KuppingerCole Report

LEADERSHIP COMPASS

By Richard Hill
June 29, 2021

Identity Governance & Administration 2021

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

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

Content

1 Introduction / Executive Summary 4

1.1 Highlights 5

1.2 Market Segment 5

1.3 Delivery Models 13

1.4 Required Capabilities 14

2 Leadership 18

2.1 Overall Leadership 18

2.2 Product Leadership 20

2.3 Innovation Leadership 23

2.4 Market Leadership 26

3 Correlated View 29

3.1 The Market/Product Matrix 29

3.2 The Product/Innovation Matrix 31

3.3 The Innovation/Market Matrix 33

4 Products and Vendors at a Glance 36

5 Product/Vendor evaluation 40

5.1 Avalon Solutions 360 42

5.2 Avatier 45

5.3 Beta Systems 48

5.4 Broadcom Inc. 51

5.5 EmpowerID 54

5.6 E-Trust 58

5.7 Evidian (was acquired by Atos) 62

5.8 Evolveum 66

5.9 Fischer International Identity 69

5.10 ForgeRock 72

5.11 Hitachi ID Systems 76

5.12 IBM 80

5.13 ideiio 84
5.14 Ilantus Technologies 87
5.15 ILEX International 90
5.16 Micro Focus 93
5.17 Nexis 97
5.18 Omada 101
5.19 One Identity 105
5.20 Oracle 109
5.21 SailPoint 113
5.22 SAP 117
5.23 Saviynt 121
5.24 SecurEnds 125
5.25 SecurID 128
5.26 Simeio Solutions 132
5.27 Soffid 135
6 Vendors to Watch 138
6.1 Accenture Memority 138
6.2 Clear Skye 138
6.3 Imprivata 138
6.4 Kapstone 139
6.5 Pirean 140
6.6 Systancia 140
6.7 Tools4ever 141
6.8 Tuebora 141
6.9 Usercube 142
7 Related Research 143
Methodology 144
Content of Figures 150
Copyright 151

1 Introduction / Executive Summary

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

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

From our interaction with organizations of varied IAM maturity across the industry verticals, we note that while some are still looking for an Identity Lifecycle Management solution with limited or no Access Governance capabilities, many others demand a strong Access Governance solution. The latter is mostly the case when organizations already have Identity Lifecycle Management in place or when their starting point is Access Governance. One of the adoption patterns we have observed in the market is where fulfilment through Identity Lifecycle Management 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 Lifecycle Management or Access Governance but do not demand an IGA solution. In most other cases where there is a need for both, IGA products are preferred over provisioning or governance 'only' solutions to achieve the desired mix of capabilities. This is generally true for greenfield IAM implementations that have a need for both Identity Lifecycle Management 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 center on Identity Governance and Administration holistically to help security leaders identify relevant IAM market segments and subsequently shortlist the most appropriate technology vendors based on their immediate IAM priorities. In this Identity Governance and Administration Leadership Compass, the primary focus is on the vendors that offer both Identity Lifecycle Management and Access Governance capabilities, either as a common product or separate but integrable product components to deliver capabilities across the IGA spectrum.

This IGA Leadership Compass is 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 Highlights

- This Leadership Compass evaluates over 20% more IGA product vendors over the previous year.
- The IGA market is growing, and although maturing it continues to evolve.
- IGA is essential to business as a strategic approach to ensure overall IT security and regulatory compliance.
- The level of identity and access intelligence has become a key differentiator between IGA product solutions.
- Automation is a key trend in IGA to reduce management workload by automating tasks and providing process workflows.
- Leading IGA vendors are increasingly focusing on supporting interoperability with other products and services through the provision of secure APIs.
- The Overall Leaders are (in alphabetical order) Avatier, Broadcom, EmpowerID, ForgeRock, Hitachi ID, IBM, Ilantus, Micro Focus, One Identity, Oracle, SailPoint, Saviynt, SecurID, and Simeio.
- The Product Leaders (in alphabetical order) are Avatier, Beta Systems, Broadcom, EmpowerID, Atos (Evidian), ForgeRock, Hitachi ID, IBM, Ilantus, Micro Focus, Omada, One Identity, Oracle, SailPoint, Saviynt, SecurID, and Simeio.
- The Innovation Leaders (in alphabetical order) are Avatier, EmpowerID, ForgeRock, IBM, Ilantus, Micro Focus, One Identity, Oracle, SailPoint, Saviynt, SecurID, and Simeio.
- Leading vendors in innovation and market (a.k.a. the \"Big Ones\") in the IGA market are (in alphabetical order) EmpowerID, ForgeRock, IBM, Ilantus, Micro Focus, One Identity, Oracle, SailPoint, Saviynt, and SecurID.

1.2 Market Segment

Identity Governance and Administration refers to the increasingly integrated Identity Lifecycle Management and Access Governance markets. Where Identity Lifecycle Management 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 Lifecycle Management and Access Governance that offers business-related insights to support effective decision making and potentially enhance governance.

While Identity Lifecycle Management 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 identifies 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 fulfilment, 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:

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

Increased adoption of cloud-based identity stores and directories such as Microsoft Azure Active Directory

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

IGA integration with other enterprise systems such as IT Service & 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 DG (Data 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 Lifecycle Management and Access Governance.

Identity Lifecycle Management:

- **Identity Repository:** Identity repositories are a core component of an IGA deployment and provide a mechanism to manage the identities, identity attributes, access entitlements and other identity related information scattered across the IT environment. Management of access rights information and other entitlements across the identity repositories are captured and correlated as part of access entitlements management process to determine the user's access across the various systems. Often bundled as part of an IGA tool, identity repository offers a consolidated view of identity data. In case of disparate identity repositories, virtualization of identity information is achieved through virtual directories.
- **Identity Lifecycle Management:** Identity lifecycle management provides the mechanisms for creation, modification and deletion of user identity and associated account information across the target systems and applications. Often referred to as Joiners, Movers and Leavers (JML) process, identity lifecycle management offers inclusive support for all identity related events either through available connectors for automated provisioning/ de-provisioning or use of workflows for manual intervention. Management of user accounts and access entitlements across a multitude of IT systems including cloud-based applications is an increasingly important requirement for identity lifecycle management capability of the IGA tools today.
- **Password Management:** Self-service password management allows for password resets and user account recovery in case of forgotten passwords on the target systems and applications. Password synchronization ensures that password changes are successfully propagated and committed across all required systems. Progressive IGA vendors offer risk-appropriate identity proofing mechanisms in case of forgotten passwords for account recovery actions, in addition to multiple form factors of user authentication for initiating password changes.
- **Access Request Management:** The self-service user interface for users to request access to IT assets such as applications, databases and other resources. Access request management encompasses the entire process of delivering a user-friendly approach for requesting the access including searching for and selecting the desired resource from the available resource catalogue to browse the available hierarchy models available in the system and request access cloning. Shopping cart approach for searching and requesting access are becoming increasingly common to deliver better experience for users. Several vendors offer the flexibility of configuring workflows to allow for modification of access requests after the request submission and before actual fulfilment based on business process requirements.
- **Policy and Workflow Management:** Policy management offers the mechanism to deliver rule-based decision making based on pre-configured rules for identity lifecycle events such as account termination, role modification, exceptional approval, rights delegation and SoD mitigation. The enforcement of policies is either triggered by lifecycle events or determined by associated workflows. Workflow management is concerned with defining the necessary actions to be undertaken in support of a successful event execution or decision-making process. This includes orchestration of tasks involved in the overall decision-making process to support the business requirements. Workflow

management should allow for easy customizations to include common business scenarios such as approval delegations and escalations.

- **Role Management:** Role management delivers capabilities for managing access entitlements by grouping them based on relevant access patterns to improve administrative efficiency. The roles can be defined at several levels, most common being people, resource and application levels. The access patterns for logical grouping of entitlements can be derived with support of role mining capabilities of IGA tools delivered as part of role management. Role governance, a critical capability within broader Access Governance, encompasses basic role management as part of the overall role lifecycle management.

Access Governance:

- **Identity Analytics & AI/ML:** Identity analytics & AI/ML uses data analytic, and machine learning techniques to derive meaningful information out of the enormous logging and auditing information generated by the systems with an objective to enhance the overall efficiency of IGA processes in an organization. This includes recommendations for efficient use of roles, risk-based mitigation of access policy violations, automated access reviews, and even correlation of identity events across disparate systems to derive actionable intelligence. Identity analytics & AI/ML is fast becoming an important vehicle to achieve visibility into the operational state of IGA processes by analyzing the operational data generated by IGA tools to evaluate process maturity and adherence to service quality standards as well as compliance mandates. Identity analytics can also feed user access information from authentication and authorization events to AI/ML tools for prototyping user access behavior patterns and detecting anomalous access.
- **Access Certification:** Another key capability to gain an organization-wide visibility in the state of access across the multitude of devices, systems and applications including access to cloud-based applications. Access certification allows process and role owners to initiate on-demand or periodic access reviews to manage attestations that users only have the access rights necessary to perform their job functions. Access certification campaigns facilitate faster and accurate reviews of access by highlighting policy violations and permission conflicts in users\' access entitlements across multiple applications that are to be revoked or approved under listed exceptions. More commonly based on resource level or hierarchy requirements, access certification capabilities are increasingly becoming risk aware to include micro-certifications based on the risk of an identity lifecycle event. Unlike periodic access certifications, event based micro-certifications contribute significantly to continuous Access Governance capabilities of an organization.
- **Role Governance:** Role governance refers to the capability of having control of and visibility into a role's entire lifecycle, from its inception to decommission. In a typical role-based access control (RBAC) setting, role governance monitors and tracks the following key processes for governing the role lifecycle. IGA tools provide varied level of support for governing each of these role lifecycle events:

1. Role Definition - Defining a role based on the business functions and logically grouping the access entitlements based on the approved prototypes
2. Role Approval - The process of seeking consent of business, process or role owners including appropriate role analysis and tracking of approvals with associated workflows
3. Role Creation - Monitoring and auditing of tasks involved in implementation of approved roles in production
4. Role Assignment -- Performing SoD and other policy checks to ensure role assignment is compliant
5. Role Modification - Ensuring that changes made to existing roles are approved, tracked and do not introduce new risks
6. Role Optimization - Using intelligence from identity analytics for identifying inefficient use of roles and approval processes and implement measures to optimize roles to improve the efficiency of user access administration.

- **SoD Controls Management:** Segregation of Duties (SoD) Controls Management refers to the controls that are important to identify, track, report and often mitigate SoD policy violations leading to substantial risks of internal fraud in an organization. These controls are essential to manage role-based authorizations across applications with complex authorization model. However, IGA controls provide more course-grained abilities to identify SoD risks than at a fine-grained entitlement level found in other complex homegrown applications, especially ERP solutions. Key controls that are offered as part of SoD controls management include cross-system SoD risk analysis, compliant user provisioning, emergency access management, advanced role management, access certifications with SoD analysis, transaction monitoring and auditing and reporting.
- **Reporting and Dashboarding:** This refers to creation of valuable intelligence in formats that are easily ingestible by business functions for the purposes of enhancing governance and supporting decision making. Reporting is facilitated by in-built reports with provisions provided for customized reporting. Dashboarding is an important auditing control that allows for easy and business-friendly abstraction of metrics and data modelling to monitor effective operation of IGA processes. IGA vendors offer in-built templates for reporting with the ability to customize reporting to suite business's auditing and reporting objectives. Most vendors allow for IGA data export using specified industry formats into third-party reporting and analytics tools for advanced data modelling and business intelligence. For the purpose of evaluation of reporting and dashboarding capabilities of IGA vendors in this Leadership Compass, besides common reporting using in-built templates, we look at the ability of vendors to provide the breadth and flexibility of data model for customized reporting as well as the dashboarding capability to support complex and granular data metrics for easy interpretations.

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

- **User Experience (UX):** UX is an important aspect of IGA for security and IAM leaders trying to bridge the gap between the inconvenience of security controls and demand for enhanced user engagement through self-service options. Traditional IGA controls are overladen with several inefficiencies including poor design of user and admin interfaces that prevent easy understanding and completion of common IGA tasks. There is an increased need for organizations to ensure that IGA tools support their UX goals. Most vendors have significantly re-engineered their user interfaces to support better UX, a shopping cart paradigm for requesting access being the most common approach today. Many others are offering mobile support for common IGA tasks such as access requests, password resets and request approvals.
- **Automation support:** Automation of common IGA tasks has always been a priority for organizations to reduce the inaccuracy and administrative inefficiency encountered by manual completion of IGA tasks in the direction of making IGA operations leaner and achieve lower TCO. Most IGA tools provide support for automated provisioning and fulfilment leading to basic automation of IGA requirements. Some organizations have advanced requirements for automation such as automated access reviews and event-driven access certifications. While some vendors have started to support these capabilities, IAM leaders must ensure the right mix of manual and automated IGA processes to ensure the effectiveness of processes is preserved by continuously monitoring them against defined key performance indicators (KPIs).
- **Ease of deployment:** A lack of skillset combined with complexity of IGA deployments has led organizations to seek external help and actively engage IAM professional service providers to help with deployments. This can increase the overall TCO of IGA deployments by nearly three folds during the initial years of your IGA deployment. It is important that IGA vendors allow for easy deployment approach for organizations to help manage with available internal resources. Besides underlying software design, IGA products should allow for easy customizations using common scripting languages as well as offer support for configuration and change management. This includes availability of features that help organizations reduce environment-based configurations such as support for DevSecOps and scripted deployments. We also evaluate ease of product upgrades along with the ease of configuring the product for operational requirements such as high availability, automated failover and disaster recovery.
- **Third-party Integrations:** IGA products are required to integrate with several other enterprise products and applications to deliver the expected business value. Most common integrations with IGA products as evidenced in the market are integrations with:

1. IT Service Management (ITSM) tools, primarily ServiceNow, to essentially offer a common front-end for users to request access and other help-desk related tasks

2. Unified Endpoint Management (UEM) tools to make IGA tasks accessible on mobile devices and even extending mobile Single Sign-On to IGA
3. Privileged Access Management (PAM) tools to offer emergency access management for complex authorization model applications and for privileged Access Governance
4. User Behavior Analytics (UBA) tools to help organizations establish a baseline of user behavior with feeds from identity analytics and detect anomalous behavior.
5. Data Governance (DG) tools to extend standard IGA controls to data and information stored across multitude of systems including device endpoints, file shares, network mounts etc.

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

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

1.3 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.

1.4 Required Capabilities

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

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

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

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

- Business-friendly user interface
- Strong and flexible delegation capabilities

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

- Connectivity
  The ability to connect to various sources of target systems, including direct connections, integration with existing Identity Lifecycle Management tools from various vendors, and integration to ITSM (IT Service Management) or Helpdesk ticketing tools. In general, we expect Access Governance solutions of today to not only read data from target systems but also initiate fulfilment and reconcile changes.
- Heritage of connectors
  Having connectors as OEM components or provided by partners is not recommended and considered a risk for ongoing support and available know-how at the vendor.
- SRM interfaces
  We expect that systems provide out-of-the-box integration to leading ITSM systems for manual fulfilment of provisioning requests.
- SPML/SCIM support
  Support for SCIM (System for Cross-domain Identity Management) is preferred over traditional SPML (Service Provisioning Markup Language) for federated as well as on-prem provisioning. However, we evaluate support for both the standards depending on specific use-cases.
- Deployment models
  Supporting multiple delivery options such as hard/soft appliances and optional MSP services gives customer a broader choice.
- Customization
  Systems that require little or no coding and that support scripting or, if programming is required, SDKs or support for a range of programming languages, are preferred. We here also look for transport mechanisms between IT environments (e.g., development, test, and production), and the ability of keeping customizations unchanged after upgrades.
- Mobile interfaces
  Secure apps providing mobile access to certain key capabilities of the product such as access request approvals etc.
- Authentication mechanisms
  We expect IGA products to support basic authentication methods but use of multi-factor authentication methods to limit the risk of fraud using these systems is considered an advantage.

Secure but simplified access for business users takes precedence.

- Internal security model
  All systems are required to have a sufficiently strong and fine-grained internal security architecture.

- High Availability
  We expect IGA products to provide built-in high-availability options or support for third-party HA components where required.

- Ease of Deployment
  Complexity of product architecture and its relative burden on time to deploy as well as configuration and integration of basic services such as authentication, single sign-on, failover and disaster recovery should be minimal.

- Multi tenancy
  Given the increasing number of cloud deployments, but also specific requirements in multi-national and large organizations, support for multi-tenancy is highly recommended.

- Shopping cart paradigm
  These approaches are 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.

- Data Governance
  Support for Data Governance, i.e., the ability to ensure access to data assets is controlled (roles, policies) and assist organizations with data compliance regulations.

- Role/SoD concept
  Should be able to analyze enterprise as well as application roles for inherent SoD (Segregation of

Duty) risks and continuously monitor for new SoD risks being introduced and offer remediation measures

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

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
- Overall Leaders are (in alphabetical order):

2.1 Overall Leadership

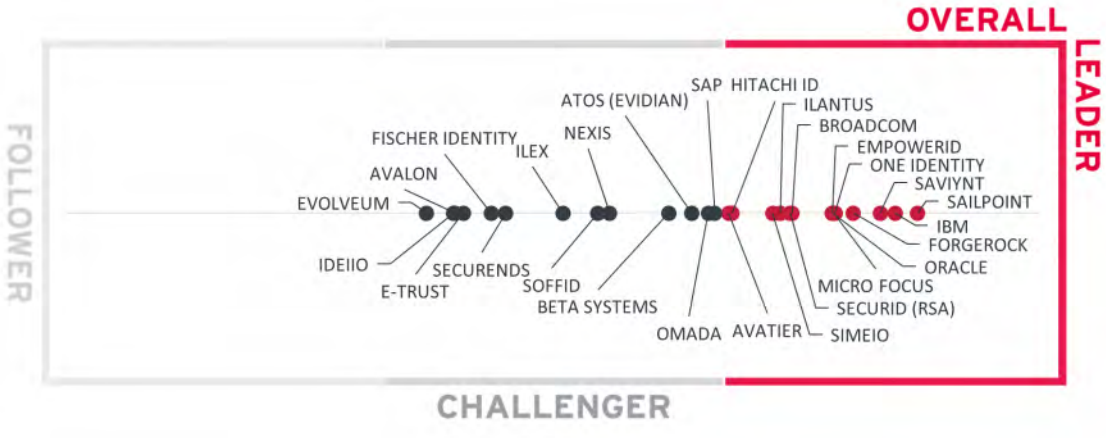


Figure 2: The Overall Leadership rating for the IGA market segment

When looking at the Leader segment in the Overall Leadership rating, we see a picture that is a typical representation of very mature markets, where a considerable number of vendors deliver feature-rich solutions. The market continues to remain crowded, with 28 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 declined participation in this year's edition.

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

Other vendors in the Overall Leaders segment for IGA include Broadcom, SecurID, Ilantus, Simeio, Hitachi ID, and Avatier. This group of vendors is a mix of established and emerging players, some being stronger in their market position, and others with a considerable push into the Overall Leader segment with their improved ratings for product, market, and innovation evaluation criteria.

The Challenger segment is less populated than the Leaders segment and features established vendors, vendors frequently being more regional-focused, and several niche vendors with fit-for-purpose IGA capabilities and preferred by many organizations over the established players. Leading in this segment are SAP, Omada, Atos (Evidian), and Beta Systems. Nexis, Soffid, and Ilex follow with some distance. Further vendors in this segment are SecurEnds, Fischer Identity, E-Trust, Avalon, ideiio, and Evolveum. The Challenger segment show vendors with good products with varying levels of IGA capabilities, market presence throughout the world, or other market niche focus.

Overall Leaders are (in alphabetical order):

- Avatier
- Broadcom
- EmpowerID
- ForgeRock
- Hitachi ID
- IBM
- Ilantus
- Micro Focus
- One Identity
- Oracle
- SailPoint

- Saviynt
- SecurID
- Simeio

2.2 Product Leadership

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

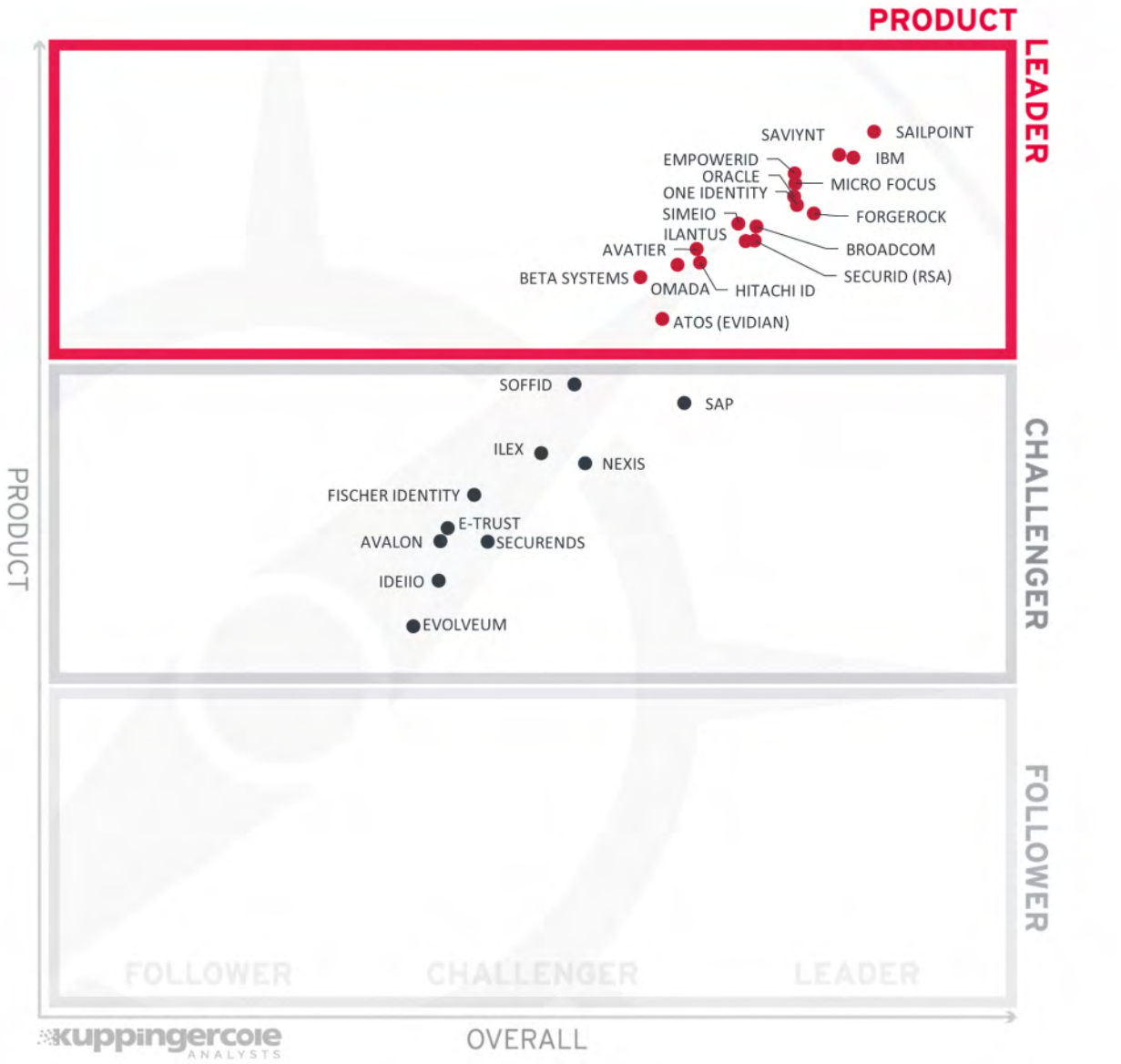


Figure 3: Product Leaders in the IGA market segment

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

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

Leading from the front in Product Leadership is SailPoint, closely followed by Saviynt and IBM. EmpowerID takes a position in the upper range of the Leader's segment, followed by a group of vendors including Micro Focus, Oracle, One Identity, ForgeRock, Broadcom, Simeio, Ilantus, SecurID, Avatier, Omada, and Hitachi ID, all of which deliver leading-edge capabilities across the depth and breadth of IGA capability spectrum evaluated for the purpose of scoring the vendors in this Leadership Compass. IAM leaders must exercise appropriate caution while evaluating these vendors as subtle differences ignored in functionality evaluation of these products could translate into greater incompatibilities for business processes during implementation. Therefore, it is highly recommended that organizations spend considerable resources in properly scoping and prioritizing their IGA requirements prior to IGA product evaluation. Beta Systems is positioned next as Leader in the product leadership segment, trailing the others from a close distance in the completeness of product leadership qualities. Atos (Evidian) appears near the bottom border of the Product Leadership segment.

In the challenger's segment of product leadership are (in alphabetical order) Avalon, E-Trust, Evolveum, Fischer Identity, Hitachi ID, ideiio, Ilex, Nexis, SAP, SecurEnds, 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.

Product Leaders (in alphabetical order):

- Avatier
- Beta Systems
- Broadcom
- EmpowerID
- Atos (Evidian)
- ForgeRock
- Hitachi ID
- IBM
- Ilantus
- Micro Focus
- Omada
- One Identity
- Oracle
- RSA Security
- SailPoint

- Saviynt
- Simeio

2.3 Innovation Leadership

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

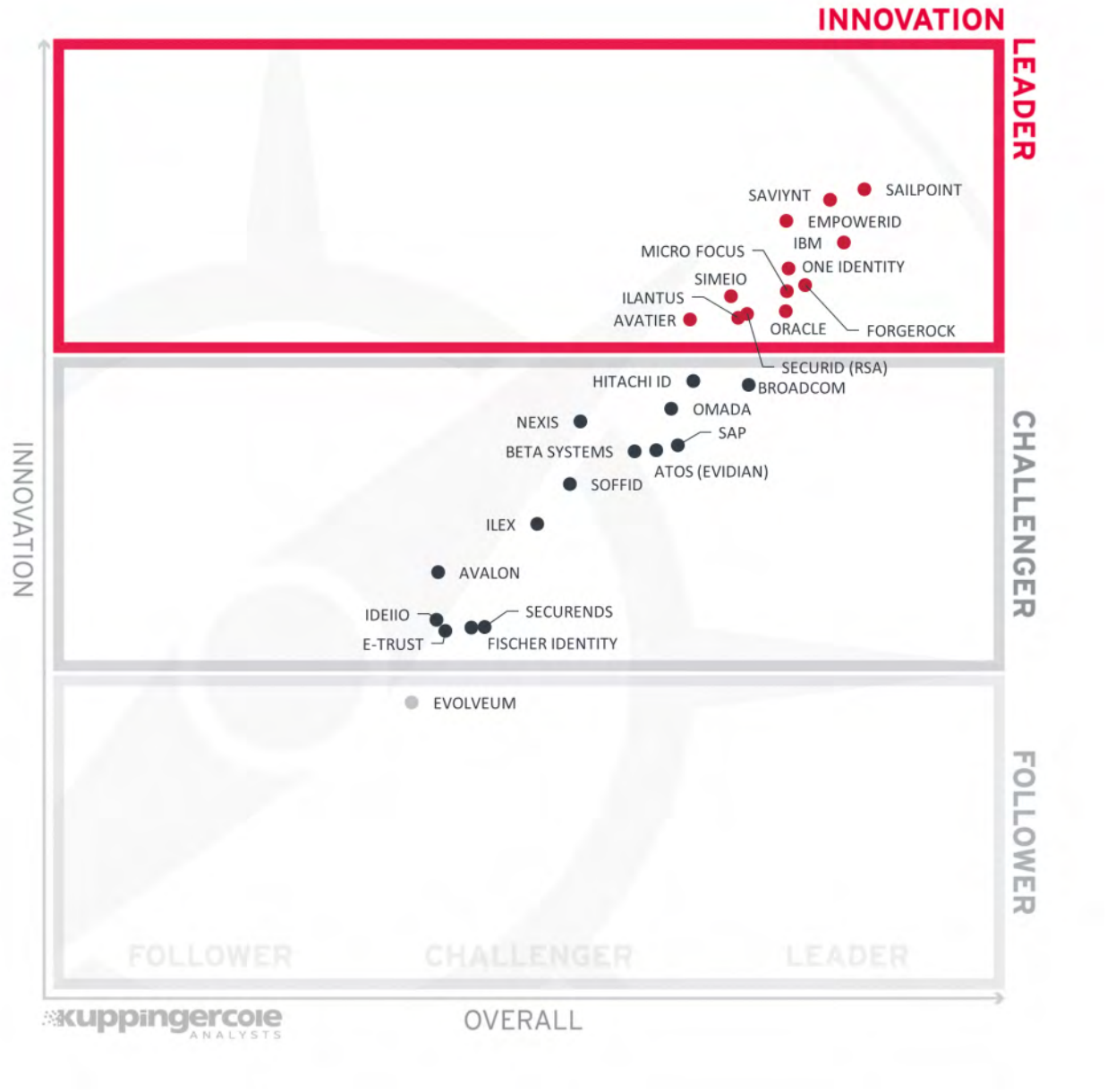


Figure 4: Innovation Leaders in the IGA market segment

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

predictive and other forms of analytics.

The graphic needs to be carefully read when looking at the Innovation capabilities, given that the x-axis indicates the Overall Leadership while the y-axis stands for Innovation. Thus, while some vendors are closer to the upper-right edge, others being a little more left score slightly higher regarding their innovativeness.

SailPoint continues to lead the Innovation Leadership evaluation, which is very closely followed by Saviynt, then by (in alphabetical order) EmpowerID, ForgeRock, IBM, Micro Focus, One Identity, and are next on the chart and continue to strengthen their IGA leadership position with constant innovation. Ranked next (in alphabetical order) are Avatier, Ilantus, Oracle, SecurID, and Simeio, making significant changes to their IGA product portfolio to be in line with other innovative vendors in the market. These vendors differ in many details when it comes to innovation and balancing it with overall product leadership. Therefore, a thorough vendor selection process is essential to pick the right vendor of all the IGA players that best fit the customer requirements.

About half of the players made it to the Innovation Challenger segment that includes Hitachi ID and Broadcom near the upper border. Another group of vendors in the upper mid-section (in alphabetical order) are Beta Systems, Atos (Evidian), ideiio, Ilex, Nexis, Omada, SAP, and Soffid. All these vendors have also been able to demonstrate promising innovation in delivering specific IGA capabilities. Another group of vendors appears in the lower half of the Challenger segment: (in alphabetical order) Avalon, E-Trust, Fischer Identity, and SecurEnds. 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
- EmpowerID
- ForgeRock
- IBM
- Ilantus
- Micro Focus
- One Identity
- Oracle
- SailPoint
- Saviynt

- SecurID
- Simeio

2.4 Market Leadership

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

Figure 5: Market Leaders in the IGA market segment

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

With a strong market position, successful execution, and strengthened IGA product features, IBM, ForgeRock, SailPoint, and Oracle are set to lead the Market Leadership evaluation from the front. Closely following these vendors in the Market Leadership segment are (in alphabetical order) Broadcom, Ilantus, Micro Focus, One Identity, SAP, Saviynt, and SecurID. Both EmpowerID and Atos (Evidian) appear near the

bottom border. All vendors in this segment have several deep-rooted complex IGA deployments across multiple industries.

In the Challenger section, we find Simeio and Hitachi ID 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 as examples. Following this group (in alphabetical order) is Avatier, Beta Systems, Evolveum, Fischer Identity, Ilex, Nexis, Omada, SecurEnds, Soffid, near the center. E-Trust, and ideiio appear close to the bottom border.

In the Follower segment, we find Avalon - 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
- EmpowerID
- Atos (Evidian)
- ForgeRock
- IBM
- Ilantus
- Micro Focus
- One Identity
- Oracle
- RSA Security
- SailPoint
- SAP
- Saviynt
- SecurID

3 Correlated View

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

3.1 The Market/Product Matrix

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

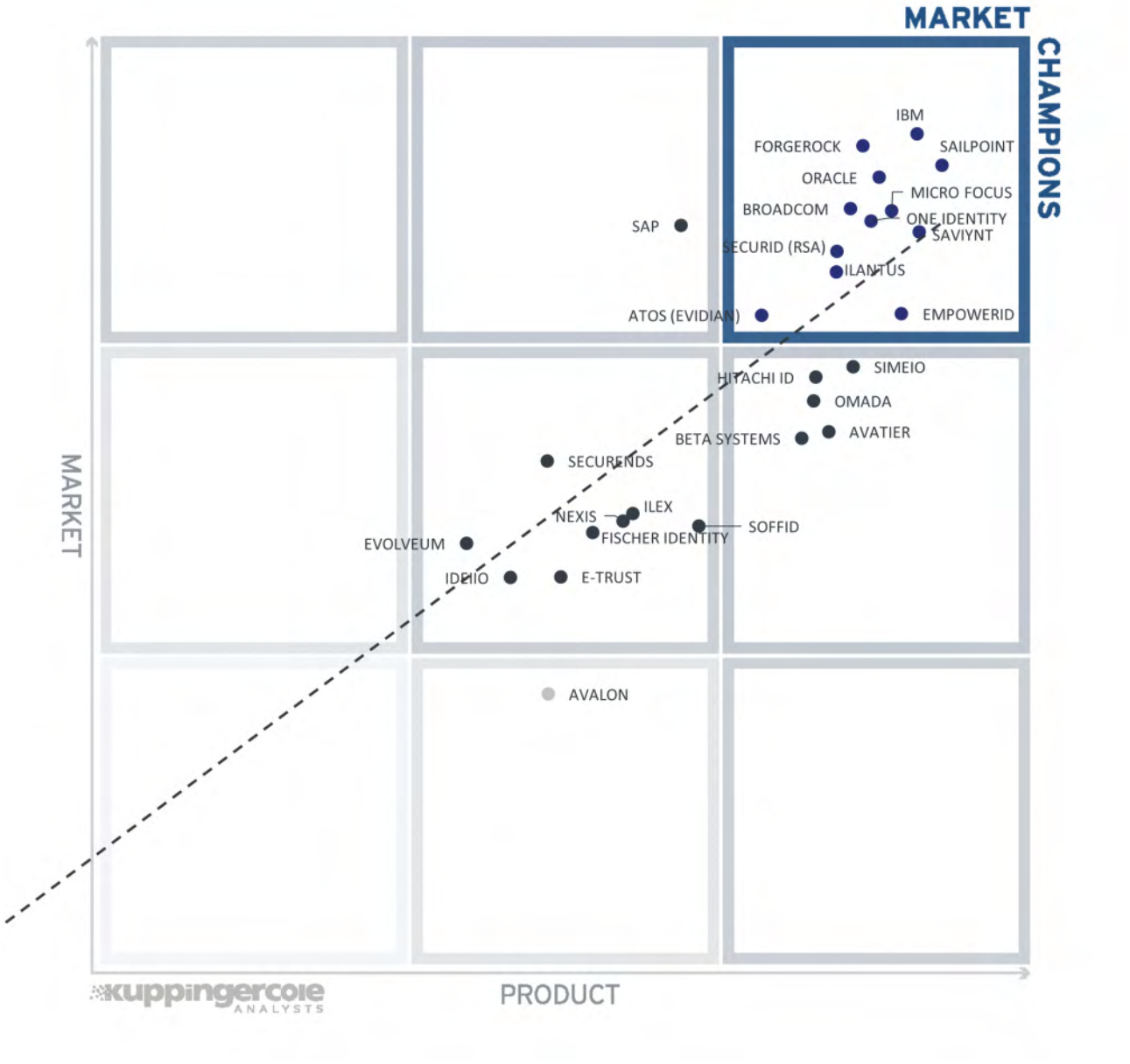


Figure 6: The Market/Product Matrix.

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

In this comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of "overperforming" in the market. All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

In the upper right segment, we find the "Market Champions." Given that the IGA market is maturing fast, we find IBM, ForgeRock, SailPoint, and Oracle 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 (in alphabetical order) Broadcom, Ilantus, Micro Focus, One Identity, Saviynt, and SecurID. Atos (Evidian) and EmpowerID appear near the bottom border. Being positioned closer to the axis, Ilantus represents a slightly better balance of market vs. product leadership. EmpowerID is positioned under the axis representing their inclination for stronger product leadership in comparison to the market leaders today.

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

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

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

Finally, in the bottom middlebox is the remaining vendor, Avalon, 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 7: The Product/Innovation Matrix.

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

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

Looking at the Technology Leaders segment, we find most of the leading vendors in the upper right corner,

scattered throughout the box. The top-notch vendor is SailPoint, closely followed by Saviynt and the remainder (in alphabetical order) Avatier, EmpowerID, ForgeRock, IBM, Ilantus, Micro Focus, One Identity, Oracle, SecurID, and Simeio - with most placing close to the axis depicting a good balance of product features and innovation.

In the top middlebox, we see Broadcom, Hitachi ID Omada, Beta Systems, and Atos (Evidian) with slightly less innovation than the leaders in this section but still have a good product feature set.

In the center middlebox, we find (in alphabetical order) Avalon, E-Trust, Fischer Identity, ideiio, Ilex, Nexis, SAP, SecurEnds, and Soffid having less product and innovations than the Technology Leaders.

Evolveum appears in the leftmost middlebox, indicating less innovation but some product strength.

3.3 The Innovation/Market Matrix

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

Figure 8: The Innovation/Market Matrix.

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

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

In the upper right-hand corner box, we find the "Big Ones" in the IGA market. We see the large ones more on top, including (in alphabetical order) IBM, Ilantus, ForgeRock, Micro Focus, One Identity, Oracle,

SecurID, SailPoint, and Saviynt. EmpowerID is placed in the same box, more towards the bottom, indicating that they haven't yet reached the same market position as the established players.

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

In the middle top box, we find Broadcom, SAP, and Atos (Evidian), 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 leadership, which includes (in alphabetical order) Beta Systems, E-Trust, Fischer Identity, Hitachi ID, ideiio, Ilex, Nexis, Omada, SecurEnds, and Soffid.

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

Finally, Evolveum is placed in the left-most middlebox, indicating their relatively weak innovativeness than market position.

4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Fraud Reduction Intelligence Platforms. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

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

Product	Security	Functionality	Interoperability	Usability	Deployment
Avalon Solutions 360 singular_id	○	○	◐	○	◐
Avatier Identity AnyWhere	●	○	●	●	○
Beta Systems Garancy IAM Suite	●	●	●	●	○
Broadcom Symantec Identity Governance and Adminstration (IGA)	●	●	○	●	○
E-Trust Horacius	○	○	◐	○	○
EmpowerID IAM Suite	●	●	●	●	○
Evidian IGA, Evidian A&I	●	○	○	●	○
Evolveum midPoint	○	◐	◐	◐	◐
Fischer Identity Suite	○	○	○	●	◐
ForgeRock Identity Governance	●	○	●	○	●
Hitachi ID Bravura Identity	●	●	●	○	●
IBM Security Verify Governance	●	●	●	●	●
ideiio IGA	○	○	◐	○	◐
Ilantus Compact Identity	●	○	●	●	○
Ilex Meibo People Pack (MPP)	●	○	○	○	◐
Micro Focus NetIQ IGA Suite	●	●	○	●	●
Nexis Controle	○	○	◐	●	○
Omada Identity	●	○	○	●	○
One Identity Manager	●	●	●	●	●
Oracle Identity Governance	●	●	○	●	●
SailPoint Identity PLatform	●	●	●	●	●
SAP Access Control & Identity Access Governance	●	○	○	○	○
Saviynt Enterprise IGA	●	●	●	●	●
SecurEnds Credential Entitlement Management	○	○	◐	○	○
SecurID Governance & Lifecycle	●	●	●	●	○

Product	Security	Functionality	Interoperability	Usability	Deployment
Simeio Identity Orchestrator	●	●	●	●	●
Soffid IAM	●	●	●	●	●
Legend		● critical	● weak	● neutral	● positive ● strong positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Avalon Solutions 360	neutral	weak	neutral	weak
Avatier	positive	neutral	positive	neutral
Beta Systems	positive	neutral	positive	neutral
Broadcom Inc.	positive	positive	strong positive	strong positive
E-Trust	neutral	weak	neutral	neutral
EmpowerID	strong positive	positive	positive	positive
Evidian (was acquired by Atos)	positive	positive	strong positive	positive
Evolveum	weak	neutral	neutral	neutral
Fischer International Identity	neutral	weak	positive	neutral
ForgeRock	strong positive	strong positive	positive	strong positive
Hitachi ID Systems	positive	positive	positive	positive
IBM	strong positive	strong positive	strong positive	strong positive
ideiio	neutral	weak	neutral	neutral
Ilantus Technologies	positive	positive	positive	positive
ILEX International	positive	neutral	positive	neutral
Micro Focus	positive	positive	strong positive	strong positive
Nexis	positive	neutral	positive	neutral
Omada	positive	neutral	neutral	positive
One Identity	positive	positive	positive	strong positive
Oracle	strong positive	positive	strong positive	strong positive
SailPoint	strong positive	strong positive	strong positive	strong positive
SAP	positive	positive	strong positive	strong positive
Saviynt	strong positive	strong positive	positive	strong positive
SecurEnds	neutral	neutral	positive	positive
SecurID	positive	neutral	strong positive	strong positive
Simeio Solutions	strong positive	positive	positive	positive
Soffid	positive	weak	neutral	positive
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

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

Spider graphs

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

Identity Lifecycle Management The ability to provision and manage identities, access entitlements, and other identity-related information in the target systems over its lifecycle. Also, other capabilities considered, among others, is the ability to access identity stores, data modeling & mapping, as well as the ability to handle different identity types.

Target System Support Considered are the number of connectors and the breadth of target systems that the solution can connect to, including, e.g., directory services, business applications, mainframe systems, etc. Connector breadth also looks at support for standard cloud services. Connector depth further examines customization capabilities for connectors through connector toolkits and standards as examples and the connectors\' abilities, especially when it comes to connecting to complex target systems such as SAP environments or mainframes.

Self-Service & Mobile Support User self-service interfaces and support for secure mobile access to selected IGA capabilities.

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.

Architecture & Hybrid Environment This category represents the combination of architecture and hybrid environment support. In architecture, we look at the type of architecture and focus on modern, modular architectures based on microservices. This also affects deployment, given that container-based deployments provide good flexibility. Also evaluated is the solution\'s ability to support a hybrid environment for customers that anticipate or are currently taking an intermediate step towards migrating from on-premises to the cloud.

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 Avalon Solutions 360

Established in 2010, Avalon Solutions 360 is a privately held Mexican software company specializing in IAM and Governance solutions. singular_id is its primary product capable of providing IGA, PAM, and DAG features within a suite. Avalon Solutions 360 customers include the telecommunications, banks, and express mail services.

Singular_id provides good Identity Lifecycle Management support and out-of-the-box provisioning connectors for most popular on-premise systems, although less out-of-the-box support for SaaS systems. Attribute mapping scripting language supports Bean shell and Java. Out-of-the-box ITSM integration supports ServiceNow. Administration and user self-service access allows for username/password and FIDO authentication options only.

Access review and review support includes good access certification and event and micro based recertification such as access risks, SoD violation, and outliers as examples. Singular_id gives automated identity data mining capabilities to assist with the assignment of accounts, eliminate duplicates or orphan account, data inconsistences and anomaly detection. Singular_id gives a colorful and functional governance viability though dashboards and reporting with unique layouts, graphs, tables and graphical workflows. Out-of-the-box support for major compliance frameworks are available.

Singular_id can be deployed either on-premise, private cloud, or public cloud. For cloud delivery, full multi-tenancy is not given. A hybrid deployment module is not given. The product can be delivered as software deployed to a server, or virtual. A managed service is also possible on customer premises. Singular_id is architected as a modular system with a data integration layer that supports REST APIs, SCIM for third-party integrations, as well as standard enterprise data sources such as directories, databases, and ERP as examples. Availability of a developer portal, product SDKs, and CLIs are not available.

Avalon Solutions 360 serves mid to enterprise organization in the Latin American region. Its singular_id give good Identity Lifecycle Management and Access Governance with some unique and interesting governance visibility features. Although, there are some limitations with deployment options, authentication and DevOps support, singular_id is a good consideration for organizations looking for IGA solutions in Latin American region.

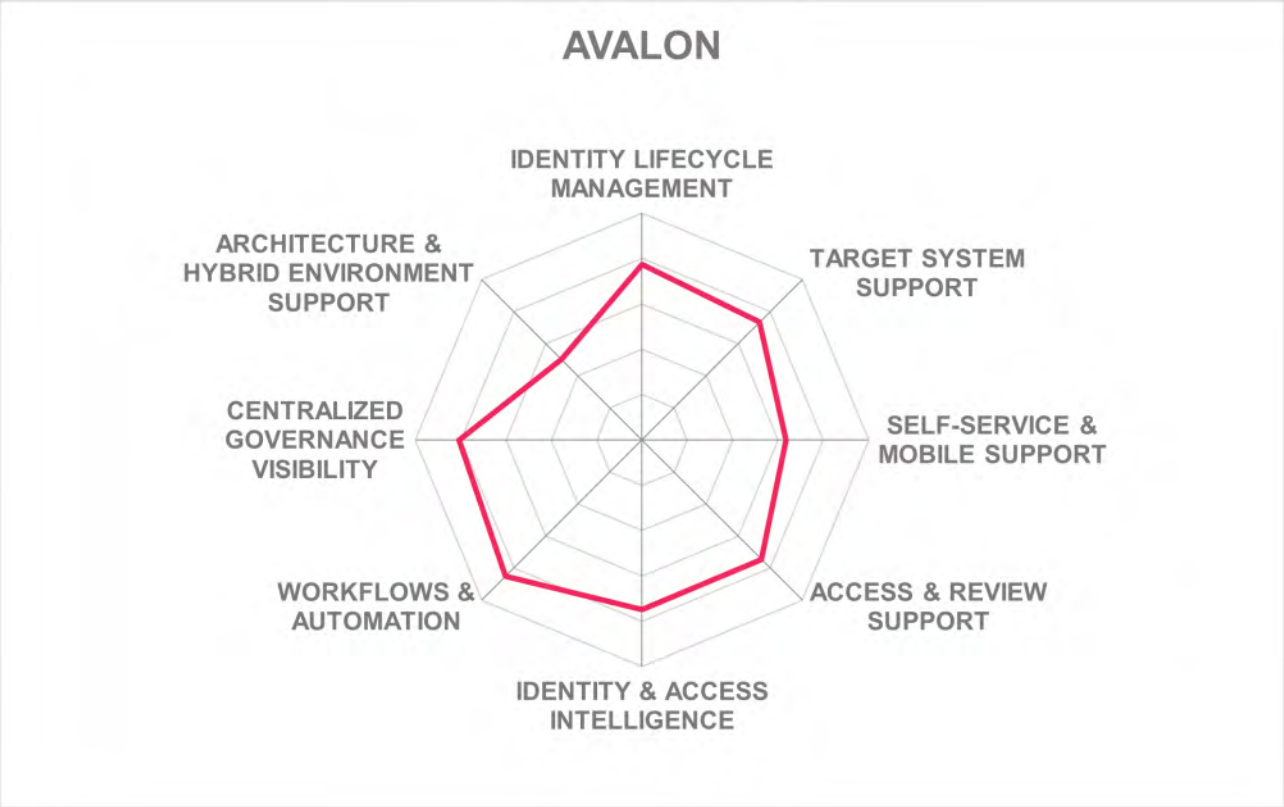
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●○○

Strengths

- Identity Lifecycle Management
- Target system support
- Access and review support
- Identity and access intelligence
- Workflow and automation
- Centralized governance visibility
- Good reporting capabilities

Challenges

- Customer base mostly concentrated in Latin America
- Small partner ecosystem
- Limited authentication options to admin and user self-service access
- On-prem or cloud deployment options without a hybrid option
- Limited DevOps support


AVALON
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.2 Avatier

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

Identity Anywhere comprises several modules providing a range of IGA functionality. Lifecycle Management is its primary Identity Provisioning component and Group Automation/Self-Service, Workflow Manager, and Identity Analyzer supporting the Access Governance capabilities. Avatier supports both SPML and SCIM for identity provisioning/de-provisioning and has a broad set of provisioning connectors available for a wide range of on-premises and cloud systems.

Avatier delivers a solution with an impressive 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 challenge advanced governance requirements of complex IAM deployments. However, the focus on simplification of user interfaces offers a great abstraction of governance features for business users who are commonly unacquainted with technical details. Although Avatier offers a good drill-down of governance details, it currently does not provide a single pane dashboard, although it\'s on the roadmap. Also provided is well thought out self-service capabilities using a shopping cart paradigm allowing users to request access to systems and allowing managers\' ability to approve or reject requests via mobile or other communication channels.

Identity Anywhere supports 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. The Identity Anywhere platform is a single container that can support the most popular container platforms and while leveraging microservices for supplemental functionality. Both the Identity Anywhere Agent or Docker container deployed on-premises can support a hybrid environment. Hardware and virtual appliances for on-premises deployment options are not available. SOAP, REST, SCIM, SAML, and OAuth API protocols are supported. A wide range of popular programming language SDKs for developers is also. The majority of Identity Anywhere functionality is accessible via REST APIs as well as some functionality via CLI.

Avatier is a privately held company that focuses on mid-market to enterprise organizations with customers and partner ecosystems located primarily in North America with growth in other regions. Avatier continues to innovate with its user-centric approach to IGA that covers a wide range of governance use cases. Overall, Avatier's Identity Anywhere container-based platform is an improvement in the IGA market. Organizations across the industry verticals seeking a solution to traditional IGA deployment challenges should consider Avatier's Identity Anywhere.

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

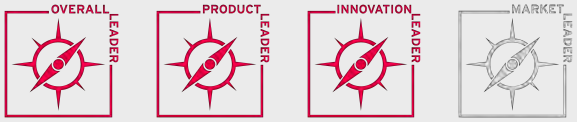
Strengths

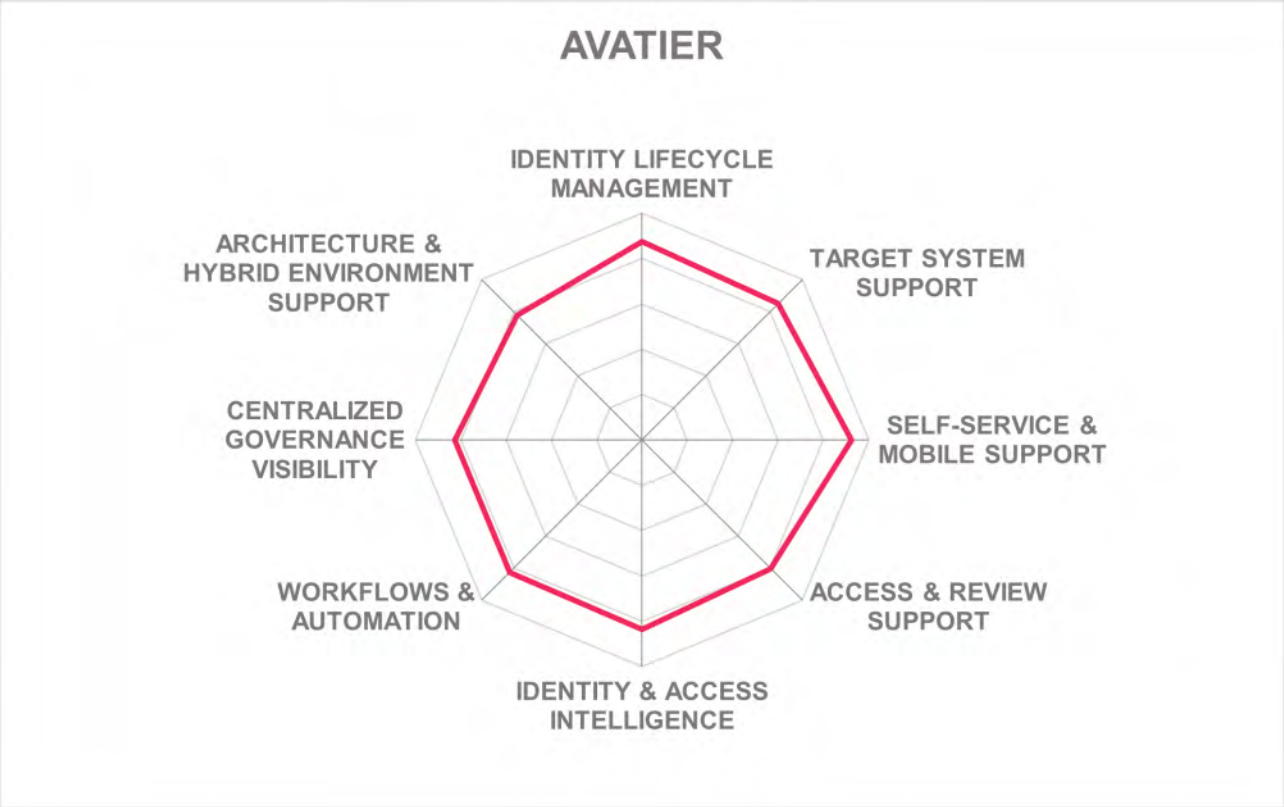
- Fully containerized IGA platform
- Innovative, user-centric approach to IGA
- Good target system support
- Flexible workflow automation capabilities
- Good reporting capabilities

Challenges

- A growing but limited partner ecosystem
- A limited footprint outside of North America
- Limited marketing visibility
- Missing single pane dashboard of governance, although on short term roadmap

Leader in




AVATIER
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.3 Beta Systems

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

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

Beta Systems supports on-premises, cloud, and hybrid deployments and can deliver its solution as SaaS, virtual appliance, Docker container, or software deployed to a server. Future roadmap items include delivering a Docker container on Kubernetes and used for SaaS as well. For cloud delivery, full multi-tenancy is not supported. Almost all of the solution\'s functionality is accessible via SOAP or REST APIs, although SDKs are limited to the Java programming language. Also, no functionality is accessible via CLIs, and a developer portal is not available. Good support for self-service and administration authentication is given with more advanced MFA options.

Beta Systems is a mature and publicly list company. It serves primary mid to enterprise organizations with a market focus in the EMEA region and a somewhat small but growing and functional partner ecosystem. Garancy IAM Suite offers comprehensive and lightweight IGA capabilities for organizations looking to deploy IGA for on-premises or cloud-based systems quickly.

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

betasystems

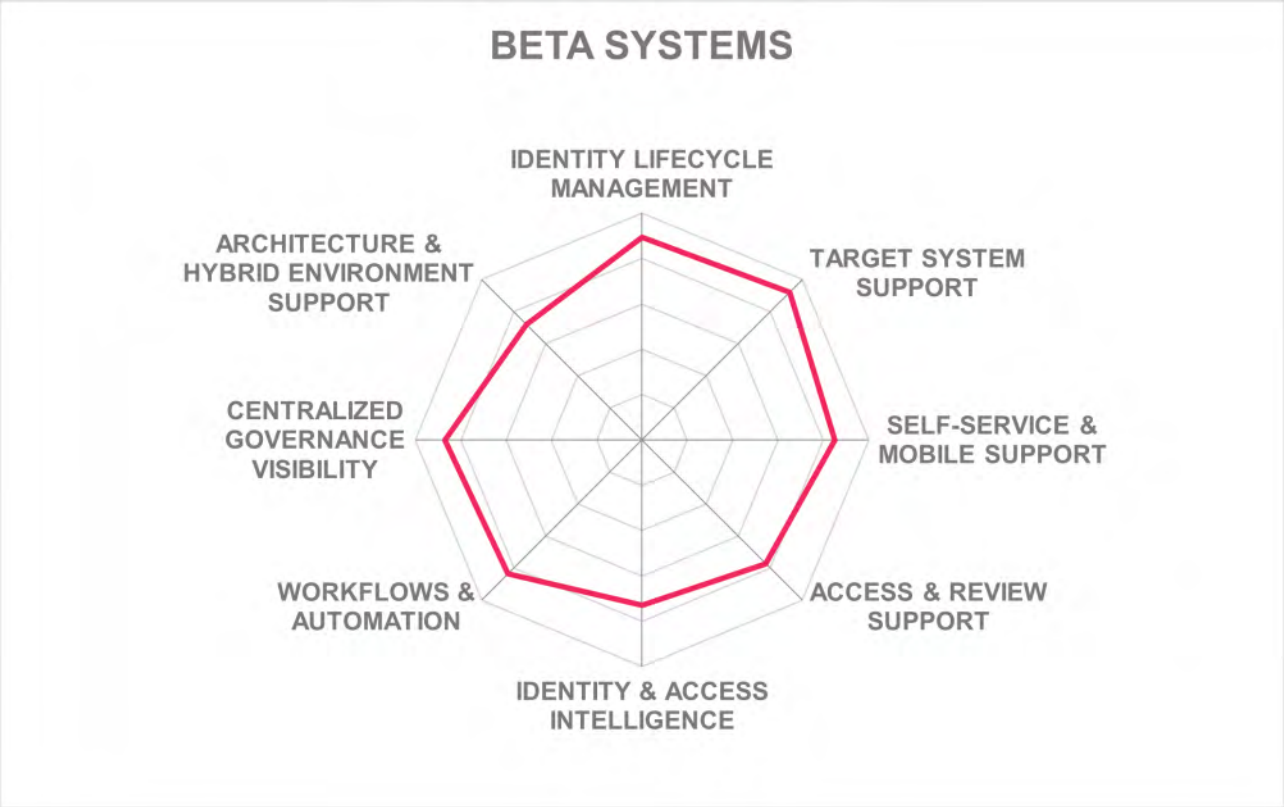
Strengths

- Identity lifecycle management
- Target system support
- Self-service support
- Good governance UI
- Workflow customization flexibility
- Support for Dynamic Authorization Management
- Granular Data Access Governance
- Dedicated mainframe environment support

Challenges

- Primarily focused in the EMEA region
- Somewhat small but growing functional partner ecosystem
- Some DevOps support limitation

Leader in


BETA SYSTEMS
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.4 Broadcom Inc.

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 expected from an established market player.

Broadcom has several large deployments of Symantec IGA globally as part of its Symantec portfolio of security products. The products, fully capable of operating in silos, offer a strong line-up of IGA capabilities, including user access certification, SoD, entitlement clean-up, role discovery, automated workflows and policy management, access certification. Also given are an access risk analyzer & simulator that can estimate a user's risk score based on the change in the context of an access request. Symantec IGA's UI is modern and user-friendly, making it productive for users given helpful context advice tools. Symantec provides an entitlement catalog and shopping cart approach to usability. However, features such as identifying and notifying potential SoD violations when selecting entitlement at shopping chart check-out are limited to SOD checks against current entitlements. Audit and compliance reporting is good, with some OOB reports for major compliance frameworks available. A wide selection of OOB integrations to ITSM tools is given, and authenticator options for user access to self-service functionality and admin UI.

Strong support for out-of-the-box provisioning/de-provisioning is given for on-premises and SaaS applications. 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 available. DevOps is aided via a UI that allows for the drag & drop of Symantec IGA services onto the virtual appliances and other machine resource indicators. The majority of admin and end-user functionality is supported via SOAP and REST APIs and support for SCIM 2.0. SDKs are also offered, including Android, iOS, Java, C/C++, JavaScript, and AngularJS programming languages.

Broadcom has a global presence and brings with it a large set of integration partners. Overall, Symantec IGA is progressively moving in a positive direction after the acquisition by Broadcom. However, there is still room to grow more advanced IGA features and deployment options for more modern DevOps environments. Still, Broadcom's Symantec IGA solution remains a mature and feature-rich product but may be more suitable for large complex IGA deployments.

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

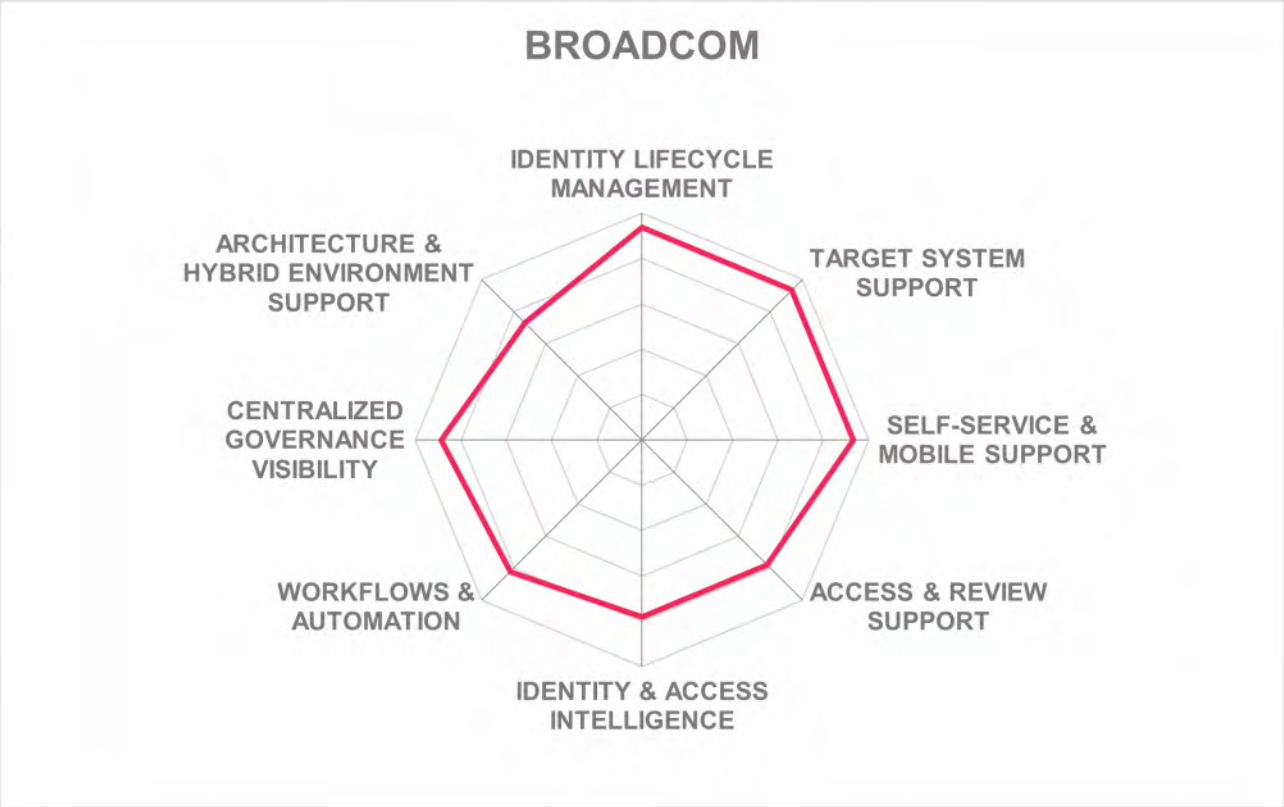
Strengths

- Identity lifecycle management
- Good OOB target system support
- Self-service & mobile support
- Workflows
- Modern & user-friendly UI
- Good reporting capabilities
- Good dashboard analytics
- Drag & drop service deployment tool

Challenges

- Limited product delivery options
- Customization is improving, although could easily grow complex and expensive
- Good shopping cart usability, although missing more advanced SoD violation identification at check-out
- Missing COTS PAM integration options other than Symantec PAM offering

Leader in


BROADCOM
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.5 EmpowerID

Founded in 2005 and based in Ohio (US), it provides multiple products in a suite and offers EmpowerID as its IGA product. The EmpowerID Identity and Access Management product suite includes Identity Lifecycle Management, Advanced Identity Lifecycle Management, Group Management, Dynamic Group Management, Password Management, Multi-factor Authentication, Risk Management, Advanced Risk Management, Access Recertification, Role Mining, Policy-Based Access Control (PBAC), Azure Identity Manager, Azure RBAC Manager, Virtual Directory (LDAP), Core Services: RBAC/ABAC/PBAC authorization, Workflow Engine, Audit & Reporting, and Identity Warehouse.

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

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

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

EmpowerID offers a comprehensive solution with strong IGA and access management capabilities. EmpowerID customers primarily reside in North America and the EMEA regions targeting mid to enterprise-

sized organizations. Its partner ecosystem can be considered small, with a concentrated focus in Europe. EmpowerID continues to modernize its platform for cloud-native containerized environments. Built on Microsoft technology, EmpowerID offers distinct integration and performance benefits for Microsoft-centric organizations. EmpowerID is a preferred choice for organizations looking for a comprehensive IGA solution with integrated access management features.

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

empowerID

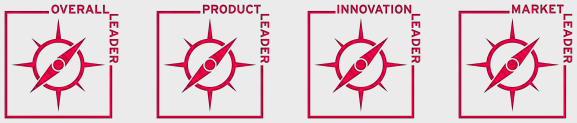
Strengths

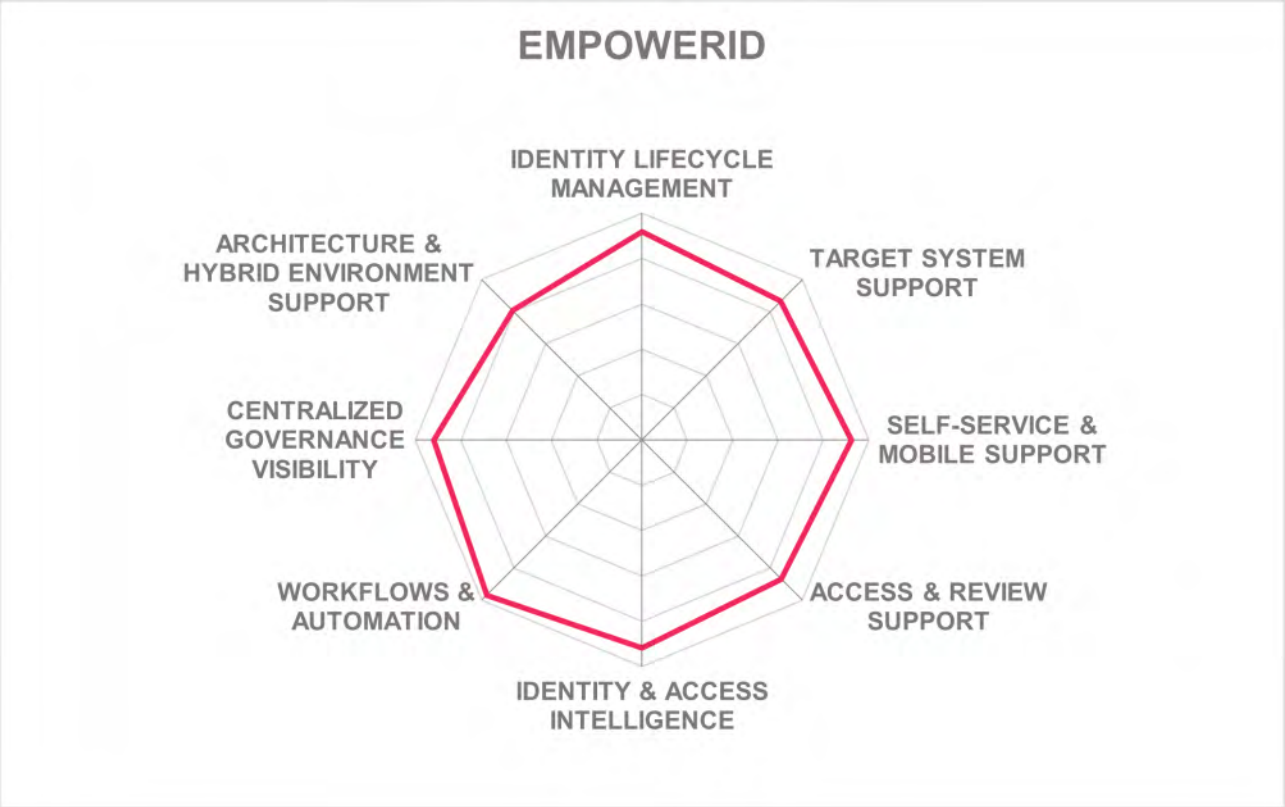
- Identity lifecycle management
- Good target system support
- Self-service and mobile support
- Access governance & review features
- Identity & access intelligence
- Strong workflow capabilities
- Modern and user-friendly UI
- Good API support

Challenges

- A small but selective partner ecosystem mostly concentrated across Europe
- Runs primarily on Microsoft platform for non-container deployments
- Missing some advanced IGA intelligence such as anomaly and outlier detection
- Missing more advanced recertification triggers for outliers

Leader in




EMPOWERID
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.6 E-Trust

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

E-Trust offers Horacius Identity & Governance as a common platform for identity provisioning and access governance. The Horacius platform is growing over time to become a mature product offering a spectrum of IGA and specific access governance functionalities. Horacius is capable of handling automated user provisioning, access reviews & attestations, orphan account monitoring, or employee and third-party contract termination use cases, as well as providing auto-discovery capabilities to identify accounts, groups, group memberships. Horacius supports a range of popular identity repositories as well as offering good breadth with some depth with out-of-the-box (OOB) connectors for on-premises systems, with less breadth regarding out-of-the-box connectors to SaaS systems. IGA policy management covers the majority of common use cases such as account termination, role modification, access exception approval, rights delegation, and SoD analysis and mitigation as a few examples, although policy authoring/editing and testing tools are not available OOB nor integration options to third-party policy tools or engine. Good support for OOB workflows that include registration, orphan account management, account request and review, and SoD, etc. are given. Access governance includes role discovery, but missing advance intelligence capabilities such as recommendations, risk scoring, anomaly or outlier detection, while access certification supports event-based micro certifications and triggers to recertify given a user's schedule, SoD violations, and organizational structure changes.

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

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 that supports Docker and rkt (Rocket) container-based platforms, SaaS, or as a managed service. 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. SPML is currently supported. With E-Trust\'s latest release, a SCIM compatible connector using REST JSON is given as well as SCIM compliant integrations with popular applications such as Azure SCIM API, Slack SCIM API, Facebook Workplace SCIM API, and others. No SDKs, CLI, or a developer portal for DevOps support are available at this time.

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

medium to mid-market, although making inroads into some enterprise-level businesses, within the Latin America region. E-Trust is a good fit for organizations with average access governance requirements to satisfy the most common identity lifecycle administration use-cases with customer-focused in the Latin American region.

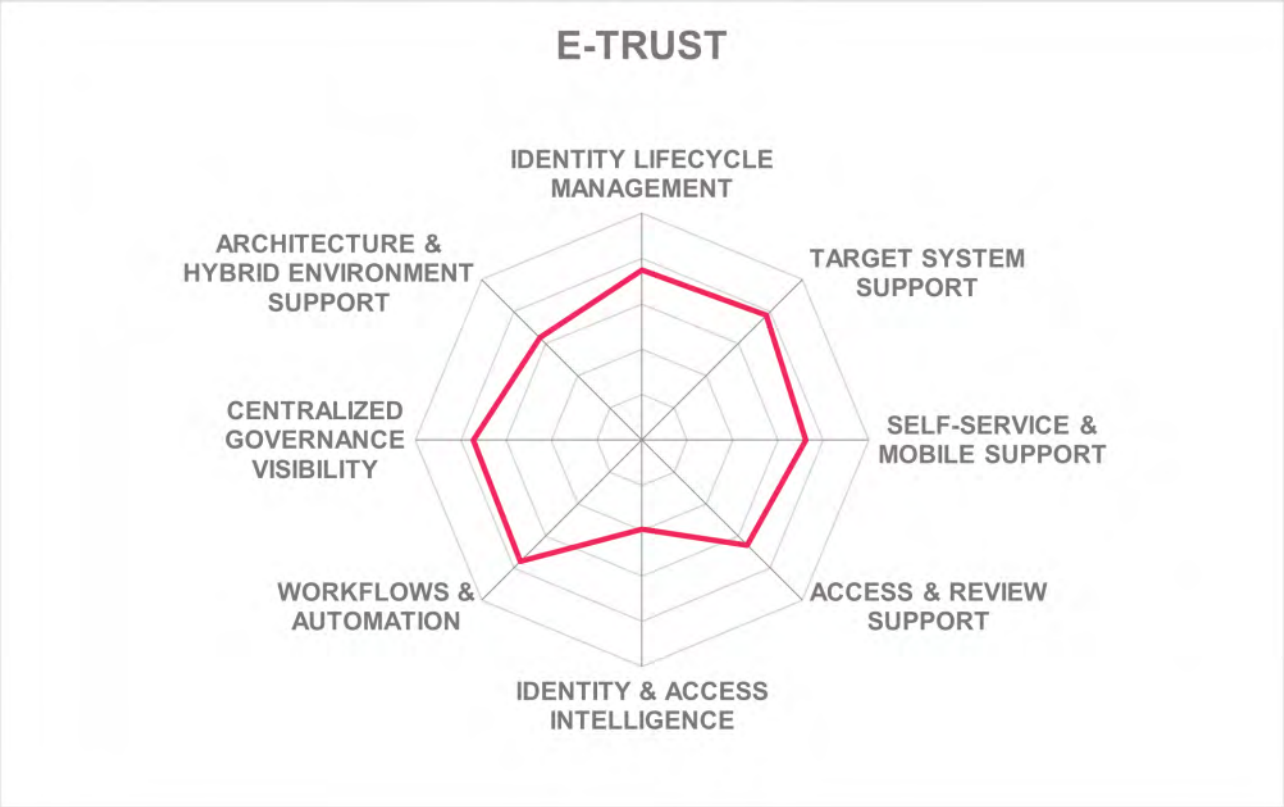
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●○

Strengths

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

Challenges

- Small partner ecosystem concentrated in South America
- Limited OOB identity & access intelligence
- Some limitations of OOB connectors to SaaS systems
- Missing DevOps support for SDKs and access to functionality via CLIs


E-TRUST
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.7 Evidian (was acquired by Atos)

Since 2015, Evidian has been part of the Digital Security Service Line at Atos, a global digital services company, headquartered in France. Evidian is an established IAM business and has more than 900 customers with over 5 million users within the Finances Services, Manufacturing, Retail, Transport, Telecom, Media, Utilities, and Public Health sectors. Both Evidian Identity Governance and Administration (IGA) and Evidian Analytics and Intelligence (A&I) are evaluated together as its overall IGA solution in this Leadership Compass.

Evidian offers multiple products in a suite. Their product, Evidian Identity Governance and Administration (IGA), offers basic Access Governance in addition to strong on-premises identity lifecycle management capabilities. 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 SaaS systems. Although Evidian Analytics and Intelligence (A&I) is a separate product offering from Evidian IGA, it meets the increasing requirements of advanced Access Governance. It uses TIBCO Jaspersoft for its reporting capabilities giving Evidian the ability to provide good A&I dashboard capabilities. Evidian IGA can ingest the components derived from the former Atos DirX portfolio, and the solution goes beyond identity lifecycle management and access governance to offer an integrated approach to core IAM requirements. Evidian supports privileged accounts and requests governance to on-premises applications and services as well as integration with external PAM solutions such as CyberArk, and Wallix PAM. The solution also offers an integrated approach to core IAM requirements by delivering an integrated IAM product that covers all significant aspects of IGA as well as being tightly integrated with the SSO (Single Sign-On) and Access Management solutions offered by Evidian.

Evidian\'s offering exhibits particular strengths in OOB IGA and AG related reporting, including major compliance frameworks. Other product strengths include workflows, policy management, and identity and access intelligence when using Evidian A&I, although access certification is limited and does not include event-based micro certification or more advanced recertification triggers based on SoD violation, outliers, or fraud indicators as some examples. However, available recertification triggers can be based on a user\'s access risks or on a schedule. The Evidian UI has an improved look & feel and provides integrations into ITSM systems such as ServiceNow and EasyVista. The latest version also includes a new feature improving compliance by verifying, when assigning rights, that a user has the required level of accreditation (training, certification, signing a charter). This feature also takes into account changes in the level of accreditation over time: granting rights upon obtaining accreditation or revoking them upon expiration of accreditation. In addition to basic SoD support, there is built-in support available for Dynamic Authorization Management.

Evidian supports on-premises, public and private cloud deployments, as well as a hybrid model. Still, the software is only delivered as software deployed to a server, although the solution can be installed in a Virtual Machine. Also, Evidian has introduced its Evidian IDaaS Access offering and intends to offer Evidian IDaaS Governance in the near future. Evidian is also available as a managed service. For DevOps, nearly all of the Evidian capabilities are exposed via SOAP or REST APIs and SCIM 2.0. SDKs for Android, iOS, Java, and JavaScript programming language are also available.

Evidian customers and partner ecosystem are primarily focus in the EMEA region with growth in the APAC and North America, serving mid-market to enterprise-sized organizations. 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 healthy partner ecosystem across Europe, ATOS acquisition is likely to help Evidian gain access to large customers and enter new geographies, and its roadmap and vision will continue to move Evidian in a more positive direction.

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

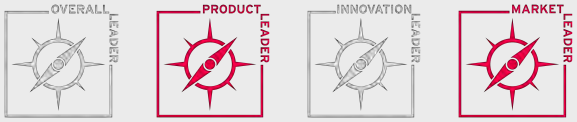
Strengths

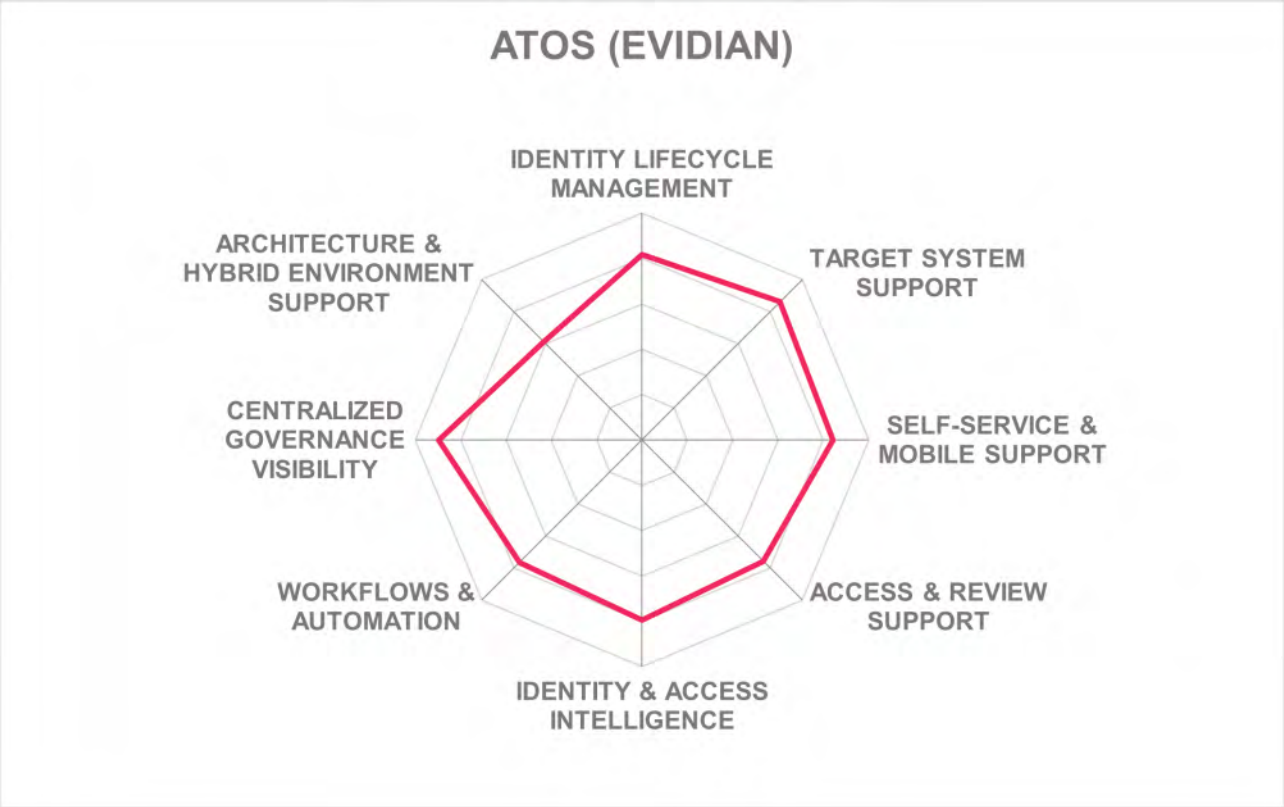
- Identity lifecycle management
- Strong OOB target on-premises system connector support
- Good governance visibility and reporting
- Workflows and automation
- ATOS acquisition helped to extend global network and reach to large customers
- Modern and user-friendly user self-service and admin portals

Challenges

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

Leader in




ATOS (EVIDIAN)
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.8 Evolveum

Evolveum is an Open Source IAM vendor based in Slovakia. Their midPoint product is provided for free but needs a subscription for professional services. MidPoint is delivered as a single platform that focuses on IGA data protection and organizational management use cases. Evolveum is in its 10th year of the midPoint project.

Evolveum's midPoint governance features include delegated administration, deputies, role catalog. In addition to the other governance basics, midPoint also supports event-based certifications and re-certification campaigns, basic role management lifecycle, and data protection. A wide range of identity repositories with a lesser degree of out-of-the-box (OOB) provisioning connectors to target on-premises systems are available. Only a few OOB connectors to popular cloud systems are given. Attribute mapping between connected systems can be scripted using Groovy, JavaScript (ECMAScript), and Python programming languages. Policies for RBAC and organizational structure are also available that can be used for SoD use cases, for example. Evolveum deliberately removed its workflow engine in favor of a workflow-less approval process that is entirely driven by policies. For instance, for approval, policy rules are applied to roles, then the approval engine will compute the approval process.

MidPoint provides a modern and functional IGA UI with good layouts and dashboards. A shopping cart paradigm is available for requesting roles, and users can choose from a role catalog. A single SoD violations check is conducted at checkout only. General-purpose reporting capabilities are available based on Jasper Reports, although missing support for major compliance frameworks OOB. Noticeably, MidPoint is missing more advanced identity and access intelligence capabilities. Customer requests guide midPoint development and currently on its near-term roadmap includes improved scalability, identity matching, features specifically for academia, and other potential features.

MidPoint provides on-premise deployments as either a standalone server that can be downloaded and run or a Docker image. A third option allows a more customizable open-source style using Apache Maven as a build system allowing for customization. A private cloud option is also available using the same deployment options as on-premise. Evolveum does not provide a SaaS option. Almost all of Midpoint\'s functionality is exposed via REST and SCIM APIs only. Roughly half of the solution\'s capabilities are available via CLIs. Only a Java SDK is given. MidPoint Studio is new and provides an integration and development environment that facilitates configuring MidPoint, creating customization, and data mapping, to name a few capabilities.

Evolveum customers are primarily in the EMEA and North America regions with inroads to APAC and Latin America and a relatively small partner ecosystem. Evolveum's customer deployments include medium to enterprise companies and universities. MidPoint provides good on-premise DevOps options but lacks support for public cloud or SaaS for organizations hoping to move towards a hybrid or a full cloud environment in the future. Overall Evolveum midPoint continues to improve and may be of interest to organizations with general IGA and solely on-premise requirements.

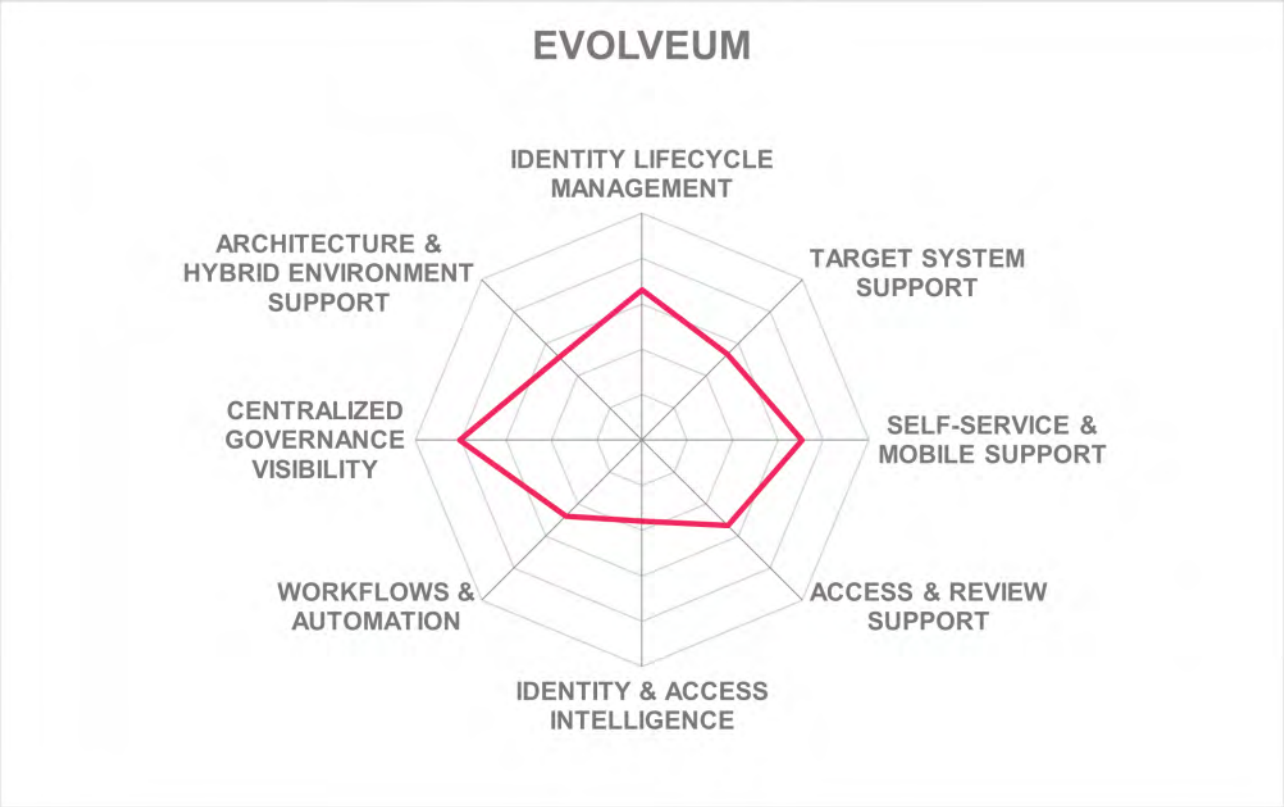
Security	●●●●○
Functionality	●●●○○
Interoperability	●●●○○
Usability	●●●○○
Deployment	●●●○○

Strengths

- Open-Source solution, provided at no (license) cost
- Connectors to on-premises systems
- Access review support
- Good DevOps support
- MidPoint Studio
- Some innovative features on the roadmap

Challenges

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


EVOLVEUM
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.9 Fischer International Identity

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

Fischer Identity supports the most popular identity repositories with synchronization of user attributes across heterogeneous IT environments. Strong support for out-of-the-box (OOB) provisioning connectors to on-premises systems is given, with fewer OOB connectors to SaaS systems. Workflows and automated identity lifecycle management are also available. Both access and event-based micro certification are provided with recertification triggers based on schedules, organization changes, outliers, or custom triggers. Good IGA policy management support with RBAC and ABAC-based authorization, allowing identity attributes to be used within access policies. Moderate SoD capabilities are included, but more advanced SoD risk analysis across roles or SoD checks embedded in role creation and user provisioning processes are not available. ITSM integration options include ServiceNow and Cherwell.

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

Although Fischer Identity supports on-premises deployments, it has a SaaS-ready design approach that can support a hybrid environment. The solution can be delivered as a Docker container or as software deployed to a server. A managed service option is also available. Its Global Identity Gateway provides a communication channel between the customer\'s premises and the cloud data center. Some functionality is available via SOAP and REST APIs, although access via CLIs is not. SDKs and a developer portal are not available. Support for SPML is available, although support for SCIM is not.

Fischer customers are primarily mid-market to enterprise organizations in North America with a limited presence in the APAC region. Their partner ecosystem is somewhat limited in size but growing and based on a few global, engaged partners. Although Fischer has some areas for improvement that are already on its near-term roadmap, Fischer offers a comprehensive IGA suite suitable for customers across most industry verticals, particularly education.

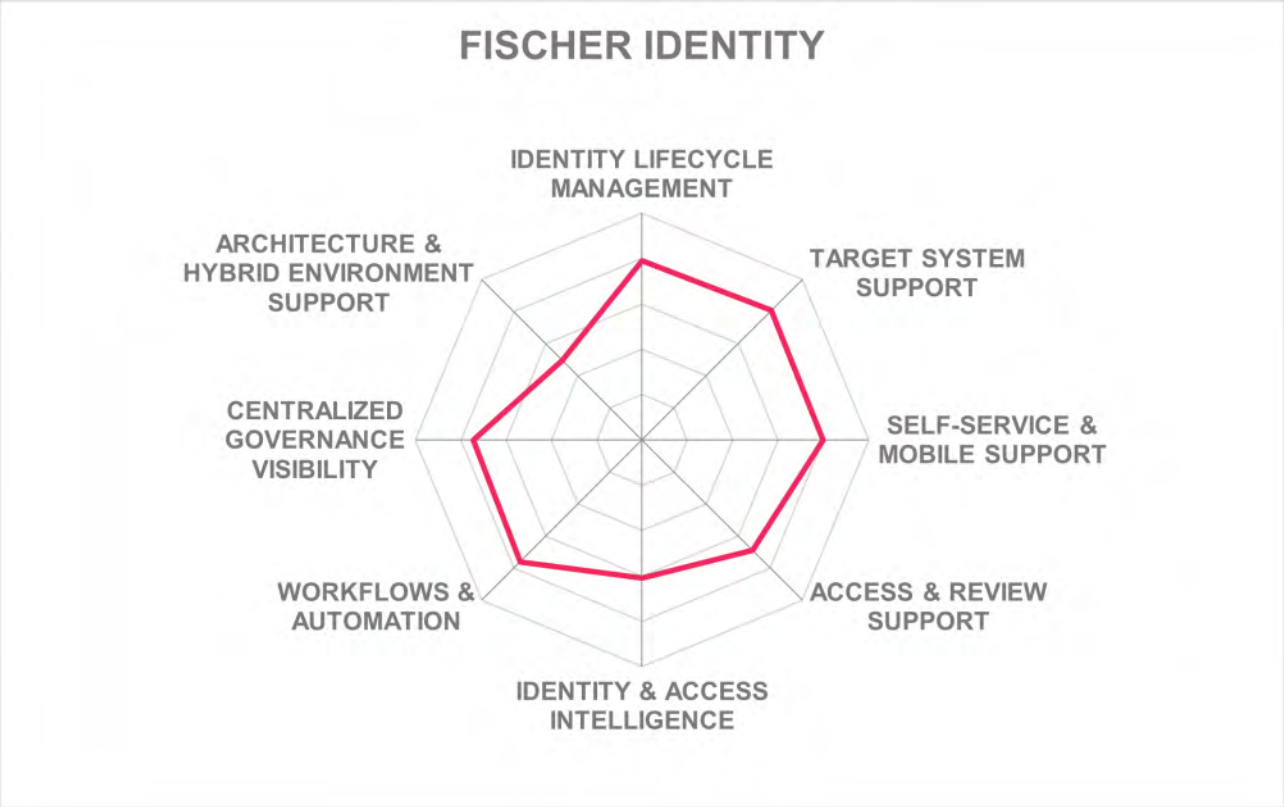
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●○○

Strengths

- Identity lifecycle management
- Good OOB on-premises connectors support
- Easy to deploy and configure for common IGA scenarios
- User self-service and mobile support
- IGA policy management
- Cost effective delivering fair value for money
- aStrong multi-tenancy support, suitable for managed IGA service providers

Challenges

- Inconsistent UIs across suite components
- Missing analytics dashboard
- Limited DevOps support
- Customer base is primarily in the North America region
- Somewhat small but growing partner ecosystem


FISCHER IDENTITY
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.10 ForgeRock

ForgeRock is a leading, venture-backed IAM vendor headquartered in San Francisco, CA but with many offices worldwide. ForgeRock supports most major IAM standards and is a significant contributor to several international standards organizations. Their overall Identity Platform serves both B2E, B2B, and B2C markets. More recently, ForgeRock released its Identity Governance product built on top of ForgeRock Identity Manager. For years, customers have been using ForgeRock identity lifecycle management (e.g., connectors to target systems, identity provisioning /de-provisioning, identity data mode, account mapping, workflows, and user self-service UIs) capabilities to address core IAM business challenges. In late 2019, ForgeRock added IGA capabilities such as access certification, access request, and entitlement management & SoD capabilities. About the same, ForgeRock also released ForgeRock Autonomous Identity, an AI-driven identity analytics and access intelligence solution. Their identity governance includes many of the same capabilities with added access risk management, role mining & engineering.

ForgeRock Identity Governance is an AI-driven identity lifecycle management solution that leverages an identity analytics engine. Out-of-the-box (OOB) connectors to various identity repositories, on-premises, and SaaS applications are well supported. A flexible and extensible data model allows for managing a wide range of identity types, including machine, bot APIs, and microservices. ForgeRock provides the ability to automate identity lifecycles by creating and managing accounts, systems, applications, or infrastructure access. SCIM 2.0 is supported for provisioning/de-provisioning. Other governance features include SoD checks during the access request process, certifications, and role mining capabilities. Access certification reviews can be ad hoc, on a periodic schedule, or event-based micro certification. Certification of high-risk user access can be prioritized as well as automatic approvals of low-risk access requests.

ForgeRock Identity Governances provides a modern user interface with intuitive views of risks with confidence scores, predictions along with justifications, and recommended actions. Consistent with other ForgeRock products offers a good user self-service. Strong authentication options are available to both users and administrators. Good IGA related reporting comes OOB, including reports on abnormal or outlier user access.

ForgeRock solutions support on-premises deployments or deployments within IaaS providers. The ForgeRock cloud service is fully multi-tenant and is built on top of GCP, which aligns with a wide range of standards, Azure and AWS. For non-SaaS customers, ForgeRock supports DevOps through Kubernetes-ready Docker's containers as well as scripted installers. All of the ForgeRock platform functionality is exposed through REST APIs, with half of the functionality available through a CLI. Both APIs and CLI are documented on ForgeRock's developer portal. Available SDKs support Android, iOS Go, and JavaScript programming languages. ForgeRock components do have a dependency on Java technology requiring a Java runtime environment using either Oracle JDK 8 or 11, IBM SDK - Java Technology Edition (WebSphere only) 8, or OpenJDK 8 or 11.

ForgeRock's entrance into the IGA market is attractive. ForgeRock already provides strong capabilities in the IAM market and is now growing in the IGA market. ForgeRock's Identity Governance solution, with its

innovative AI-driven and autonomous features, makes a compelling consideration for an IGA evaluation.

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

FORGEROCK

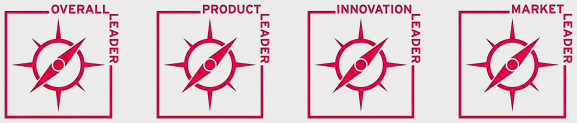
Strengths

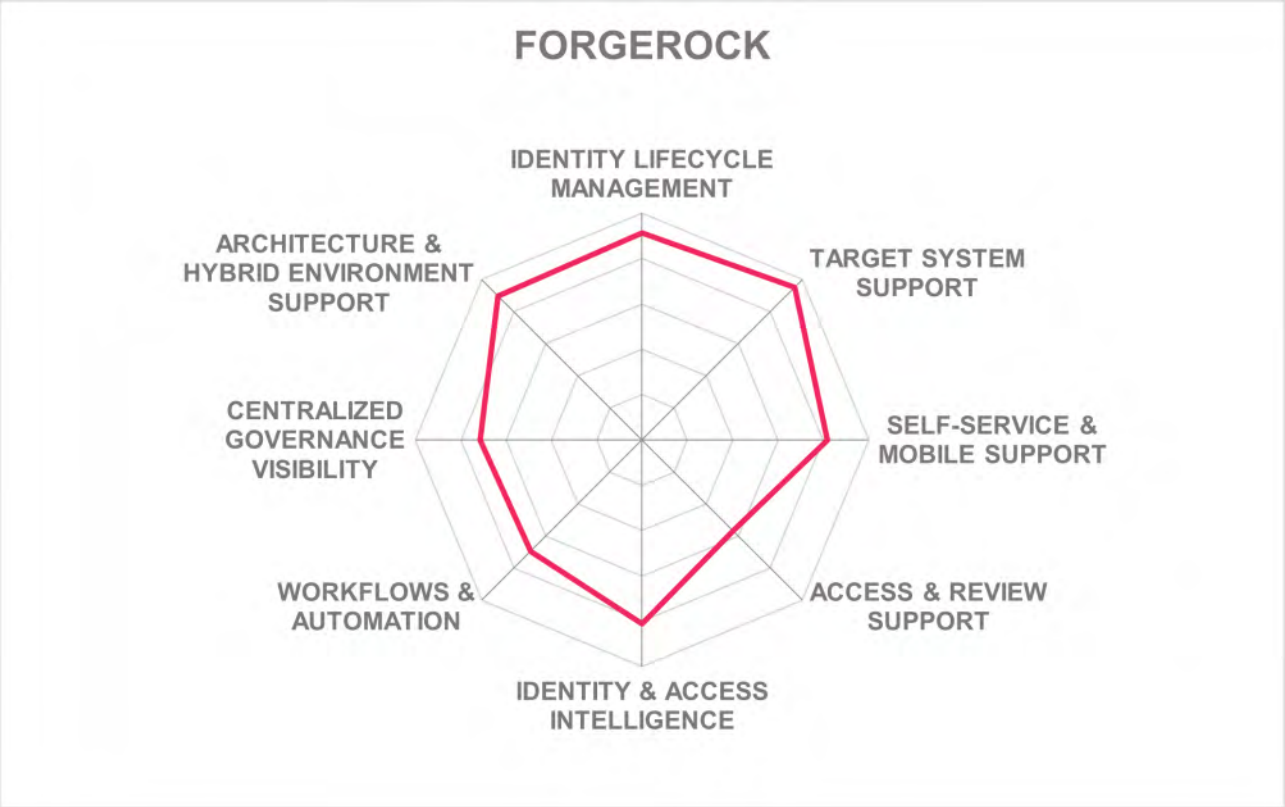
- Identity lifecycle management
- Target system support
- User self-service
- Automated access reviews
- Intelligent Access Request
- Strong identity and access intelligence
- Workflows
- Modern and user-friendly UI
- Strong ITSM & PAM integration

Challenges

- Moderate access governance support although good access intelligence and automation is provided
- Java runtime dependencies
- Upgrades and configuration promotion from test to production require using command line tools and REST/JSON

Leader in




FORGEROCK
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.11 Hitachi ID Systems

Bravura Identity is part of the Hitachi ID Bravura Security Fabric, all of which is built on a common platform. Bravura Identity supports identity lifecycle management automation, access governance, workflows, and analytics. The common platform provides consistent UIs, database, connectors, API throughout the other components in the Hitachi ID security fabric.

Hitachi Bravura Identity covers a wide range of governance use cases that include on-premises, cloud, privileged, and infrastructure access, APIs, RPAs, and microservice-related containers K8 workloads. ID Bravura Identity provides identity lifecycle management automation. Robust OOB on-premise connectors with over 140 included. Good, but less OOB connector support for SaaS systems is given. Automated provisioning and de-provisioning of accounts, entitlements, and passwords are a core strength of Bravura Security Fabric, and support for synchronizing user attributes across heterogeneous IT environments such as SAP and LDAP directories is also given. Data mapping between identities and target systems can use workflow approval before processing. Python can be used for expression evaluation or data formatting within its web UI and regular Expression for bulk pattern matching for filters and association. SoD analysis and mitigation capabilities are given, and good access and event-based micro certification and trigger features for recertification are available, including SoD violations and related compensatory controls. Good support for access and identity analytics and intelligence is available in the areas of outlier detection, role mining, and recommendation capabilities, with some exceptions, such as access modeling and anomaly detection.

Hitachi ID security fabric provides a unified and modern UI for both users and administrators. Good user self-service capabilities include submitting access requests through chatbots or other messaging platforms, although user and admin authenticator options exclude FIDO options. Good audit and IGA related reporting features, including strong support of reports for major compliance frameworks OOB. A wide range of support ITSM integration options is available.

Hitachi ID Bravura Identity supports all major deployment and delivery models, including Docker containers and hybrid environments. For hybrid cases in which Bravura Identity is deployed to the cloud and must manage applications and services on-premises, a connector proxy will need to be deployed on-premises. SOAP APIs can access every part of the system, including the workflow queue, product configuration, and password management operations, although REST API provide more limited capabilities. CLI access to functionality is also given. OOB SDKs include support for Java, C/C++, .NET, Python, and JavaScript. A developer portal is also available. SPML and SCIM for identity provisioning/de-provisioning is not given, although SCIM is its short-term roadmap.

Hitachi ID is well established in the Identity Management market. Its security product line under its Bravura Security Fabric platform offers other integrated IAM components that complement Bravura Identity with its IGA capabilities. Hitachi ID security customers are principally mid to enterprise organizations with a partner ecosystem primarily in North America, with a footprint in the EMEA region and some presence in other parts of the world. Overall, Hitachi ID Bravura Identity is a balanced product with a scalable architecture and

broad feature set, providing good flexibility. It thus is an interesting alternative to established products and should be evaluated when looking for good IGA capabilities.

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

Hitachi ID

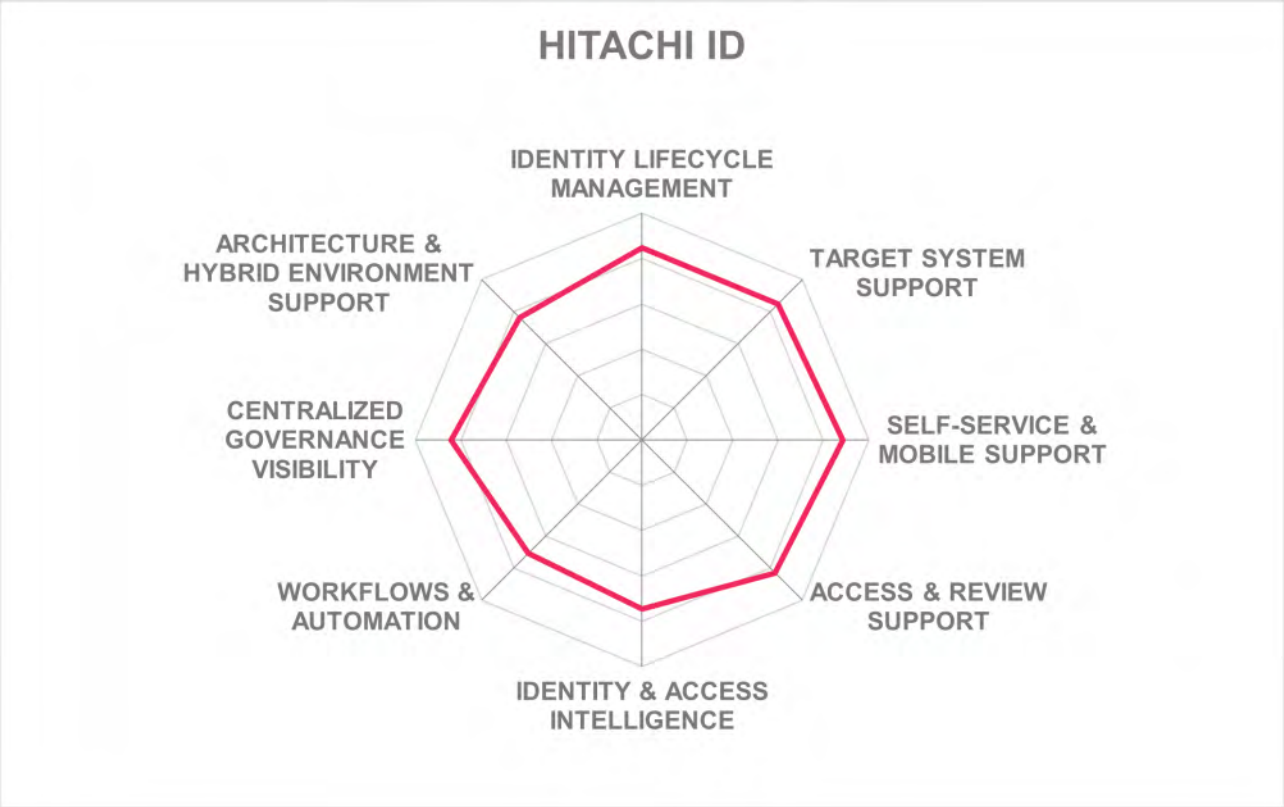
Strengths

- Identity lifecycle management
- On-prem target system support
- User self-service
- Access and review support
- Flexible workflow and policy management
- Reporting options and compliance framework support
- Good deployment and delivery options
- DevOps support

Challenges

- Somewhat limited footprint and partner ecosystem outside of North America
- Missing SCIM support, although it's on the near-term roadmap.
- Greater feature access with SOAP APIs than REST
- Missing FIDO authenticator options

Leader in


HITACHI ID
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.12 IBM

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

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

IBM Security provides a good and functional UI, although with a slightly dated look & feel. A Quick insights dashboard provides a consolidated view of governance risk indicators and suggested action recommendations to take. A good user self-service is also given with a shopping cart-based approach to searching, selecting, and requesting access to applications and services or access roles and privileged access. User self-service is also available via a mobile phone app. Good user authenticator options are given that include passwordless authenticators such as QR code, FIDO2, and FIDO2 U2F. For administrators, basic authenticator options are offered. However, Verify Governance provides a built-in repository for admin users and allows external user repositories as well.

Between IBM Security Verify Governance and SaaS, all deployment models and most delivery options are available, including SaaS, virtual appliance, software deployed to a server. A managed service of Verify Governance is available by IBM security services and through IBM business partners. A container-based delivery option is not offered for Verify Governance, although the Verify SaaS identity analytics solution can be delivered as a Docker container. More than half of VG's functionality is available via REST APIs, although SOAP is not supported. Less access to functionality via CLIs is given. Almost all of the solutions are available via SDKs, which supports some of the most popular programming languages, including Android, iOS, Java, Python, and JavaScript.

Overall, IBM Security Verify Governance continues move its long line of mature IGA offerings in a positive

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

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

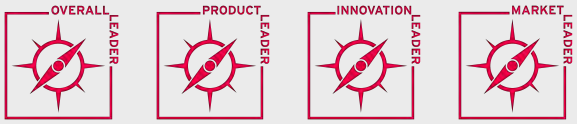
Strengths

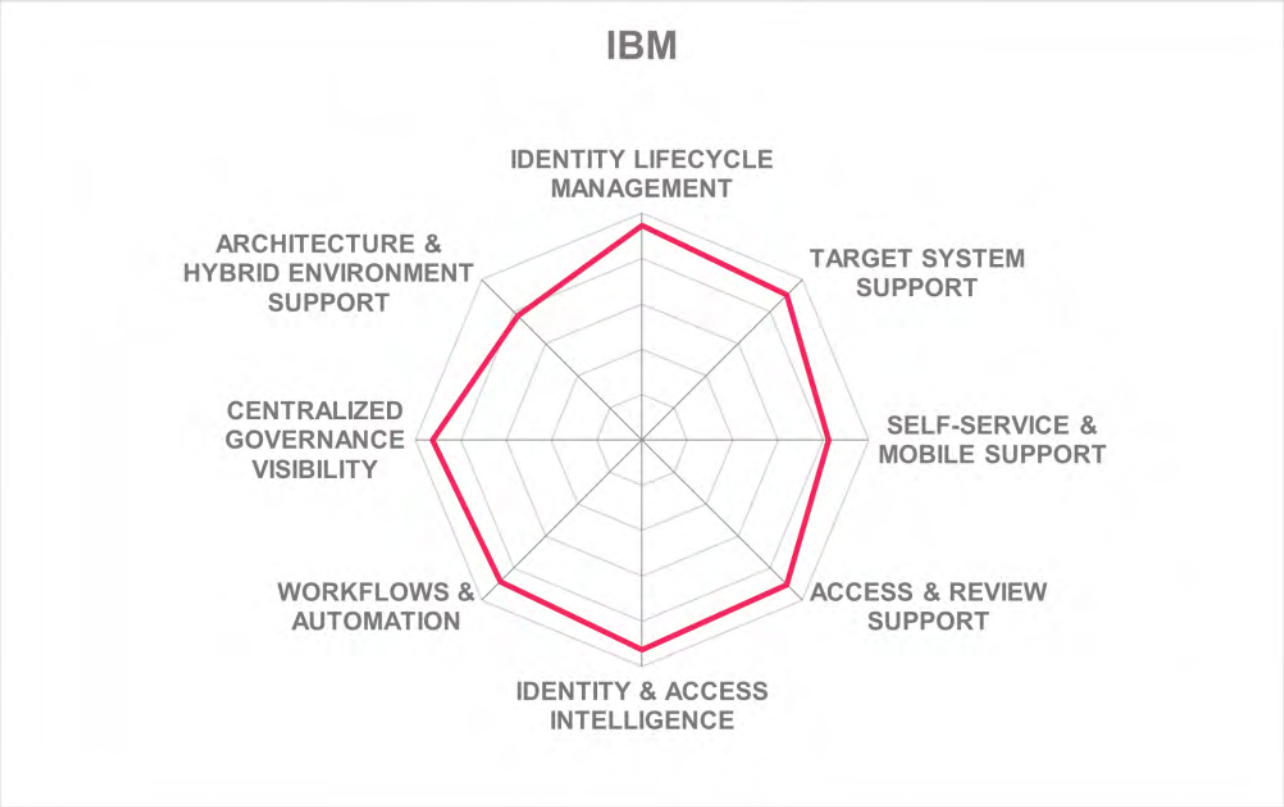
- Identity lifecycle management
- Target system support
- User self-service and mobile support
- Good access governance and review
- Strong identity and access intelligence
- Flexible workflow capabilities
- Functional and useful UI and dashboard
- Easy integration with IBM Security portfolio
- Strong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

Challenges

- The user interface has been redesigned in recent releases but still has limited flexibility to customize
- Missing OOB reports for major compliance frameworks.
- Container-based delivery options are limited
- Some limitation on admin authenticator options

Leader in




IBM
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.13 ideiio

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

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

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

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

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

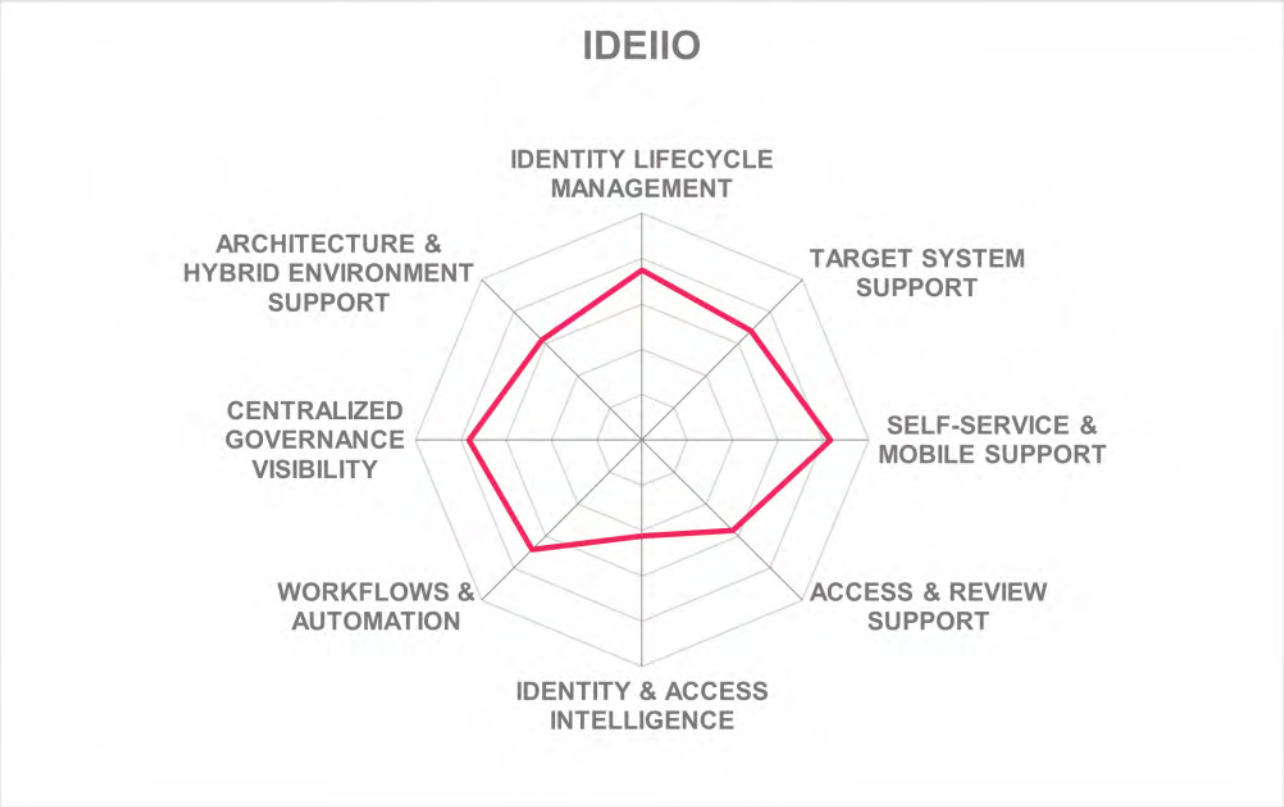
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●○○

Strengths

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

Challenges

- Limited technology integrations and partner ecosystem, although growing in Europe
- Missing intelligent governance & risk insights through AI or analytics dashboards
- Limited user and admin authenticators without third party IDP integrations


IDEIIO
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.14 Ilantus Technologies

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

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

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

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

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

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

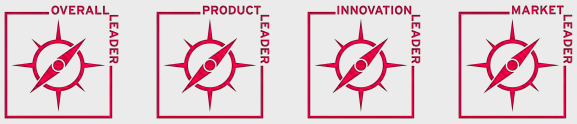
Strengths

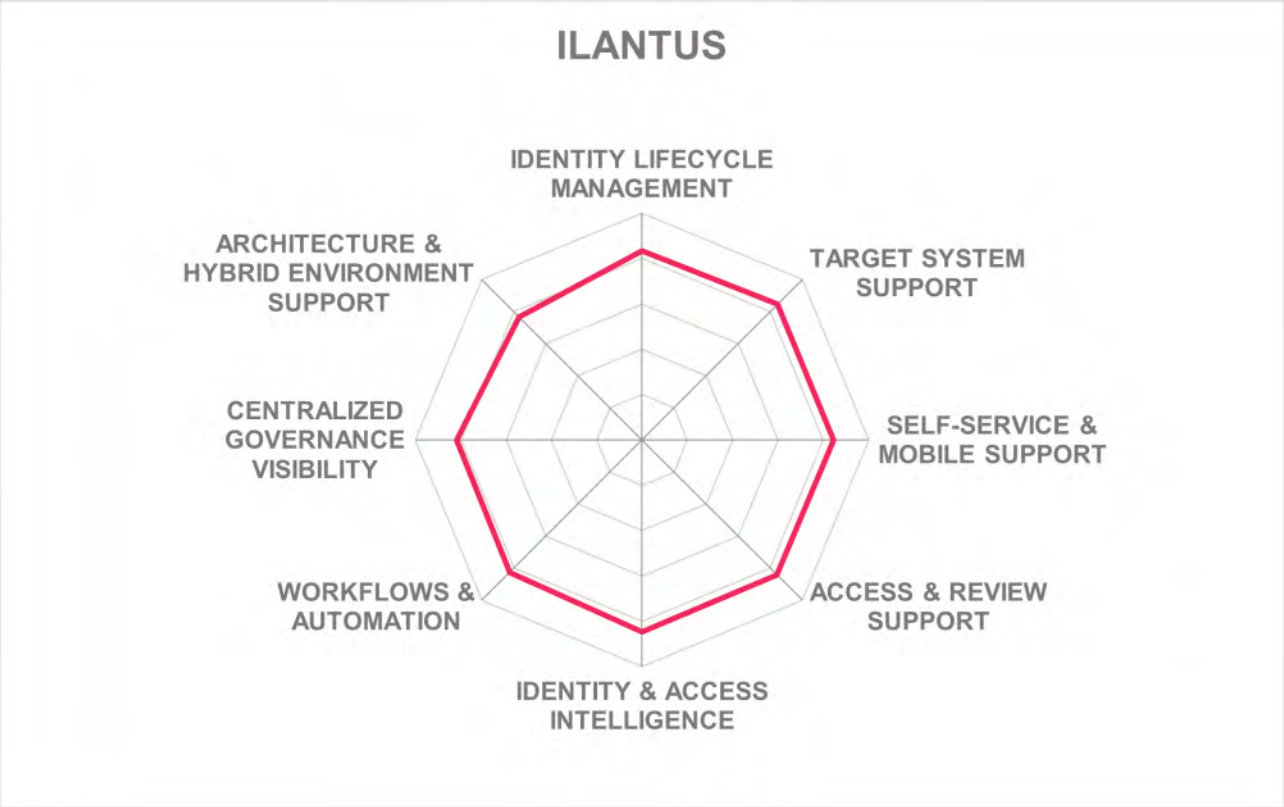
- Identity lifecycle management
- Target system support
- User self-service capabilities
- Identity and access intelligence
- Flexibility for customization including policy and workflow customizations
- Intuitive and user-friendly UI
- Good deployment and delivery options

Challenges

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

Leader in




ILANTUS
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.15 ILEX International

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

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

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

Ilex is limited to delivering its solution as SaaS, software deployed to a server or a managed service. No container-based options are available, although it's on the roadmap. The SaaS option is hosted with a French cloud provider with both data and support service in France. The solution is Java/J2E based providing independence from the OS. Both SOAP and REST APIs allow access to most features, although administration features are not all available via API. Both SPML and SCIM is supported for identity provisioning/deprovisioning. SDK support includes Android, iOS, Java programming language. A developer port is not given, but administrative documentation can be accessed online.

Ilex has a good mid-market customer base and a small partner ecosystem, both primarily within the EMEA region with some growth in the APAC region. ILEX Meibo Identity Management can be both -- a tool to build a custom IGA solution and an add-on to existing IGA deployments to enhance the overall flexibility. Both Meibo People Pack (MPP) and Sign&go Global SSO together offer a complete IGA solution. Also, the Ilex SaaS offering is hosted in France, fully compliant with the GDPR, and making it a good alternative solution set to consider in their primary geographic region.

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

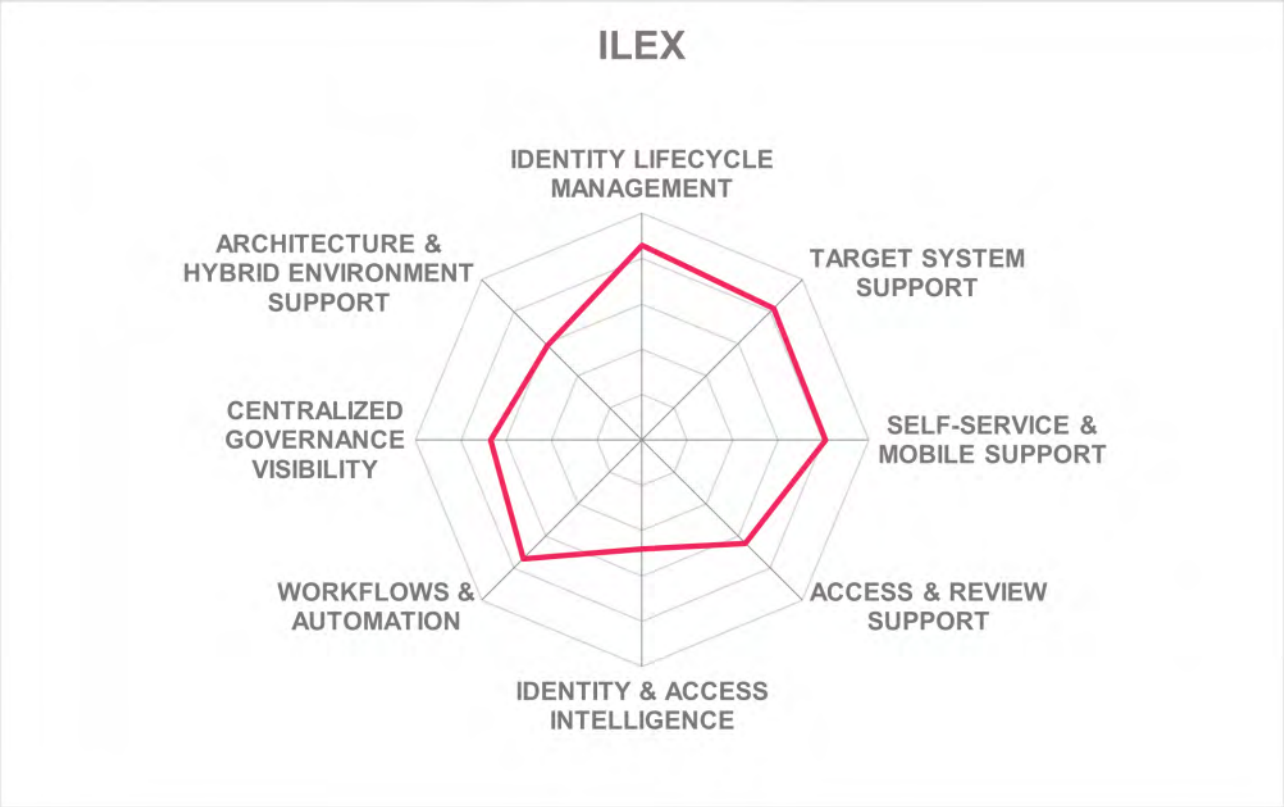
ilex International

Strengths

- Identity lifecycle management
- On-premise target system support
- Good policy management
- Easy integration with its own Sign&Go SSO/Access Management solution
- MFA and adaptive authentication options
- User self-service and mobile support
- Pre-packaged solution reducing time to value

Challenges

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


ILEX
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.16 Micro Focus

UK-based Micro Focus offers an Identity and Access Management Platform as a set of solutions that include Identity Governance and Administration, Access Management, Advanced Authentication, Data Security, Privileged Access Management and Security Information and Event Management. Identity Manager aimed primarily at Identity Provisioning and lifecycle management, and Identity Governance for Access Governance, Identity Intelligence, and Identity Tracking to deliver a wide range of IGA capabilities. Micro Focus executed a significant shift in its product strategy to build some market-leading Access Governance features during 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 is a robust product for Identity Provisioning with mature and comprehensive capabilities for identity lifecycle management and fulfillment. A full range of identity repositories as well as on-premises and SaaS application connectors are available out-of-the-box (OOB). 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 distinct and improved governance features. Micro Focus gives identity correlation and user profiling, anomaly detection, risk scoring, and role mining as some examples for data mining and analytics. Identity Tracking gives the capability to monitor user activity in real-time. Micro Focus is also capable of detecting and reacting to identity at the time of change. A more autonomous governance model is given through the use of unsupervised machine learning capabilities via its Interset and Vertica analytics product. Also, a continuous compliance model is applied to identity transactions in addition to the traditional time-based certification.

NetIQ IGA Suite a very modern and user-friendly UI that utilizes identity and access intelligence to provide useful insights and recommendations. Micro Focus also offers a wide range of IGA related reporting capabilities, including support for major compliance frameworks. Strong user self-service is given with many user and administrator authenticator options available. Although Micro Focus is continually improving its rich set of functionalities, it can sometimes seem complex to understand and implement. Future roadmap items toward autonomous IGA should provide simplification on the customer end.

Micro Focus supports on-premises, public or private cloud, and SaaS and Hybrid SaaS or Cloud deployment models. Currently, Micro Focus IGA-as-a-Service architecture is containerized, supporting Docker, Rancher Labs, Pivotal, Mesosphere, and SUSE platforms. An on-premises \"Cloud Bridge\" component can bridge a customer\'s SaaS and On-Premises solutions by streaming on-premises data sources to the IGA service and providing fulfillment back to the on-premises systems. All capabilities are exposed via SOAP, REST, and SCIM APIs as well as managed using CLI. A wide range of SDKs for popular programming languages is available, with some exceptions, such as Android and iOS. Developer documentation and samples are provided through a community portal.

Micro Focus is a well-established company with a customer base predominantly focused on mid to enterprise-level organizations located in North America and EMEA regions. Micro Focus Identity Manager, Governance, and Intelligence products offer a good range of IGA capabilities from flexible workflow and policy management to enhanced analytics-driven user activity reporting. Micro Focus continues to improve towards a more modern and flexible product with more innovative features on its roadmap. However, it runs the risk of de-focusing due to its aggressive feature roadmap. Overall, Identity Manager and Governance products from Micro Focus remain leading-edge products in the IGA market space with its broad, mature, and evolving functionality with a good partner ecosystem on a global scale.

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

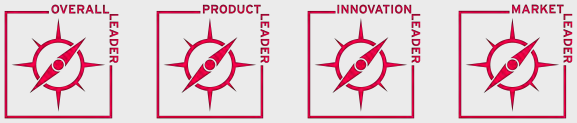
Strengths

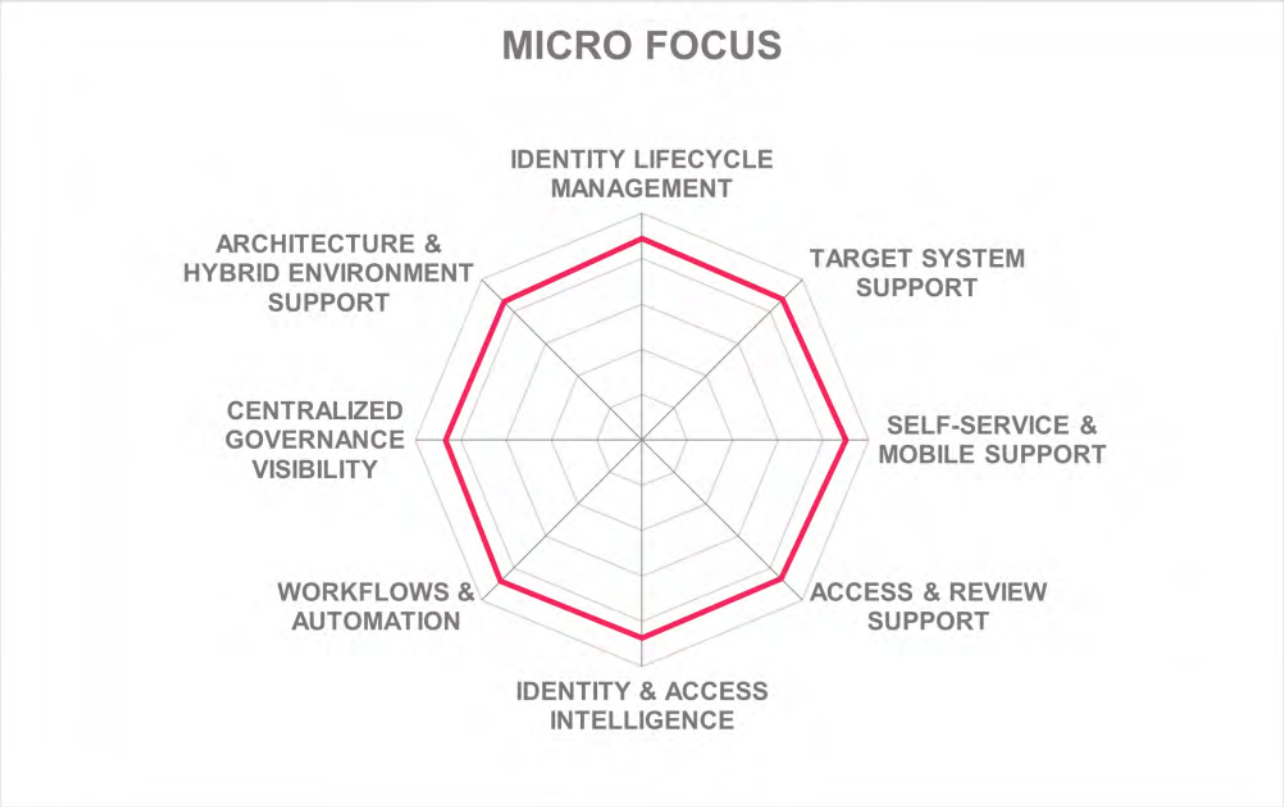
- Identity lifecycle management
- Good target system support
- User self-service and admin support
- Good access governance
- Strong support for IGA analytics and access intelligence capabilities
- Good workflow and automation capabilities
- Aggressively moving to a more modernized and flexible architecture
- Very large customer base and strong partner ecosystem

Challenges

- Rich functionality sometimes complex to understand and implement
- Missing popular SDKs for Android and iOS
- Weaker marketing messaging and execution compared to competitors
- Risk of de-focusing due to aggressive feature roadmap

Leader in




MICRO FOCUS
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.17 Nexis

Founded in 2009 and based in Regensburg, Germany, Nexis started with NEXIS Controle, first released in 2014, which builds used a plug-and-play approach to access governance as its core focus. Since then, Nexis has made some significant improvements on core products, now called NEXIS 4. The NEXIS 4 feature set includes access governance, analytics and modeling engine, a fully configurable UI, workflows, policy management, as well as other interesting integration options.

Nexis takes a different approach to the provisioning of target systems. Nexis doesn't provision identities directly but instead provisions the assignment of identities to business roles existing systems such as a customer's IAM solution. Connections to a wide variety of identity repositories are given, although out-of-the-box (OOB) connectors to on-premises systems are limited to some Microsoft products such as Microsoft AD, SQL server, SAP, LDAP, and database connectors. OOB connectors to SaaS applications are not available. However, NEXIS 4 does provide a synchronization engine that can define synchronization rules to detect changes on the target application or push back information to the connected application. Integrations with third-party ITSM tools such as Remedy and ServiceNow. Good policy management and workflow capabilities are available. Access certification includes campaigns, event-based micro certification, and recertification trigger, and the event engine can listen to a wide range of change information. NEXIS 4 gives access and risk intelligence that includes access modeling, current, and future state comparisons, anomaly, entitlement, and role outlier detection. Also, real-time SoD checks in which a third-party application can ask for SoD violations, and NEXIS 4 will respond to those requests. Also, time-based analytics and policy triggers are available that can start workflows. Dynamic filters can find such things as critical business roles that may expire in the next 30 days at a specific office location.

NEXIS 4 offers significant improvements to UI. Nexis provides a user-friendly and fully configurable UI design that supports 150+ corporate identity settings and a WYSIWYG UI component editor. End-user request services are stakeholder-centric, and dashboards use a card-based interaction to display specific target information and buttons to trigger an action. Both user self-service and administration portal access are limited to basic authenticator options. Good IGA/AG related reporting is given, although support for OOB reports for major compliance frameworks is not available.

NEXIS 4 supports on-premises, public & private cloud, or in a hybrid environment. The solution can be delivered as SaaS (e.g., on Azure, AWS), virtual appliance or software deployed to a server with Windows or Linux OS. A hardware appliance and Docker container-based delivery are also possible when required by customers. A managed service available through its partner network. For cloud delivery, Nexis supports partial but not full multi-tenancy. Some of the solution\'s capabilities are available via SOAP or REST APIs. SDKs for Java and scripting via JavaScript are also available. Access to the solution\'s capabilities via CLI and a developer portal with documentation, tutorials, examples, etc., are not available.

Nexis customers are mainly mid to enterprise organizations in the EMEA region and support a relatively small but growing partner ecosystem. NEXIS 4 offers capabilities for a niche market in which customers have an existing provisioning tool but needs a strong access governance solution with good analytics and a

customizable UI, or customers who need these capabilities on top of their current IAM solution enhance it further. NEXIS 4 provides strong product usability with its zero-code approach, configurable UI components, dashboards, and end-user services. Also, NEXIS 4 has good value as a stand-alone solution as well. For customers in the EMEA region, NEXIS 4 offers an interesting solution that complements rather than replacing existing IAM implementations.

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

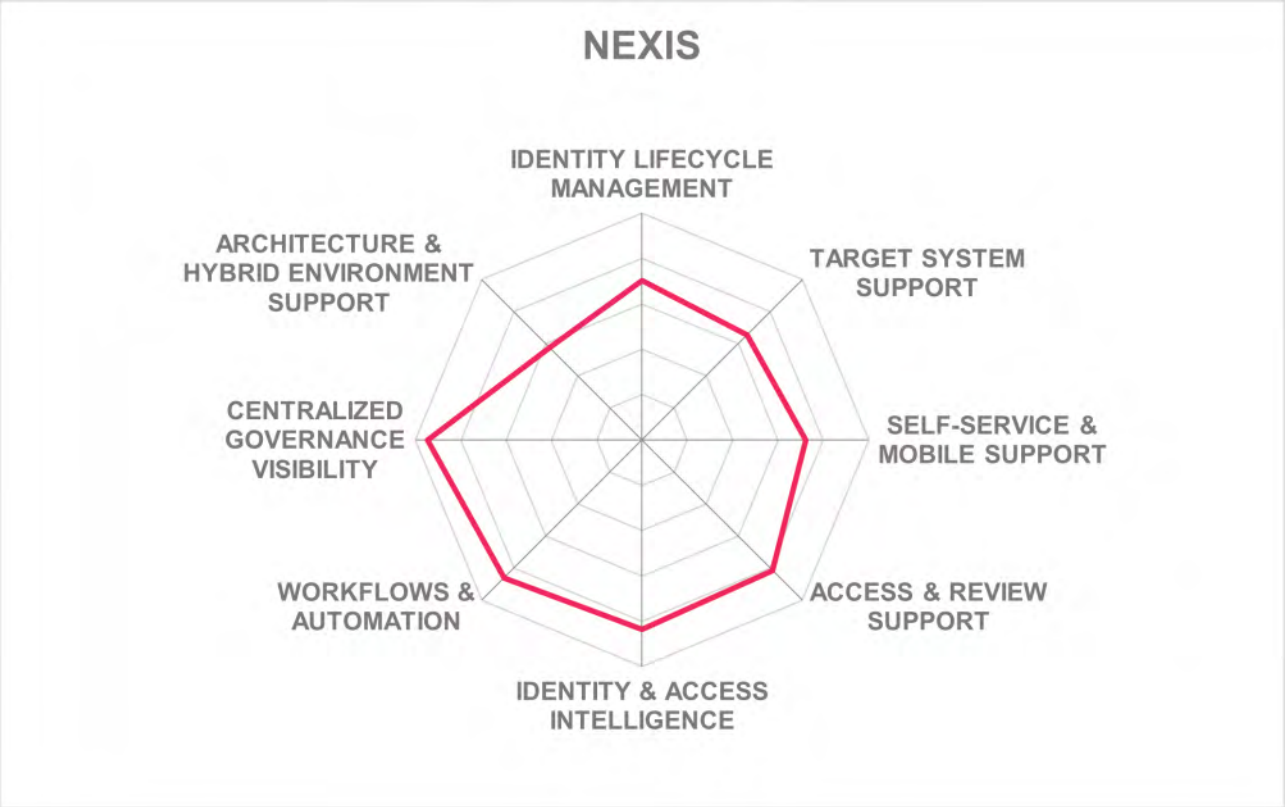
NEXIS Controle

Strengths

- Supports the majority of access governance use-cases
- Access certification support
- Innovative governance visibility support through a modern and user-friendly UI
- Integrated SoD Controls capabilities
- Workflow capabilities
- Access and risk intelligence

Challenges

- Limited user and admin authenticator options
- Limited set of OOB on-premises system connectors
- Missing OOB SaaS connectors, although generic export plugins are provided
- Small but growing partner ecosystem
- Limited presence outside of DACH region


NEXIS
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.18 Omada

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

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

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

Omada Identity can be delivered as software deployed to a server or container-based. Omada Identity Cloud is its cloud-native SaaS solution. Omada partners deliver a managed service. Also, the solution uses Microsoft SQL Server components for ETL operations, reporting, and data analysis. The majority of Omada functionality is available via its OData (REST) and SOAP APIs. Access to functionality via CLI is not

supported. A .NET and JavaScript SDKs are available for customizations. Also, a developer portal is available through the Omada Hub for customer DevOps and partners.

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

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

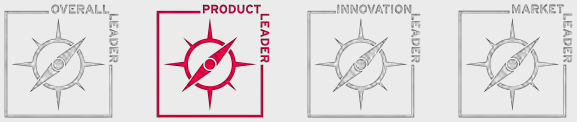
Strengths

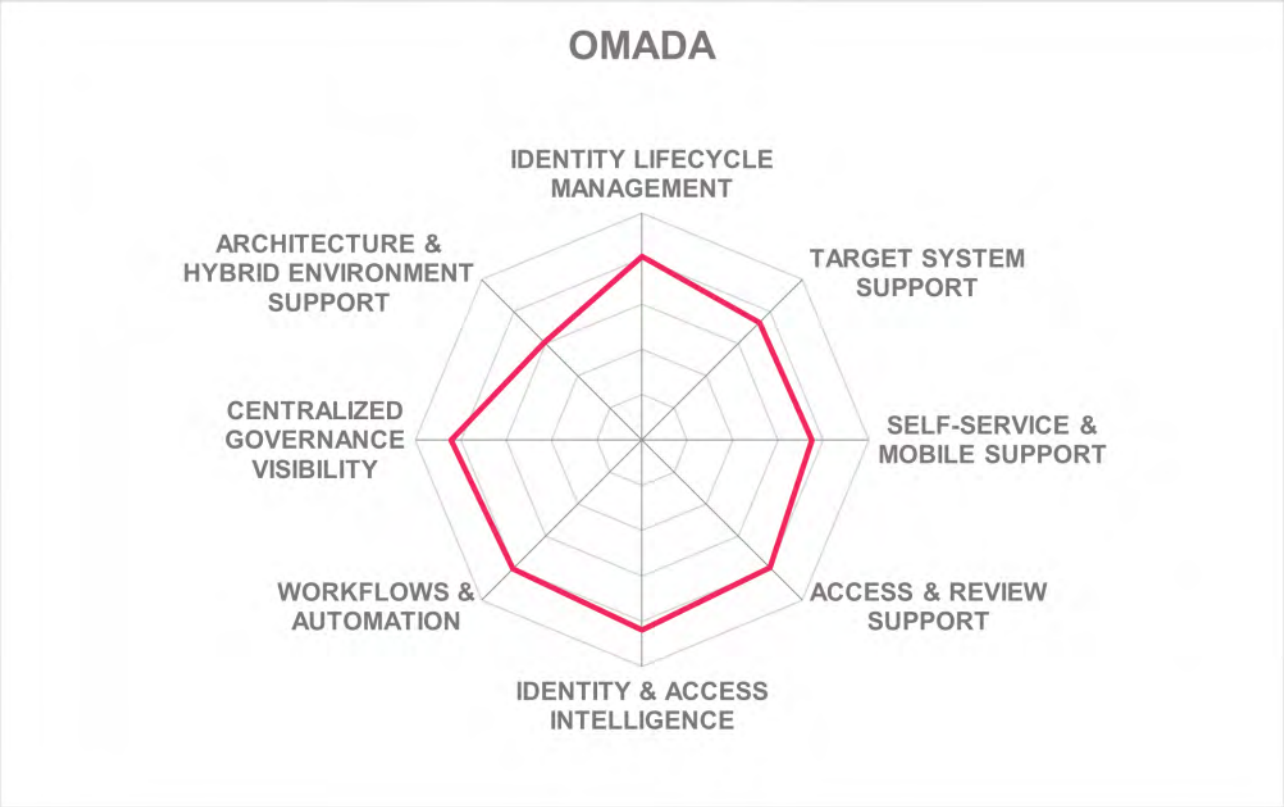
- Identity lifecycle management
- User self-service support
- Efficient approach for onboarding new applications
- Identity and access intelligence
- Mature solution with strong workflow and role management capability
- Policy management
- Good governance visibility
- IGA best practices process framework,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

Challenges

- Moderate support of out-of-the-box connectors to on-premises and SaaS systems, although configurable template connectors are available for standard protocols
- Limited authentication options for user self-service and administrative access
- Customer presence is predominantly focused on the EMEA, although growing in North America and the APAC regions

Leader in




OMADA
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.19 One Identity

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

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

One Identity provides a modern UI with some unique features, such as a department risk index heatmap that allows drill-downs to more details and 360 overviews of user access and the relationships between applications or even access violations. User self-service is good utilizing a shopping cart-based approach for access requests, features such as the ability to simulate the effect of changes to access entitlements or role definitions remain unique. Additionally, all access request management capabilities are available via mobile devices. Moderate support is given for user self-service and administration authenticator options but does include FIDO2, mobile app, and biometric options. Additionally, Identity Manager provides an OAuth/Open ID Connect authentication module to integrate with access management products such as Okta, Ping, and Azure. Identity Manager includes analytics and intelligence base on risk from inheritance and risk from roles. This information is available on dashboard views in reports and indicators in access reviews, for example.

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

available as part of the product ISO.

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

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

ONE IDENTITY

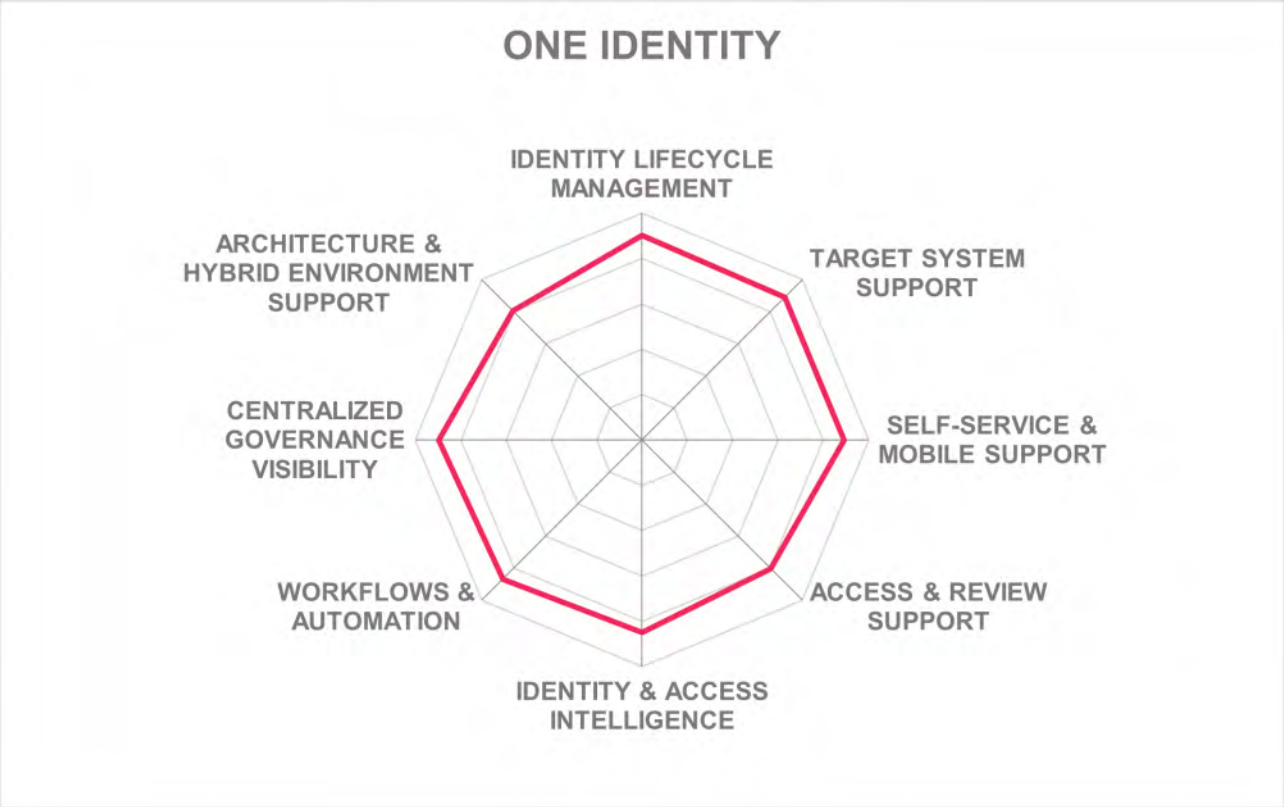
Strengths

- Identity lifecycle management
- Target system support
- User self-service and mobile option
- Access and review support
- Workflows and automation
- Modern UI with some unique features
- Integrates well with its access management and privilege management capabilities
- Advanced role management with strong SoD support
- Strong sales and marketing execution

Challenges

- Moderate list of authenticator options for user and admin access, although it can integrate with third-party IAM
- Cloud delivery does not support full multi-tenancy for all components
- Missing continuous monitoring of access compliance and User Activity Monitoring
- Missing access governance support for containers and container orchestration platforms such as Kubernetes

Leader in


ONE IDENTITY
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.20 Oracle

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 over the years, especially the integration of modules and the ease of its deployment. Oracle remains a preferred vendor for organizations with a substantial investment in Oracle Fusion Middleware and requires high flexibility for customizations to accommodate complex business processes.

Oracle Identity Governance can cover a wide range of IGA use cases. For identity lifecycle management, Oracle offers strong support to out-of-the-box (OOB) integrations to identity repositories for managing the identities and supports synchronization of user attributes across heterogeneous IT environments, workflows, and attribute mapping from source to target properties. Java/Groovy can be used for mapping expressions. A wide range of on-premises and SaaS application connectors are provided OOB, and both SPML and SCIM are available for SCIM for identity provisioning/de-provisioning. Application templates are provided to facilitate application onboarding and automatic provisioning to the applications. Access Governance includes certification with event-based micro certification and basic triggers to recertify but missing some advanced outlier and fraud indicator types of triggers. Policy management is good and will improve based on Oracle's current roadmap, although integration with third-party policy tools or engines is not available. The solutions provide good identity and access intelligence that includes access modeling, role mining, anomaly detections, and other outlier detection. OOB ITSM integration includes BMC Helix ITSM.

Oracle Identity Governance Suite cuts across its competition through its enhanced UIs. User self-service is well supported and includes features like utilizing a shopping cart approach to improve the UX. The solution also provides a full set, from basic to advanced, authenticator options for both users and administrators. OOB reports for major compliance frameworks are available and strong support for OOB IGA/AG-related reports.

On-premises deployments can be delivered as a virtual appliance, Docker container-based, software deployed to a server, and private or public cloud. The cloud delivery currently does not support a full multi-tent solution, although it is on the roadmap---a managed service through Oracle advanced customer services and Oracle partners. Oracle\'s on-premises deployments have a dependency requirement for an Oracle database. The majority of functionality is exposed through APIs via SOAP or REST. Slightly less functionality is accessible via CLIs. A developer portal is also available. Oracle offers SDKs for Java, C/C++, and .NET programming languages. Oracle continues to improve its on-premises solution by moving to a module model rather than interdependent upgrades. Also, new binaries will take care of any dependence changes programmatically, and containers come with auto-scaling.

Overall, Oracle Identity Governance Suite counts among the leading IGA products in the market. It continues to improve, providing a broad set of features focused on Identity Lifecycle Management, Access Governance, and Intelligence, as well as good support for enterprise-level architectures and good DevOps support and improved on-premises deployments. OIG still makes an excellent choice for large IGA

implementations requiring scalability and flexibility to support complex IAM scenarios.

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

ORACLE®

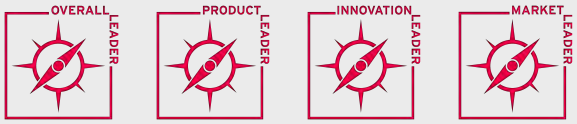
Strengths

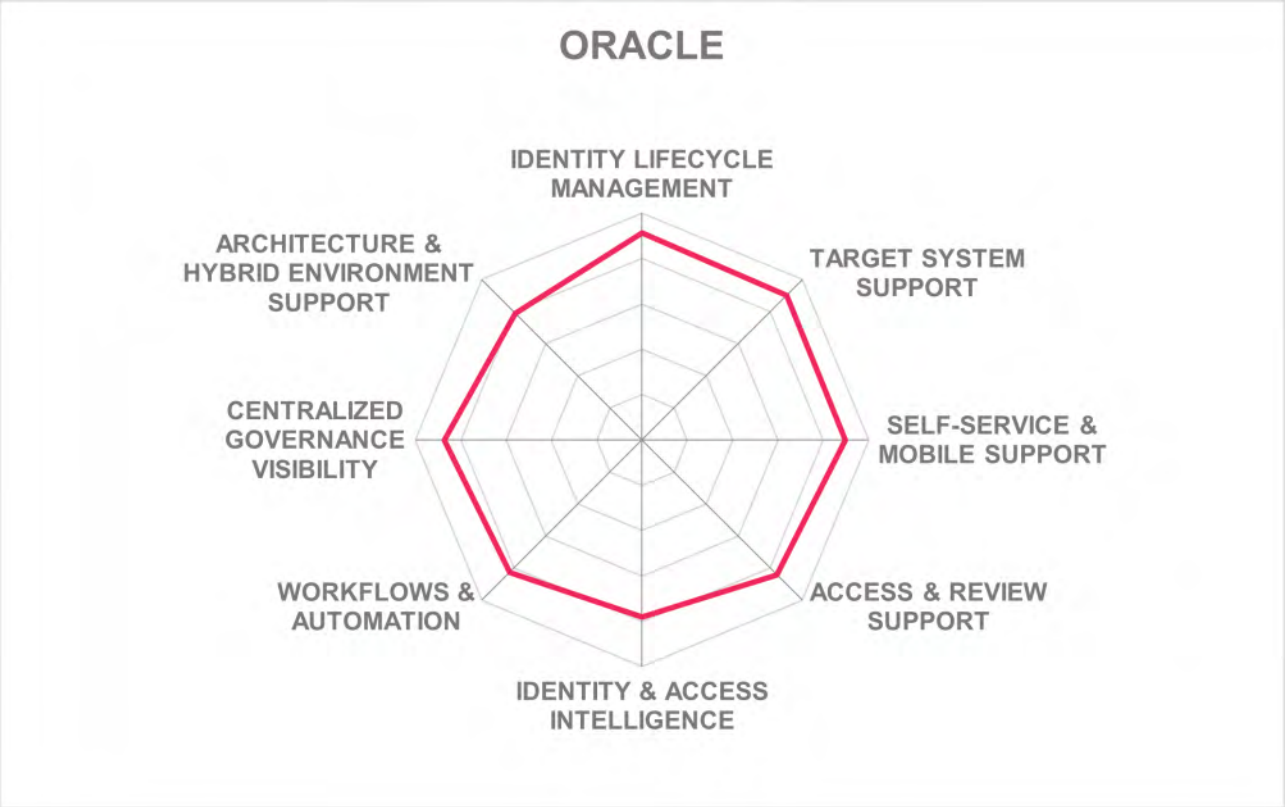
- Identity lifecycle management
- Target system support
- Enhanced and modern UI
- Good user self-service and admin support
- Access governance support
- Improving workflow and automation
- Strong IGA related reporting OOB
- Significant improvements for deployments
- Good devops support
- Global customer base with strong channel partner network

Challenges

- More advance recertification triggers are not available
- Oracle database is required, and not included in the license
- Integration with third-party policy tools or engines is not available

Leader in




ORACLE
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.21 SailPoint

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

Strong support for identity data and life cycle management can connect to a wide range of different identity repositories. A definitive list of out-of-the-box (OOB) on-premises and SaaS connectors are also available. Attribute mapping from source to target properties includes workflows, customization of mapping rules, and synchronization of user attributes across heterogeneous IT environments. The solution also supports both SPML and SCIM for identity provisioning/de-provisioning. Beyond the core governance capabilities such as access certification, SoD, access request, provisioning, and password management, SailPoint\'s AI & ML investment enhances its core identity platform with access insights, recommendations, access modeling, and cloud governance capabilities. Strong support for different identity types such as machine and Bot/RPAs is also given. OOB integration with ITSM tools includes ServiceNow, BMC Helix ITSM, and Atlassian JIRA Service Desk.

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

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

SailPoint has been a leading vendor in the IGA market, providing strong Access Governance capabilities. In addition, SailPoint has built excellent support for identity and role lifecycle management as part of the IGA offering with an increased focus on identity and access intelligence. SailPoint's early recognition of Access

Governance requirements in heavily regulated industries such as banking combined with strong marketing messaging and execution has led it to be one of the most evaluated IGA vendors for mid-to enterprise-sized organizations. SailPoint continues to enhance its provisioning, automation, and predictive intelligence in a positive direction, making it a recommended consideration in any IGA evaluation.

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

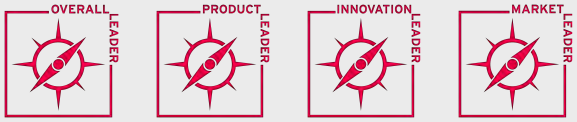
Strengths

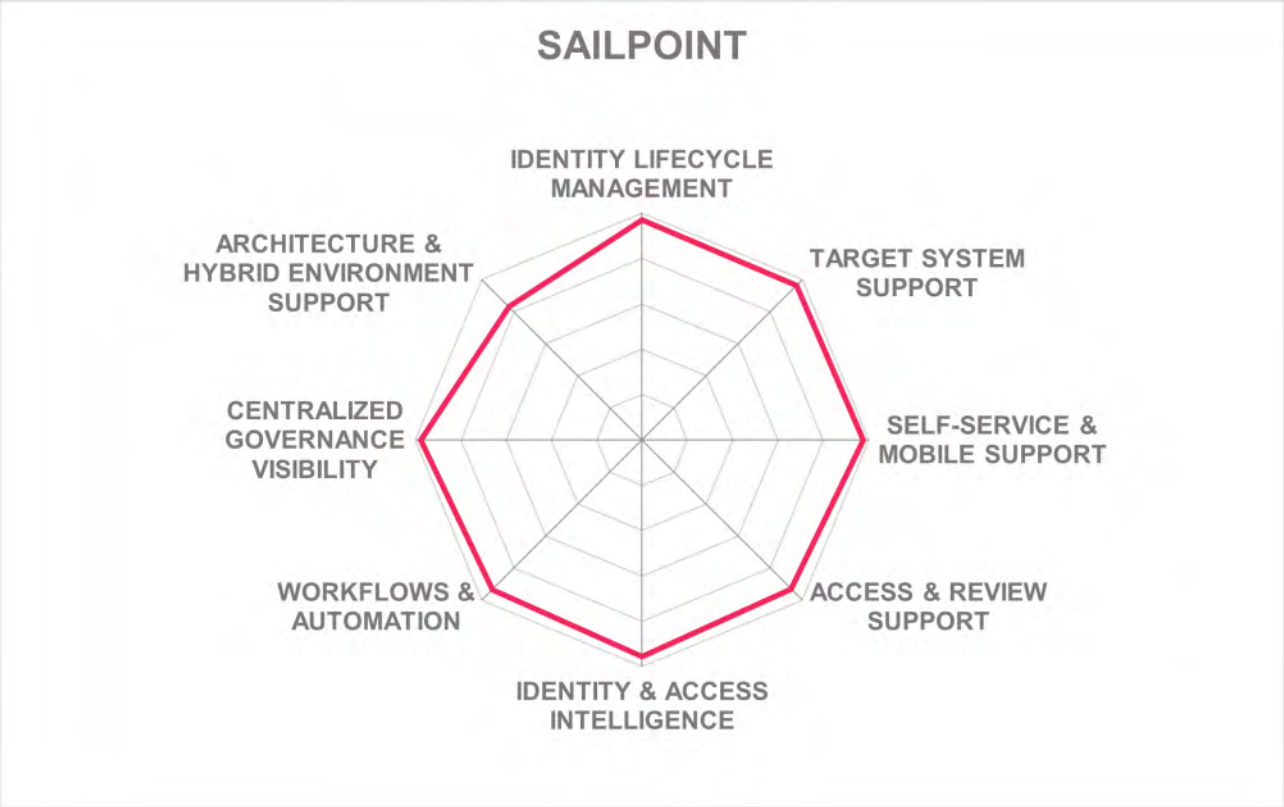
- Identity lifecycle management
- Strong target system support
- Strong support for identity and access intelligence
- User self-service support
- Access & review support with innovative features
- Modern, well thought out and user-friendly interfaces
- Workflows and automation
- A large and effective channel partner network

Challenges

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

Leader in




SAILPOINT
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.22 SAP

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

For SAP Identity Access Governance, a relatively small set of supported identity repositories compared to other offerings in the market. SAP gives good support for out-of-the-box (OOB) provisioning connectors for on-premises systems, but noticeably less support for SaaS other than some of the most popular applications. Automated workflow for provisioning/de-provisioning and auto-discovery capabilities to identify accounts, groups, group memberships is possible through role mining and analytics. Access Governance capabilities, including flexible workflows, support for automated assignment of entitlements based on roles, approval processes, and self-service functionalities, are available. Strong policy management is available and includes an SAP XACML policy integration that enables real-time SoD checking. The solutions also provide intelligence to the customer through outlier and anomaly detection, risk scoring, and recommendations. Good access certification, event-based micro certification, and triggers to initiate recertification are given. SAP Access Governance capabilities come 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. OOB integration to popular third-party ITSM tools is not given, although a workflow interface does help extend capabilities.

SAP provides a very modern and professional look and feel within its UI and dashboards. Good support for user access self-service is given, including support for access requests through chatbots and messaging platforms. Authenticator options to both user and admin portals are based and missing FIDO and other biometric options. The product delivers good IGA related reporting and auditing capabilities, although support of out-of-the-box reports for major compliance frameworks is limited to SOX. Integration support for SIEM solutions is not given.

SAP Access Control is on-premise or in the cloud via Private Cloud Extended (PCE) option, with SAP Identity Access Governance as their fully multi-tenant cloud solution. For hybrid deployments, SAP Cloud Identity Access Governance (integration edition) is available for extending SAP Access Control for SaaS applications. The delivery option for on-premise is a virtual appliance. On-premise delivery as a hardware appliance, software deployed to a server, or container-based options is not given. Both SaaS and managed services are also available as well. Less than half of the product\'s functionality is exposed via REST APIs, and SOAP APIs are not available. Missing is CLI and SDK support, although a toolkit for integration connectors based on web services is given.

SAP maintains a significant customer base in North America and the EMEA regions, with less presence in

the other regions of the world. Overall, SAP provides a well-rounded set of IGA features. Despite the limitations mentioned, SAP Identity Management remains a contender in the IGA market and a preferred vendor for organizations with significant investments in SAP software.

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

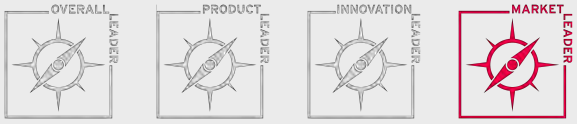
Strengths

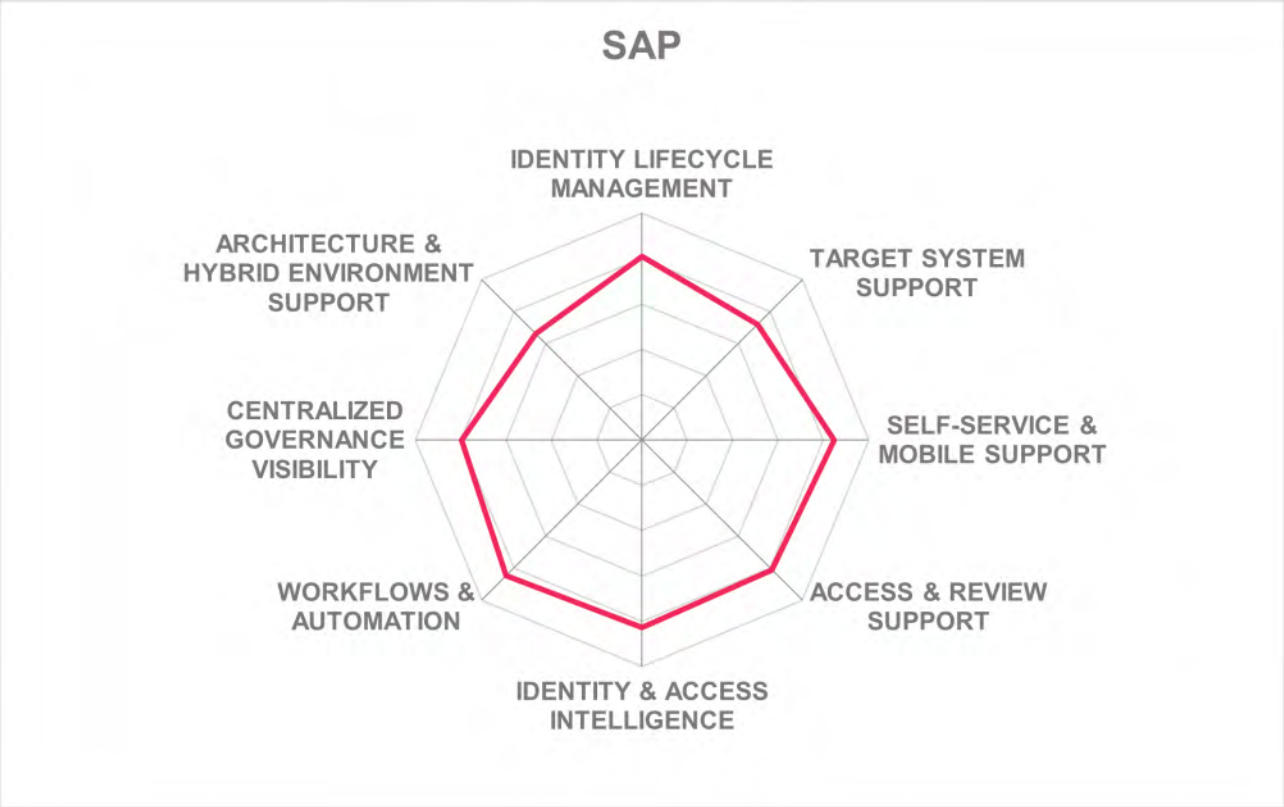
- Identity lifecycle management
- Identity Provisioning feature set
- Access review & risk analysis capabilities
- Good role management
- Identity and access intelligence
- Workflow and automation support
- Useful and modern UI
- Excellent integration into SAP environments, including SAP Access Control

Challenges

- Strong connector support for on-premises systems, but some gaps particularly for non-SAP business applications and SaaS applications
- Limited on-premise deliver options
- Basic user self-service and admin authenticator options

Leader in




SAP
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.23 Saviynt

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

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

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

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

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

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

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

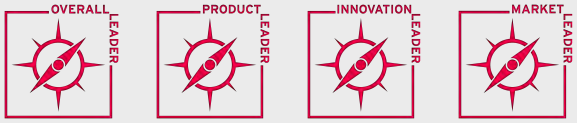
Strengths

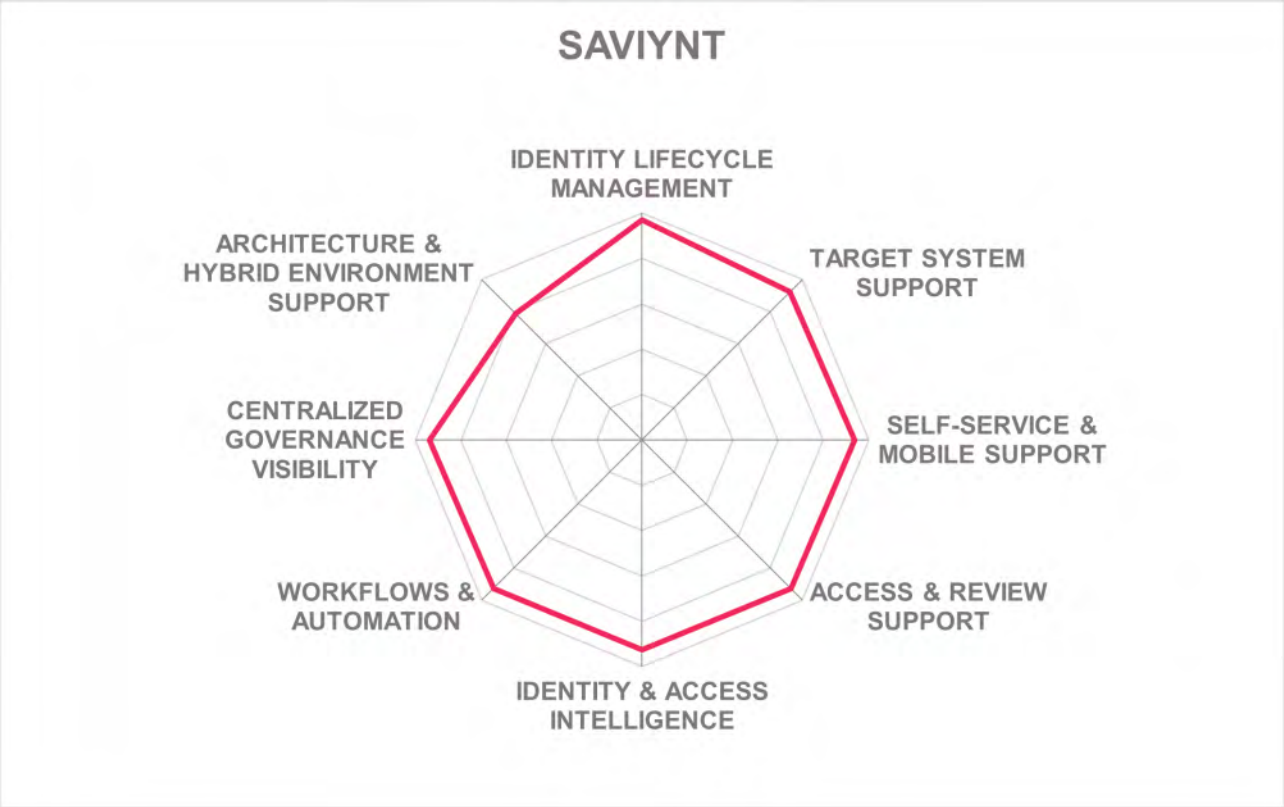
- Good identity lifecycle management
- Strong target system support
- Automated application on-boarding
- Built-in RPA for legacy applications
- Flexible policy and workflow management
- Well laid out and user-friendly UI
- Good use of intelligence throughout
- Mature DAG and SoD risk management
- Good deployment and delivery options

Challenges

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

Leader in




SAVIYNT
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.24 SecurEnds

SecurEnds is an Access Management vendor with their Credential Entitlement Management (CEM) solution offering an alternative to traditional Identity Governance. SecurEnds provides a cloud-based identity governance platform between its customer\'s identity stores and the applications and services. The SecurEnds platform addresses many of the governance challenges experienced by organizations by providing IGA related capabilities from access governance to identity risk analysis.

SecurEnds provides a wide range of connectors to the most common and popular identity repositories. Although a moderate range of out-of-the-box (OOB) connectors to SaaS systems are given, fewer OOB connectors are available for on-premise systems. Alternatively, SecurEnds Flex-Connectors provide a solution for more complex connection use cases, such as connections to legacy systems. All connectors are currently RESTful API-based, and third-party SCIM connectors are available as well. Good access certification features include event-based micro-certification and a good range of recertification triggers such as access risk, schedules, outliers, and fraud indicators. Separation of Duty (SoD) policies can be created, queried or SoD review campaigns can be conducted in a similar manner as the applications and entitlements access review campaigns. Supported ITSM integrations include ServiceNow, Jira, Zendesk, and TrackIT.

One of the SecurEnds strengths lies within its well throughout and useful web UI. The SecurEnds dashboards of its Identity Risk & Analytics solution provide real-time graphics of user data. The SecurEnds Identity Analytics module has many features, including mind maps of identities and entitlements and other AI/ML analytics. The identity mind map graphically represents identities, applications, credentials, and entitlements with an identity-centric view across all entitlements and applications. For a given identity, all applications or services are listed. Selecting any of the user's applications will further expand to show all user groups, roles, or entitlements for that application. All graphical data can be exported for additional analysis or reporting. The user self-service portal capabilities are good, although they lack support for more advanced access request support through chatbots or messaging platforms (e.g., slack). Basic authenticator options are available for both user self-service and administrative portals.

SecurEnds CEM is microservice-based capable of supporting cloud, on-premise, and hybrid deployment models, which can be delivered as either SaaS, hardware appliance, Docker container, or software deployed to a server. A managed service is also offered. To run the solution as-a-service, SecurEnds agents need to be installed on-premises. The solution\'s capabilities are not exposed via APIs or CLIs. SDK support is not available.

SecurEnds is an emerging privately held company established in 2016, with mid-market to enterprise customers primarily located in North America with growth in the EMEA and APAC regions. Overall, SecurEnds Credential Entitlement Management provides good access governance capabilities for organizations looking for a fully integrated Identity suite with a good centralized governance view of their applications and services.

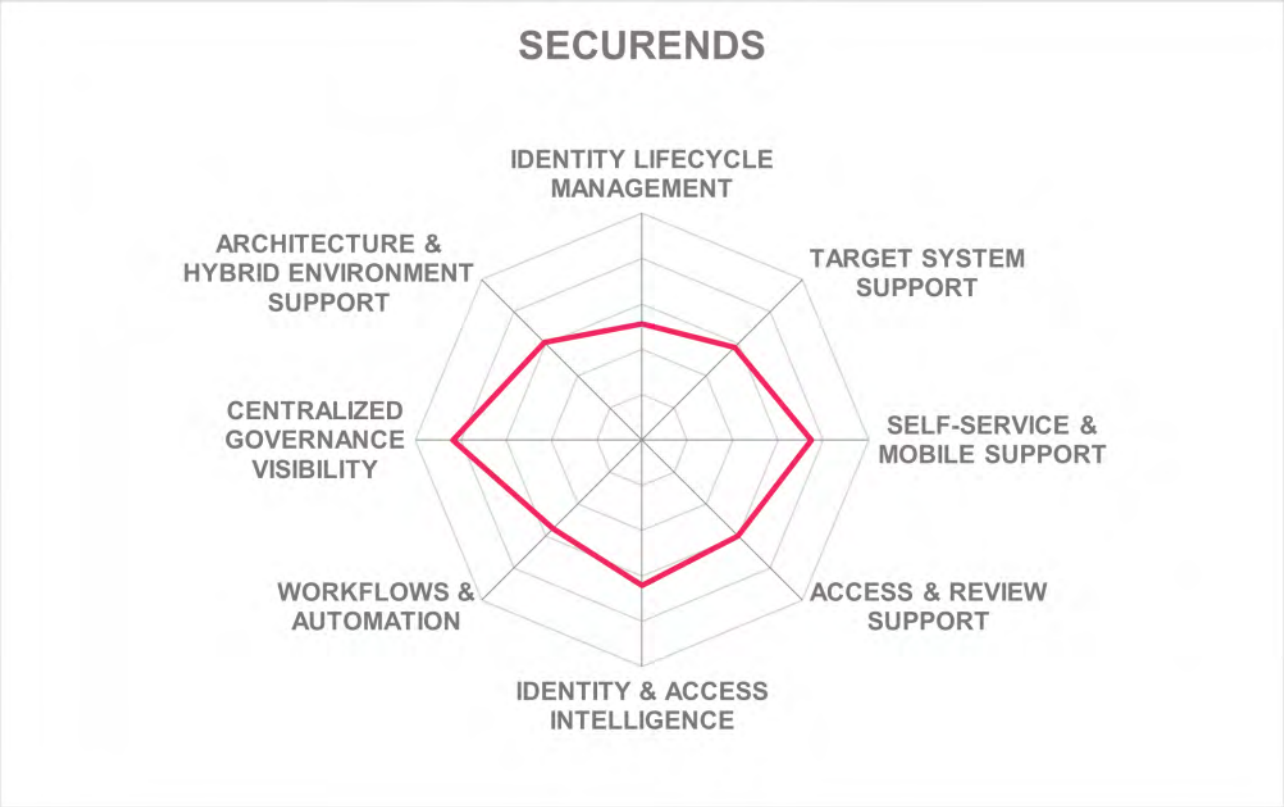
Security	● ● ● ● ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

Strengths

- Centralized governance visibility
- Identity & access intelligence
- User self-service
- Access review capabilities
- Flex connector for complex use cases
- Modular and scalable appliance-based architecture

Challenges

- Limited market presence outside North America
- Partner ecosystem still in early stages
- Reliance on third-party SCIM connectors
- Limited DevOps support (APIs, CLIs, SDKs)


SECURENDS
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.25 SecurID

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

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

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

SecurID G&L can be deployed as a hardware appliance, virtual application, software-only, or bundled. It can also be delivered as a Docker container model. Additionally, a set of database views are available for customers requiring data access views. In addition to on-premises deployment options, SecurID offers all on-premise functionality available in its cloud-based offering as well as managed service offerings that are available from both SecurID partners and SecurID Professional Services. In addition to the user interface, SecurID provides access to over half of its solution functionality via REST-based APIs. SDKs are only available for Java and JavaScript programming language with much less access to the functionality than their REST-based APIs. SPML and SCIM support is available for identity provisioning/de-provisioning. RSA Link also provides an interactive community portal for product, engineering, services, support, and other information.

SecurID security maintains a substantial global customer base in mid to enterprise-level organizations. SecurID's dominance of GRC and authentication markets have helped SecurID cross and upsell SecurID G&L for IGA. Further, SecurID G&L takes a risk-based approach to Access Governance. SecurID G&L is a

good choice for organizations with existing deployments of SecurID products and has primary IGA requirements for identity task automation, Access Governance, and identity & access intelligence while avoiding extensive customizations.

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

RSA SecurID®

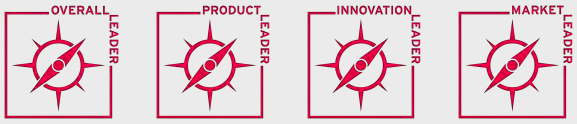
Strengths

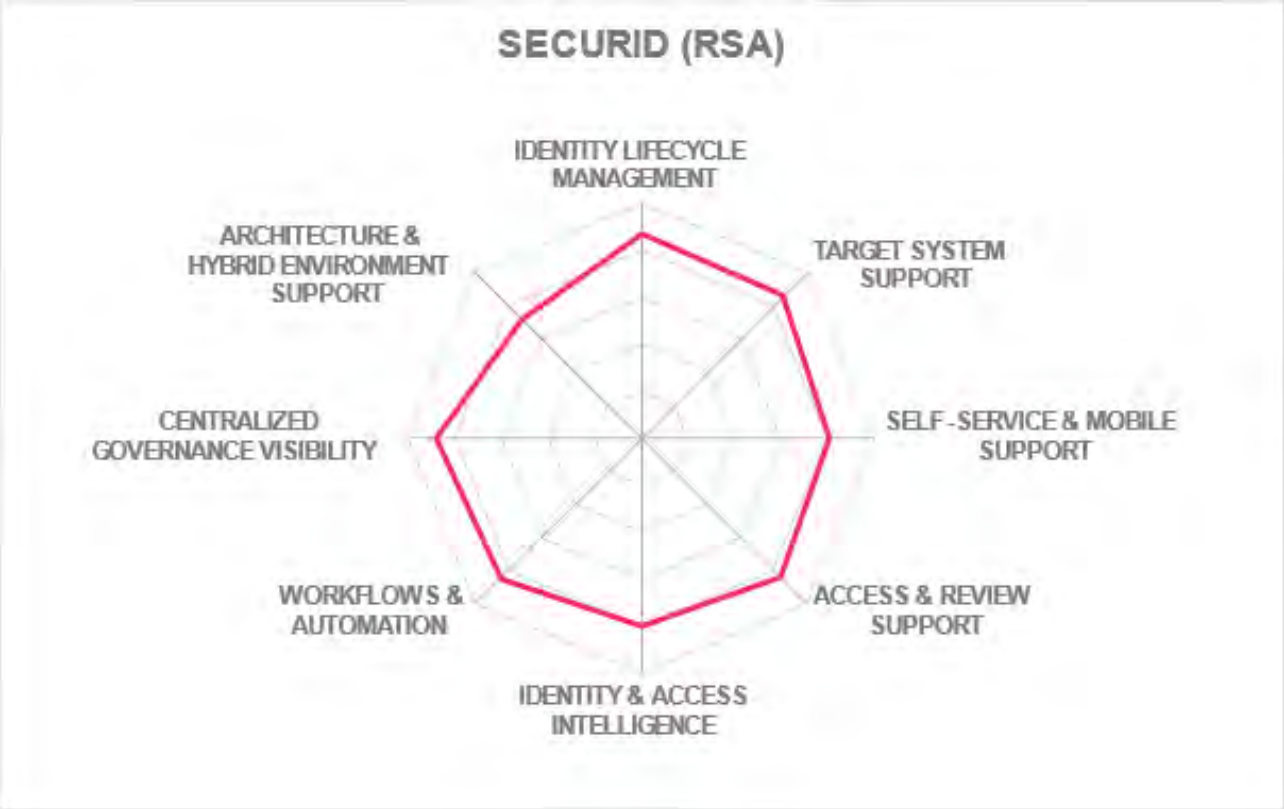
- Identity lifecycle management
- OOB on-premise and SaaS connector support
- Risk-based Access Governance
- User-friendly interfaces
- Identity & access intelligence capabilities
- Strong partner ecosystem
- Global presence across all industry verticals
- Useful user community portal

Challenges

- The effects of acquisitions and spin-offs with EMC, Dell, and now STG left the product strategy unclear, although the recent business alignment of the SecurID product line may increase focus and investment moving forward
- 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




SECURID (RSA)
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.26 Simeio Solutions

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

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

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

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

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

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

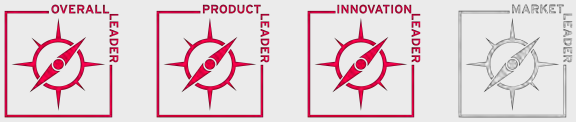
Strengths

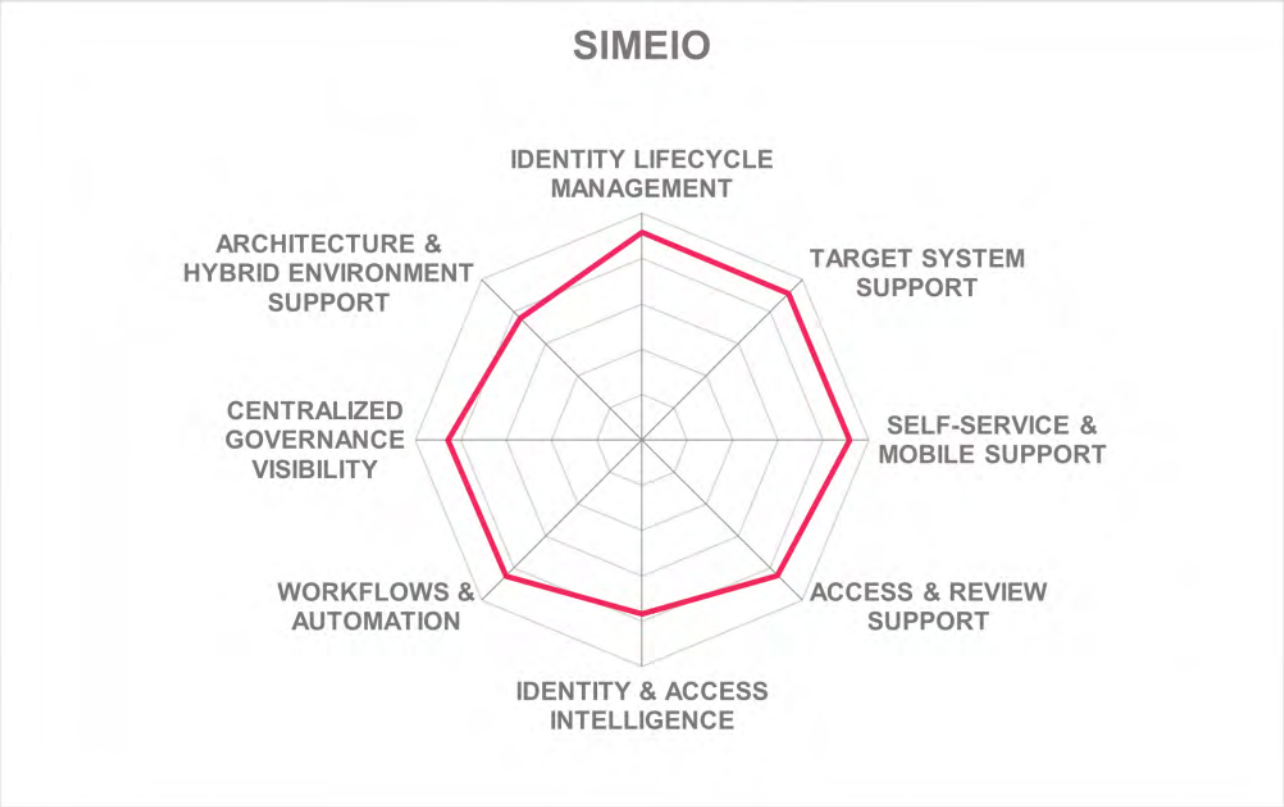
- Identity lifecycle management
- OOB connectors to on-premises and SaaS target systems
- User self-service
- Access & review support
- Identity & access intelligence
- Modern and user-friendly UI
- Workflow and automation
- Mobile application

Challenges

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

Leader in




SIMEIO
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

5.27 Soffid

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

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

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

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

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

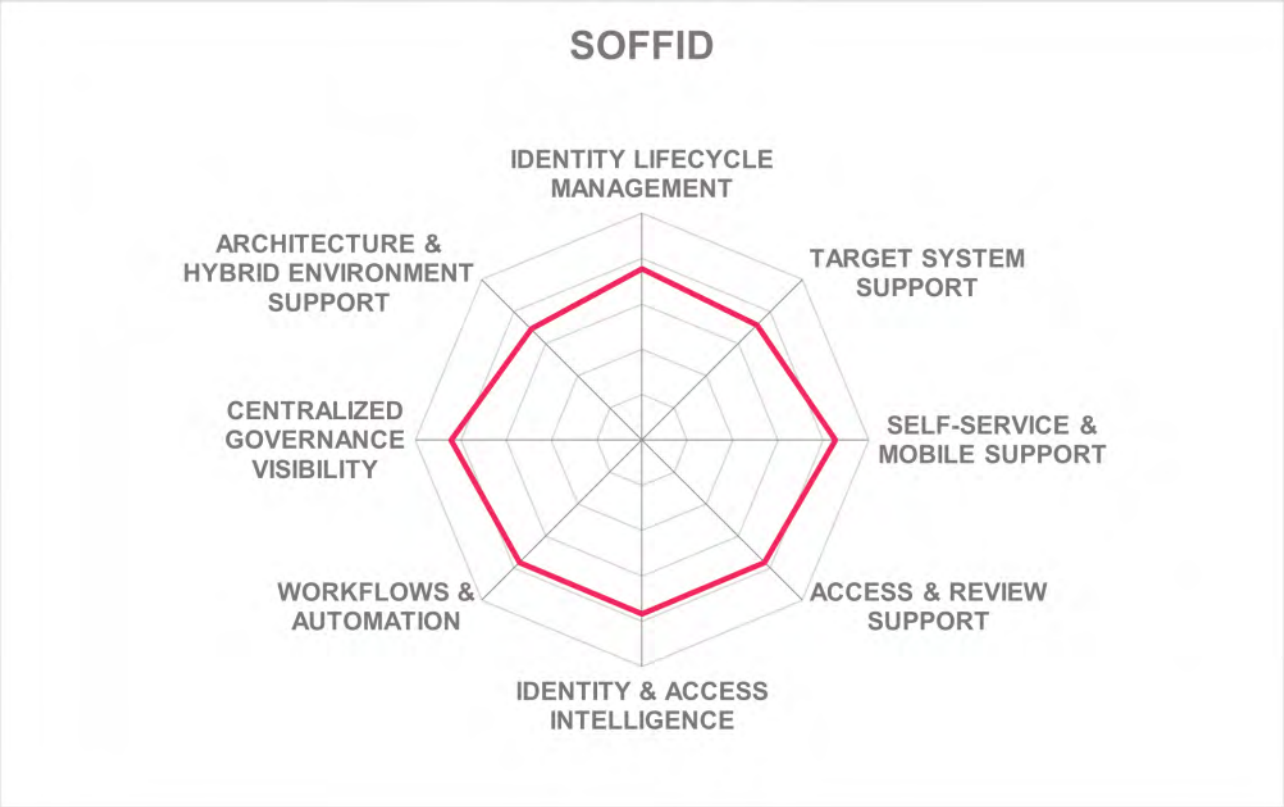
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●○

Strengths

- OOB on-premises target system support
- Flexible attribute mapping
- Good self-service & administration access authentication options
- All functionality exposed via APIs
- OOB workflow templates
- IGA related reports OOB
- Good IGA related policy management

Challenges

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


SOFFID
IDENTITY LIFECYCLE MANAGEMENT
TARGET SYSTEM SUPPORT
SELF-SERVICE & MOBILE SUPPORT
ACCESS & REVIEW SUPPORT
IDENTITY & ACCESS INTELLIGENCE
WORKFLOWS & AUTOMATION
CENTRALIZED GOVERNANCE VISIBILITY
ARCHITECTURE & HYBRID ENVIRONMENT SUPPORT

6.1 Accenture Memority

Accenture Memority is provided by a unit within Accenture Security, delivering an IDaaS solution. Memority started as an independent software vendor and has become part of that larger group three years ago. Thus, Accenture Memority 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 Memority 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 Memority 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.

Altogether with the ability of Accenture to support customers in their Digital Transformation initiatives, Accenture Memority has the potential to become the backbone of future IAM of digital businesses.

Why worth watching: Amongst other capabilities, Accenture Memority has a strong focus on providing a consistent and comprehensive API layer and IoT support as part of its solution.

6.2 Clear Skye

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

Why worth watching: Clear Skye IGA help organizations that require lower barrier IGA products or where existing IGA solutions are manual process intensive, and benefit customers that would like to leverage their existing ServiceNow investment complementing it with Clear Skye IGA.

6.3 Imprivata

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

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

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

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

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

6.4 Kapstone

Founded in 2013 with headquarters on the east coast in the northeastern US, Kapstone released its Access Review product with Day Zero Application Onboarding and Attestation in 2016, and introduced Kapstone's Provisioning Gateway and Intelligent Identity products the following year. More recently, Kapstone added both Autonomous IGA and Cloud Governance to its product portfolio. Today Kapstone's Autonomous IGA provides an innovative platform that focuses on three key capabilities - Automation, Intelligence, and Modularity.

Beyond core IGA capabilities, Kapstone Autonomous IGA gives some more advanced features that include service discovery, delegated administration, intelligent identity, application discovery and IGA application on-

boarding, role discovery and automated access policies, IDaaS configuration management and analytics, as well as AWS, OCI governance. Kapstone also provides services to map IAM controls to such things as the NIST or HIPPA requirements as well as assessing an organizations security posture.

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

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

6.5 Pirean

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

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

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

6.6 Systancia

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

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

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

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

6.7 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.

Why worth watching: With a good product roadmap and execution capability, TOOLS4EVER can make some good progress over the next few years to be able to contend with the existing IDaaS players in the region.

6.8 Tuebora

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

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

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

6.9 Usercube

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

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

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

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

7 Related Research

https://www.kuppingercole.com/report/lc80063

https://plus.kuppingercole.com/article/ev80319/forgerock-access-management/

https://plus.kuppingercole.com/article/ev80399/hitachi-id-iam-suite/

https://plus.kuppingercole.com/article/ev80438/ibm-security-verify-for-ciam/

https://plus.kuppingercole.com/article/ev80177/ilantus-compact-identity/

https://plus.kuppingercole.com/article/ev80103/micro-focus-identity-governance/

https://plus.kuppingercole.com/article/ev80158/nexis-controle-3.4/

https://plus.kuppingercole.com/article/ev80506/omada-identity-suite/

https://plus.kuppingercole.com/article/ev80413/one-identity-active-roles/

https://plus.kuppingercole.com/article/ev80436/oracle-cloud-guard/

https://plus.kuppingercole.com/article/ev80149/ideiio/

https://plus.kuppingercole.com/article/ev80321/identityiq-sailpoint/

https://plus.kuppingercole.com/article/ev80150/securends-credential-entitlement-management/

https://plus.kuppingercole.com/article/ev80151/simeio-identity-orchestrator/

https://plus.kuppingercole.com/article/wp80424/overcoming-identity-governance-challenges-with-forgerock-autonomous-identity/

https://plus.kuppingercole.com/article/wp80432de/identity-governance-herausforderungen-mit-forgerock-autonomous-identity-bewaeltigen/

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

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

Figure 3: Product Leaders in the IGA market segment

Figure 4: Innovation Leaders in the IGA market segment

Figure 5: Market Leaders in the IGA market segment

Figure 6: The Market/Product Matrix.

Figure 7: The Product/Innovation Matrix.

Figure 8: The Innovation/Market Matrix.

Copyright

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

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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