kuppingercole
ANALYSTS

Access Governance
Nitish Deshpande
May 8, 2023

LEADERSHIP
COMPASS
2023

The Access Governance (AG) market is continuing to evolve through more intelligent solutions. This Leadership Compass will give an overview and insights into the IGA market, providing you a compass to help you find the products that can meet the criteria necessary for successful IGA deployments.

Contents

Figures

Introduction / Executive Summary

The KuppingerCole Leadership Compass provides an overview of vendors and the services and products they offer in a particular market segment. This Leadership compass focuses on the market segment of access governance, including specific capabilities for access intelligence. While most vendors offer either identity provisioning or access governance focused products, many others offer combined or separate products for both identity provisioning and access governance integrated into what is today frequently called IGA (Identity Governance and Administration).

The AG 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 AG market with notable vendors and their products or services in the market.

From our interaction with organizations of varied IAM maturity across industry verticals, we note that while some are still looking for an identity provisioning solution with limited or no access governance capabilities, many others have emerging requirements for a promising and stand-alone access governance solution. As security leaders consider access governance to be an important part of their overall IAM strategy to build a robust identity analytics platform, we see a considerable shift in the product roadmap of IAM vendors to support access governance features and build better access intelligence capabilities. There is an increased demand for access governance 'only' products in the market, especially from organizations that already have an identity provisioning tool in place or whose entry point for IAM is access governance. One of the more common adoption patterns we have observed in the market is where fulfilment through identity provisioning is achieved via a managed service, and access governance is run by and within the organization itself to retain absolute control over governance functions. Several other adoption patterns for access governance products are witnessed in the industry, including where an organization's primary requirement is better access governance for enhanced audibility and role governance.

One of the adoption patterns we have observed in the market is Access Governance, which 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 a customer's immediate requirements are limited to Access Governance but do not demand an IGA solution. It is important that organizations scope their AG requirements well before starting to evaluate products that differ in the strength of functionalities, making most of them better aligned for either provisioning or governance focused deployments.

Based on these adoption trends, changing customer priorities, and deployment patterns, we decided to center on Access Governance holistically in this leadership compass to help

security leaders identify relevant IAM market segments and subsequently shortlist the most appropriate technology vendors based on their immediate IAM priorities. In this Access Governance Leadership Compass, primary focus is on access governance and Intelligence capabilities, with required integrations into own or third-party entitlements and/or account repositories. We look at complete AG offerings here to if they have strong access governance & Intelligence capabilities.

This AG Leadership Compass follows a published Leadership Compass for Identity and Governance Administration (IGA). 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. This Leadership Compass on Access Governance is a specialized version which will evaluate vendors based on core access governance capabilities. It will not include vendors who have strong ILM capabilities. A Market Compass (MC) on IAM solutions for mid-sized organizations is in development, while a leadership compass on Identity Fabrics replaces LC IAM Suites.

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

Highlights

- This Leadership Compass evaluates 25 AG product vendors.
- The AG market is growing, and although maturing it continues to evolve.
- AG is essential to business as a strategic approach to ensure overall IT security and regulatory compliance.
- The level of identity, access and risk intelligence has become a key differentiator between AG product solutions.
- Automation is a key trend in AG to reduce management workload by automating tasks and providing process workflows.
- Leading AG 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, Beta Systems, Broadcom, EmpowerID, Evidian, IBM, Microsoft, OpenText (Micro Focus), Netwrix Corporation, Omada, One Identity, Oracle, RSA, SAP, SailPoint, Saviynt, Simeio
- The Product Leaders (in alphabetical order) are Avatier, Beta Systems, Bravura Security, Broadcom, EmpowerID, Evidian, IBM, Microsoft, OpenText (Micro Focus), Netwrix Corporation, Omada, One Identity, Oracle, RSA, SailPoint, Saviynt, Simeio
- The Innovation Leaders (in alphabetical order) are Avatier, Broadcom, EmpowerID, IBM, Microsoft, OpenText (Micro Focus), Netwrix Corporation, Omada, One Identity, Oracle, RSA, SailPoint, Saviynt, Simeio
- Leading vendors in innovation and market (a.k.a. the "Big Ones") in the IGA market are (in alphabetical order) Broadcom, EmpowerID, IBM, OpenText (Micro Focus), Microsoft, Netwrix Corporation, One Identity, Oracle, RSA, SailPoint, Saviynt, Simeio.

Market Segment

Access Governance & Intelligence is an IAM focused risk management discipline that facilitates business involvement in the overall management of access rights across an organization's IT environment. Access governance provides necessary (mostly self-service) tools for businesses to manage workflows and access entitlements, run reports, access certification campaigns, and SOD checks. Access intelligence refers to the layer above access governance that offers business-related insights to support effective decision making and potentially enhance access governance. Data analytics and machine learning techniques enable pattern recognition to deliver valuable intelligence for process optimization, role design, automated reviews, and anomaly detection.

Access governance concerns the access mechanisms and their relationships across IT systems and is instrumental in monitoring and mitigating access-related risks. These risks most commonly include information theft and identity fraud through unauthorized changes and/ or subversion of IT systems to facilitate illegal actions. During the last few years, many prominent security incidents originated from poorly managed identities and proved the need to address these issues across all industry verticals. Data thefts, loss of PII (Personal Identifiable Information), breach of customer's privacy, and industrial espionage are becoming common security risks in virtually every industry today.

Access Governance, an IAM focused risk management discipline, focuses on providing answers to three key questions:

- Who has access to what?
- Who has accessed what and why?
- Who has granted that access?

That is done via a set of functionalities, which include the following features:

- Access Warehouses: Collecting current and previous access information from different systems. The collection can be done via direct or extensible connectors using established standards such as HTTP or webservices. Provisioning connectors or flat file imports are commonly used for the purpose.
- Access Certification: Requiring the responsible persons (such as resource owners or application managers) to do scheduled or ad-hoc reviews of the current status of access controls and request changes if required.
- Access Analytics and Intelligence: Analytical capabilities to facilitate business-friendly understanding of the current status of access controls, sometimes complemented by adding real-time monitoring information about access to IT assets.
- Access Risk Management: Using a risk-based approach to evaluate and assign risk score for access requests and invoking relevant access workflows and notifications based on configured policies.
- Access Request Management: Providing interfaces to request access to specific information or systems including workflow policy configurations to define and manage request flows.

- SoD controls and enforcement: Definition and enforcement of business rules to identify and prevent Segregation of Duty risks.
- Enterprise Role Management: A complementary technology given that roles are the typical method used to manage access. Thus, Enterprise Role Management, including the capability of analyzing and defining roles, is mandatory.

Access governance is one of the key IAM technologies for any organization due to the massive impact of potential security risks arising from the lack of proper access governance controls. Access risks can have a severe operational impact and can be derived from organizational-wide security risks – the Barings Bank incident and the Société Générale scandal being prominent examples of such risks that could have been prevented with appropriate access governance in place. There are several other access-related security risks in today's organizations that have a direct impact on business, including but not limited to, intellectual property theft, occupational fraud in ERP systems including SOD conflicts and other policy violations, reputational damage due to the loss of customer information and privacy-related data, and many more. Thus, an adequate access governance framework is essential for organizations dealing with continually changing paradigms of security and risk management.

Access governance products focus on implementing and governing the controls for access management. This includes controls for attestation and recertification processes as well as auditing, reporting, and monitoring capabilities, which, in turn, invoke active management of preventive controls to identify and mitigate the access risks. Additional aspects are data analytics for pattern recognition to drive process automation, effective role management, anomaly detection, and access simulation as part of access intelligence capabilities.

From KuppingerCole's perspective, a complete access governance approach must go beyond the governance of "standard users" to include privileged users as well. Most access certification reviews today are conducted at the application level. It is becoming increasingly important for organizations to have a consolidated view of a user's access entitlements, including access to privileged accounts. Conducting separate access certification campaigns for standard and privileged access can be complex and time-consuming. While privileged users are pretty much the same as "standard" users from an access governance perspective, Privilege Management tools add features such as restricting elevation of rights at run-time and managing shared account passwords. Complete solutions would require tight integration between both groups of capabilities to identify the risks in access governance and mitigate them by using specific Privilege Management capabilities. Some privilege management vendors are beginning to offer access governance features of their own, while most others offer integration with access governance tools to deliver a common access governance platform for standard and privileged users.

We also see the need for looking at advanced, integrated capabilities of managing access controls within the target systems such as SAP environments or Microsoft Windows File Server/Active Directory environments. Some vendors are moving in the direction of Data access governance.

From a KuppingerCole view, there is a need for specific tools to provide in-depth governance and management functionality under the integrated layer of CCM (Continuous Controls Monitoring) or IT GRC. While there is some functional overlap, we don't expect the available GRC tools to deliver even basic capabilities to meet the access governance requirements of organizations. An integration with GRC tools, however, is a recommended approach for several reasons, including gaining better visibility in the state of access-related compliance and feeding any regulatory changes into the access governance framework.

To summarize, we consider the following features as core elements of an access governance solution:

- Role Management to define, create and assign roles for users. Role management also includes role mining based on the most relevant and efficient grouping of access entitlements. Advanced role management capabilities include pattern and risk analysis as well as role simulations for efficient policy administration and effective provisioning.
- Attestation and Recertification as a continuous control activity which besides supporting periodic access attestation, allows organizations to detect modifications and invoke ad-hoc recertifications while continuing to analyze the status of access controls in a structured way.
- Auditing and Analysis features which support an after the fact view of access-related events and provide valuable intelligence for enhanced governance.
- Access Request Management as the standard interface for users to request access to IT assets from access catalogue and managers to review and approve the requests. Includes workflow and policy management to define and automate request flows, including automated reconciliation.
- Integrated privilege management features for extending these controls to privileged users, which aren't typically covered by the standard access governance tools today.

Over time, a deep integration with Dynamic Authorization Management Systems are used to centrally define policies for application as well as the requirement for system security. However, there are still few solutions in the market which provide minimal integration.
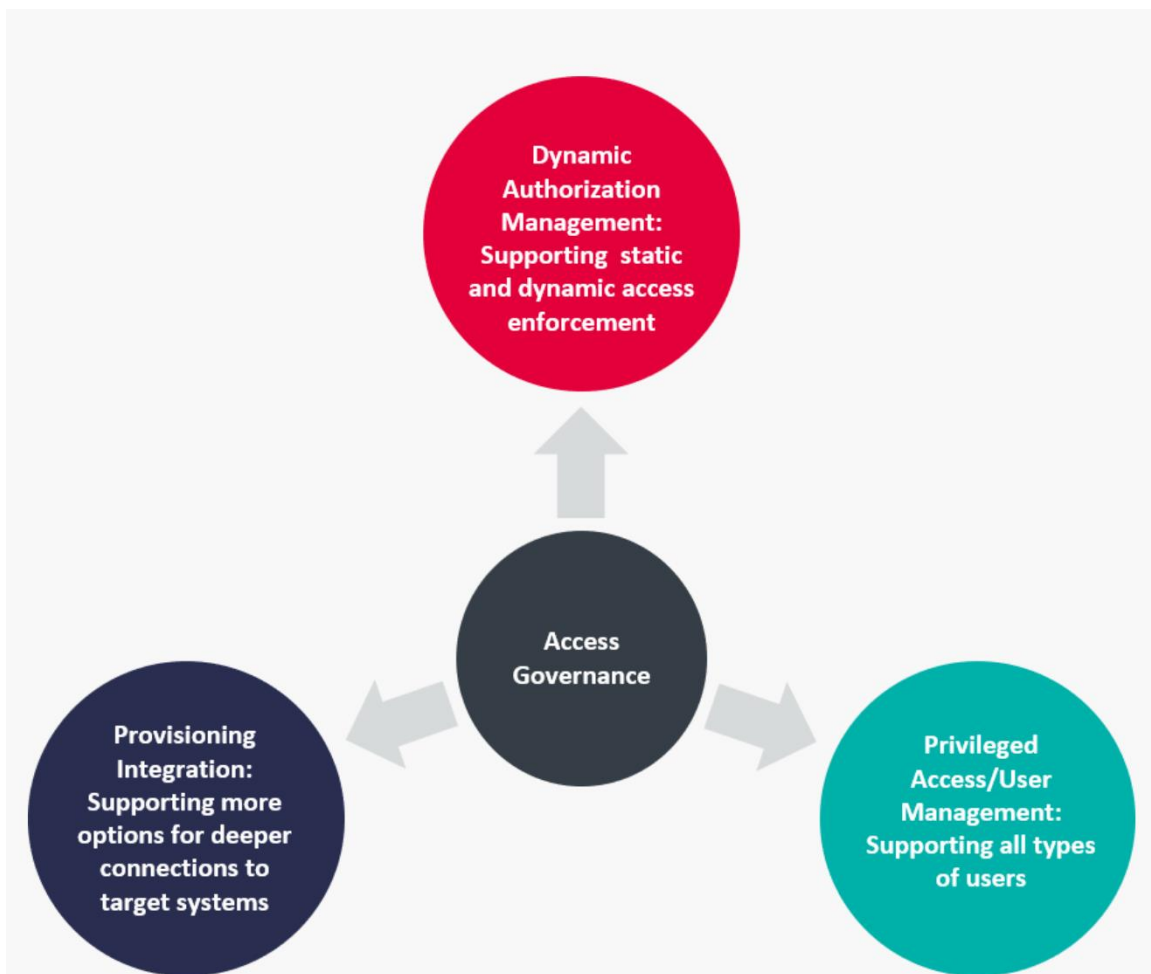
Figure 1: The Status and Expected Evolution of Access Governance

Delivery Models

This Leadership Compass is focused on products that run on-premises, either at the customer site or hosted by a Managed Service Provider (MSP) at their site or solution provided as as-a-Service (SaaS) hosted by the vendor.

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

Required Capabilities

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

- 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 management
- Tools that graphically support creating and customizing workflow
- Centralized access entitlement repository ("Access Warehouse")
- Access Intelligence capabilities
- Support for flexible role management
- Support for flexible definition of both access review campaigns and targeted access review requests triggered by e.g., events, risk scores, etc.
- Support for SoD policies and their enforcement
- Flexible customization of the UI to the specific demand of the customer organization
- Baseline connectivity to target systems and to identity provisioning systems
- Cloud connectors, adding access governance support for common cloud services
- Customization of mapping rules between central identities and the accounts per target system
- Business-friendly user interface
- Strong and flexible delegation capabilities

Beyond that, we also considered some specific features. These include, amongst others:

- Connectivity
  The ability to connect to various sources of target systems, including direct connections, integration with existing identity provisioning tools from various vendors, and integration to ITSM (IT Service Management) or Helpdesk ticketing tools. In general, we expect access governance solutions of today to not only read data from target systems but also initiate fulfilment and reconcile changes.
- Heritage of connectors
  Having connectors as OEM components or provided by partners is not recommended and considered a risk for ongoing support and available know-how at the vendor.
- SRM interfaces
  We expect that systems provide out-of-the-box integration to leading ITSM systems for manual fulfilment of provisioning requests.
- 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.
- Deployment models

Supporting multiple delivery options such as hard/soft appliances and optional MSP services gives the 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 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 access governance systems 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 all systems to provide built-in high-availability options or support for third-party HA components where required.

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

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

- Shopping cart paradigm
  These approaches are popular for simplifying the access request management process by using shopping cart paradigms familiar to the users.

- 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 in access governance, what counts is the quality and flexibility of role and risk models. These models should not only look nice but must have a strong conceptual background and sufficient flexibility to adapt to the customer's needs. Unfortunately, not

every tool that looks nice at first glance is sophisticated enough to cover all a customer's requirements. It should not be the customer adapting to the tool, rather the tool adapting to the customer.

- 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.

The support for these functions is added to our evaluation of the products. We have also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other solutions available in the market.

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify 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 various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

When looking at the Leader segment in the Overall Leadership rating, we see a picture that is a typical representation of very mature markets, where a considerable number of vendors deliver feature-rich solutions. The market continues to remain crowded, with 25 vendors chosen to be represented in our Leadership Compass rating. There were a few other vendors that did not meet our basic evaluation criteria, who are new entrants into the market listed in the "vendors to watch" section and those declined participation in this year's edition.
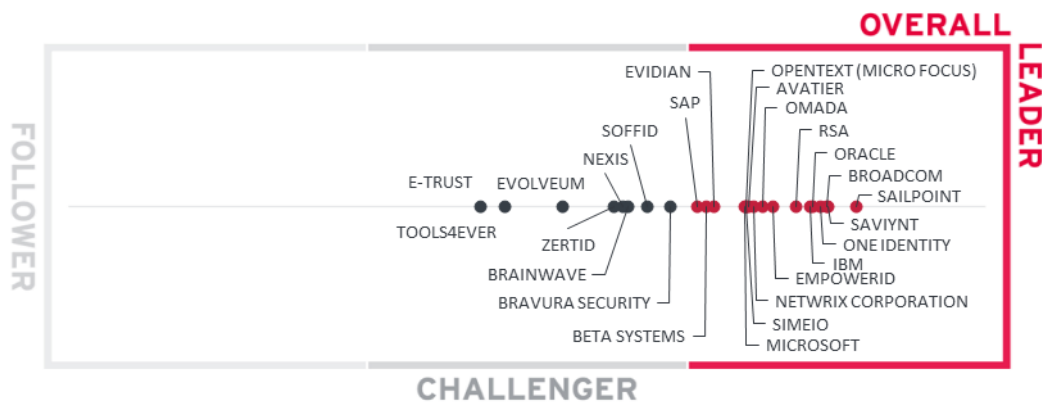
Figure 2: The Overall Leadership rating for the AG market segment

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

Other vendors in the Overall Leaders segment for AG include Avatier, Beta Systems, EmpowerID, Evidian, Microsoft, OpenText (Micro Focus), Netwrix Corporation, Omada, Simeio, SAP and Simeio. 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 AG capabilities and preferred by many organizations over the established players. Leading in this segment are Bravura Security, Soffid, Brainwave, Nexis and Zertid and Evolveum follow with some distance. Further vendors in this segment are E-Trust and Tools4ever. The Challenger segment shows vendors with good products with varying levels of AG capabilities, market presence throughout the world, or other market niche focus.

Overall Leaders are (in alphabetical order):

- Avatier
- Beta Systems
- Broadcom
- EmpowerID
- Evidian
- IBM
- Microsoft
- OpenText (Micro Focus)

- Netwrix Corporation
- Omada
- One Identity
- Oracle
- RSA
- SAP
- SailPoint
- Saviynt
- Simeio

Product Leadership

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

Figure 3: Product Leaders in the AG market segment

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services. As Access Governance (AG) is constantly maturing, we find several vendors qualifying for the Leaders segment as well as several vendors adding AG capabilities to their portfolio of product features. As vendors offer a wide variety of AG capabilities and differ in how well they support these capabilities, it is important for organizations to perform a thorough analysis of their AG requirements to align their priorities while evaluating an AG solution.

Leading from the front in Product Leadership is SailPoint, very closely followed by Saviynt and Omada. One Identity takes the position in the upper range of the Leader's segment, followed by a group of vendors including (in alphabetical order) Broadcom, EmpowerID, IBM, Oracle, and RSA, all of which deliver leading-edge capabilities across the depth and breadth of AG capability spectrum evaluated for the purpose of scoring the vendors in this Leadership Compass. IAM leaders must exercise appropriate caution while evaluating these vendors as subtle differences ignored in functionality evaluation of these products could translate into greater incompatibilities for business processes during implementation. It is therefore highly recommended that organizations spend considerable resources in properly scoping and prioritizing their AG requirements prior to AG product evaluation. Avatier, OpenText (Micro Focus) and Simeio are positioned next as leaders in the product leadership segment, followed by Evidian, Bravura Security, Beta Systems, Netwrix Corporation and Microsoft towards the bottom edge of the leaders' segment.

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

Product Leaders (in alphabetical order):

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

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 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 AG market segment

We rated just over half of all vendors as Innovation Leaders in the Access Governance (AG) market. Given the maturity of AG solutions, the amount of innovation we see is fairly 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 AG products, desired levels of scalability and flexibility can considerably affect the ease of deployment for most large AG 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 and Saviynt leads the Innovation Leadership evaluation followed by a group of vendors of Broadcom, One Identity and Oracle. A group of vendors of Avatier, EmpowerID, Omada, and IBM is closely following the leaders. RSA, Simeio, and Netwrix Corporation continue to strengthen their AG leadership position with constant innovation. Microsoft and OpenText (Micro Focus) appear in the lower of the segment with considerably less innovation. These vendors are making significant changes to their AG product portfolio to be in line with other innovative vendors. These vendors differ in many details when it comes to innovation and how they balance innovation with overall product leadership. Therefore, a thorough vendor selection process is essential to pick the right vendor from all the AG players which best fit the customer requirements.

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

Innovation Leaders (in alphabetical order):

- Avatier
- Broadcom
- EmpowerID
- IBM
- Microsoft
- OpenText (Micro Focus)
- Netwrix Corporation
- Omada
- One Identity
- Oracle
- RSA
- SailPoint
- Saviynt

- Simeio

Market Leadership

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

Figure 5: Market Leaders in the AG market segment

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

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

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

Market Leaders (in alphabetical order):

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

Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking for both a product leader and a vendor who will deliver a solution that is both feature-rich and continuously improved. This is indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

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

The Market/Product Matrix

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

Figure 6: The Market/Product Matrix

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

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

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

In the upper right segment, we find the "Market Champions." Given that the AG market is maturing fast, we find SailPoint, Broadcom, IBM, RSA, One Identity and Oracle as market champions positioned in the top right-hand box. Close to this group of established AG players, in the same box, are (in alphabetical order) Beta Systems, Evidian, Microsoft, Netwrix Corporation and OpenText (Micro Focus). Being positioned closer below the axis, Bravura Security, EmpowerID, Saviynt and Simeio represents their inclination for stronger product leadership in comparison to the market leaders today.

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

In the middle right-hand box, we see the two vendors that deliver strong product capabilities for AG but are not yet considered Market Champions. Avatier and Omada 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) Brainwave, E-Trust, Evolveum, Nexis, Soffid, Tools4ever and Zertid.

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 while those 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 Omada and the remainder (in alphabetical order) Avatier, Broadcom, EmpowerID, IBM, OpenText (Micro Focus), Microsoft, Netwrix Corporation, One Identity, Oracle, RSA and Simeio - with most placing close to the axis depicting a good balance of product features and innovation.

In the top middlebox, we see Beta Systems, Bravura Security and 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) Brainwave, E-Trust, Evolveum, Nexis, SAP, Soffid, Tools4ever and Zertid having less product and innovations than the Technology Leaders.

The Innovation/Market Matrix

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

Figure 8: The Innovation/Market Matrix

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

In the upper right-hand corner box, we find the "Big Ones" in the IGA market, including (in alphabetical order) Broadcom, IBM, OpenText (Micro Focus), Microsoft, Netwrix Corporation, One Identity, Oracle, RSA, SailPoint, and Saviynt. EmpowerID and Simeio are placed in the same box, towards the bottom, indicating relatively lower market position as compared to the other established vendors.

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

In the middle top box, we find Beta Systems, Bravura Security, Evidian and SAP 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) Brainwave, E-Trust, Evolveum, Nexis, Soffid, Tools4ever and Zertid.

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Access Governance Platforms. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. This allows identification of highly innovative but specialized vendors or local players which provide strong product features but do not yet 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. Since some vendors may have multiple products, these are listed according to the vendor's name.

Product(s) from Vendor	Security	Functionality	Deployment	Interoperability	Usability
Avatier	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Beta Systems	Strong Positive	Positive	Positive	Positive	Strong Positive
Brainwave	Positive	Positive	Positive	Positive	Neutral
Bravura	Strong Positive	Positive	Strong Positive	Positive	Positive
Broadcom	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
EmpowerID	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
E-Trust	Positive	Neutral	Positive	Neutral	Positive
Evidian	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
Evolveum	Positive	Positive	Positive	Positive	Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
OpenText (Micro Focus)	Strong Positive	Positive	Positive	Positive	Strong Positive
Microsoft	Strong Positive	Positive	Positive	Positive	Strong Positive
Netwrix Corporation	Positive	Strong Positive	Positive	Positive	Strong Positive
NEXIS GmbH	Positive	Positive	Positive	Positive	Strong Positive

Omada	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
One Identity	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Oracle	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
RSA	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
SailPoint	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
SAP	Strong Positive	Positive	Positive	Positive	Positive
Saviynt	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Simeio	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Soffid	Positive	Positive	Positive	Positive	Strong Positive
Tools4ever	Positive	Neutral	Neutral	Neutral	Positive
Zertid	Positive	Positive	Positive	Positive	Strong Positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Avatier	Strong Positive	Neutral	Positive	Positive
Beta Systems	Neutral	Positive	Strong Positive	Strong Positive
Brainwave	Positive	Positive	Neutral	Positive
Bravura Security	Neutral	Positive	Neutral	Strong Positive
Broadcom	Strong Positive	Strong Positive	Strong Positive	Strong Positive
EmpowerID	Strong Positive	Positive	Positive	Positive
E-Trust	Weak	Neutral	Neutral	Neutral
Evidian	Positive	Positive	Positive	Strong Positive
Evolveum	Weak	Neutral	Weak	Strong Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive
OpenText (Micro Focus)	Positive	Strong Positive	Strong Positive	Positive
Microsoft	Positive	Strong Positive	Strong Positive	Strong Positive
Netwrix Corporation	Positive	Strong Positive	Strong Positive	Strong Positive
Nexis	Neutral	Neutral	Neutral	Neutral
Omada	Strong Positive	Neutral	Neutral	Positive
One Identity	Strong Positive	Strong Positive	Positive	Strong Positive
Oracle	Strong Positive	Strong Positive	Strong Positive	Positive
RSA	Positive	Positive	Strong Positive	Strong Positive
SailPoint	Strong Positive	Strong Positive	Strong Positive	Strong Positive
SAP	Positive	Strong Positive	Strong Positive	Strong Positive
Saviynt	Strong Positive	Positive	Positive	Strong Positive
Simeio	Positive	Positive	Positive	Positive
Soffid	Positive	Positive	Positive	Positive
Tools4ever	Weak	Positive	Positive	Neutral
Zertid	Neutral	Neutral	Neutral	Positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

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

Spider graphs

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

- Target System Support
  This category signifies baseline connectivity to target systems and identity provisioning systems, as well as the number of connectors and the breadth of target systems, including e.g., directory services, business applications, mainframe systems, and more. Broad support for standard cloud services is also considered. The depth of connector capabilities is also analyzed, particularly when it comes to connecting to complex target systems such as SAP environments or mainframes. Also looked at are customization capabilities for connectors through connector toolkits.
- Access Request and User Self-Service
  The ability to provide interfaces to request access to specific information or systems such. Also, the usability of user self-service interfaces is considered as well as features such as assigning risk scores for access requests or requesting access to IT assets from an access catalog. Also, evaluated are features that provide the ability to facilitate the review & approval process.
- Access Review Support
  Integrated Access Governance capabilities that support activities such as the review and disposition of user access requests, certification definitions & campaigns, and access remediation as examples.
- Access & Risk Intelligence
  Access and risk intelligence that provides business-related insights supporting effective decision making and potentially enhancing governance. Advanced capabilities that use machine learning techniques that enable pattern recognition for process optimization, role design, automated reviews, detection of compliance violations (e.g., SoD) and other types of anomaly detection are considered. Other capabilities can include the use of user access information from authentication and authorization events to analyze user access behavior patterns, detect anomalous access, or to mitigate access-related risks.
- Workflow and Access Policy Mgmt.
  This category looks at the solution's level of policy management features. Examples include the types of policies available, dynamic, or coarse-grained policies, capacity to make rule-based decisions, and the ability to define policies that ensure compliance, prevent SoD, and other policy violations as examples. Workflow capabilities are also

evaluated. Which includes workflow and policy management to define and automate flows, automated workflow reconciliation, as well as workflow policy configurations to define and manage request flows or evaluate and assign risk scores that invoke relevant access workflows.

- Audit, Compliance, & Reporting
  The ability to demonstrate compliance, support auditing, and forensic activities through capabilities such the logging of a user's access to resources, or administrators changes to the system, as well as running out-of-the-box, ad-hoc or custom reports in various formats.
- Authentication
  Level of support for strong and adaptive authentication for both administrators and end users accessing the service.
- Access Governance and role management
  This category includes ability to provide access governance and role management for features around but not limited to User Activity Monitoring (UAM), role mining, access risk management, certifications, and access governance for IoT devices.

Avatier – Avatier Identity Anywhere

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

Identity Anywhere supports all core Access Governance components such as group Automation/Self-Service, Workflow Manager, and Identity Analyzer. SPML and SCIM is supported for identity provisioning/de-provisioning and the solution has a broad set of OOB provisioning connectors available for a wide range of on-premises and cloud systems. Avatier can develop and implement custom connectors based on requirements within a two-week period. OOB integration is available to ServiceNow, Cherwell, BMC Helix ITSM and Atlassian Jira ServiceDesk. Solution has good support for a wide range of container-based platforms. SOAP, REST, SCIM, SAML, and OAuth API protocols are supported. Wide range of popular programming language SDKs for developers is also. The majority of Identity Anywhere functionality is accessible via REST APIs as well as some functionality via CLI. Good, centralized role management is given with role discovery capabilities as well as role mining support. Support for access and risk intelligence includes access modeling, anomaly, and outlier detection of entitlements and roles. Other intelligence capabilities include recommendations for potential re-certification candidates or similar peer access rights as examples.

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

Avatier is a privately held company that focuses on mid-market to enterprise organizations with customers and partner ecosystems located primarily in North America with growth in other regions. Avatier continues to innovate with its user-centric approach to AG that covers a wide range of governance use cases. Planned features include a full compliance control integration by regulatory framework and creation of user specific dashboards for audit, compliance, privacy, and security. Overall, Avatier's Identity Anywhere container-based platform is an improvement in the AG market. Organizations across the industry verticals seeking a solution to traditional AG deployment challenges should consider Avatier's Identity Anywhere.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 3: Avatier Identity Anywhere's rating

Strengths

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

Challenges

- Limited but growing presence and partner ecosystem outside North American market
- Multi tenancy not supported
- Limited marketing visibility

Leader in

AVATIER
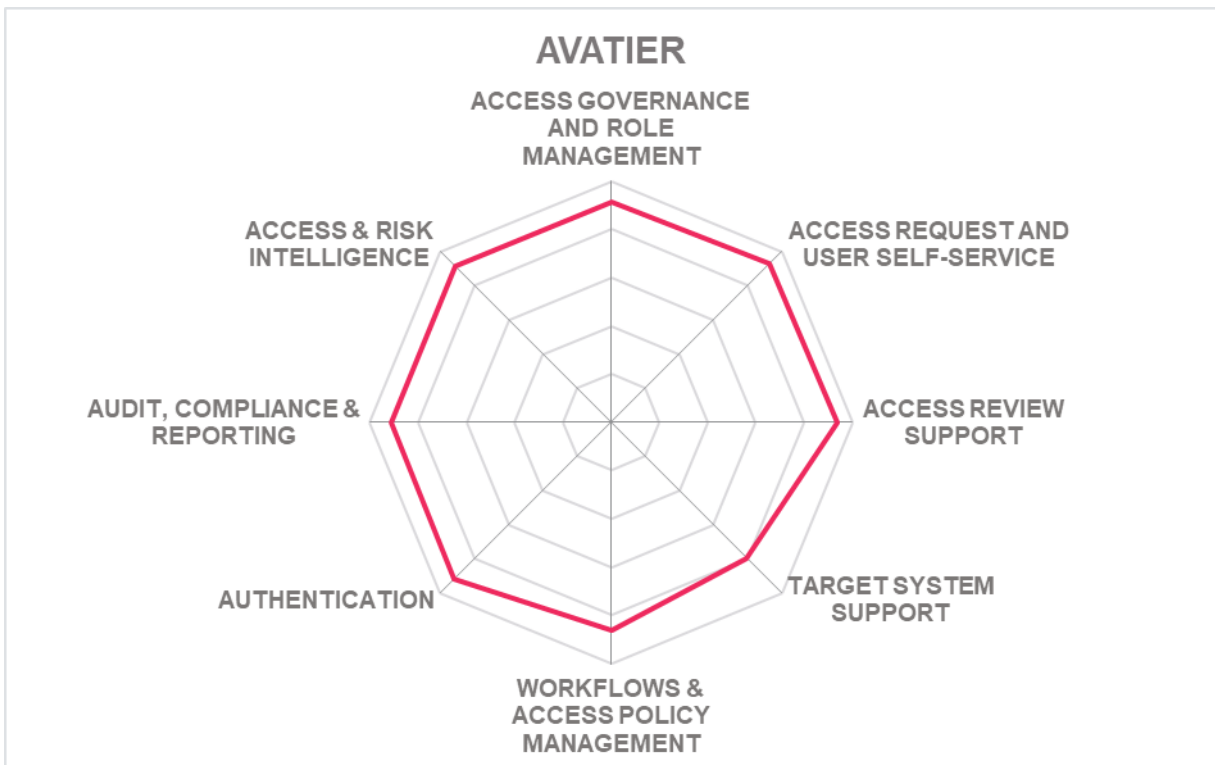
Beta Systems – Garancy IAM Suite

Garancy IAM suite supports on-premises as well as public and private cloud deployment, however, multi tenancy is not supported. This solution also supports hybrid installation with Garancy Identity Manager on-premises for identity administration and fulfillment, while AG modules on cloud.

Garancy IAM suite can be delivered as a service, virtual appliance, managed service and as a software deployed to the server. From 2022, support for container (Docker) based delivery is supported but hardware appliance delivery is missing. OOB integration to ITSM includes ServiceNow, Atlassian Jira ServiceDesk and BMC Helix ITSM. Garancy IAM's all functionalities are exposed via SOAP, REST, SCIM, LDAP and XML APIs while SDK support is limited to Java and JavaScript.

Garancy IAM suite supports SCIM and SPML for identity provisioning and deprovisioning. It offers strong support for a wide range of OOB connectors for on-premises and SaaS systems. There is good user self-service with wide range of authenticator options including passwordless authentication for admin and delegation of workflows. It has API based availability for micro services from this year, which allows orchestration for third party system. The solution supports reverting back changes after acting, for example, deletion or reinstating of orphaned accounts. Strong support for a wide range of IGA related OOB report types and reports for major compliance frameworks are available OOB. The built-in role management capability allows for the efficient and automated assignment of entitlements. Beta Systems also provides the Garancy Data Access Governance module that manages user access entitlements and authorizations for unstructured data at a granular level. The DAG is a separate module but can be integrated with other Garancy modules to offer a complete IGA solution. Access intelligence is given, providing strong reporting and dashboarding capabilities, although basic support for SOD risk analysis and transaction monitoring.

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

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

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 4: Beta System Garancy IAM Suite's rating

Strengths

- Good Workflow customization flexibility
- Strong user self-service support
- Impressive list of connectors for target system support
- Strong support for analytics
- Support for Dynamic Authorization Management
- Strong support for compliance and reporting

Challenges

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

Leader in

BETA SYSTEMS
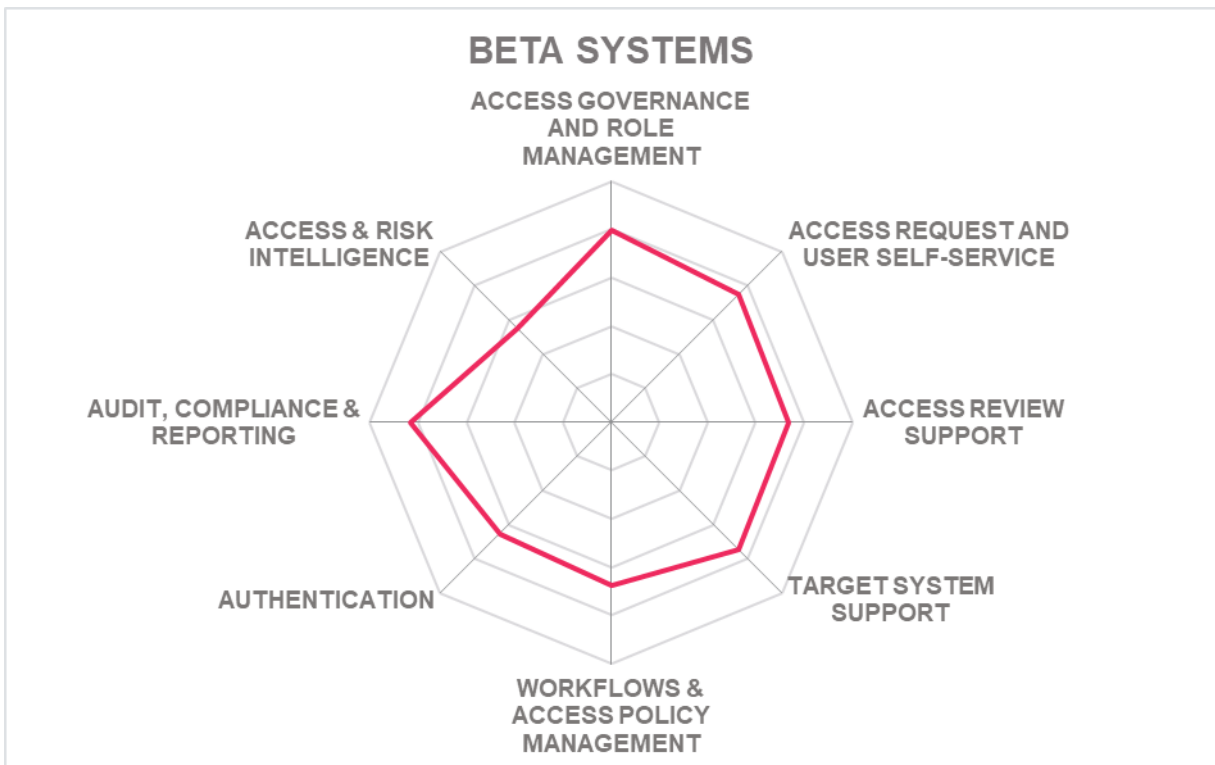
Brainwave – Brainwave Identity GRC

Brainwave is based in France and was founded in 2010. The company offers Brainwave Identity GRC as its core analytics based GRC solution. An extension to AG capabilities can be accomplished with ServiceNow as the "lifecycle" component of the solution. Brainwave's customers are primarily within the EMEA region, with a growing presence in North America with a partner ecosystem commensurate to the geographic distribution of their customer base. Radiant Logic signed on February 1st, 2023, a definitive agreement to acquire Brainwave GRC.

Brainwave supports on-premises and private cloud deployment models that can be delivered as SaaS, as a managed service and software deployed to a server. Docker container-based deployment is supported through additional support based on customers' requirements. A managed service is possible in a single tenant dedicated cloud environment. Brainwave states that 100% of the Brainwave Identity GRC functionality is available via APIs. REST APIs are available, although SOAP is not. CLI access to workflows and alters is given. SDK support is limited to Server-Side JavaScript, Java and Powershell. Brainwave solution is java based and it runs on an Apache Tomcat web server. Data is located in a database instance (SQL server, PostgreSQL). Authentication is managed through an IdP which is not part of the solution (Brainwave acts as a service provider).

The UI has an interactive 360 view of identities, access requests, groups and rights with a strong analytics engine. The analytics engine is configurable with over 150 automated analytics repository controls. Good out-of-the-box connector support is given for on-premises target applications, although slightly less support is available for SaaS target systems. There is very strong support for Access Governance related reports which include access risks, accounts, attestations, groups, roles, users, and privileged access, as well as reports related to SoD, unstructured data, PAM, and IAS is given. Moderate support is also available for out-of-the-box reports for major compliance frameworks. Policies can be defined to support account termination, role modification, access exception approval, and SoD use case, although less support is given for workflows such as registration or data mapping, for example.

Brainwave has a strong identity analytics engine which uses machine learning for detecting anomalies and can define the level of risk to conduct SOD risk analysis beyond SAP ERP platforms into hybrid ERP platforms that support RESTful APIs for identity and access entitlements exchange. Brainwave GRC has an innovative user access review platform which can be integrated with third party solutions. The solution uses a data mining algorithm to enable bulk access review. Brainwave's java-based access intelligence platform is both flexible and easy to customize. However, this flexible, risk-based approach to access intelligence can require significant development and integration efforts by the end user as well as the aide of training and technical assistance from Brainwave. The more advanced feature, user activity monitoring (UAM), is supported through the consolidation of access rights and access logs to perform user behavior analysis based on access logs with a peer group approach.

Brainwave can require significant development efforts to achieve common access governance tasks. With specialized java development skills inhouse and a dedicated solution for CyberArk in the roadmap, Brainwave could be a product of choice for organizations that are guided by internal strategic decisions for open-source technology adoption to build an access governance platform. Brainwave is a preferred product for medium to enterprise-sized organizations that require flexibility to tailor workflows for internal business processes.

|	
Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Neutral

Table 5: Brainwave Identity GRC's rating

Strengths

- Strong identity analytics engine which uses Machine Learning
- Flexible and easy customization
- Good OOB on-premise connectors support
- Strong AG reporting support
- Integrated SOD checks within role management
- Risk-based approach to governance
- User activity monitoring (UAM) support

Challenges

- Growing but limited market presence outside the EMEA
- Missing user self-service support
- Authentication options only apply to administrative access
- Partner ecosystem mainly present in EMEA market

BRAINWAVE
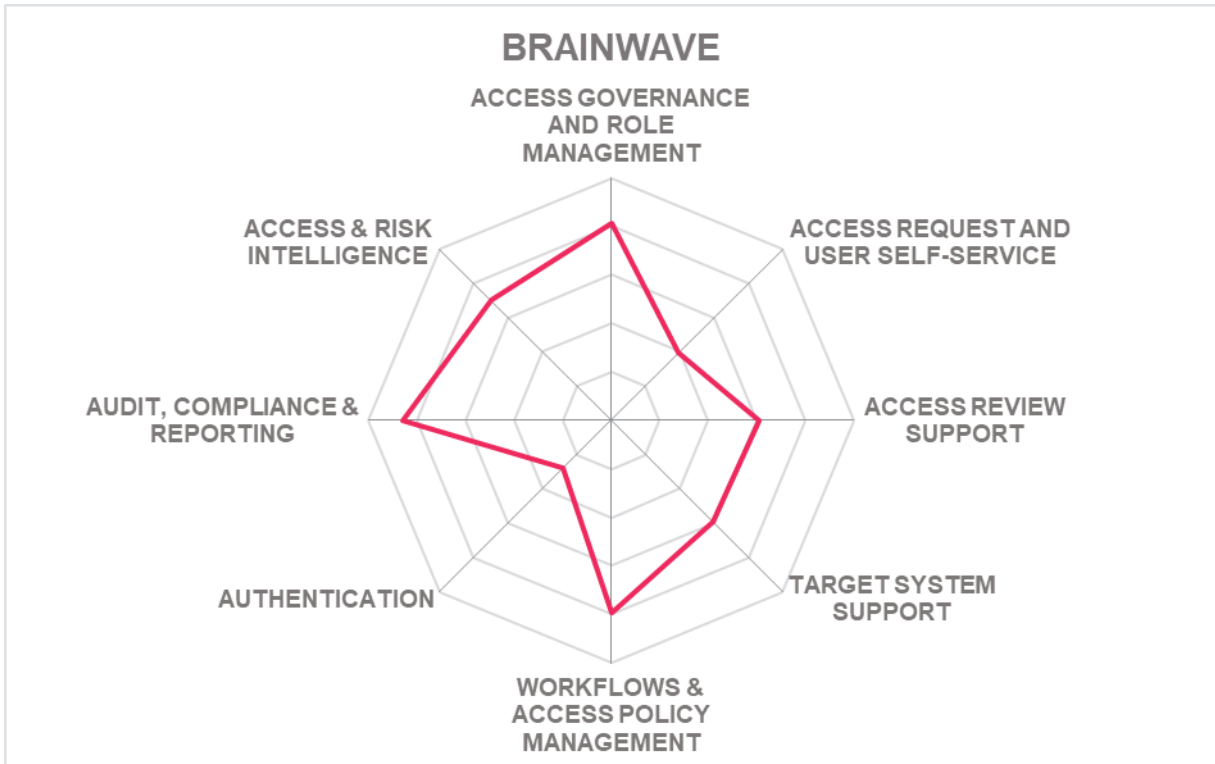
Bravura – Bravura Security Fabric

Bravura Security, previously known as Hitachi ID, was recently acquired by the Volaris group. The Bravura Security Fabric supports identity lifecycle management automation, access governance, workflows, self-service identity, multi factor authentication, privileged access automation, decentralized credentials, and analytics. A common platform underpins their Bravura Pass, Privilege, and Identity products which provides consistent UIs, database, connectors, and API. Bravura Safe and OneAuth are SaaS native applications. The current solution feature's self-service identity, federation and multi factor authentication, privileged access management, identity automation, privilege automation and decentralized credentials.

Bravura provides all SaaS offerings in a single tenant architecture to ensure strict data confidentiality. When Bravura Pass, Privilege, and Identity are deployed in an on-premises deployment, customers can host in public clouds, private clouds, or server class hardware. Bravura Security uses a multi-region architecture which supports hyper scaling. All the functionalities of the solution are exposed via SOAP, REST APIs as well as CLIs, which are used for rich and complex secret management scenarios. SDK support is limited to 75% via Python. Strong support for reporting, as well as major compliance framework reporting, is available out-of-the-box.

The solution provides off-the-shelf universal connectors including support for SCIM, REST, Python, Powershell, ODB and GraphQL. Strong support for OOB on-premises and SaaS connectors is offered. Good user self-service with a decent range of authenticators for access is present with good support for FIDO2. The solution supports secure sharing of credentials, as well as onboarding for privileged and Just-In-Time (JIT) identities.

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

|		
Security	Strong Positive	
Functionality	Positive	
Deployment	Strong Positive	Bravura Security
Interoperability	Positive	
Usability	Positive	

Table 6: Bravura Security Fabric's rating

Strengths

- Good governance policies
- Good features for role and SoD management

- Strong support for access review and certification support
- Good support for user Self-service access
- Good deployment and delivery options
- Good support for reporting options and compliance framework support

Challenges

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

Leader in
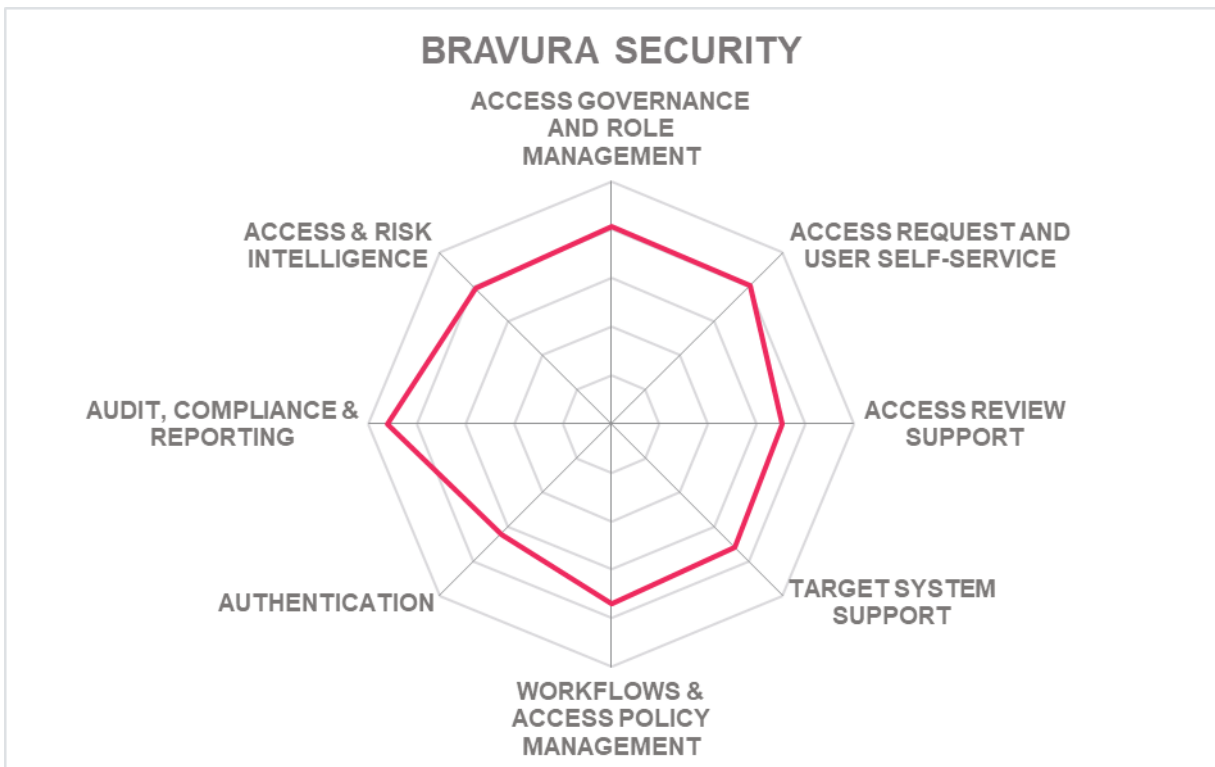
Broadcom – Symantec IGA

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

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

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

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

Security	Strong Positive	
Functionality	Strong Positive	**BROADCOM**®
Deployment	Positive	
Interoperability	Positive	
Usability	Strong Positive	

Table 7: Broadcom Symantec IGA's rating

Strengths

- Broad range of authenticators for user self-service and admin access

- Good capabilities for role management
- Strong Policy management capabilities
- Workflow management
- Strong UI for Mobile
- Dashboard for analytics and reporting

Challenges

- Relatively smaller technology partner ecosystem in comparison to other established players in the market
- Limited product delivery options
- Some limitations in authentication options

Leader in
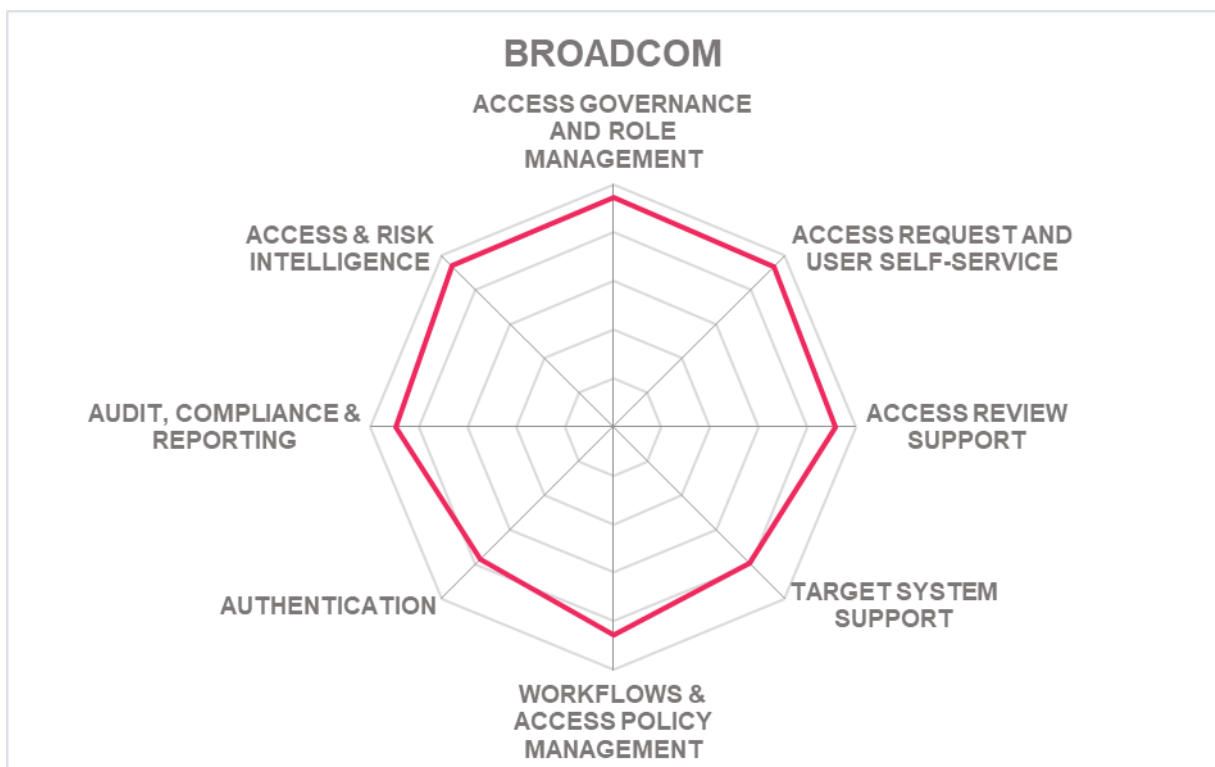
EmpowerID – EmpowerID IAM Suite

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

For the traditional AG model, EmpowerID is built on an identity warehouse, which is an inventory of an organization's systems. SCIM and SCIM 2.0 is supported for identity provisioning deprivation, however SPML is missing. OOB on-premises systems are extensive with deep SAP connector options. Connectors to SaaS systems are less extensive but include some of the more popular applications. It offers a strong custom connector model to create SCIM compliant connectors. EmpowerID provides strong role governance features that support role design and SoD compliance. It uses a polyarchal model for access where it leverages RBAC policies and location codes for giving appropriate access to people on same positions. Other advanced governance features, such as identity analytics and access intelligence support, risk-based analysis of identities, role mining, recertification recommendations, and various outlier detections are provided.

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

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

|	
Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 8: EmpowerID's rating

Strengths

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

Challenges

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

Leader in
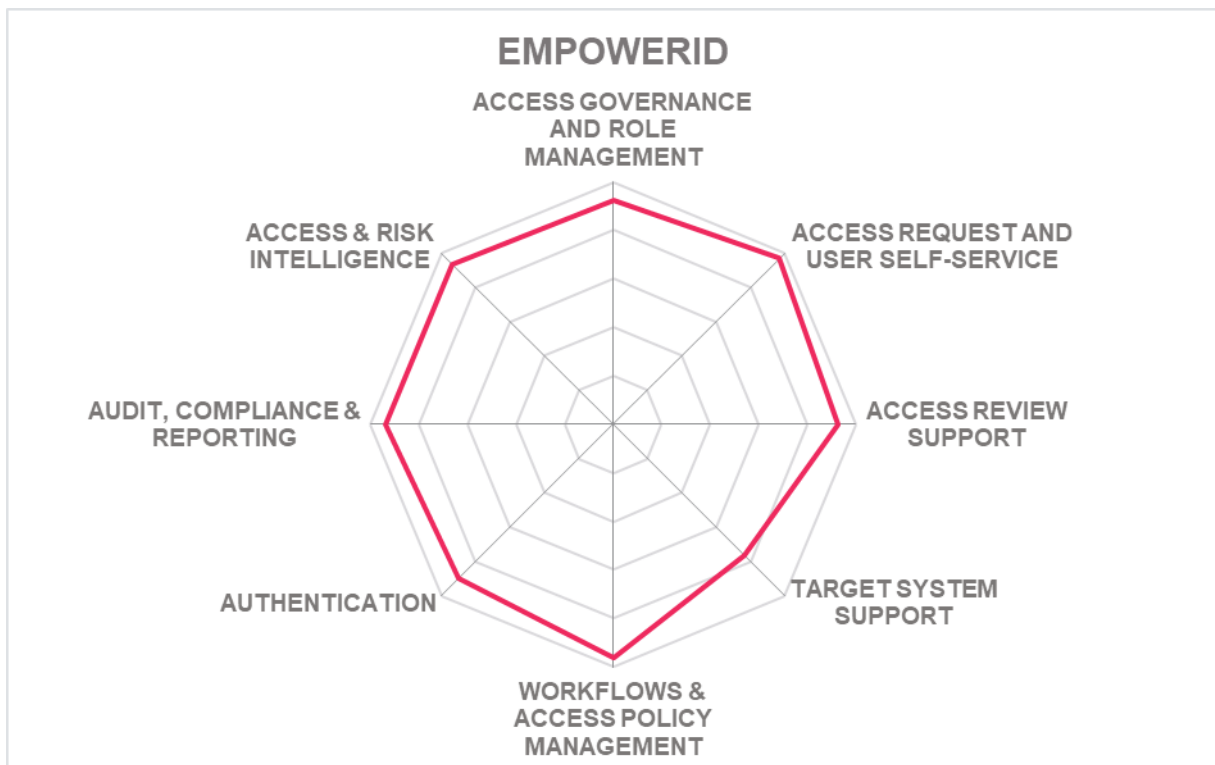
E-Trust – Horacius IAM

E-Trust was founded in 1999 with headquartered in Brazil with an initial focus on information security. In2006, E-Trust launched their Identity Access & Governance product Horacius. Horacius provides user provisioning and access governance capabilities that include access request, recertification, account mapping, and role & SoD management, with more advanced features such as workflows and identity analytics.

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

Horacius IAM has a decent, customizable UI, especially for workflows. They have an easily accessible pricing structure, which includes full support. The home page is defined with clear tile graphs for admin and managers. Customization of business rules can be done easily. Reporting has a slightly outdated UI however, detailed reporting of access rights for auditing is available. There are a variety of authentication options available for user self-service and admin access which supports biometrics, MFA and SAML mobile tokens.

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

E-Trust has continued to gain good momentum over the last few years. E-Trust customers are primarily medium to mid-market, although making inroads into some enterprise-level businesses mainly in Brazil. E-Trust is a good fit for organizations with average access governance requirements to satisfy the most common identity lifecycle administration use-cases with customer-focused in the Latin American region.

|	
Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Neutral
Usability	Positive

Table 9: Horacius IAM's rating

Strengths

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

Challenges

- Market presence currently limited to Brazil
- Developer portal is missing
- Some limitations of OOB connectors to SaaS systems
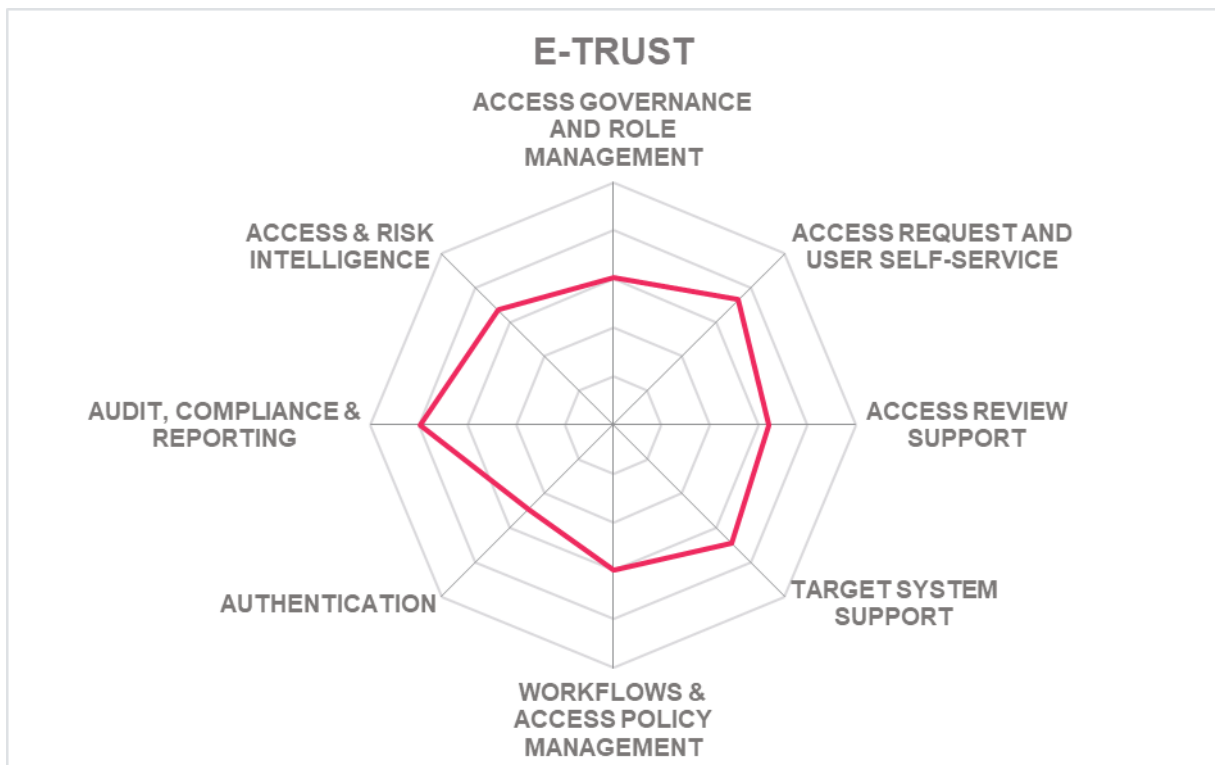
Evidian – Evidian IGA, Evidian Analytics – IDaaS Governance

Eviden is an Atos business that brings together its digital, cloud, big data and security business lines. Evidian Identity & Access management (IAM) is a software solution of Eviden. 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 AG solution in this Leadership Compass.

Evidian offers multiple products in a suite. Their product, Evidian Identity Governance and Administration (IGA), offers Access Governance capabilities. SPML and SCIM is supported for identity provisioning. OOB integration to ITSM tools includes ServiceNow, JIRA and EasyVista. Support for additional ITSM tools can be expanded using the provided SDK. Strong support for OOB provisioning connectors for on-premises systems is provided, however, connector support for SaaS is limited. Evidian Analytics and Intelligence (A&I) is a separate product offering however it meets the increasing requirements of advanced Access Governance. It uses TIBCO Jaspersoft for its reporting capabilities, giving Evidian the ability to provide good A&I dashboard capabilities.

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

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

Evidian customers and partner ecosystem are primarily focused in the EMEA region serving mid-market to enterprise-sized organizations. Beginning of 2023 Evidian has delivered new analytics capabilities and IDaaS Governance features.

Overall, Evidian delivers good provisioning capabilities with moderate Access Governance, making an interesting alternative to the leading IGA vendors in specific industry verticals, particularly healthcare. With a regional but strong partner ecosystem across Europe, being part of Eviden, an ATOS business is likely to help Evidian IAM products gain access to large customers and enter new geographies.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 10: Evidian IGA's rating

Strengths

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

Challenges

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

Leader in

EVIDIAN
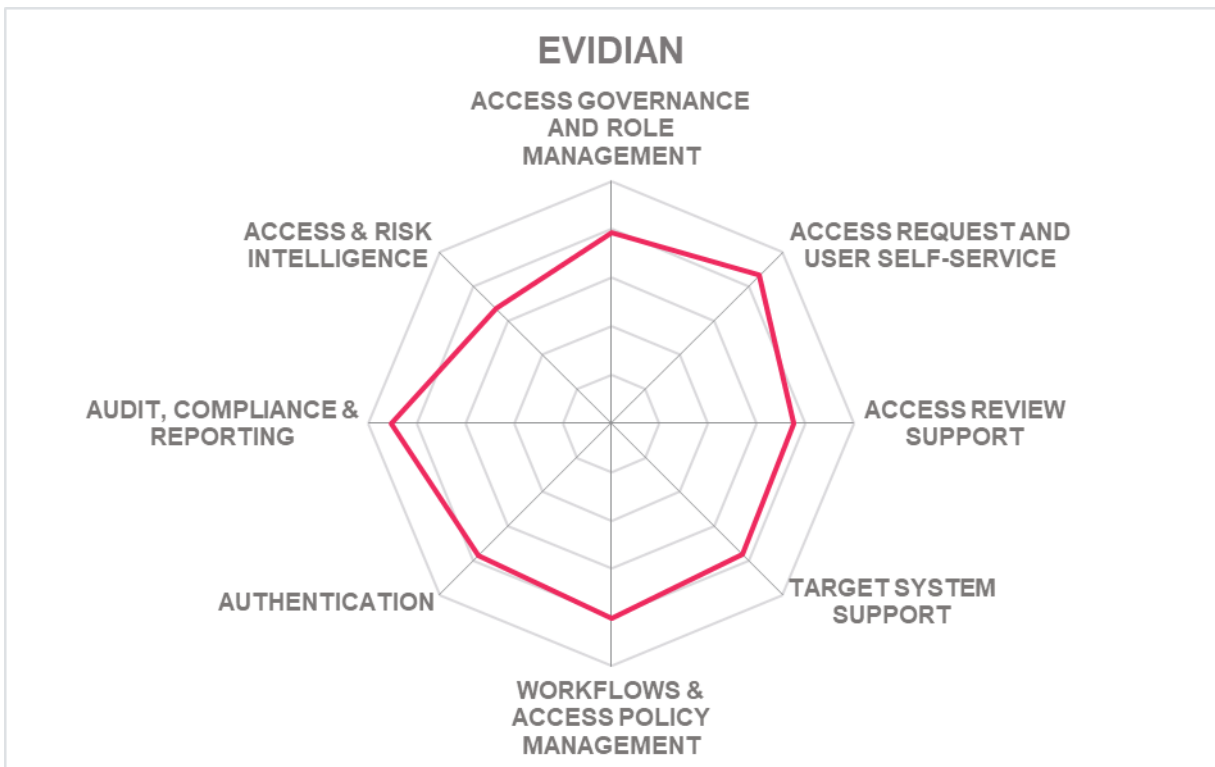
Evolveum – MidPoint

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

Evolveum's MidPoint access governance features include a centralized role management that consist of role discovery support, but not supported is role mining that can create or modify entitlement groups or roles. In addition to the other governance basics, midpoint also supports re-certification campaigns, basic role management lifecycle, and data protection. Good support for defining policies is also given. Policies for RBAC and organizational structure are also available that can be used for SoD use cases. Some access governance intelligence such as access modelling is available, although more advanced anomaly or types of outlier detection is not supported.

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

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

MidPoint has a good UI with functional and configurable dashboards and widgets. Requesting roles is given via a shopping cart paradigm and the status of the access request is displayed. There is good workflow in place for the approval of requests, as well as the ability to enable bulk approval. SoD policies can be configured. Reporting capabilities are available based on native report mechanism, although missing support for major compliance frameworks OOB. Updated UI is a strong improvement from the previous version and focuses on low code approach for end users.

Evolveum customers are primarily focused in the EMEA region with North America coming in as the second most important region. Evolveum's customer deployments include medium to enterprise companies and universities. MidPoint provides good on-premises DevOps options and hopes to move towards a hybrid or a full cloud environment in the future. Overall

Evolveum MidPoint continues to improve and may be of interest to organizations with general IGA and solely on-premises requirements. Evolveum has plans to further enhance and work on identity analytics, role mining and a next gen user self-service support.

|	
Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 11: Evolveum MidPoint's rating

Strengths

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

Challenges

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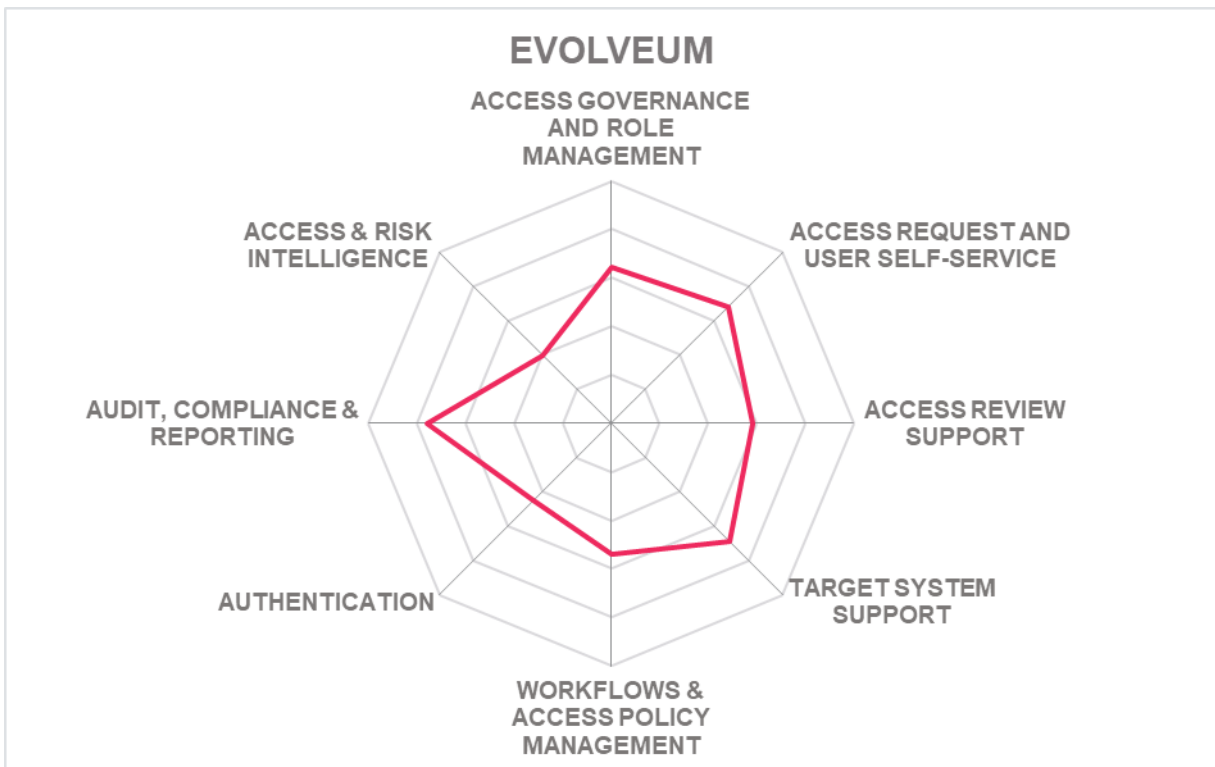
IBM – IBM Security Verify

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

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

IBM Security Verify supports all known servers, databases or virtual directories which can be used as identity repositories. SCIM is supported for identity provisioning/ deprovisioning however a customer adapter is required for SPML. OOB integration to ITSM tools is limited to ServiceNow. Verify Service Desk is a ServiceNow plugin published in ServiceNow store. It supports access request and manual fulfilment tickets management. Java and JavaScript languages are available to support attribute mapping expressions. A good set of out-of-the-box (OOB) provisioning connectors are available to both on-premises and SaaS systems. The Compliance Module gives good support to access reviews and certification campaigns and event-based micro certifications. Identity lifecycle management covers all aspects from onboarding to off boarding and uses AI and machine learning to analyze parameters of user and requested access.

IBM Security provides a modern UI with all required functionalities in the dashboard. The Lifecycle Module provides applications and users onboarding, automated account provisioning and password management, access request with role & attribute-based access control, and audit & reporting. Good user self-service is given with a strong list of authenticator options for access including passwordless authenticators such as QR code, FIDO2, and FIDO2 U2F. Access request and access review is supported by a risk level is shown in terms of entitlements. Configurable OOB policies based on best practice in place for the analytics model.

Overall, IBM Security Verify Governance continues to move its long line of mature AG 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 AG market. IBM also benefits from its own strong professional services and excellent partner ecosystem, plus easy integration within the overall IBM Security product portfolio.
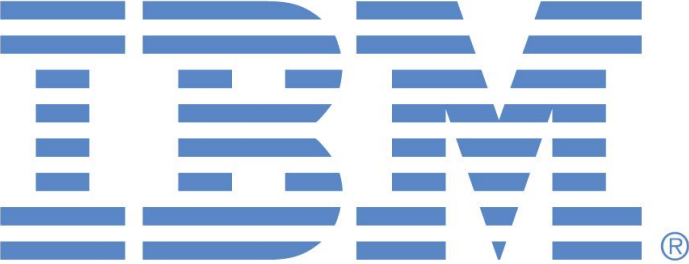
Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

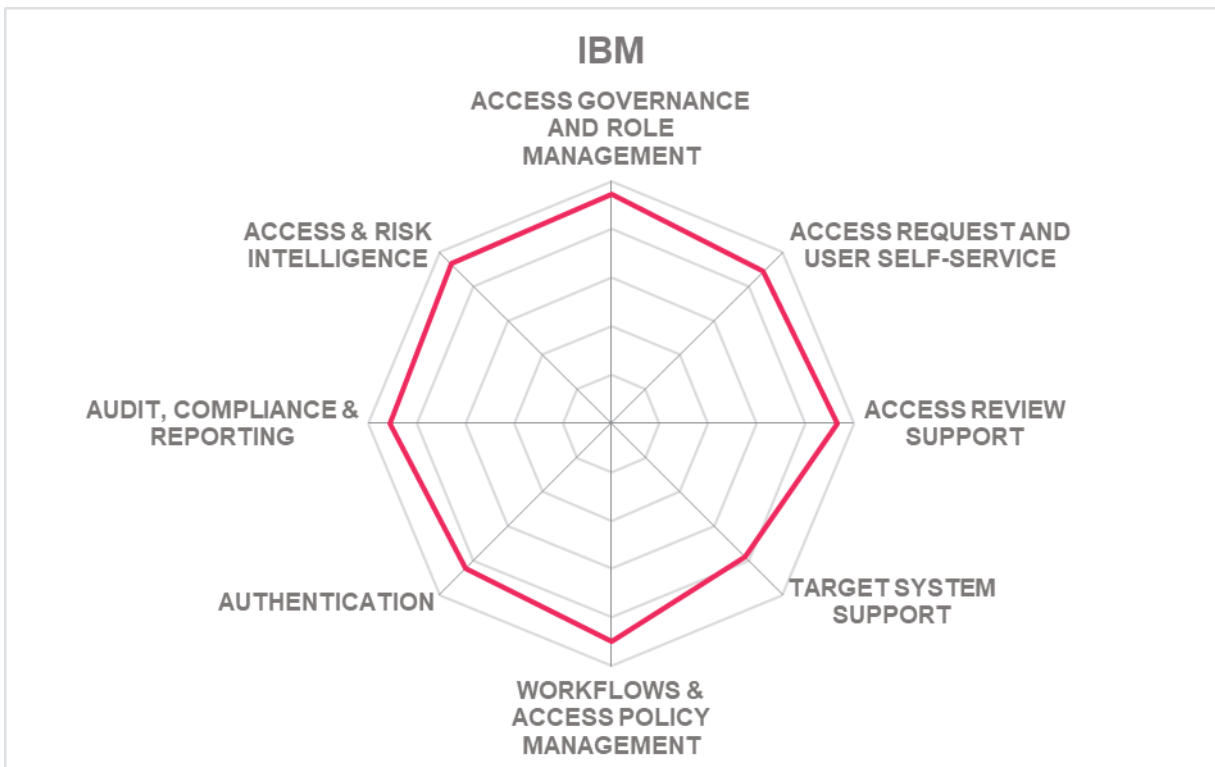Table 12: IBM Security Verify's rating

Strengths

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

Challenges

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

Leader in

IBM access governance capability radar chart showing: ACCESS GOVERNANCE AND ROLE MANAGEMENT, ACCESS REQUEST AND USER SELF-SERVICE, ACCESS REVIEW SUPPORT, TARGET SYSTEM SUPPORT, WORKFLOWS & ACCESS POLICY MANAGEMENT, AUTHENTICATION, AUDIT, COMPLIANCE & REPORTING, ACCESS & RISK INTELLIGENCE.

Microsoft – Entra Identity Governance

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

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

SCIM is widely supported for identity provisioning and has a good range of OOB SaaS connectors. Support for OOB on-premises connectors is limited due to the nature of the deployment and delivery of the product. OOB integration to ITSM tools for SSO and privileged access includes ServiceNow and Atlassian Jira Service Desk. Privileged access also supports Just-In-Time (JIT). There is a good set of authenticators for user self-service and admin access, however, FIDO support is missing. Portals for managing identities and resetting passwords are available via a web browser and render well on desktop and mobile platforms. Strong policies are in place for attribute-based access. Provisioning analysis and policy for user activity monitoring is also supported. Policies are in place for supporting elevation of PAM. However, the solution does not use AI/ML for supporting workflows related to recommending access rights based on comparison of employees or other similar functions.

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

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 13: Microsoft Entra Identity Governance's rating

Strengths

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

Challenges

- Support for OOB reports for major compliance frameworks limited to GDPR
- Use of AI/ML currently limited to access reviews
- Event based micro certification is missing

Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER
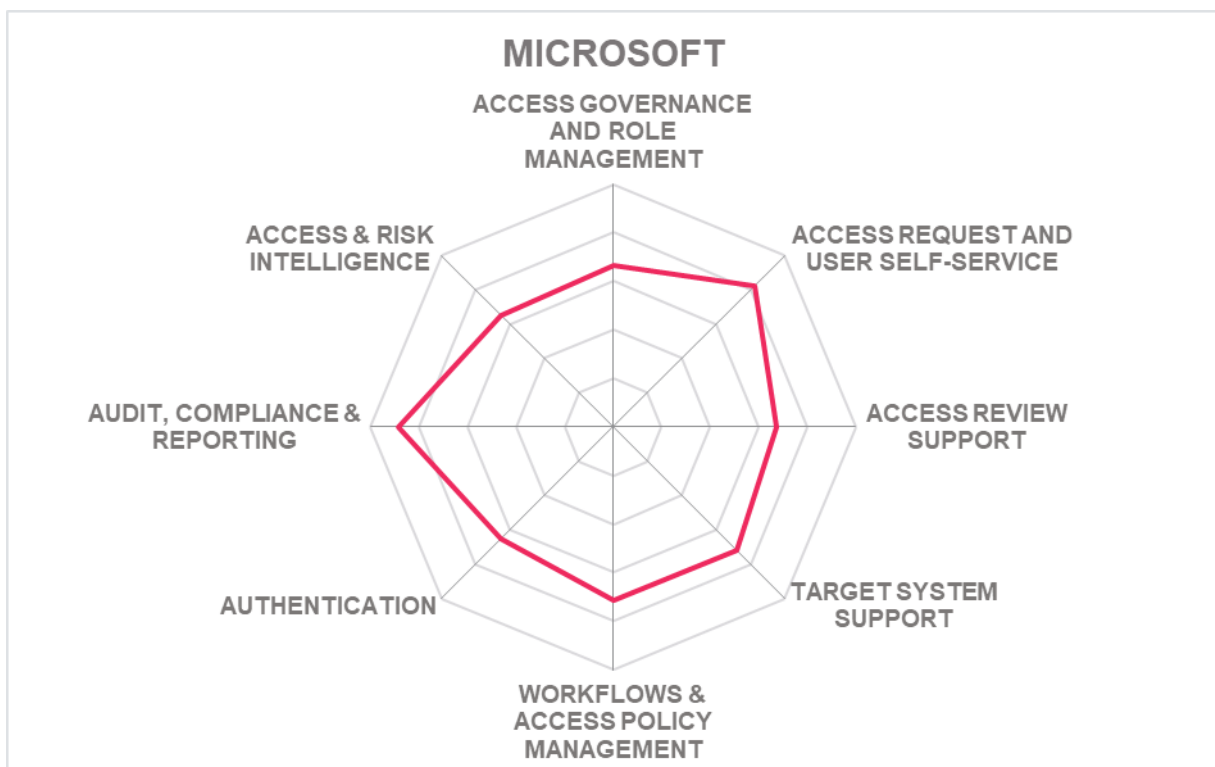
MICROSOFT

Netwrix Corporation – Netwrix Usercube

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

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

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

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

Security	Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 14: Netwrix Usercube's rating

Strengths

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

Challenges

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

Leader in

NETWRIX CORPORATION
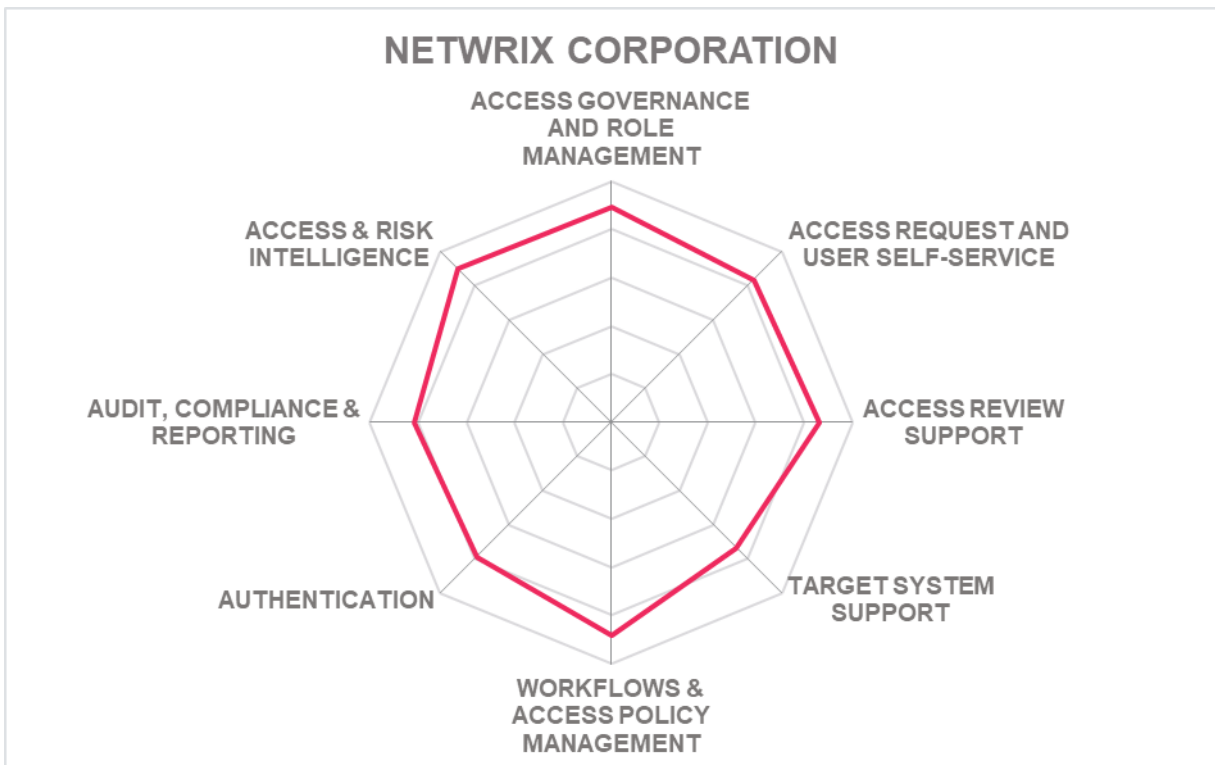
NEXIS GmbH – NEXIS 4

Based in Regensburg, Germany, Nexis started with NEXIS Controle, first released in 2014, which builds upon a plug-and-play approach to access governance and role lifecycle management as its core focus. Since then, Nexis has made some significant improvements to their core products, which is 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. The latest release (4.1) offers further improved User Experience and a new feature: Management of authorization concepts.

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

NEXIS 4 has good access governance features around SoD checks, risk intelligence and simulating models for anomaly of entitlement structures, role outlier detection and role optimization simulations as well as real time SoD violation checks. The product supports all known identity repositories. Since NEXIS 4 in most deployments acts as an extension of an existing IGA solution, it just needs to connect to the provisioning products. Therefore, native connectors to target systems are not focused by Nexis. For some systems like AD, AAD and SAP, connectors are available to access deep entitlement structures. OOB connectors to most major IGA solutions exist, such as SailPoint IIQ, One Identity Manager, OpenText (Micro Focus) NetIQ, Microsoft Identity Manager, Beta Systems Garancy, Omada, Oracle and Atos DirX. Custom connectors using plugins that are based on a comprehensive API and are written in Java are also supported. Integrations with third-party ITSM tools such as Remedy and ServiceNow are supported with the addition of Cherwell since 2022.

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

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

of these documents automates many manual processes. Daily reconciliation additionally assure consistency with reality.

|	
Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 15: NEXIS 4's rating

Strengths

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

Challenges

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

NEXIS
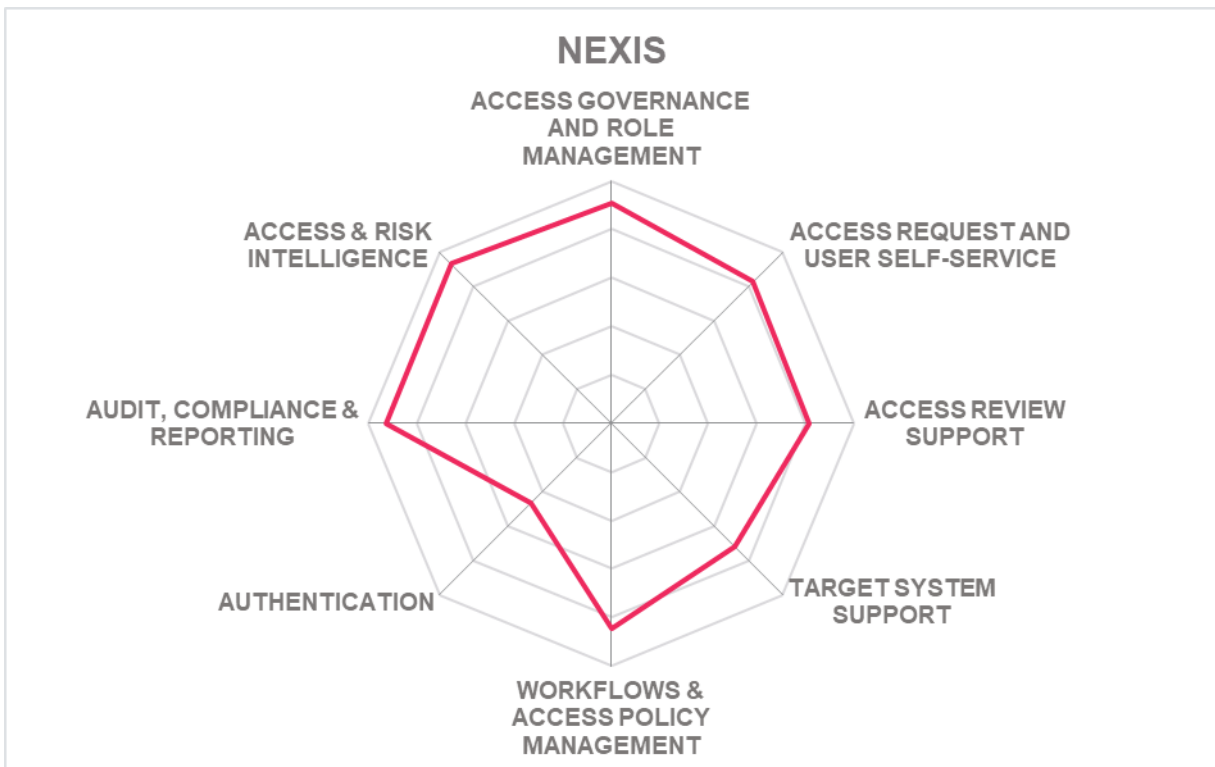
Omada – Omada Identity

Omada, headquartered in Denmark, counts among the established providers of solutions for IGA. Omada provides Omada Identity as an on-premises solution and Omada Identity Cloud for customers wanting a cloud-native SaaS solution - both delivering a full range of IGA functionalities with feature parity between the delivery models. The Accelerator Package allows customers to be operational within 12 weeks. Omada has built up strong knowledge from a considerable number of IGA deployments over the last 20 years. Omada has formalized these into the IdentityPROCESS+ best practice framework. IdentityPROCESS+ describes the most important processes needed to ensure a successful IGA deployment and helps organizations implement well-proven best practice processes, reducing the need to re-invent the wheel Omada components include an enterprise server portal and services for provisioning, data warehouse, and role & policy engine.

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

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

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

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

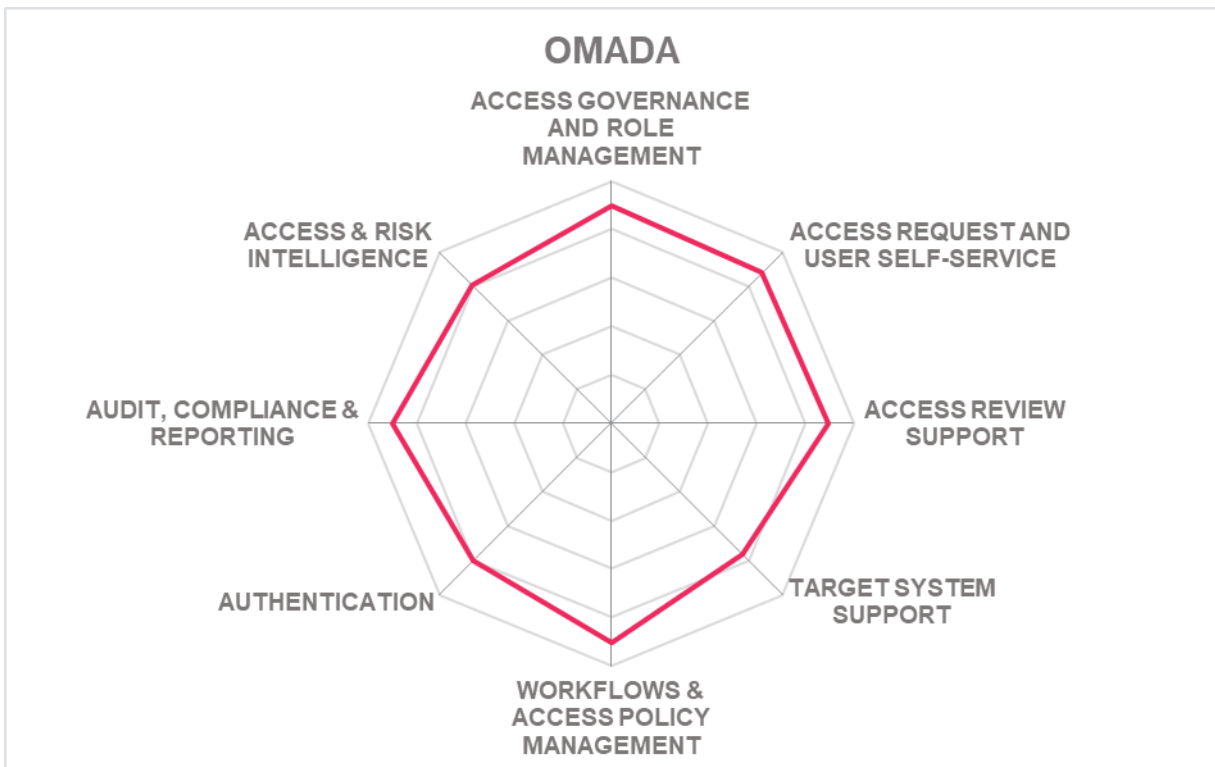Table 16: Omada Identity's rating

Strengths

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

Challenges

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

Leader in

OMADA radar chart showing capability ratings across: Access Governance and Role Management, Access Request and User Self-Service, Access Review Support, Target System Support, Workflows & Access Policy Management, Authentication, Audit, Compliance & Reporting, Access & Risk Intelligence.

One Identity – One Identity Manager

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

One Identity Manager has access governance capabilities such as strong AI for risk score system, peer group analysis, entitlement right sizing and future capabilities will include AI support for recertification requests, access requests. The risk dashboard is interactive and can show role and entitlement sprawl. One Identity Manager supports strong governance use cases including governance of devices, APIs and microservices in terms of versioning.

The product has a strong architecture model which is flexible and supports cloud governance, data access governance, application governance, privileged governance and identities and entitlements. The product supports a wide range of repositories as authoritative systems for managing identity lifecycle however, its own identity repository only supports MS SQL and Azure SQL Managed Instance. Schema extensions for adding new identity types over existing identities is available. SCIM is supported for identity provisioning and accelerating application onboarding. OOB integration to ITSM tools is limited to ServiceNow. Connectors to ITSM can consume data and grab ServiceNow catalog which is the product's unique capability. Integration of other ITSM tools is available based on customer requirements. Strong support for OOB provisioning connectors to on-premises and SaaS systems is available. Configurable policies for governing automated provisioning are supported along with Just-In-Time provisioning.

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

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

One Identity is a privately held company with a large customer base predominantly in the EMEA region, followed by North America and expansion into the APAC and Latin America

regions. It also maintains a good partner ecosystem proportionally in the same areas. Overall, One Identity continues to enhance the product's functional capabilities, establishing itself amongst the leaders in the market. One Identity remains a recommendation from us for evaluation in product selections.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 17: One Identity Manager's rating

Strengths

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

Challenges

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

Leader in
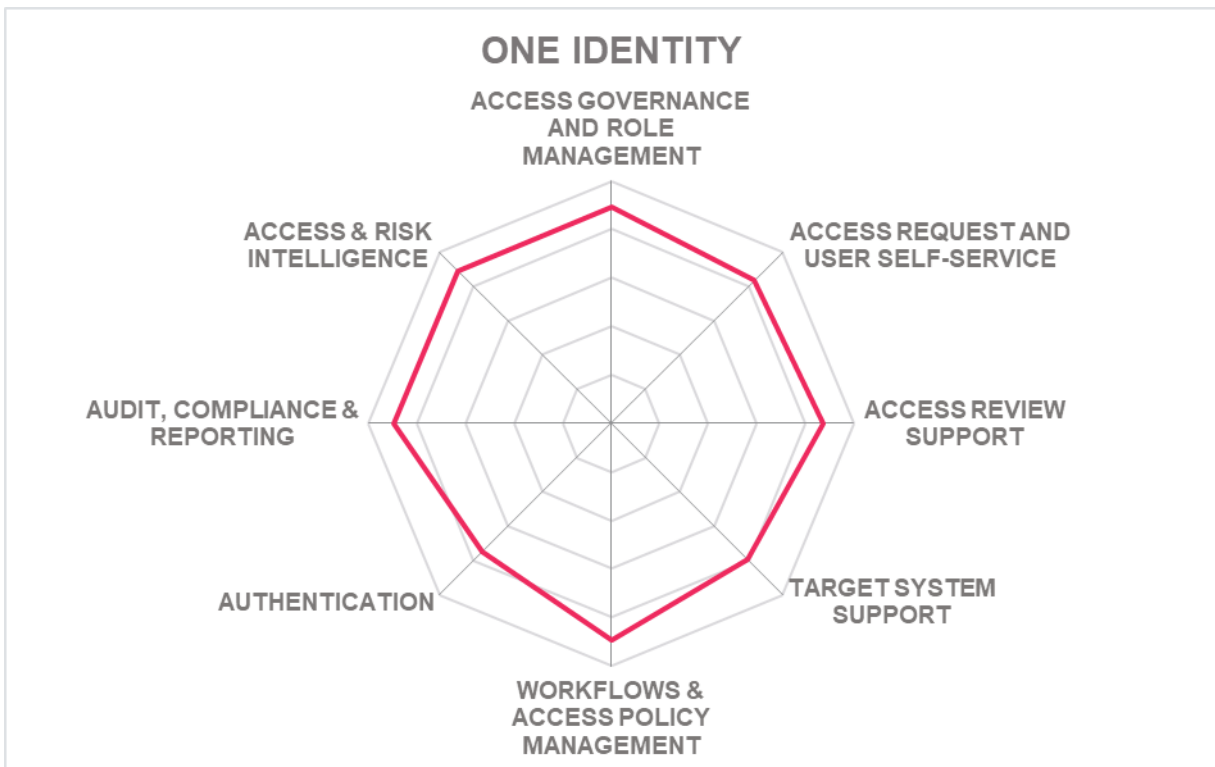
ONE IDENTITY

OpenText (Micro Focus) – NetIQ IGA Suite

Based in the UK and recently acquired by Open Text, Micro Focus offers an Identity and Access Management Platform as a set of solutions which includes Identity Governance and Administration, Access Management, Advanced Authentication, Data Security, Privileged Access Management and Security Information and Event Management. Identity Manager is 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.

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

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

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

OpenText (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. OpenText (Micro Focus) Net IQ Identity Manager, Governance, and Intelligence products offer a good range of IGA capabilities from flexible workflow and policy management to enhanced analytics-driven user activity reporting. Micro Focus continues to

improve towards a more modern and flexible product with more innovative features for advanced analytics using AI and ML on its roadmap. Overall, Identity Manager and Governance products from Micro Focus remain leading-edge products in the IGA market space with its broad, mature, and evolving functionality with a good partner ecosystem on a global scale.

Security	Strong Positive	
Functionality	Positive	**opentext**™ | Cybersecurity
Deployment	Positive	
Interoperability	Positive	
Usability	Strong Positive	

Table 18: OpenText (Micro Focus) NetIQ IGA's rating

Strengths

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

Challenges

- Missing popular SDKs for Android and iOS
- Relatively outdated UI
- Lacking innovative features in the roadmap

Leader in

OPENTEXT (MICRO FOCUS)
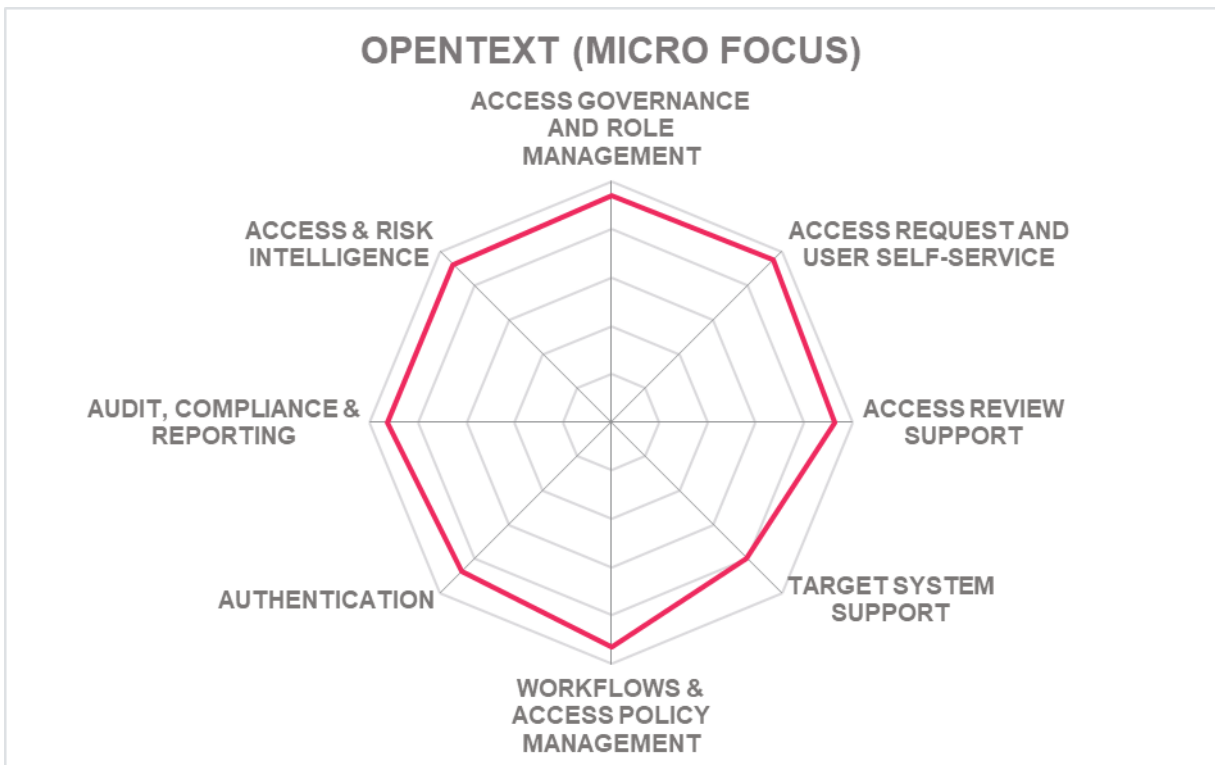
Oracle – Oracle Identity Governance

Oracle Identity Governance (OIG) Suite offers both on-premises offering called Oracle Identity Manager and Oracle Identity Analytics as well as native cloud service called Oracle Access Governance, within Oracle's IAM portfolio. Oracle Identity Governance is Oracle's primary AG 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. Beginning from summer 2022, Oracle introduced a cloud native service called Oracle Access Governance. Its prescriptive analytics-based actionable insights and recommendations for access reviews tasks enable managers and access reviewers to make informed decision about user accesses. It has the capability to perform near real time access reviews and provides options for reviewers to accept AI/ML generated recommendations or review further. In this study, we focus on Oracle Identity Governance as Oracle's primary AG offering.

Oracle's access governance features include risk-based access certification. It offers good analytics for access review campaigns, which can be exported as CSV. The analytics are AI and machine learning driven. Access request has a recommendations' feature which uses analytics to suggest access based on entitlement or attribute of the user.

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

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

Oracle Identity Governance Suite cuts across its competition through its enhanced UIs, recent pricing adjustments, enterprise-level design, support for modern architectural concepts, and an extensive partner network. User self-service support has a good UI with a

customizable landing page. The solution uses a shopping cart paradigm and SoD violation checks are performed at checkout.

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

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 19: Oracle Identity Governance's rating

Strengths

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

Challenges

- Some SDKs missing
- Oracle database is required
- Modification of access requests after request submission or before request fulfillment is missing

Leader in
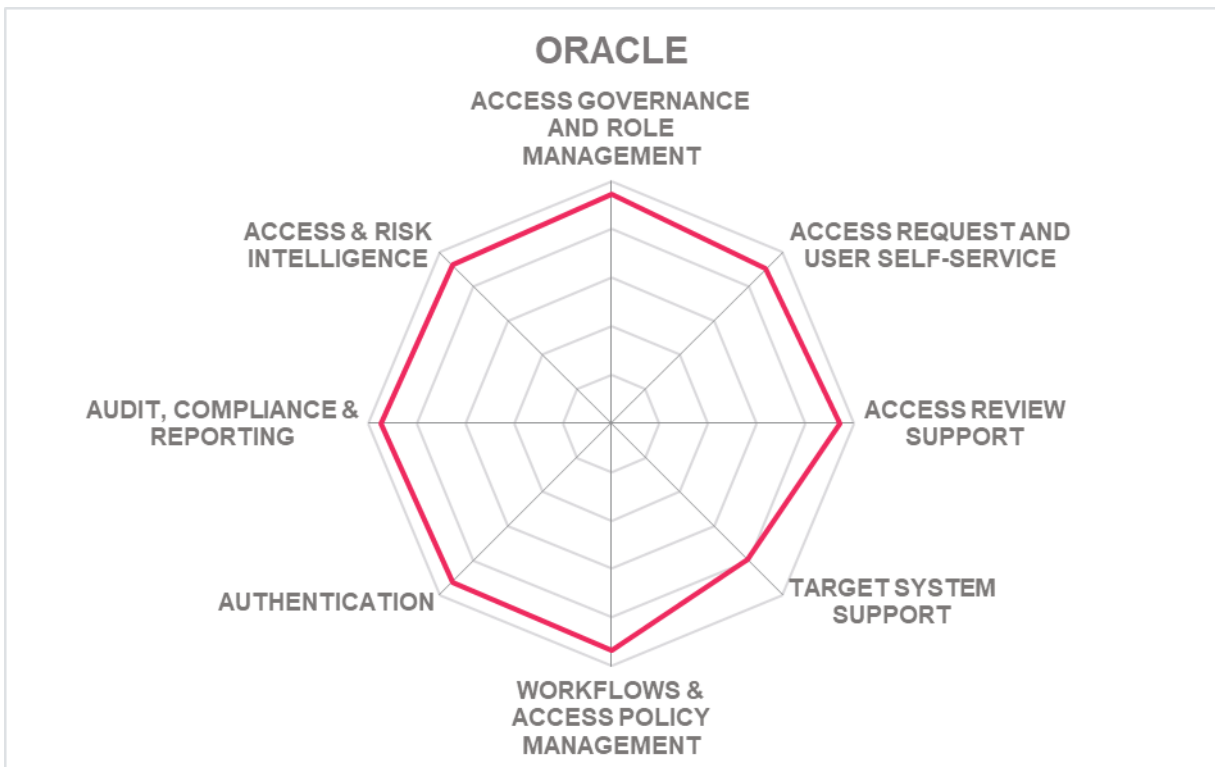
RSA – RSA Governance and Lifecycle

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

RSA Governance & Lifecycle (G&L) offers core AG capabilities, including automated access certifications, compliance audit reporting and analytics, SoD policy enforcement, rules and policy management, role management and mining, and data access governance. G&L supports all known databases, servers, or virtual directories for identity repositories. The solution supports automated discovery of access, automated provisioning of birth rights, continuous risk-based access assurance approach including governance for entire identity lifecycle management. SPML and SCIM is supported for identity provisioning/ deprovisioning. Policy in place to do bulk importing of identities and bulk approval/ rejections based on SoD violations. OOB integration to ITSM tools is available for ServiceNow, Cherwell, BMC Helix ITSM and Jira. It supports a wide range of out-of-the-box (OOB) connectors to both on-premises and SaaS systems.

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

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

|		
Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 20: RSA's rating

Strengths

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

Challenges

- Cloud delivery is currently a single tenant model
- Some limitations on SDK programming language options and access to product functionality via the SDK
- Container based platform support limited to Docker with support for Kubernetes coming in 2023

Leader in

OVERALL LEADER   PRODUCT LEADER   INNOVATION LEADER   MARKET LEADER

RSA
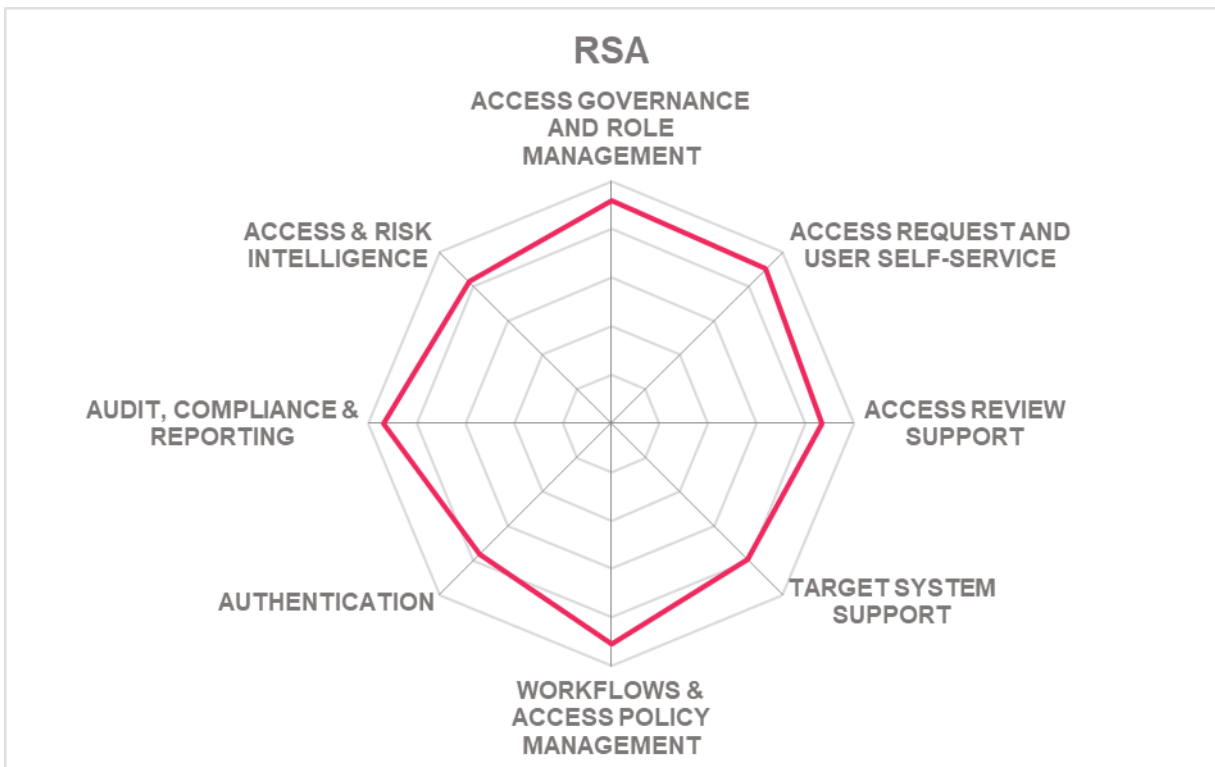
SailPoint – SailPoint Identity Security Platform

Based in Austin, Texas, SailPoint started as a vendor specialized in Access Governance and made heavy investments in Identity Provisioning capabilities over the years. SailPoint Identity Security Platform is a single platform that adds AI-based capabilities to AG and cloud governance via SaaS deployment. The platform has several 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 unstructured data and file storage platforms, amongst other capabilities depending on the customer requirements.

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, data access governance and cloud governance capabilities. SailPoint supports mapping of SOD policies from SAP GRC to form a coherent SOD policy across the enterprise and has a dedicated mapping UI for attribute mapping. The solution also supports both SPML and SCIM for identity provisioning/de-provisioning. OOB integration with ITSM tools includes ServiceNow, BMC Helix ITSM, and Atlassian JIRA Service Desk. There is very strong support for OOB provisioning connectors for SaaS and on-premises systems with a dedicated list of options.

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

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

SailPoint has been a leading vendor in the AG market, providing strong Access Governance capabilities. In addition, SailPoint has built excellent support for 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 AG vendors for mid-to enterprise-sized organizations. SailPoint continues to enhance its provisioning, automation, AI driven risk mitigation, and reporting capabilities in a positive direction, making it a recommended consideration in any AG evaluation.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 21: SailPoint Identity Security's rating

Strengths

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

Challenges

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

Leader in

![Kuppingercole Analysts logo]

SAILPOINT
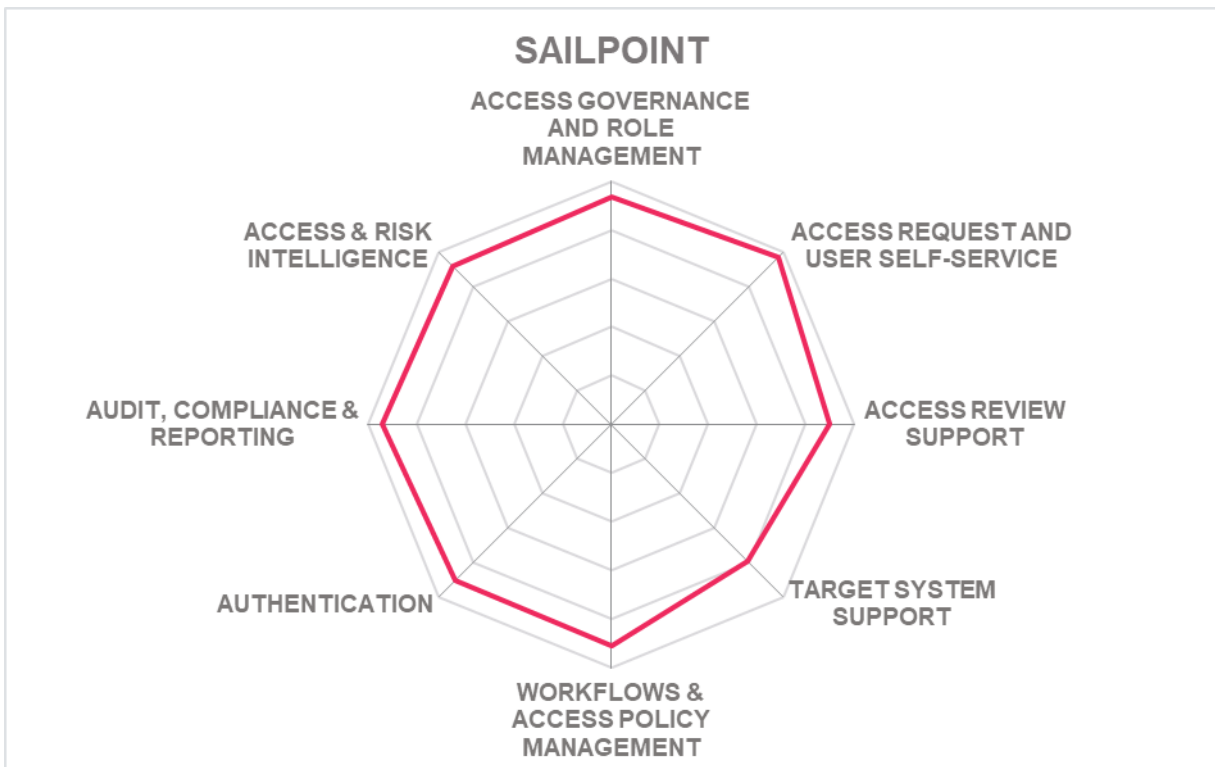
SAP – SAP Access Control, SAP Access Governance

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

SAP Identity Access Governance supports a good set of identity repositories including AD/ Azure, LDAP, SAP HR, SAP IDM, SuccessFactors, as well as any SCIM supported repository natively with IGA solutions. SAP IDM is available for synchronization with any supported identity repositories. OOB integration to popular third-party ITSM tools is not given, although a workflow interface does help extend capabilities. Good support is given for out-of-the-box (OOB) provisioning connectors for on-premises systems, but noticeably less support for SaaS. SCIM and SPML is supported for target system connectivity. Automated provisioning is supported and policy in place for RBAC when onboarding. Definition of business rules for birth right access is given. Just-In-Time (JIT) provisioning is supported with transaction definitions. The solution uses machine learning for flagging malicious transactions/ anomalies and allows user to review the actions. The product comes with standard Access Governance capabilities, including flexible workflows, support for automated assignment of entitlements based on roles, approval processes, and self-service functionalities.

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

SAP Access Control is on-premises or in the cloud via Private Cloud Extended (PCE) option, with SAP Identity Access Governance as their fully multi-tenant cloud solution. SAP IAG is a multi-tenant SaaS solution whereas Access Control, IDM, Enterprise SSO are offered as private cloud editions and deployed like containerized solutions. Less than half of the product's functionality is exposed via REST APIs, and SOAP APIs are not available. Missing is CLI and SDK support, although a toolkit for integration connectors based on web services is given.

SAP maintains a significant customer base in North America and the EMEA regions, with comparatively lesser presence in APAC and Latin America. Overall, SAP provides a well-rounded set of AG 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	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 22: SAP Access Governance's rating

Strengths

- Excellent integration into SAP environments, including SAP Access Control
- Good access governance capabilities
- Good role management capabilities
- Audit & compliance reporting support
- Self-service capability with mobile self-service support
- Good support for flexible workflow and automation
- Machine learning integration into various functions
- Modern and user-friendly UI

Challenges

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

Leader in

SAP
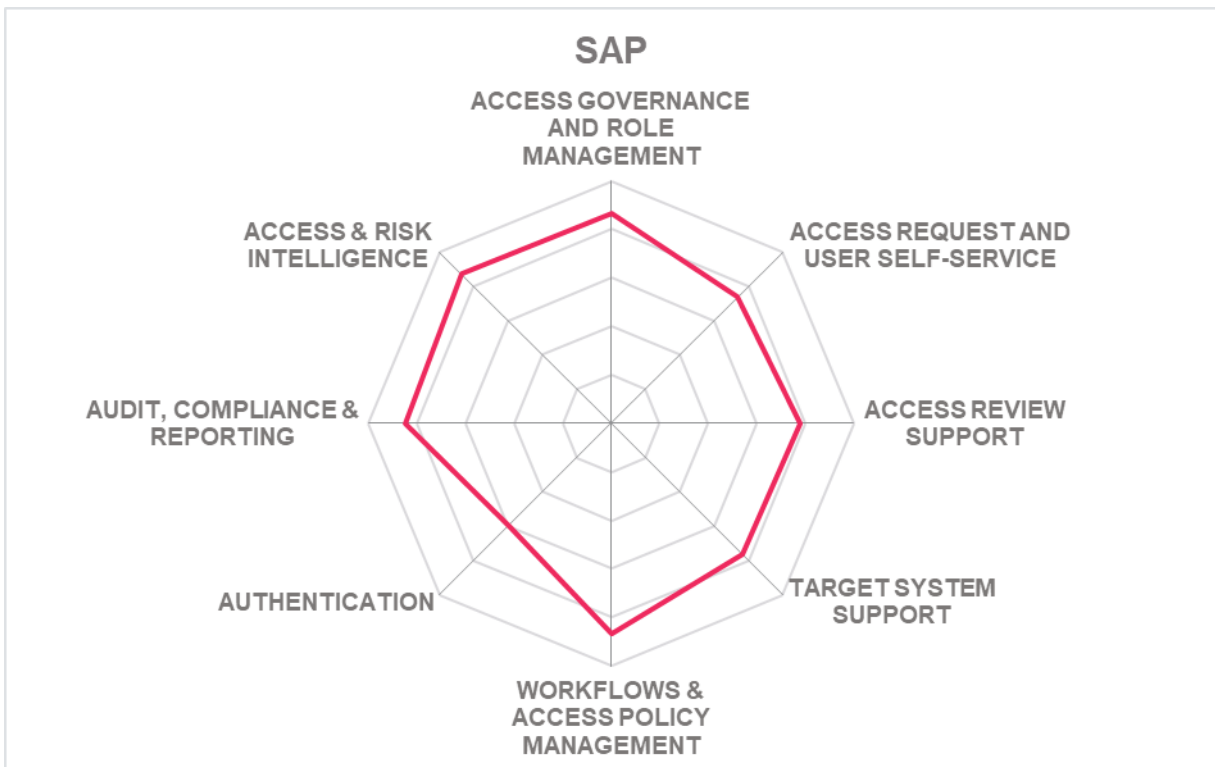
Saviynt – Enterprise Identity Cloud Platform

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

Saviynt EIC Platform is a cloud-based solution. Saviynt offers a strong lineup of IGA, including cloud PAM, Application Access Governance, Third-Party Access Governance, and Data Access Governance through its EIC. Saviynt also offers ID Risk Exchange and the Saviynt Exchange products to their portfolio, a collaborative platform with their customers to exchange insights. Strong Access Governance support is given throughout a number of capabilities. Good user self-service support is given, although with a very impressive list of authentication options available. Intelligence appears across a wide range of applications and infrastructure. Strong audit and compliance reporting support is available. Saviynt also offers granular Data Access Governance and cross-application SOD risk management capabilities. Strong support for connecting to a wide range of identity repositories. SCIM and SPML is supported for identity provisioning/ deprovisioning. A very impressive list of OOB provisioning connectors for on-premises and SaaS systems is available. Saviynt has also added a built-in Identity RPA Bot that can deploy on-premises for a hybrid deployment. It can be used for rapid onboarding and convert disconnected applications to connected applications for automated reconciliation, provisioning, and account management.

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

The UI dashboard can be tailored from a simplified view for line managers to more detailed views for analysts and application owners displaying different aspects of access, activity, and vulnerability risk. Persona based mini applications are visible and support is given for governing bots and external risks. Risk based SoD violations is shown and the risk weightage is configurable. The solution has an inbuilt hybrid SoD analysis model for discovering entitlements and suggesting roles. Access request/ approval is comprehensive with zero code approach for workflow configuration. The dashboard for reporting is well laid out.

Saviynt has maintained a steady customer-focused trajectory over the years focused on large enterprise organizations with customer and partner ecosystems primarily located in North America with expansions into the EMEA and APAC regions. Saviynt's roadmap features for the EIC includes zero trust model, identity proofing, advanced identity analytics and its existing IGA capabilities make it a recommended product.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 23: Saviynt EIC's rating

Strengths

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

Challenges

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

Leader in

SAVIYNT
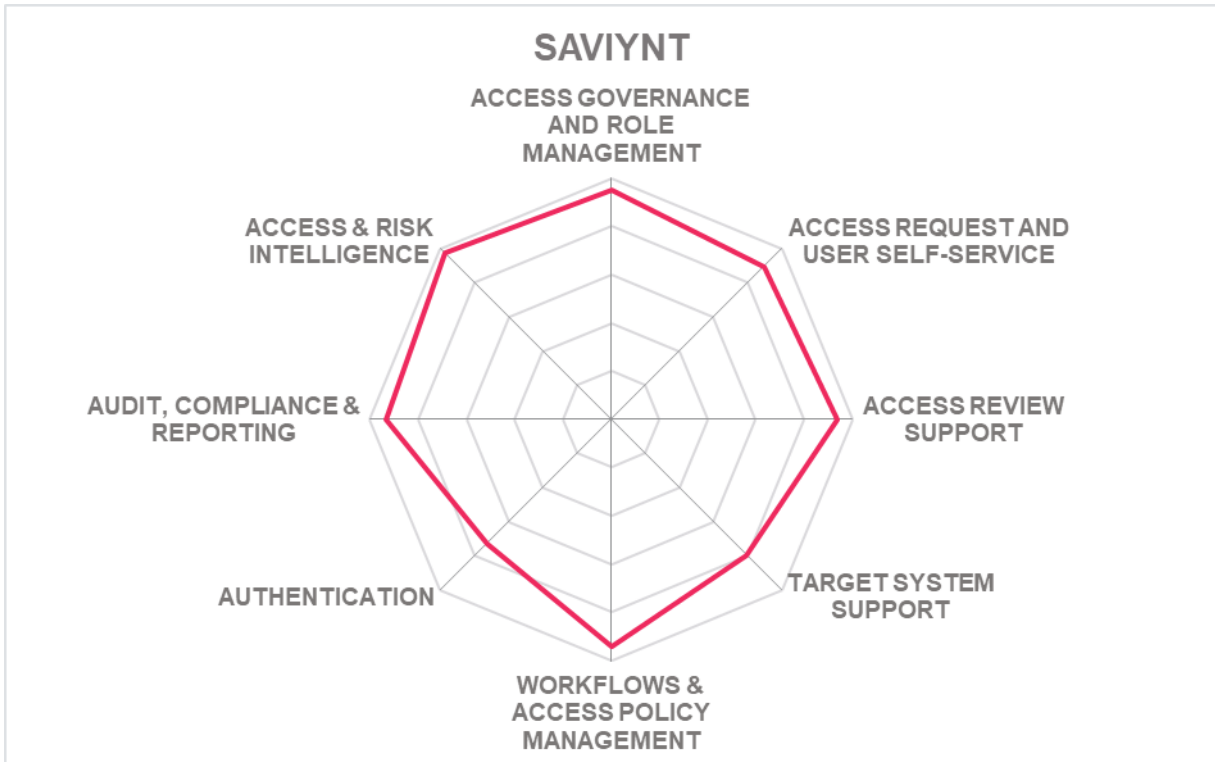
Simeio – Simeio IGA Managed Services

Founded in 2007 and based in Atlanta, Georgia (US), Simeio Solutions observed significant growth when shifting from its IAM system integration business into a full-fledged IDaaS service provider over the past few years. Simeio IGA managed services includes orchestration platforms. The platform provides a simple and efficient solution for application on boarding to various different IAM technologies from IGA to Access Management and PAM from one Simeio IO Platform. Simeio IGA Managed Services is its primary IGA service, although the Access Governance component of that service is evaluated here.

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

Simeio IGA Managed Services supports all known types of deployment models including containerized deployment. Simeio primarily focuses on providing a SaaS, it also offers a virtual appliance, software deployed to a server, and container-based options that can deploy on a standard orchestrator platform like Kubernetes or OpenShift for on-premises delivery. Almost all capabilities of the solution are exposed via REST, SCIM and LDAP APIs.

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

Simeio is a privately held company that supports large enterprises and mid-market organizations, primarily in North America with a growing client presence in Europe while currently operating from the UK. Simeio has significantly increased its platform and IGA capabilities over the last year – moving into a Product Leadership position. Simeio also combines its IAM development experience and systems integration expertise providing an alternative to several established vendors. Overall, Simeio offers good innovation capabilities in RPA and bots and good AG capabilities as part of the Simeio IGA Managed Services solution which should be considered by organizations primarily in the North American and EMEA regions.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 24: Simeio IGA Managed Services' rating

Strengths

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

Challenges

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

Leader in

SIMEIO radar chart showing ratings across: Access Governance and Role Management, Access Request and User Self-Service, Access Review Support, Target System Support, Workflows & Access Policy Management, Authentication, Audit, Compliance & Reporting, Access & Risk Intelligence
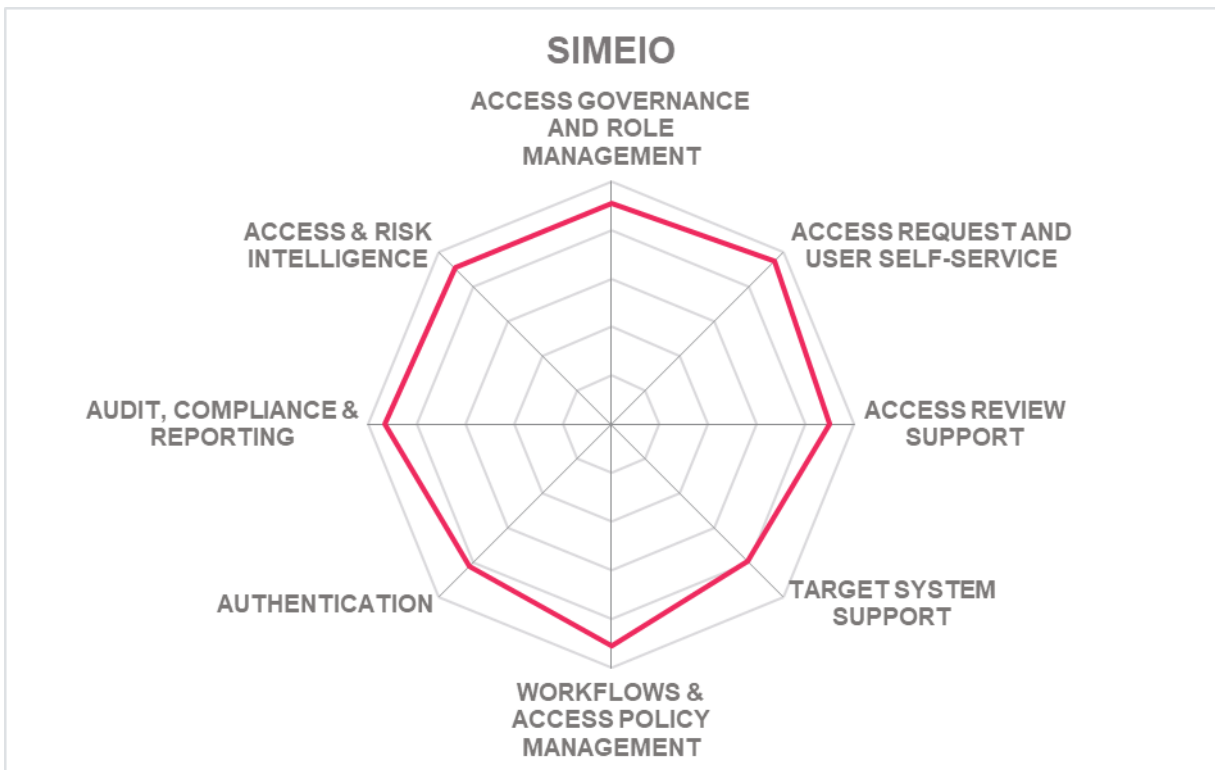
Soffid – Soffid IAM

Based in Spain and established in 2013, Soffid IAM provides a united IAM Platform that brings together Access Management (AM), Single Sign-On (SSO), Identity Governance (IGA), Identity Risk & Compliance (IRC) and Privileged Account Management (PAM) into one comprehensive and converged solution. Soffid offers a subscription service to an enterprise edition of the software product. Technical support service is only provided to the enterprise edition product. Consulting and deployment services are also available through Soffid services. Soffid offers IGA related provisioning, access governance, and SSO capabilities of its Soffid IAM solution for this on-premises Leadership Compass report.

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

Soffid IAM supports a wide range of identity repositories with additional support for integrating into legacy directory solutions of customers. Support for generating new identities is available. A wide range of OOB provisioning on-premises and SaaS connectors is supported. The solution uses a smart engine to fetch and post information from target systems. OOB integration to ITSM includes ServiceNow and Atlassian JIRA service desk.

Regarding Access Governance, Soffid IAM has improved performance and scalability, offering good user self-service capabilities for access requests including roles and privileged access as well as approval workflows. Password and policy management capabilities are also available. Policies can be defined to address account termination, role modification, access exception approval, rights delegation, or SoD analysis and mitigation use cases as examples. Soffid provides good Access Governance reporting support, although out-of-the-box support for major compliance frameworks is not available.

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

Soffid IAM currently focuses on enterprise organizations but also serves small, medium organizations but with customers primarily in Europe and Latin America and growing in North America, and the Middle East region. Soffid's partner ecosystem is relatively small and located in the customer's geographic locations. Soffid offers an alternative open-source solution to organizations with a reasonably well-balanced set of IAM and AG capabilities.

|	
Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 25: Soffid IAM's rating

Strengths

- Good IGA related policies for onboarding and offboarding
- Good support for IGA related reports
- OOB SaaS and on-premises target system support
- Wide range of user and admin authenticator options
- Good web workflow editor
- All functionality exposed via APIs

Challenges

- Limited market presence and partner ecosystem in Europe
- No support for OOB reports for major compliance frameworks
- Event based micro certification is missing
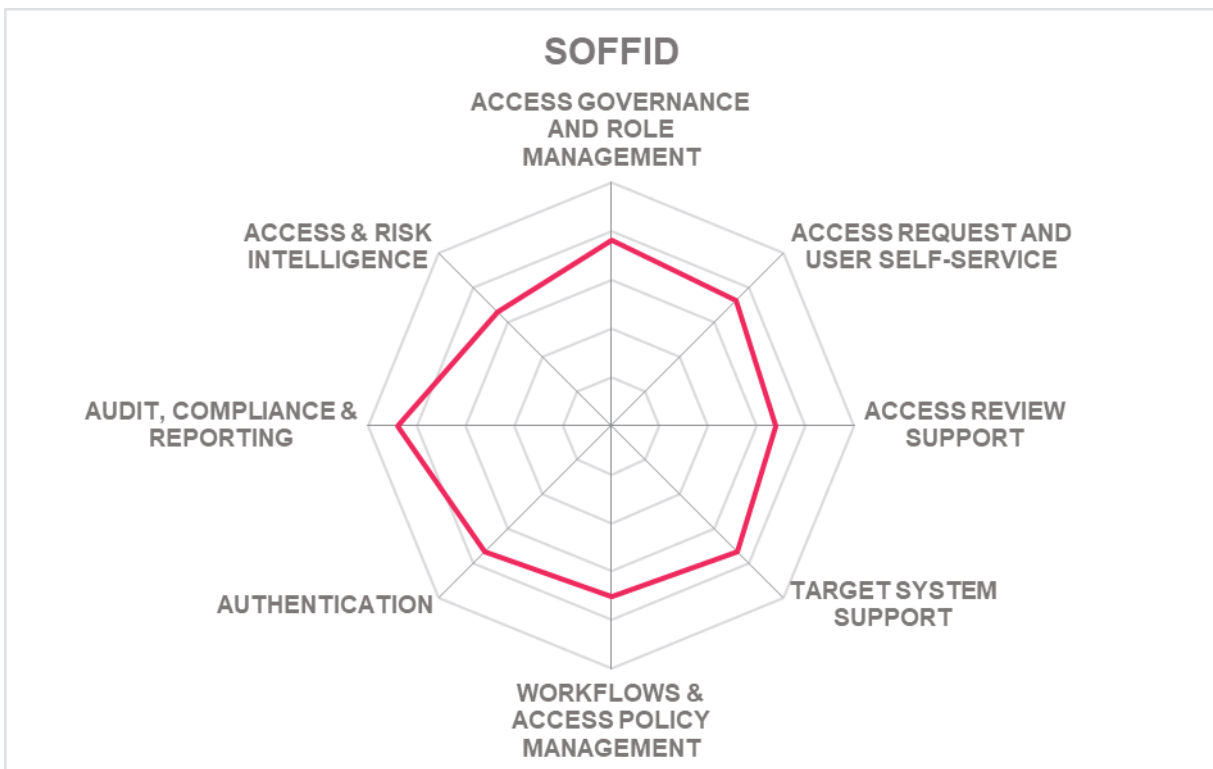
Tools4ever – HelloID

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

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

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

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

With a good product roadmap and execution capability, Tools4ever can make progress towards being a contender with the already existing IDaaS players in the region. Its current customers are based mainly in Europe and North America, and it is a dominant market leader in the Netherlands.

|	
Security	Positive
Functionality	Neutral
Deployment	Neutral
Interoperability	Neutral
Usability	Positive

Table 26: HelloID's rating

Strengths

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

Challenges

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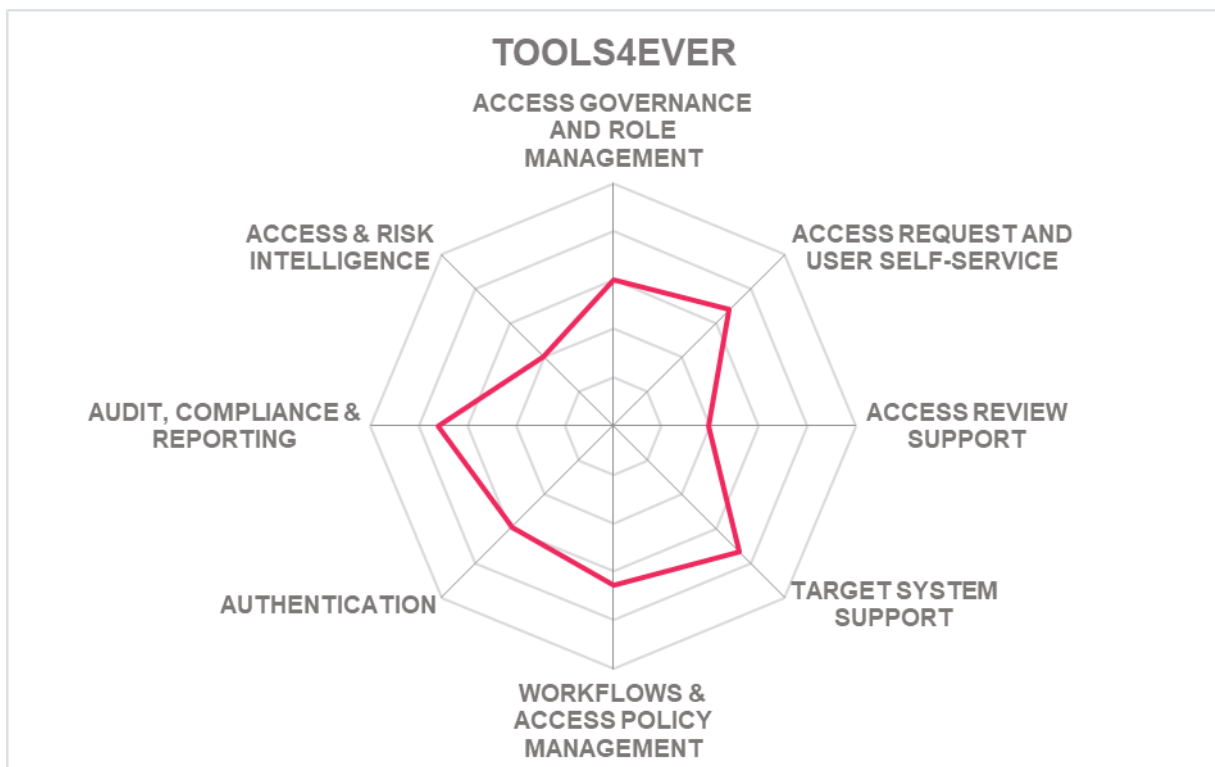
Zertid – Zertid

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

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

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

Zertid primarily supports mid-market businesses focused on the APAC region with a growing focus in the North American market from 2023. Recent updates include an RPA capability for orchestrating access provisioning to third-party systems that are not electronically (API, Data Base etc.) connected with Zertid. This capability uses ServiceNow's relatively new RPA engine. Further update includes a built-in PAM solution with AG workflows providing deep level Privileged Access Governance (PAG). With its strong governance capabilities and target system support, Zertid further plans to expand its list of pre-built connectors and incorporating the use of AI and machine learning showing its innovation roadmap.

|	
Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 27: Zertid's rating

Strengths

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

Challenges

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

ZERTID
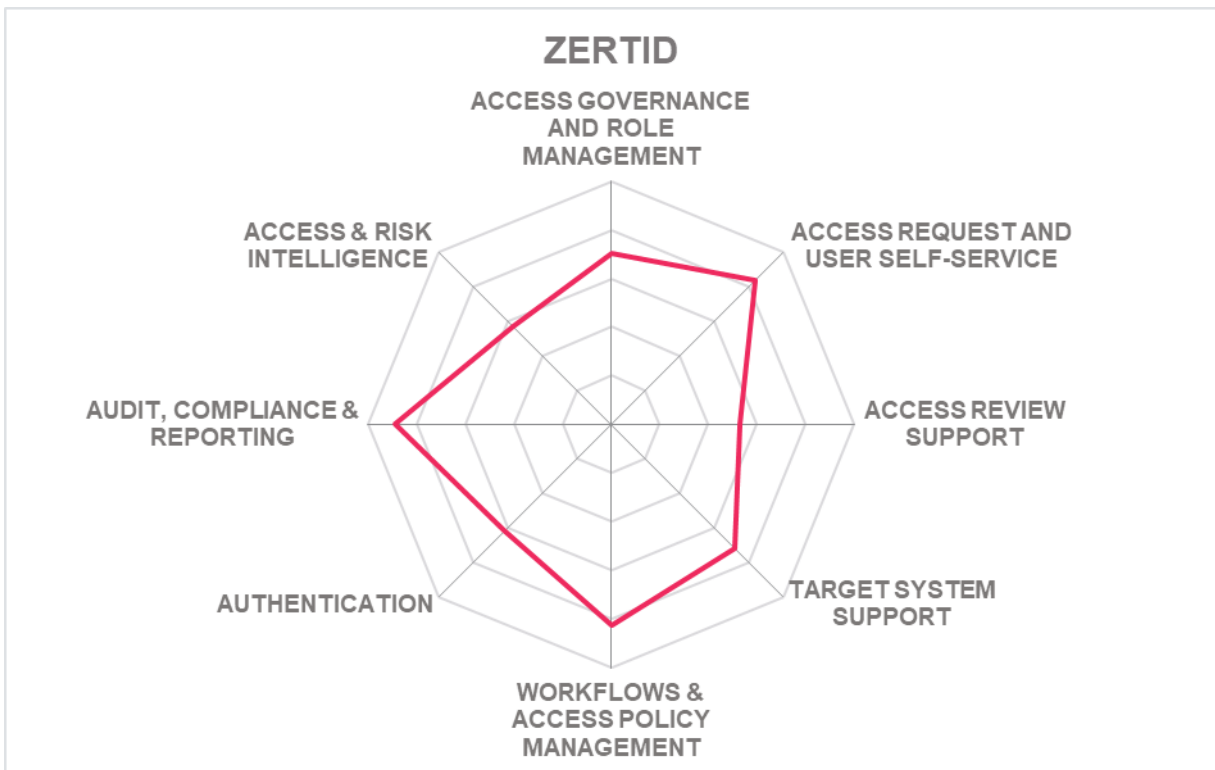
Vendors to Watch

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

Elimity

Founded in 2017, Elimity has its headquarters based in Belgium. The Elimity platform specializes in providing visibility and insights to enable the organizations to meet the high security standards. Elimity sees themselves as focused on User Access Governance (UAG) with a good set of connectors primarily focused on reading information. Roadmap includes shifting from visibility to access governance and potentially towards a full IGA in the future.

Why worth watching: Elimity see their sweet spot in organizations that don't have IGA (yet) but need visibility of the "as is", and to compare and automated checks of risks arising out of orphaned accounts, admin privileges and change requests that are forwarded to ITSM.

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 solely within ServiceNow. Customers install the application directly from the ServiceNow application store. Clear Skye capabilities include Entitlement Management, Access Requests, Audit, Policy Management, Certifications (access reviews), Identity Analytics, and Workflows. Clear Skye IGA uses the standard ServiceNow Service Portal as the interface to request access whereas an end user portal focuses on IGA for workers and supervisors.

Why worth watching: Clear Skye is focused on the Access Governance aspects and excels in its integration to ServiceNow and in supporting certain ServiceNow specific integrations.

Fastpath

Fastpath recently acquired ideiio to create a more complete AG package by addressing the missing functionalities. They have a solution covering broad cross-system IGA plus in-depth access control/governance for SAP and other Line of Business Applications). It takes over the capabilities of ideiio, having a strong support to all known directories servers, databases, or virtual directories used as identity repositories.

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

Fischer Identity

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

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

Ilex International

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

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

Imprivata

Founded in 2002, Imprivata is headquartered on the East Coast of the US. Imprivata provides implementation services for Identity Governance themselves, with a small number of resellers and implementation partners in North America. 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.

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

Kapstone

Founded in 2013 with headquarters on the East Coast in the north-eastern US, Kapstone added both Autonomous IGA and Cloud Governance to its product portfolio. Today Kapstone's Autonomous IGA provides an innovative platform that focuses on three key capabilities - Automation, Intelligence, and Modularity. Beyond core IGA capabilities, Kapstone Autonomous IGA gives some more advanced features that include service discovery, delegated administration, intelligent identity, application discovery and IGA

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

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

Systancia

Based in France, Systancia offers an Access Management platform that includes multiple products within a suite to secure end user's digital workspace. The platform includes remote, privileged, virtual access, and IAM capabilities. Systancia Identity provides basic AG capabilities, focusing on automated provisioning, user self-service, and workflows.

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

Tuebora

Found in 2001 and based in San Francisco, California, Tuebora provides a self-driven identity and access management platform. Tuebora relies on AI and machine learning for Identity Analytics and Access Governance. It is powered by predictive analytics and intelligence for its functioning of a self-driven IAM model. Tuebora offers its own Data Access Governance (DAG) and web access management (WAM) products as Tuebora DAG and SSO respectively.

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

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

Related Research

Methodology

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

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

Types of Leadership

We look at four types of leaders:

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

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

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers

using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview 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
- Deployment
- Interoperability
- Usability

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

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

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

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

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

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

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

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

Vendor rating

We also rate vendors on the following characteristics:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

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

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

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

Rating scale for products and vendors

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

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

Positive   Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral   Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.

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

Critical   Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

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

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

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

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

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

Related Research

Leadership Compass: Access Governance & Intelligence - 80098
Leadership Compass: API Management and Security - 80477
Leadership Compass: Cloud-based MFA Solutions - 70967
Leadership Compass: Enterprise Authentication Solutions - 80062
Leadership Compass: IDaaS Access Management - 790

Leadership Compass: Identity Governance and Administration 2022

Leadership Compass: Access Management

Leadership Compass: SASE Integration Suites

Executive View: SailPoint Identity Security Cloud

Whitepaper: Cloud Access Governance

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.