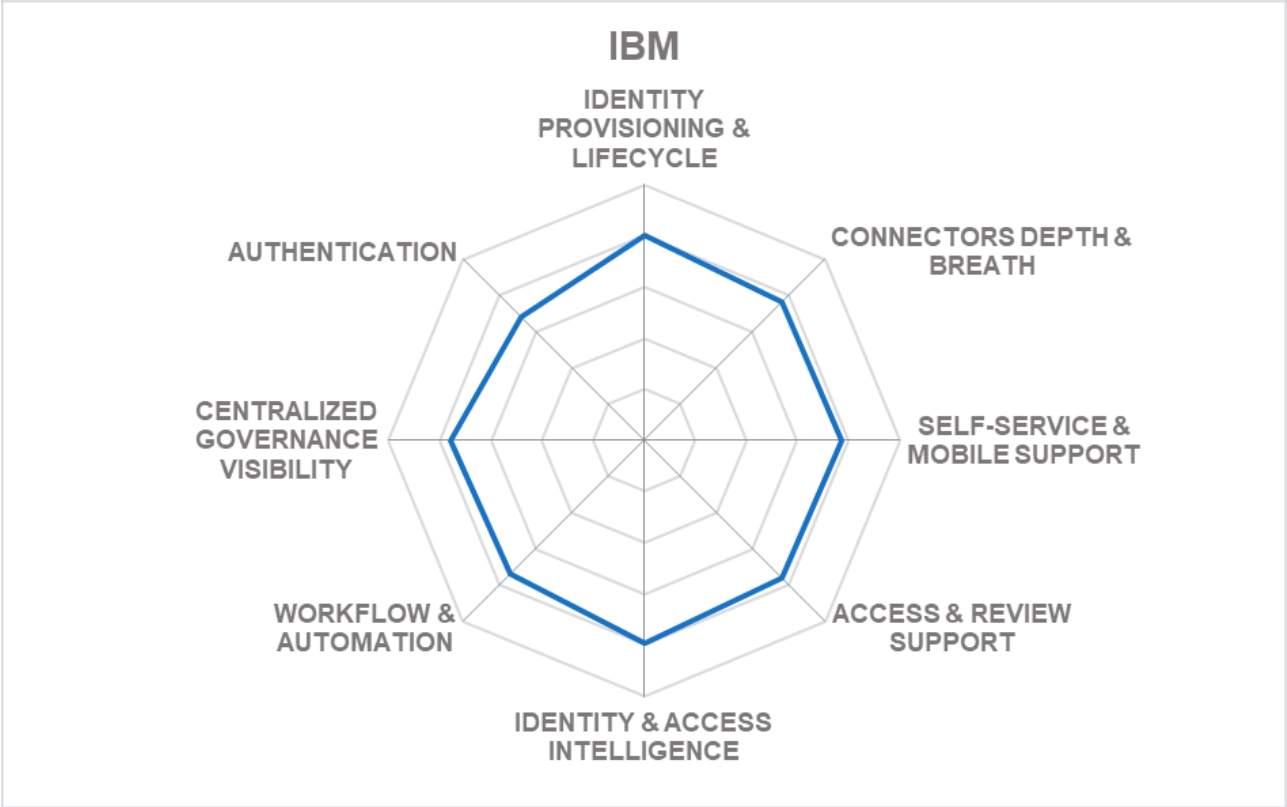
- Mature product with support for strong IGA capabilities
- Wide range of OOB connectors
- Strong support for SOD Controls
- Flexible workflow capabilities
- Good OOB reporting options
- Easy integration with IBM Security portfolio

Challenges

- Product configuration and customization can be complex, although some assets and features are available to help simplify the process
- The user interface has been redesigned in recent releases but still has limited flexibility to customize
- Lack of focus on mid-market segment

Leader in





5.11 Identity Automation RapidIdentity

Founded in 2004, Identity Automation introduced its RapidIdentity IAM solution later in 2010. In 2018, Identity Automation acquired HealthCast, a vendor specializing in IAM solutions for the healthcare industry. By combining the two portfolios, Identity Automation now delivers a comprehensive IAM solution for healthcare organizations that spans all core IAM capabilities, including automated Identity Lifecycle Management, Access Governance, Multi-Factor Authentication, and Single Sign-On. Integrated Privileged Access Management (PAM) capabilities that restrict and control access of privileged users is also available.

RapidIdentity started as an on-premises solution but has grown to handle other deployment models with their recent IDaaS released in 2020. The RapidIdentity solution can be delivered as a virtual appliance, SaaS, or even as a managed service.

Identity Automation offers full Identity Lifecycle Management capabilities with a focus on automation. Supported identity source is primarily Microsoft AD, Microsoft AAD, OpenLDAP, or eDirectory, although the supported types of identity types cover both human and non-human use cases. The breadth of on-premises provisioning connectors covers most major enterprise identity applications out-of-the-box. Supported out-of-the-box are provisioning connectors for SaaS systems that include most of the better-known applications.

Identity Automation provides access review and certification campaign features with good delegation options. RapidIdentity provides user self-service capabilities, and most authentication options are available. To help with automation, RapidIdentity provides a useful workflow designer/builder UI. Regarding access intelligence, Identity Automation takes a bring-your-own analytics approach. Identity Automation makes available all data within their solution to be used with third-party analytics products and services.

Identity Automation started as a system integrator turned identity software provider. Based on the experience and expertise from the integration business, Identity Automation's software product, RapidIdentity, aims to offer expanded IAM capabilities to mid-market companies. Although its customer base is skewed towards the healthcare and higher education industries vertical with a small partner ecosystem primarily limited to North America, Identity Automation is now actively expanding in other geographic regions as well.

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

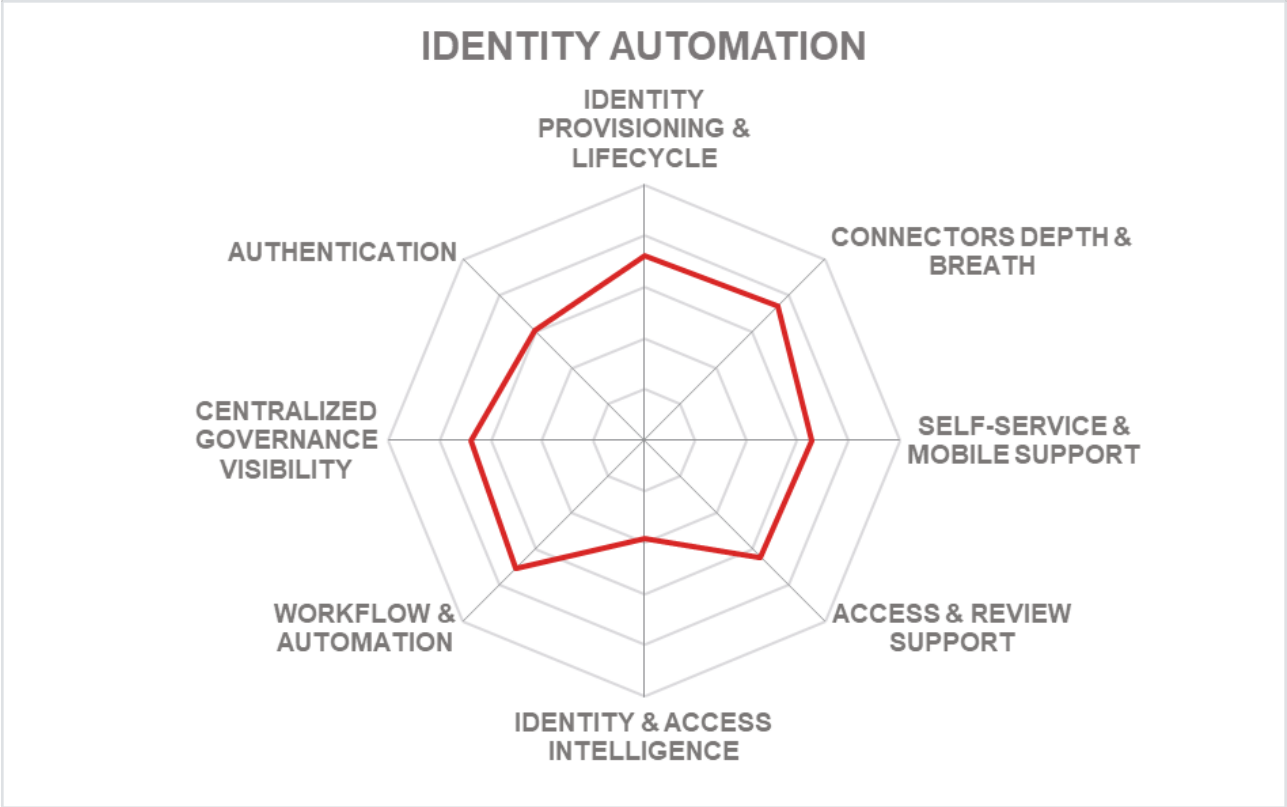


Strengths

- Identity Lifecycle Management
- Breath of connectors
- Certification campaign support
- Delegation support
- Strong workflow features
- Focus on automation

Challenges

- Relatively small partner ecosystem, specifically outside of North America
- Limited identity repositories supported
- Strong reliance on third parties for analytic capabilities



5.12 Ilantus Compact Identity

Ilantus, which started as a system integrator, has moved to provide offerings targeted at different types of customers. Their solution Compact Identity focuses on delivering IGA and AM capabilities from a single codebase that can meet more complex requirements on IGA and Access Management requirements in the market.

In 2014, Ilantus merged all of its product offerings into one single IDaaS platform. For cloud deployments, Ilantus provides an on-premise agent with connections to their cloud platform. Alternatively, they can deploy their cloud solution to customers on-premises data-centers and private clouds.

Ilantus's on-premises Compact Identity product features cover identity administration, access management through authentication, SSO, authorization, password management, and access governance, but also offers PAM, Basic CIAM, and Identity Risk Analytics capabilities as well.

The workflow capabilities are flexible and support a basic registration workflow as well as access request and approval workflows, with many additional workflows on the roadmap, although Compact Identity falls short in the case of access exception approvals as well as rights and registration delegation. For Access Governance, Ilantus delivers standard Access Review support, including multi-level campaigns, but also additional Access Intelligence capabilities. It also offers Robotic process automation (RPA) capabilities integrated with SSO and user lifecycle management connectors.

Ilantus continues to add innovative features now and on their roadmap, such as identity analytics that supports anomaly and other types of detections, as well as robotic process automation (RPA) capabilities integrated for SSO and user lifecycle management activities.

Ilantus is currently serving mid-market companies in North America and the APC regions, as well as their partner ecosystem. Ilantus continues to move in a positive direction with the completion of future capabilities on its roadmap.

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

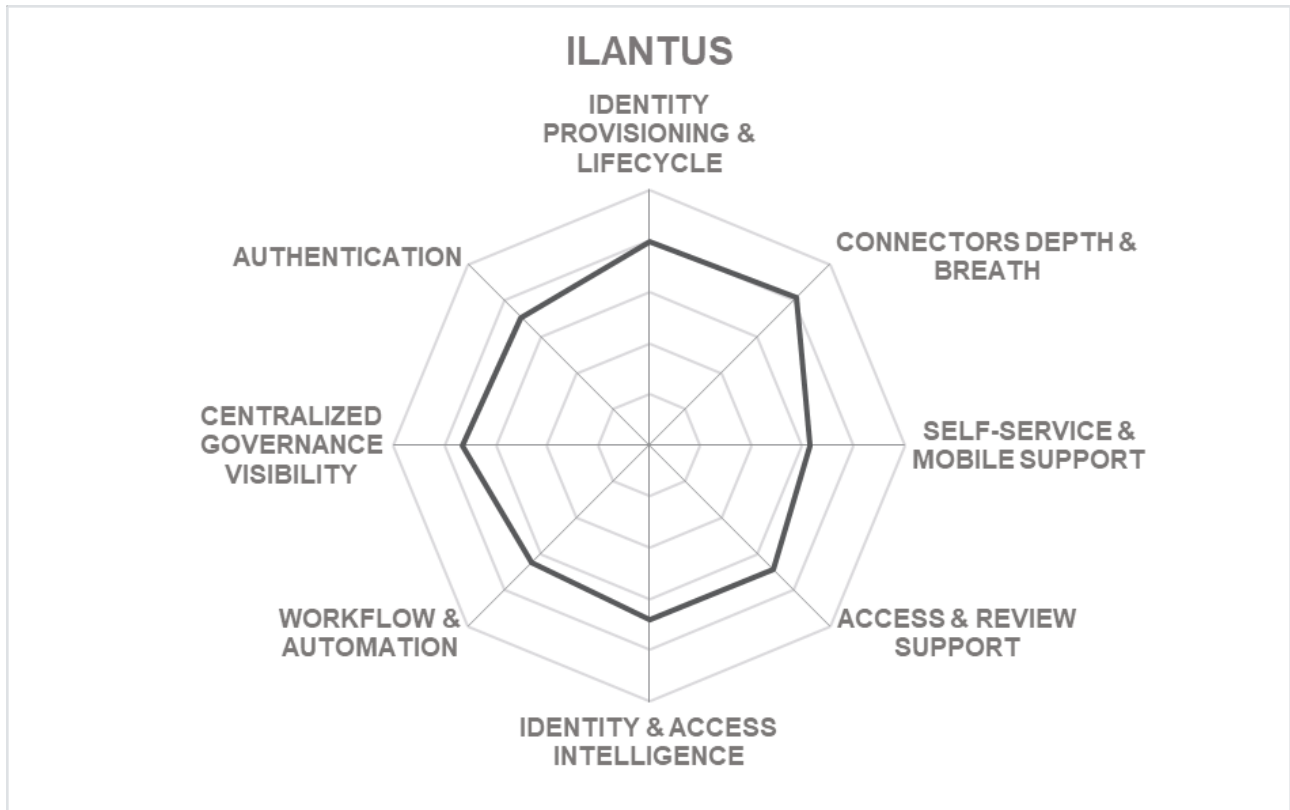


Strengths

- Identity Provisioning & Lifecycle
- Depth and breadth of connectors
- Identity and access intelligence
- Flexibility for customization including policy and workflow customizations
- Innovative list of capabilities on roadmap

Challenges

- A somewhat small but quickly growing partner ecosystem
- Customer presence is still primarily focused on the US and few Asian countries, still low in EMEA
- Missing out-of-the-box reporting for major compliance frameworks



5.13 Ilex Meibo People Pack (MPP)

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. The products considered for evaluation in this Leadership Compass are Meibo People Pack (MPP) and Sign&go Global SSO.

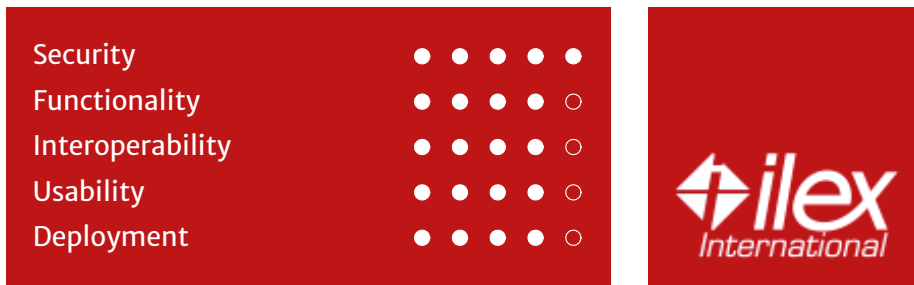
Ilex's MMP and Sign&go are separate products that integrate with each other. Ilex is limited to delivering their solution as software to deploy to a server or as a managed service. A large portion of the solution's functionality is available via SOAP or REST APIs, although not all administration features APIs are available. SDKs are given for both Android and iOS for mobile development as well as an SDK for the Java programming language.

Ilex MMP provides provisioning identity lifecycle, entitlement management, user rights review capabilities, while Sign&go Global SSO provides the single sign on including mobile SSO to more easily access provisioned applications, as well as access control, self-service, MFA and adaptive authentication features. Missing are identity and access analytics and intelligence capabilities.

Ilex provides a good set of out-of-the-box connectors provisioning on-premises systems, but less support for out-of-the-box connectors to SaaS systems although support is given for standards such as SCIM. Good support for authentication options to both self-service and administration access is also given. Dashboard capabilities are limited to some operational indicators and rather Ilex customer integrators to design the dashboard according to their specific requirements.

Ilex customer base and partner ecosystem is primarily within the EMEA region with some growth in the APAC region. Overall, ILEX Meibo Identity Management can be both – a tool to build a custom IGA solution and an add-on to existing IGA deployments to enhance the overall flexibility. Both Meibo People Pack (MPP) and Sign&go Global SSO together offers a more complete IGA solution, although some partner engineering/integration support may be needed to fulfill all customer dashboard requirements.

Still, Ilex offers an alternative solution set for SMB organization to consider in their primary geographic region.

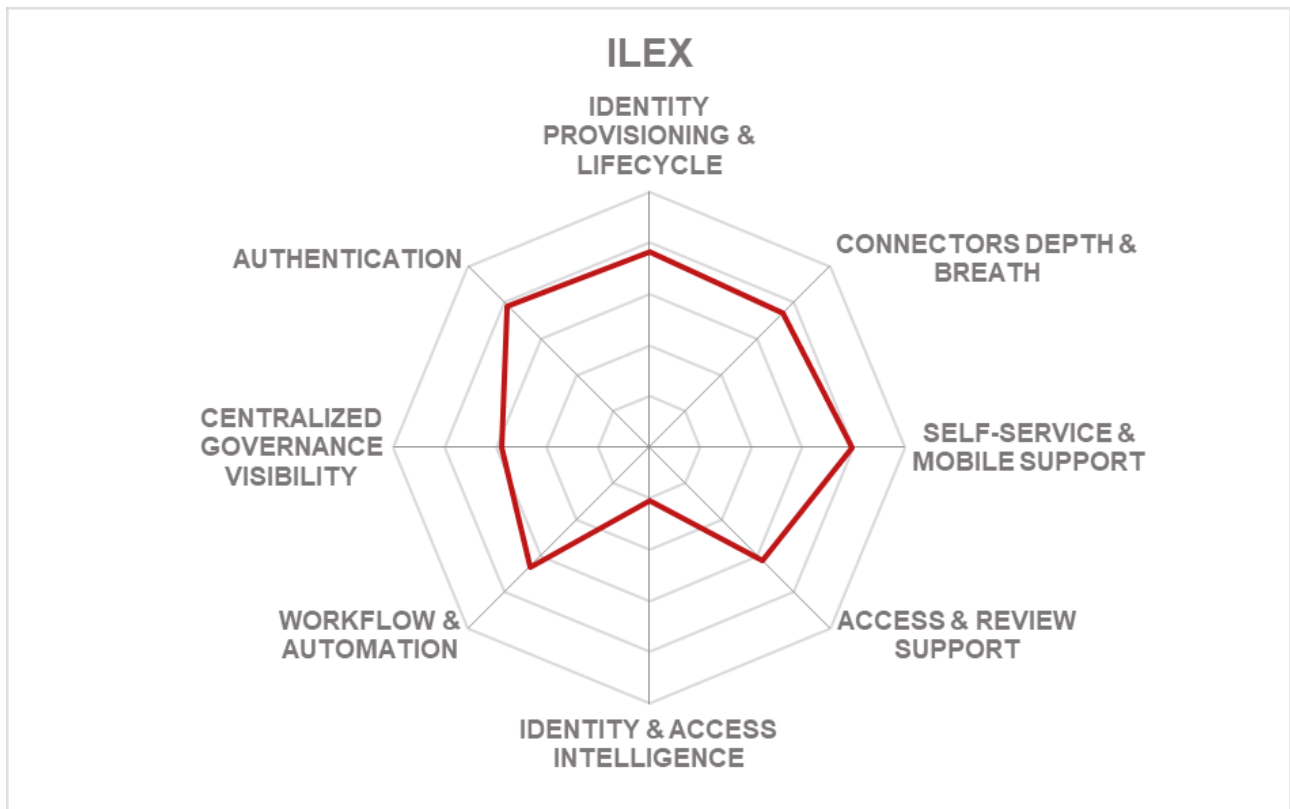


Strengths

- Support for both RBAC and ABAC models
- Easy integration with its own Sign&Go SSO/Access Management solution
- MFA and adaptive authentication options
- Supports required industry standards for an integrated IGA approach

Challenges

- Lack of SOD controls and granular authorization management capabilities
- Lack of identity and access intelligence
- Lack of full dashboard capabilities
- Customer and partner base are primarily limited to the EMEA region (France and Benelux)



5.14 Micro Focus Identity Manager Suite

UK based Micro Focus offers 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 executed a significant shift in its product strategy to build some market-leading Access Governance features during the time of its merger with Hewlett Packard Enterprise (HPE). The effects of this merger are believed to offer a comprehensive security portfolio with a sharper focus on integrated IAM technologies and boost its market presence with strong professional services around the globe. Micro Focus Identity Manager, Governance, Intelligence, and Tracking products offer a good range of IGA capabilities from flexible workflow and policy management to enhanced analytics-driven user activity reporting.

Micro Focus supports an on-premises containerized deployments as well as a or a more traditional deployment into a VM or onto a customer's server, although all other cloud and hybrid deployment models are also supported. Currently, Micro Focus IGA-as-a-Service architecture, is containerized and offers an on-premises bridge soon to stream on-premises data sources to the IGA service and provided fulfillment back to the on-premises systems.

Micro Focus Identity Manager is a robust product for Identity Provisioning with mature and comprehensive capabilities for identity lifecycle management and fulfillment. Micro Focus Identity Governance is an enhanced governance product offering mature and in-depth capabilities with some functionality overlap to Identity Manager. 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. Integrated role mining, adaptive access certification, and risk-based analytics are some of its distinct and improved governance features.

Identity Intelligence provides analytics and reporting capabilities for IGA data. Virtica is a behavioral analytics platform that was acquired through the HPE acquisition, in which IGA capabilities of Virtica are packaged into their Identity Intelligence offering. More recently, Micro Focus acquired Intersect for their machine learning and AI capabilities, although currently not integrated with their IGA solution. For data mining and analytics, Micro Focus gives identity correlation and user profiling, anomaly detection, risk scoring, and role mining as some examples. Identity Tracking gives the capability to monitor user activity in real-time. The products combined offer a comprehensive IGA platform that offers good flexibility and scalability.

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. Also, Micro Focus is building on an excellent partner ecosystem on global scale.



Strengths

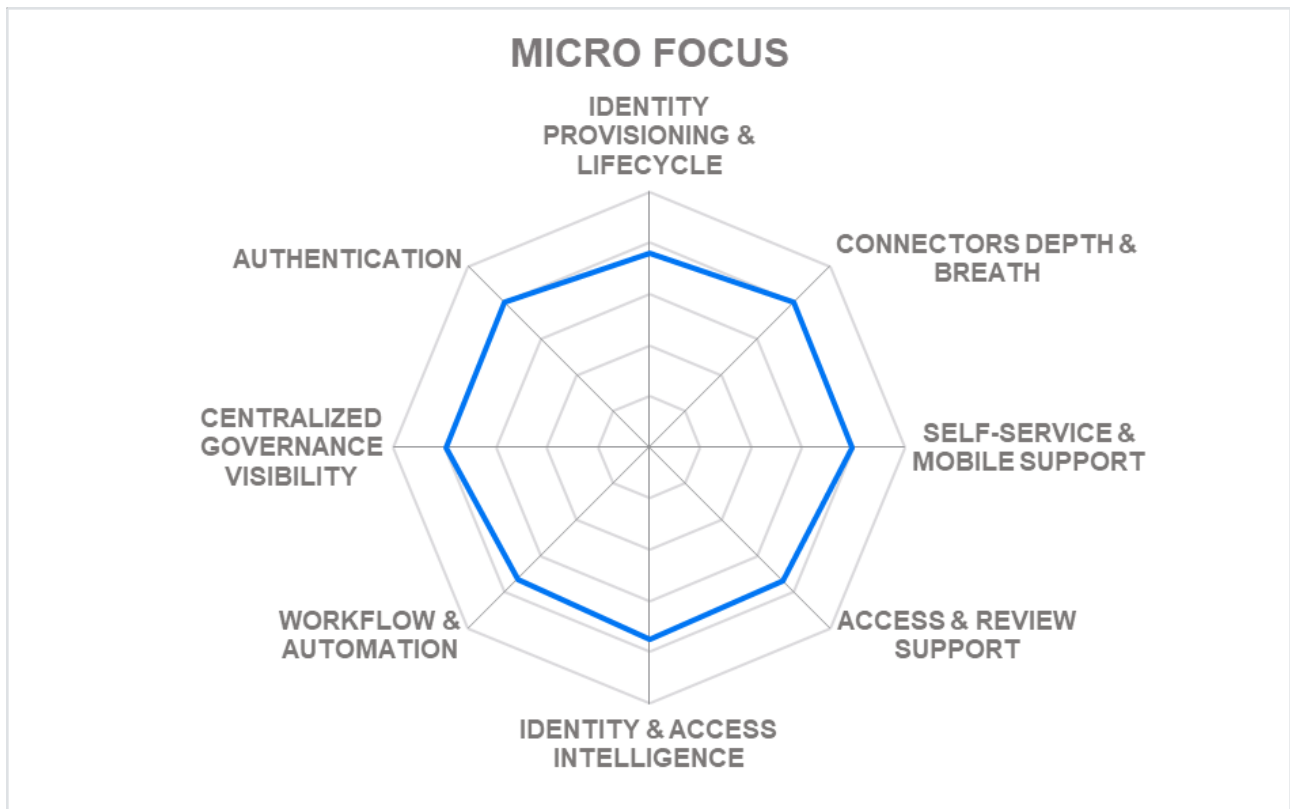
- Strong, mature functionality covering all major aspects of Identity Provisioning and Access Governance
- Aggressively moving to a more modernized and flexible architecture
- Strong support for a variety of target systems
- Strong support for IGA analytics and access intelligence capabilities
- Very large customer base and strong partner ecosystem

Challenges

- Rich functionality sometimes complex to understand and implement
- The merger with HPE created some uncertainties with certain security product functionality overlap, although the acquisition of Vertica through HPE showed some benefit
- Weaker marketing messaging and execution compared to competitors

Leader in





5.15 One Identity Manager

One Identity, based in California, is a Quest Software business. It owns the IAM portfolio that came from Dell Software. One Identity Manager, which historically went into the Quest portfolio through the acquisition of a German vendor Völcker Informatik, remains the core product of One Identity's IGA portfolio. One Identity Manager builds on a sophisticated, consistent concept that allows for intuitive user experience, rapid customization, and easy deployment. Besides offering a rich role framework to support complex role management requirements, One Identity also supports dynamic rule-based provisioning to applications with complex role structures. With one of the broadest ranges of provisioning connectors in the market and advanced role management capabilities, One Identity Manager offers Data Access Governance capabilities for managing access to unstructured data. The standard user interfaces of the product are innovative and have been significantly improved in the latest product release. Recent enhancements also include product re-architecture to make it more modular and scalable.

One Identity Manager can be deployed on-premise, cloud, or hybrid configurations. The solution is delivered is containerized, although traditional software deployed to a server is also supported as well as a managed service. Support was recently added for MS Azure SQL Managed Instances. Nearly all or solutions functionality is exposed via SOAP or REST APIs. SDKs are given for both C/C++ and C# .NET programming languages. Both SCIM and SPML support is given for identity provisioning/de-provisioning.

With a shopping cart-based approach for access requests, features such as the ability to simulate the effect of changes to access entitlements or role definitions remain unique. Both breadth and depth of out-of-the-box connectors are available for both on-premises and SaaS applications. Customizations are straightforward, mainly done through policy configurations and workflow extensions. The flexibility regarding customization and product architecture have been greatly improved over the past few year.

Basic to advance authentication options are given for self-service access. Authentication options for administration access are missing some more advanced options such as biometrics, although other 3rd party authentication options supporting OAUTH2/OpenID Connect can be integrated such as Ping, Okta, AAD, and ForgeRock out-of-the-box. Good report capabilities are available, reports for major compliance frameworks out-of-the-box are not. One Identity Manager provides analytics and intelligence base on risk from inheritance and risk from roles. This information is available on dashboard views in reports and indicators in access reviews, for example.

Overall, One Identity has made significant enhancements to the functional capabilities of the product to establish itself amongst the leaders in the market. It gets a definite recommendation from us for evaluation in product selections.



Strengths

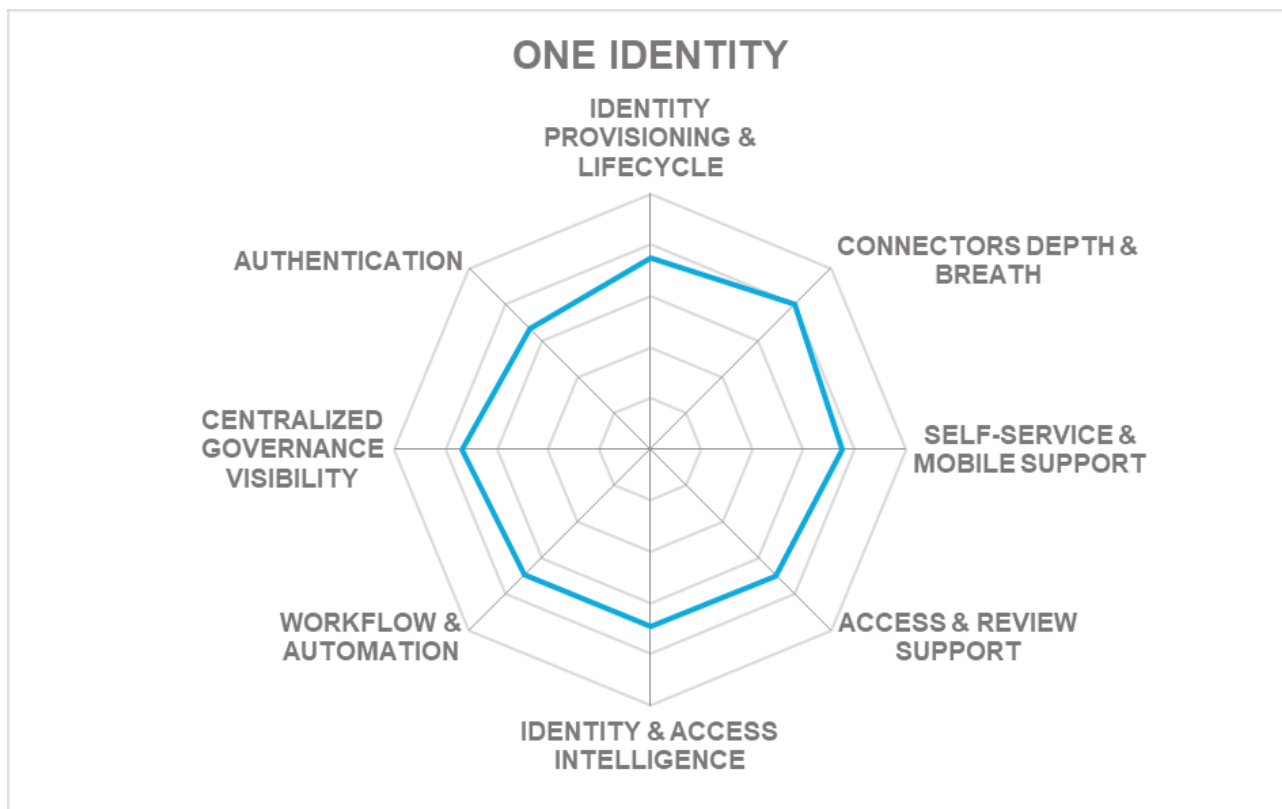
- Innovative, user-friendly interfaces
- Strong sales and marketing execution
- Very good depth and breadth of connector support
- Integrates well with its access management and privilege management capabilities
- Advanced role management with strong SOD support

Challenges

- Process-driven approach requires some training, but is highly efficient
- Inconsistent transition path and messaging for existing Dell-Quest customers
- Missing some more advanced authentication options for administration access
- A limited but growing professional services network

Leader in





5.16 Oracle Identity Governance

Oracle Identity Governance (OIG) Suite is the on-premise 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 in the 12c release, especially the integration of modules along with the ease of their deployment. Oracle remains a preferred vendor for organizations that have a substantial investment in Oracle Fusion Middleware and require high flexibility for customizations to accommodate complex business processes.

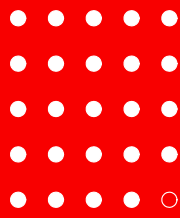
On-premises deployments can be delivered as a virtual appliance, container-based, software deployed to a server, as well as a managed service through Oracle advanced customer services and Oracle partners. Oracles on-premises deployments have a dependency on an Oracle database. Nearly all functionality is exposed through APIs via SOAP or REST. Oracle offers SDKs for Java, C/C++, and .NET programming languages. Java/Groovy can be used for mapping expressions. Both SPML and SCIM is available for SCIM for identity provisioning/de-provisioning.

Identity Governance features access request and profile management, access certification, automated provisioning and reconciliation, policy and role management, as well as for analytics and reporting. Out-of-the-box reports for major compliance frameworks are available for GDPR, HIPPA, and SOX. Customizations can be done without extensive coding in most situations and are clearly segregated from Oracle code. Features like shopping cart approaches have been implemented to improve the UX.

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.

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.

Security
Functionality
Interoperability
Usability
Deployment



ORACLE®

Strengths

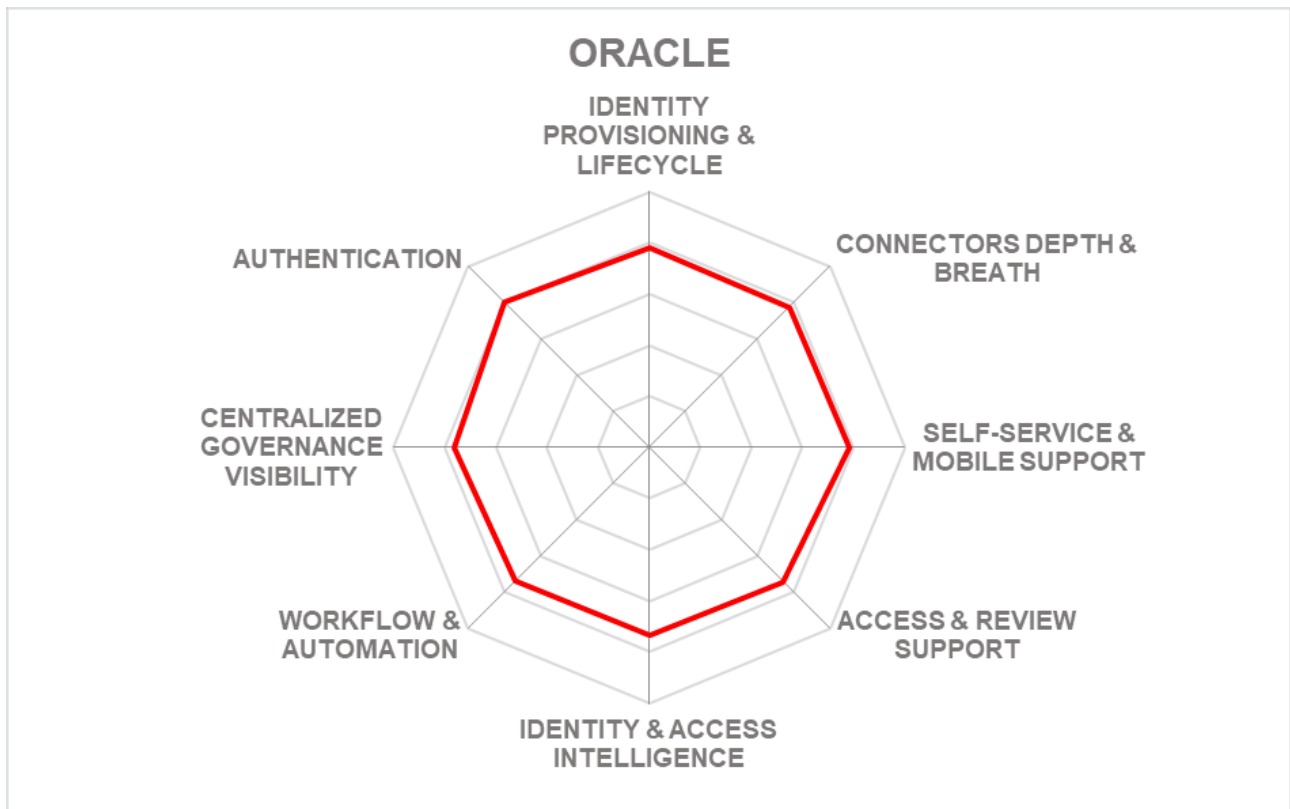
- Mature, feature-rich product focused on Identity Provisioning
- Significant improvements for deployment and customization
- Very broad support for different and modern environments with an enterprise-level architecture
- Global customer base with strong channel partner network

Challenges

- Long and complex product deployment and upgrade cycles
- Dependence on an Oracle database
- Depending on use cases, there exist some dependencies between various components of the Oracle IAM portfolio; however, for Identity Provisioning only when adaptive authentication is required

Leader in





5.17 RSA SecurID Suite

RSA, a leading provider of security solutions, offers RSA SecurID Suite, which includes RSA SecurID Access (Multi-factor Authentication, Access & SSO), and RSA Identity Governance & Lifecycle (IGL). RSA Identity Governance and Lifecycle is its IGA product delivering both Identity Provisioning and Access Governance capabilities. In 2013, RSA acquired Aveksa and has continued to expand and evolve the solution into the current RSA IGL offering. RSA IGL takes a risk-based business-friendly approach to Access Governance. With a broad range of target system connectors, RSA IGL works in conjunction with RSA Archer Suite solution to consume user and policy matrices to dynamically determine application risk-ratings, which in turn influence request and approval workflows to drive Access Governance.

In addition to on-premises deployment options, RSA offers capabilities to deploy RSA IGL in AWS cloud-based environments as well as managed service offerings that are available from both RSA partners and RSA Professional Services. Currently, a Docker container model is on their roadmap. In addition to the user interface, RSA provides access to the majority of its solution functionality via REST-based APIs. SOAP API support is available for provisioning connectors and workflow capabilities. SDKs are only given for the Java programming language with much less access to the functionality than their REST-based APIs. Both SPML and SCIM support is available for identity provisioning/de-provisioning.

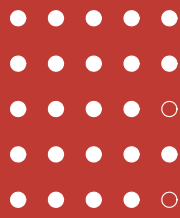
Besides extensive support for Identity Provisioning and lifecycle management, RSA IGL offers strong policy and role management capabilities due to its native support for granular entitlements with an elaborate role meta-data. Access requests and certification management are also given. Custom extensions to metadata, however, can be complex although extensions to object schema, metadata and attributes can be performed through the user interface. Tight integrations with RSA Archer Suite and RSA NetWitness Platform enable risk-based monitoring and event detection and response in real-time. RSA IGL provides identity and access analytics with insights into access patterns and peers analytics as examples, which allows for intelligent prioritization and guidance to those in the governance role.

RSA IGL also offers easy integration with RSA SecurID Access to deliver integrated access management capabilities for its customers. RSA IGL shows specific strength in depth and breadth of out-of-the-box connectors to both on-premises and SaaS systems, as well as authentication options for self-service and administration access. RSA IGL also shows strong support for reporting and out-of-the-box reports for major compliance frameworks. In addition, RSA Link supports an online user community in which customers can access documentation, downloads, advisories, knowledge base articles and more, while also participating in real-time discussions with other customers, partners, and RSA employees.

With a substantial customer base around the globe, RSA's dominance of GRC and authentication

markets has helped RSA to cross and upsell RSA IGL for IGA. RSA IGL makes an excellent choice for organizations that have existing deployments of RSA security products and have primary IGA requirements for identity task automation, strong Access Governance, and identity & access intelligence while avoiding extensive customizations.

Security
Functionality
Interoperability
Usability
Deployment



RSA

Strengths

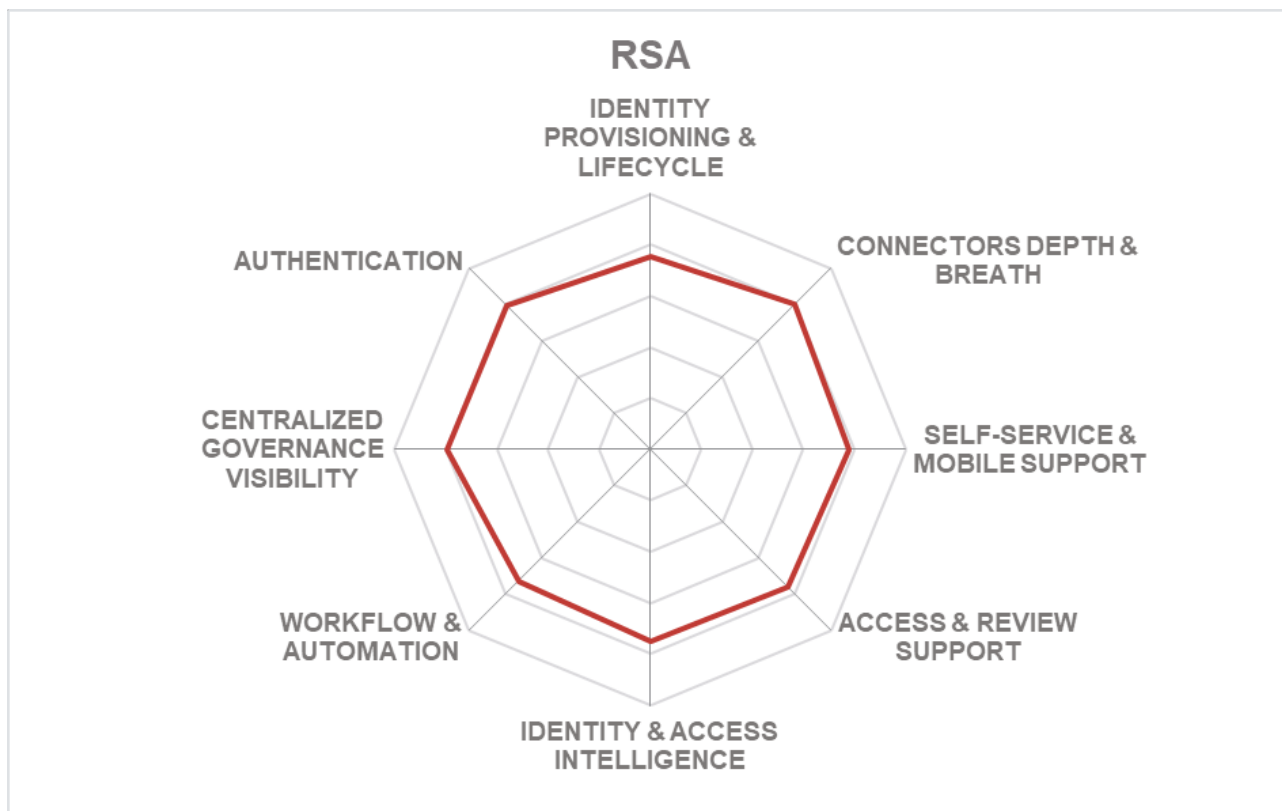
- Strong risk-based Access Governance
- Offers cloud-based delivery
- Integration with RSA Archer GRC, NetWitness and SecurID Access
- User-friendly interfaces
- Growing identity & access intelligence capabilities
- Well functioning strong partner ecosystem
- Global presence across all industry verticals
- Useful user community forum (RSA Link)

Challenges

- Effects of acquisitions and spun-offs with EMC and then Dell on product strategy is still unclear
- Cloud delivery is currently a single tenant model
- Some limitations on SDK programming language options and access to product functionality via the SDK

Leader in





5.18 SailPoint Predictive Identity Platform

SailPoint originally started as a vendor specialized in Access Governance, and significant technology and personnel investments in its Identity Provisioning capabilities over the last several years have accelerated the IGA capabilities of its product. The SailPoint Predictive Identity platform delivers multiple SaaS services into a single solution delivering AI and analytics support via the cloud to both IdentityIQ and IdentityNow customers. SailPoint has massively enhanced its provisioning and predictive intelligence support over the past few years.

The base on-premises deployment of IdentityIQ is a Java application server model that can also be delivered in the cloud as container-based, or managed service. For cloud delivery, the product does not support full multi-tenancy. All of the product's functionality is exposed via SOAP or REST APIs, as well as the majority of the functionality is accessible via CLI.

SDKs expose nearly all functionality and can be extended via the Java programming interface as well as JavaScript, Angular, and jQuery options. The solution supports both SPML and SCIM for identity provisioning/de-provisioning.

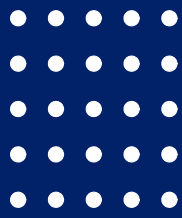
Beyond the core governance capabilities such as access certification, SoD, access request, provisioning, and password management, SailPoint brings strong support to access insights, recommendations, access modeling, and cloud governance to the platform's forefront. Strong support for different identity types such as Bot/RPAs is also given. Full reporting support is available, as well as out-of-the-box reports for major compliance frameworks.

Due to its origin in the Access Governance market, the user interfaces are geared towards business users. The approach, in general, is very much business-driven and less technology-focused than what some of the “classical” vendors in that market provide. The user interfaces are well laid out and user-friendly with some superior dashboard graphics.

Regarding out-of-the-box connectors to on-premises and SaaS systems, they have not only extended the number of connectors, but also the depth of various connectors such as the one for SAP systems to meet governance requirements of complex scenarios. Besides supporting connectivity to target systems via identity provisioning, the product also directly supports integration with ITSM (IT Service Management) tools.

SailPoint has been a leading vendor in the IGA market, providing strong Access Governance capabilities. In addition, SailPoint has built excellent support for Identity Provisioning 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 vendors for IGA.

Security
Functionality
Interoperability
Usability
Deployment



Strengths

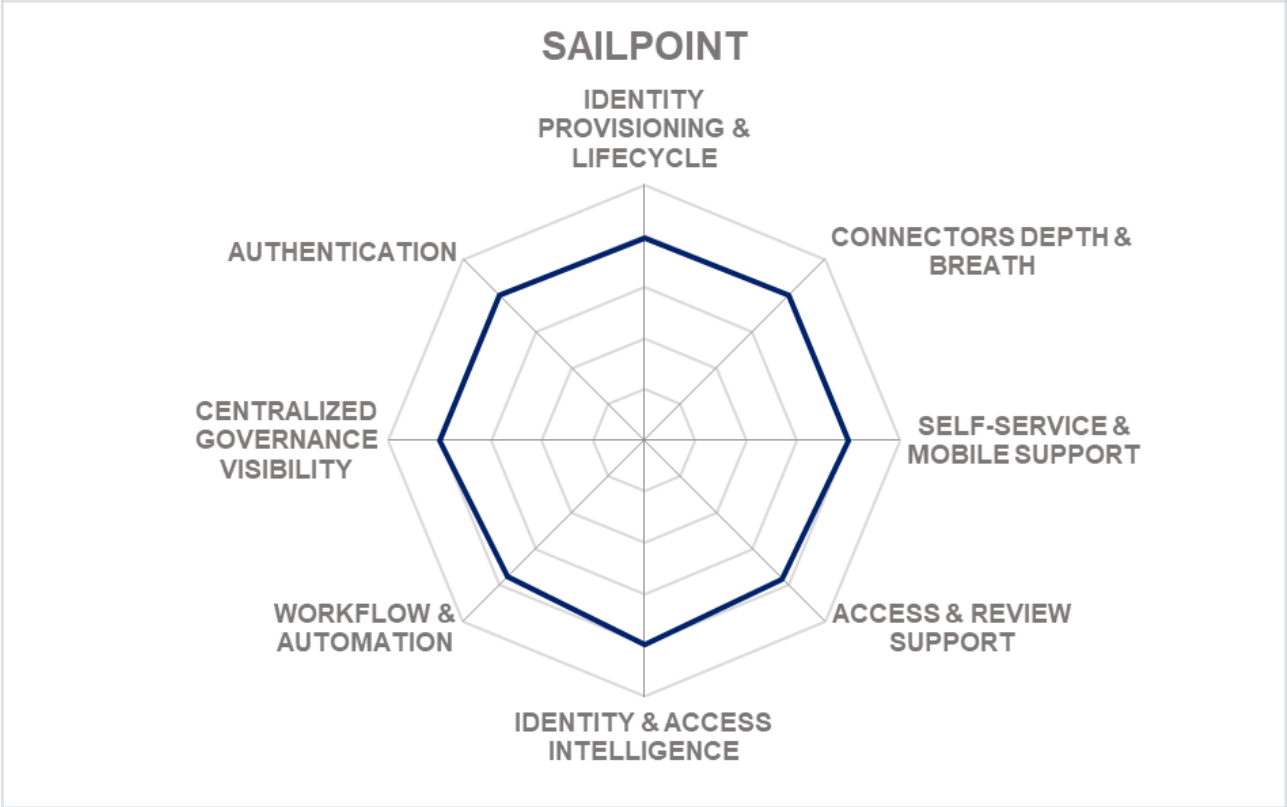
- Strong integrated Identity Provisioning and Access Governance capabilities
- Strong support for identity and access intelligence
- Integration capabilities with other provisioning systems and SRM out-of-the-box
- Well thought out and user-friendly interfaces
- Strong and effective governance focused marketing messaging
- A large and effective channel partner network

Challenges

- Lack of SOD controls for transaction monitoring and emergency access management
- While IdentityNow serves mid-to-large market segment, IdentityIQ remains primarily focused on IGA needs of large enterprises
- Lack of multi-tenancy support for IdentityIQ concerns IAM professional service providers offering managed IGA services

Leader in





5.19 SAP Access Control

SAP has established a considerable IAM portfolio over the past few years, and its recent acquisition of Gigya shows its continued commitment to grow and compete in the space.

SAP offers the SAP Access Control and SAP Identity Access Governance products as an IGA solution, which is well-integrated with other SAP solutions such as SAP Business Suite to provide excellent Access Governance capabilities for SAP and few other ERP applications.

SAP's Access Governance portfolio is part of a number of different products within their SAP Finance & Risk product category, also known as their governance, risk, and compliance (GRC) offering. SAP Access Control is on-premise, with SAP Identity Access Governance as their fully multi-tenant cloud solution. For hybrid deployments, SAP Cloud Identity Access Governance (integration edition) is available extending SAP Access Control for SaaS applications. The delivery option for on-premise is a virtual appliance, although SaaS and managed services are available as well. The majority of the product's functionality is exposed via SOAP or REST APIs, although no CLI and little SDK support. The solution supports both SPML and SCIM for identity provisioning/de-provisioning.

SAP has made significant progress with its offerings over the past few years, including product re-architecture, to expose a comprehensive set of APIs for simplified customization and integration. The product comes with standard Access Governance capabilities, including flexible workflows, support for automated assignment of entitlements based on roles, approval processes, and self-service functionalities. It also delivers good reporting and auditing capabilities, although less support of out-of-the-box reports for major compliance frameworks.

A primary challenge has been the relatively small set of connectors when compared to other offerings in the market. SAP gives good support for out-of-the-box provisioning connectors for on-premises systems, but less support for SaaS other than some of the most popular applications. Also, the Access Governance capabilities are limited to role management and auditing with more complex requirements such as SOD controls served by another SAP product, SAP Access Control. While SAP Access Control has excellent support for role management and Access Governance across SAP and SAP-like applications with complex role structures, it is often criticized for associated maintenance overheads both in terms of cost and deployment complexity.

SAP maintains a significant customer base in North America, with less presence in other regions. Despite all of the shortages mentioned, we rate SAP Identity Management as a strong contender in the IGA market and a preferred vendor for organizations with significant investments in SAP software.

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



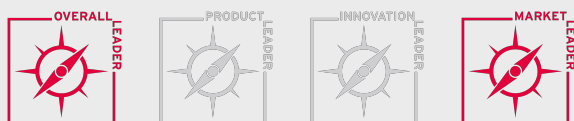
Strengths

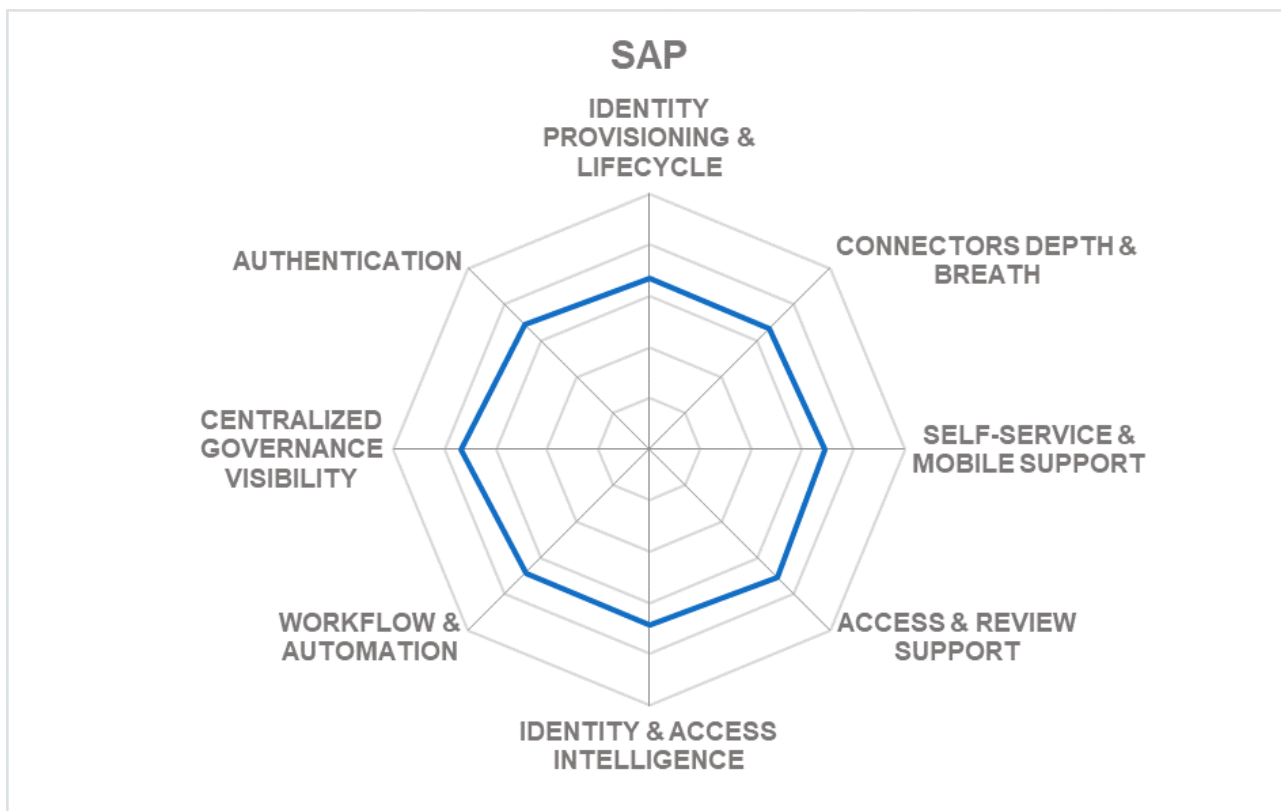
- Excellent integration into SAP environments, including SAP Access Control
- Identity Provisioning feature set
- Integrates identity virtualization
- Good role management capabilities
- Risk analysis capabilities

Challenges

- Strong connector support for on-premises systems, but some gaps particularly for non-SAP business applications and SaaS applications
- Some gaps in baseline Access Governance, but covered by other SAP offerings
- Costly and complex product deployment and upgrades, although efforts are being made to address this by providing more options to customers
- Primary customer focus in North America, with less of a foot print in the EMEA, followed by some presence in the rest of world.

Leader in





5.20 Saviynt Security Manager

Founded in 2010 and based in California (US), Saviynt offers Saviynt Security Manager – Enterprise Identity Governance Administration as its IGA product combining Identity Provisioning and Access Governance capabilities. In a relatively short time, Saviynt has established itself as a key player in the market, demonstrating timely response to market trends and quality innovation.

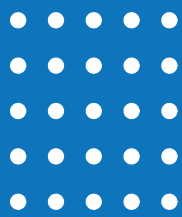
For on-premise deployments, Saviynt has a virtual appliance-based offering for customers not yet ready or can't move to the cloud. For cloud deployments, Saviynt delivers a fully multi-tenant SaaS as well as managed service. Nearly all of the product's functionality is exposed via REST APIs, although SOAP is not. Support for a Java-based SDK is provided, although with much less access to the functionality of the product. JSON, JavaScript, RegEx can be used to construct attribute mapping expressions. The solution also supports both SPML and SCIM for identity provisioning/de-provisioning.

Saviynt offers a strong lineup of IGA, application GRC, a cloud security analyzer, and cloud PAM. More recently, Saviynt added ID Risk Exchange and the Saviynt Exchange products to their portfolio, which is a collaborative platform with their customers to exchange insights. Workflow management with a drag-and-drop feature is also given. Intelligence appears across a wide range of applications and infrastructure. Saviynt also offers granular Data Access Governance and cross-application SOD risk management capabilities. Intelligent access request capabilities are available to allow more ways to request access, such as through Slack or MS Teams, for example. Saviynt has also added a built-in connector RPA Bot that can be deployed on-premises for a hybrid deployment. It can be used to onboard and convert disconnected applications to connected applications for automated reconciliation, provisioning, and account management.

The UI dashboard can be tailored from a simplified view for line managers to more detailed views for analyst and application owners displaying different aspects of access, activity, and vulnerability risk. Saviynt does provide a mobile application, although there are limited UI features on the mobile app. Also, with additional Data Access Governance and cross-application SOD risk management capabilities, Saviynt offers one of the most comprehensive Access Governance portfolios available in the market today.

Saviynt customers are focused at enterprise organizations with customer and partner ecosystems primarily located in North America with growth in the EMEA region. Customers looking for an integrated risk-based approach to IGA across the range of on-premise and cloud-based applications should consider evaluating Saviynt.

Security
Functionality
Interoperability
Usability
Deployment



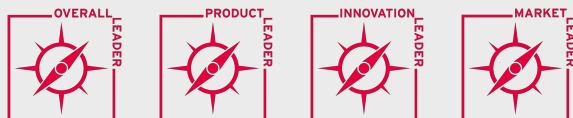
Strengths

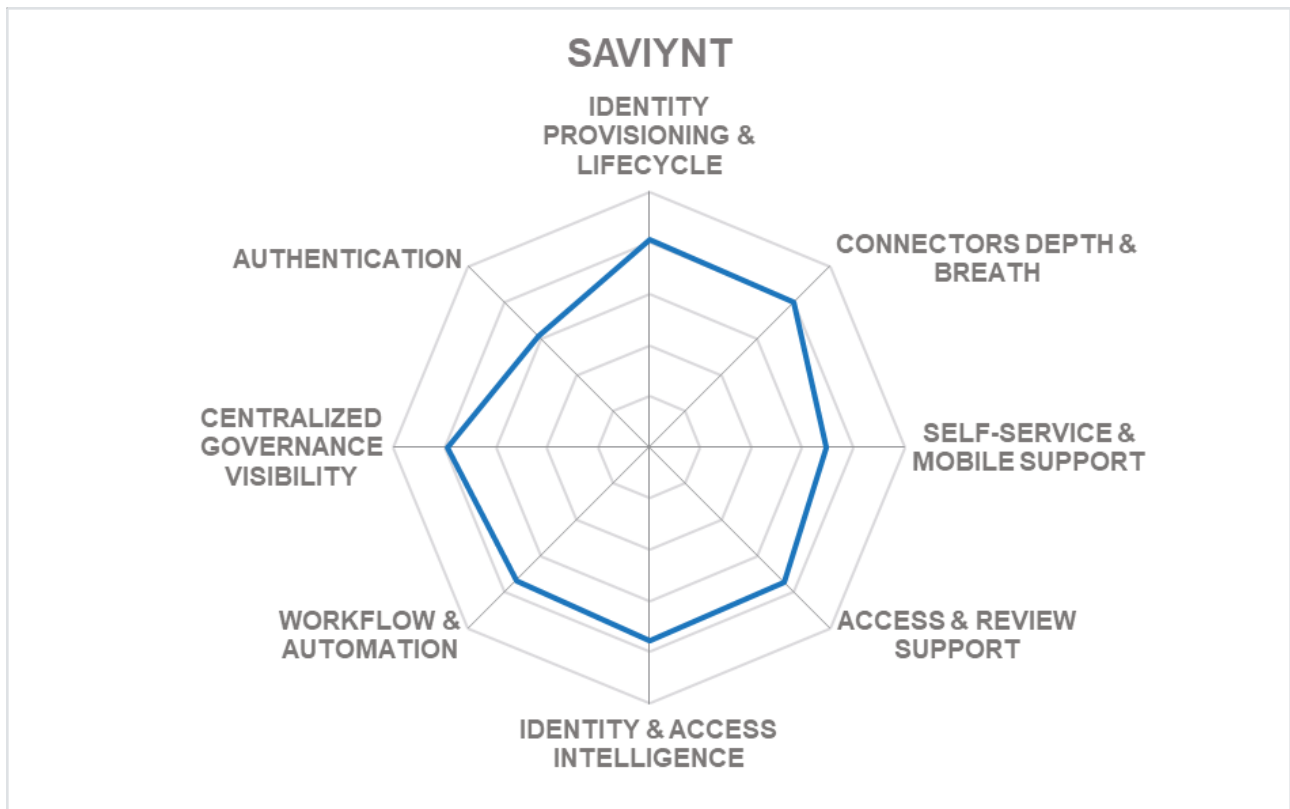
- An innovative integrated risk-based approach to Access Governance
- Strong role engineering and governance
- Flexible policy and workflow management
- Well laid out and user-friendly UI
- Good use of intelligence throughout
- Mature DAG and SOD risk management
- Depth & breadth of OOB connectors to on-premises and SaaS applications

Challenges

- Pricing is in the higher end of the spectrum
- Limited self-service and administration authentication options
- Weak brand awareness in regions outside North America

Leader in





5.21 Simeio Identity Orchestrator

Founded in 2007, Simeio Solutions witnessed significant growth when shifting from its IAM system integration business into a full-fledged IDaaS service provider over the past years. Previously offering dedicated hosted services underpinned by other IAM vendor's products, Simeio enters the mainstream IDaaS market with Simeio IDaaS. Simeio Identity Orchestrator is its primary IGA service.

Simeio offers a platform with a fully integrated suite of IGA, AM, and PAM domains as well as providing add-on capabilities via 3rd party functionality such as Splunk integration and certified integrations with commercial solutions like BeyondTrust and CyberArk as examples. Simeio Identity Orchestrator (IO) gives clients the ability to access their entire IAM infrastructure within a single platform. Although Simeio has a focus on providing a SaaS, it also offers hardware and virtual appliance, and software deployed to servers and container-based options for on-premises delivery.

Simeio IO features include a user onboarding invitation service, access request & approval, access certification, password management, delegated administration, and privileged check-out as well as risk and security intelligence capabilities. Interfaces to Simeio IO includes a web UI, mobile application, and REST APIs options. SOAP service APIs are not supported. Its mobile app interface provides the ability to the user to conduct activities such as access request approvals and access certifications.

Simeio provides options for identity repository support limited to Microsoft AD & ADD, and Oracle ODSEE, although MySQL and Ping Directory can also be supported. Most out-of-the-box connectors to major on-premises and SaaS systems are supported. Both basic and some more advanced authentication options are given to user self-service and administration access. There is some limitation to available out-of-the-box IGA reports and reports for major compliance frameworks. Support for policies that give flexible entitlement models using attributes is primarily focused on roles and organizations. Some identity and access intelligence are shown through capabilities such as role discovery and mining, as well as access modeling.

Simeio supports organizations primarily in North America with a growing footprint in the EMEA and APAC regions. Simeio combines its IAM development experience and systems integration expertise to present a viable alternative to several established vendors, particularly for organizations that lack IAM knowledge and expertise internally and will require detailed guidance and support for transitioning existing on-prem access management to IDaaS.

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

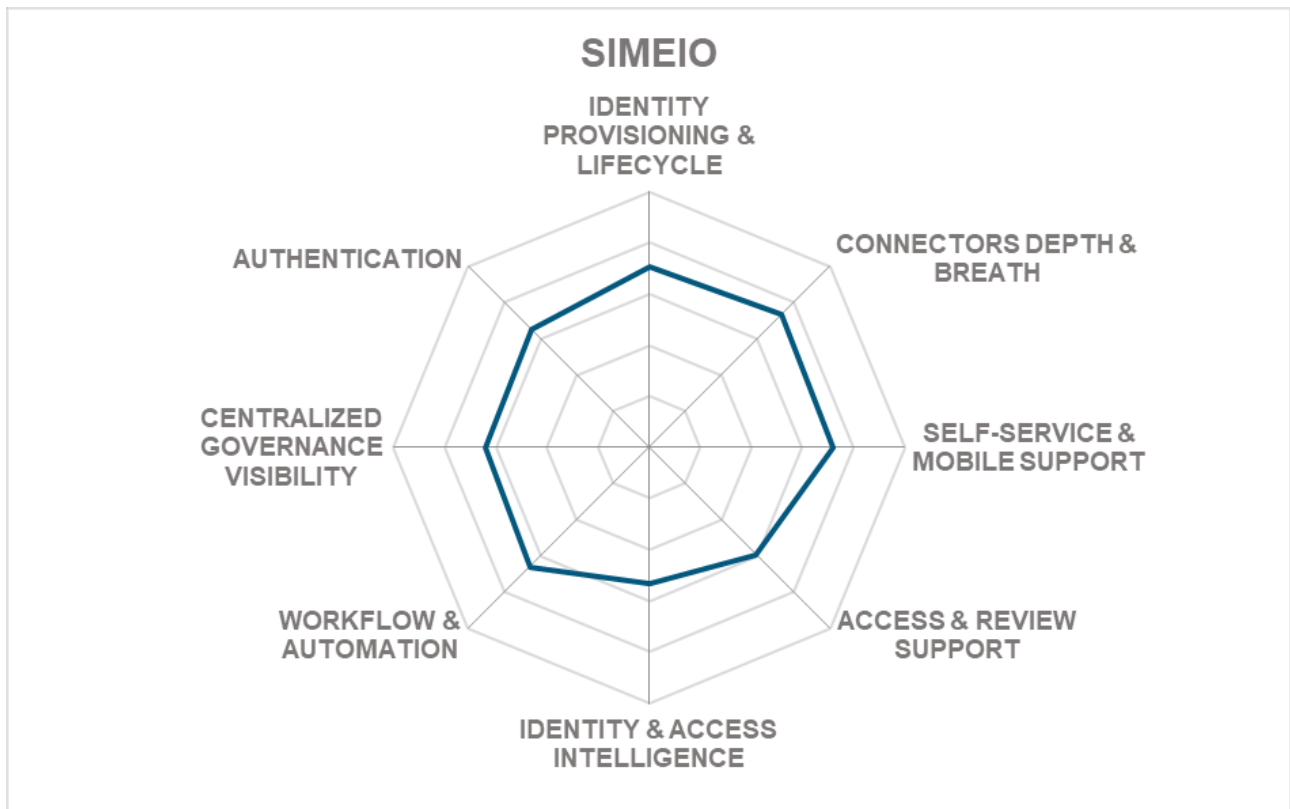


Strengths

- Core IGA features
- Breadth of OOB connectors to on-premises and SaaS systems
- Basic and some advanced authentication options available
- Mobile application
- Flexible deployment options

Challenges

- Some limitations on supported identity repository options, although the most prominent repositories are supported
- OOB IGA reporting options are limited
- Limited partner ecosystem
- The wide-spread reputation of primarily being only a global SI vendor



5.22 Soffid IAM

Based in Spain and established in 2013, Soffid IAM provides an open-source Identity and Access Management (IAM) and Single Sign-On (SSO) solution. Soffid offers a subscription service to an enterprise edition of the software product and technical support service. Consulting and deployment services are also available through Soffid services.

Soffid IAM is capable of supporting not only on-premises but also public & private cloud and hybrid deployment models. The solution can be delivered as a hardware appliance, container-based, and as a managed service, although a virtual appliance option is not available. Soffid states that 100% of the solution's functionality is exposed via SOAP and REST APIs. Only Java SDKs are available for use by developers.

Soffid IAM offers password management and policies, provisioning for user onboarding and offboarding. Flexible attribute mapping tools and a JavaScript editor Soffid are given. Soffid provides the ability to fully audit the system as well as support for other audit and compliance features. In addition, Soffid IAM provides SSO and the capability to record sessions and keystrokes. Additional features include a workflow web editor, recertification capabilities, and adaptive authentication with biometrics. An XACML policy editor and PEP configuration tools are also given.

Soffid provides a functional dashboard with the ability to customize dashboard widget based on customer requirements. Some analytics and intelligent features are shown through status and risk indicators. Additionally, role mining capabilities are also available.

Soffid IAM primarily serves medium to mid-market organizations with some inroads to enterprise-level organizations. Customers are focused in the EMEA region, with some expansion into APAC and Latin America. Soffid's partner ecosystem is relatively small and located in the customer's geographic locations. Soffid offers a reasonably well balanced IAM and governance product as an alternative open source solution to mid-market organizations.

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

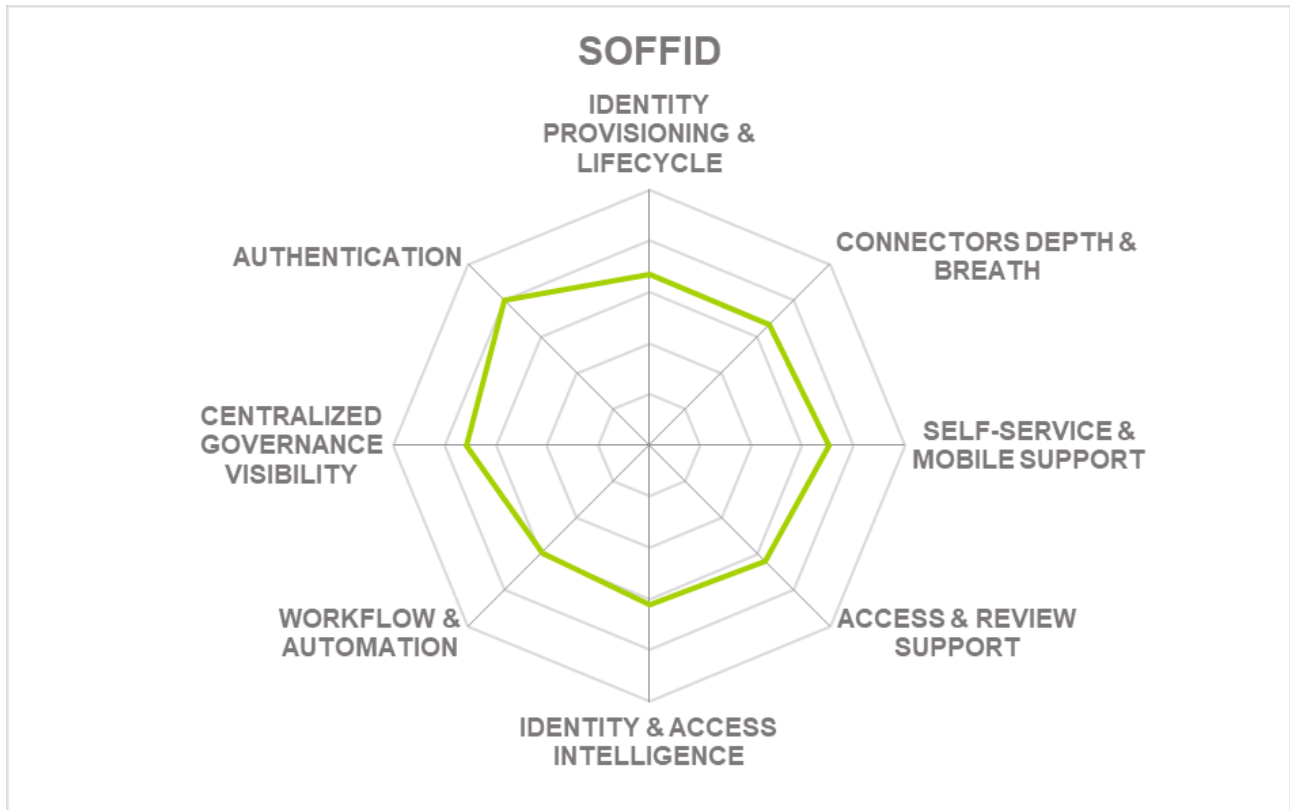


Strengths

- Flexible attribute mapping
- Breadth of OOB provisioning connectors to on-premises systems
- Good self-service & administration access authentication options
- All functionality exposed via APIs
- IGA related reports OOB
- Dynamic authorization management

Challenges

- Small partner ecosystem
- Limited market presence outside Europe
- Some limitations on OOB provisioning connectors to SaaS systems beyond Microsoft AD/O365, Workday, & SAP/HANA
- Missing OOB reports for major compliance frameworks such as GDPR or SOX



6 Vendors and Market Segments to watch

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

6.1 Accenture Memory

Accenture Memory is provided by a unit within Accenture Security, delivering an IDaaS solution. Memory started as an independent software vendor and has become part of that larger group three years ago. Thus, Accenture Memory benefits from the global network of resources and the strengths Accenture can offer in their understanding of business challenges and the transformation of business towards new digital services. They are a provider of an Identity Fabric that connects all types of users to all types of services.

Accenture Memory is an IDaaS solution that supports both IDaaS IGA and IDaaS AM use cases. It supports all major feature areas, from Identity Provisioning and Access Governance capabilities to Access Management, Single Sign-On to cloud services and Adaptive Authentication. Based on this comprehensive set of capabilities, Accenture Memory offers good support for common IDaaS IGA requirements and beyond. Additional capabilities such as Consent Handling are also part of the solution, positioning it well as a foundation for Digital Transformation projects.

Accenture Memory, amongst other capabilities, has a strong focus on providing a consistent and comprehensive API layer as part of its solution. Another specific strength is the IoT support of the offering. Altogether with the ability of Accenture to support customers in their Digital Transformation initiatives, Accenture Memory has the potential to become the backbone of future IAM of digital businesses.

6.2 Atos

Atos, having acquired Evidian indirectly via the Groupe Bull acquisition, has also acquired the former Siemens Business Services which includes the Siemens DirX portfolio. Products and capabilities from both the acquisitions are now united under the brand Evidian, which is the joint offering we have evaluated in this Leadership Compass. However, the DirX products will still be available and maintained by Atos.

DirX Identity has been a proven solution, but Atos has managed it well to modernize the tool and

bring it to the level of current standards of IGA tools, with some areas of specific strength. Amongst these areas are the depth of connectors, the underlying support for identity attributes based on the meta-directory capabilities, the high availability configurations, and the strong fulfilment capabilities.

From a feature perspective, DirX Identity comes as an offering that delivers both leading-edge Identity Provisioning capabilities and a strong risk-based Access Governance feature set. Atos has made significant improvements when it comes to the ease and flexibility of customization and added a modern, responsive user interface together with RESTful interfaces. However, its Access Governance capabilities can still be enhanced. DirX Identity counts amongst the strong Identity products in the IGA market.

6.3 Clear Sky

Founded in 2016, Clear Sky is a small privately-owned company headquartered in the San Francisco Bay area. The Clear Sky IGA solution is built on and exists within ServiceNow. Clear Sky IGA provides a portal that gives a single control set for application access. Clear Sky IGA capabilities include Identity Lifecycle, Entitlement Management, Access Requests, Audit, Policy Management, Certifications, Identity Analytics, and Workflows.

Clear Sky IGA can help organizations that require lower barrier IGA products or where existing IGA solutions are manual process intensive. Clear Sky IGA can also benefit customers that would like to leverage their existing ServiceNow investment complementing it with Clear Sky IGA.

6.4 ForgeRock

ForgeRock is a leading, venture-backed IAM vendor, headquartered in the US but with many offices around the world. ForgeRock supports most major IAM standards and is a significant contributor to several international standards organizations. Their overall Identity Platform serves both B2E and B2C markets.

More recently, ForgeRock released its Identity Governance product built on top of the ForgeRock Identity Manager capabilities. These capabilities customers have been using for years that include connectors to target systems, identity provisioning, identity data mode, and account mapping, workflows, as well as good user self-service UIs. In the last quarter of 2019, ForgeRock added IGA capabilities such as access certification, request management, and role & SoD management. About the same, ForgeRock also releases identity analytics and access intelligence. Their access governance includes many of the same capabilities with added access risk management, role mining & engineering.

ForgeRock's entrance into the IGA market will be interesting. ForgeRock already provides strong capabilities in the IAM market and is expected to do well in the IGA market as well.

6.5 Ideiio

Ideiio is a fairly new vendor in the IGA space; spun out from ProofID – an IAM professional services provider and system integrator based in Manchester, UK, and Colorado Springs, US – Ideiio builds upon the pre-existing and mature ProofID IGA product. ProofID has offered ProofID IGA as its primary IGA product for several years and has now segregated its software development activities from its IAM services portfolio in a new company called ideiio. Ideiio's IGA offering is targeted primarily at mid-market and B2B market segments.

6.6 Imprivata

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

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

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

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

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

6.7 Nexis

Nexis, based in Germany, offers Nexis Controle as its combined identity provisioning and access

governance offering. Controle, first released in 2014, builds on an innovative plug and play approach to access governance, which remains its core focus. Controle is delivered as a physical appliance with a built-in database. While it offers the width of capabilities across access governance, complex governance scenarios requiring a depth of certain functionalities could be a challenge. It takes a risk-based approach to access certifications. Nexis has made significant enhancements to its access review capabilities to include incremental as well as event-based certifications. Integrated SOD controls and data access governance capabilities stand out for a vendor of this size and maturity.

6.8 Omada

Omada, a Danish vendor, provides the Omada Identity Suite as an integrated Access Governance and Identity Provisioning platform to deliver a range of IGA functionalities. Omada focuses on adaptable business-centric and collaborative features such as workflows, attestation, and advanced access analysis, role management, reporting, governance and compliance, and application management. Over the past years, Omada has decided for a major strategic shift by adding its Identity Provisioning layer, instead of solely relying on the integration with Microsoft Identity Manager (MIM). Thus, Omada nowadays also competes in the pure-play Identity Provisioning market but shows its full strength in IGA and Access Governance use cases.

Omada Identity Suite has undergone major changes over the past years. Aside from adding its Identity Provisioning layer and removing the former dependency on Microsoft Identity Manager, Omada also has re-architected the solution, changing the data model to be more flexible and massively enhancing scalability. Also, the UIs have undergone significant modernization.

Omada takes IGA a step further by supporting customers by providing an IGA best practices framework called IdentityPROCESS+ along with IdentitPROJECT+ IGA project methodology, and an IGA Academy that provides training. Also given are IGA as-a-Service and Software for governing and automation IGA processes.

Omada Identity Suite is an interesting IGA solution for enterprise customers that need to build a governance layer on top of their Microsoft Identity Manager implementations. With recent enhancements to its product capabilities, Omada has become a strong contender to traditional players in the IGA market segment.

6.9 Pirean

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

Pirean's Access: One provides a diverse set of capabilities that offers a fully-featured end-to-end IAM solution. Access: One 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.

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

6.10 Singular ID

Avalon Solutions is a small, mid-market company that services the Latin American region. Their product, singular_id, can be deployed on-premises, cloud, as well as a managed service. singular_id is capable of providing IGA, PAM, and DAG features.

singular_id IGA capabilities include risk monitoring and ratings, access surveillance, profile and privilege mining, role management, and privileges by activity setup. Also available are dashboards, reporting, and analytics that give correlations, behavioral, and predictive analysis. Out-of-the-box provisioning connectors are given, although less than vendors in the IGA market.

Although singular_id currently shows greater strength in access governance, roadmap items include future improvements provisioning capabilities making them a vendor to watch in the IGA market for companies in the Latin American region.

6.11 Tools4ever

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. Their main offering for identity provisioning is Identity & Access Manager, which covers the major features we expect to see in this market segment.

We see particular potential in large medium-sized organizations and large family-owned businesses, where Tools4ever Identity & Access Manager can be a good fit. Overall, Tools4ever has made significant progress over the past years and moved to the level of a contender for the established players in the identity provisioning market. With offices in the U.S., UK, France, Germany, and the Netherlands, they have matured into an interesting alternative.

6.12 Tuebora

Tuebora, based in California, offers Tuebora Governance as its primary IGA product. One of the earliest IGA vendors to leverage machine learning techniques for Identity Analytics and Access Governance, Tuebora offers its own Data Access Governance (DAG) and web access management (WAM) products as Tuebora DAG and SSO respectively. Tuebora combines Identity Provisioning

and Access Governance with its machine learning and identity analytics platform to detect access risks based on real-time tracking of provisioning and user access behavior.

Founded in 2001 and headquartered in the San Francisco Bay area, Tuebora focuses on mid-market to enterprise access governance, risk, and compliance offerings. Tuebora's customer base is located in the EMEA, North America, and APC regions. It makes a good choice for organizations looking for risk-based IGA capabilities. It equally appeals to managed IAM service providers considering offering a 'white-labeled' service in partnership.

6.13 Usercube

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

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

Usercube provides identity management, provisioning, governance, analytics, and reporting. Usercube can use all significant identity repositories and any LDAP compatible, SQL based, or API based directories. All identity types are also supported, including departments, work sites such as a meeting room, applications, or machine identity like IoT or RPA bots. Overall, Usercube has a well-balanced set of IGA capabilities as well as making good use of identity and access intelligence.

7 Related Research

[Executive View: Atos DirX Identity - 80166](#)
[Executive View: Avatier Identity Management Suite - 71510](#)
[Executive View: Beta Systems Garancy IAM Suite - 71530](#)
[Executive View: EmpowerID - 70297](#)
[Executive View: Evidian Identity & Access Management - 70872](#)
[Executive View: Hitachi ID IAM Suite - 72543](#)
[Executive View: Imprivata - 71514](#)
[Executive View: Oracle Identity Governance - 80157](#)
[Executive View: Pirean Consumer IAM Platform - 70223](#)
[Executive View: RSA® Identity Governance and Lifecycle - 71052](#)
[Executive View: SailPoint SecurityIQ - 70849](#)
[Executive View: Saviynt Security Manager for Enterprise IGA - 80325](#)
[Executive View: Simeio IAM for SMB - 79071](#)
[Leadership Compass: Access Governance & Intelligence - 71145](#)
[Leadership Compass: Access Management and Federation - 71147](#)
[Leadership Compass: IDaaS Access Management - 79016](#)
[Leadership Compass: Identity API Platforms - 79012](#)
[Leadership Compass: Identity as a Service \(IDaaS\) IGA - 80051](#)
[Leadership Compass: Identity as a Service: Single Sign-On to the Cloud \(IDaaS SSO\) - 71141](#)
[Leadership Compass: Identity as a Service \(IDaaS B2E\) - 70319](#)
[Leadership Compass: Identity Provisioning - 71139](#)
[Whitepaper: Pirean: Orchestrated Identity for Meeting IAM & CIAM Requirements -70225](#)
[Whitepaper: SailPoint: Governance for all data: Get a grip on unstructured data - 79046](#)

Methodology

About KuppingerCole's Leadership Compass

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

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

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

Types of Leadership

As part of our evaluation of products in this Leadership Compass, we look at four leadership types:

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

For every leadership type, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains products which lag behind in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even the 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 a given market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, as well as other sources.

Product rating

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

KuppingerCole uses the following categories to rate products:

- **Security**
- **Functionality**
- **Integration**
- **Interoperability**
- **Usability**

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole Analysts IT Model. Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such

issues and the way a vendor deals with them.

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

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

Interoperability – interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs.

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

interface design.

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

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

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product security, functionality, integration, interoperability, and usability which the vendor has provided are of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

Vendor rating

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

- **Innovativeness**
- **Market position**
- **Financial strength**
- **Ecosystem**

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

Market position – measures the position the vendor has in the market or the relevant market

segments. This is an average rating overall markets in which a vendor is active, e.g. being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

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

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

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

Rating scale for products and vendors

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

Strong positive

Outstanding support for the feature area, e.g. product functionality, or outstanding position of the company, e.g. for financial stability.

Positive

Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. for market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral

Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., a regional-only presence.

Weak

Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical

Major weaknesses in various areas. This rating most commonly applies to company ratings for

market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

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

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

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

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

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

Content of Figures

Figure 1: Business Value of Integration

Figure 1: Representation of core IGA functions by 'Identity Provisioning' and 'Access Governance' categories.

Figure 3: The Overall Leadership rating for the IGA market segment

Figure 3: Product Leaders in the IGA market segment

Figure 3: Innovation Leaders in the IGA market segment

Figure 3: Market Leaders in the IGA market segment

Figure 7: The Market/Product Matrix.

Figure 8: The Product/Innovation Matrix.

Figure 9: The Innovation/Market Matrix.

Copyright

©2020 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 back 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.