KuppingerCole Report

LEADERSHIP COMPASS

By Richard Hill
August 20, 2020

Access Governance & Intelligence

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

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

Content

1 Introduction 4
1.1 Market Segment 5
1.2 Delivery models 8
1.3 Required capabilities 8
2 Leadership 12
2.1 Overall Leadership 12
2.2 Product Leadership 13
2.3 Innovation Leadership 15
2.4 Market Leadership 18
3 Correlated View 21
3.1 The Market/Product Matrix 21
3.2 The Product/Innovation Matrix 23
3.3 The Innovation/Market Matrix 25
4 Products and Vendors at a glance 28
5 Product/service evaluation 32
5.1 Avatier Identity AnyWhere 34
5.2 Beta Systems Garancy IAM Suite 37
5.3 Brainwave Identity GRC Platform 40
5.4 Broadcom Symantec Identity Governance and Adminstration (IGA) 43
5.5 E-Trust Horacius 46
5.6 EmpowerID 49
5.7 Evidian IGA 52
5.8 Evolveum midPoint 55
5.9 Fischer International Identity Suite 58
5.10 Hitachi ID Identity Manager 61
5.11 IBM Security Identity Governance & Intelligence 64
5.12 Identity Automation RapidIdentity 68
5.13 Ilantus Compact Identity 71

5.14 Micro Focus Identity Manager Suite 74
5.15 Nexis Controle 77
5.16 Omada Identity 80
5.17 One Identity Manager 84
5.18 Oracle Identity Governance 87
5.19 RSA SecurID Suite 90
5.20 SailPoint Predictive Identity Platform 94
5.21 SAP Access Control & Identity Access Governance 97
5.22 Saviynt Security Manager 100
5.23 Simeio Identity Orchestrator 103
5.24 Soffid IAM 106

6 Vendors and Market Segments to Watch 109

6.1 Imprivata 109
6.2 Kleverware 110
6.3 N8 Identity 110
6.4 SecurEnds 111
6.5 Tuebora 111
6.6 Usercube 112

7 Related Research 113

Endnotes 114

Methodology 115

Content of Figures 121

Copyright 122

1 Introduction

The KuppingerCole Leadership Compass provides an overview of vendors and their product or service offerings 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).

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's 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 fulfillment 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.

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

- LC Access Governance: This Leadership Compass focuses primarily on access governance and Intelligence capabilities, with required integrations into own or third-party entitlements and/or account repositories. We look at complete IGA offerings here too if they have strong access governance & Intelligence capabilities.
- LC Identity Governance and Administration: In this Leadership Compass, the primary focus is on the vendors that offer both identity provisioning and access governance capabilities, either as a common product or separate but integrable product components to deliver capabilities across the IGA spectrum.

These two LCs are complemented by two other Leadership Compass documents – LC IGA for SMBs (small and midsize businesses) that identifies and focuses on functional and operational IGA requirements of SMBs that are different in both objective and magnitude than large organizations. The other Leadership Compass is LC IAM Suites that focuses on comprehensive IAM suites and evaluates vendors for their completeness and functional depth of IAM portfolios to include core and even adjacent IAM capabilities such as Privilege Management, Enterprise SSO, Identity Federation, Web Access Management, API Gateways, Fraud Detection and Prevention, etc. in addition to IGA as an integrated offering.

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

1.1 Market Segment

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 thus 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 technology 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 risk in access governance and mitigate it 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 Entitlements and access governance (EAG)[1] or 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 most relevant and efficient grouping of access entitlements. Advanced role management capabilities include pattern and risk analysis as well as role simulations for an 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.
- Support for EAG (Entitlement and access governance).

Over time, a deep integration with Dynamic Authorization Management Systems which are used to centrally define policies for application and system security is required as well. However, there are still few solutions in the market providing even minimal integration.

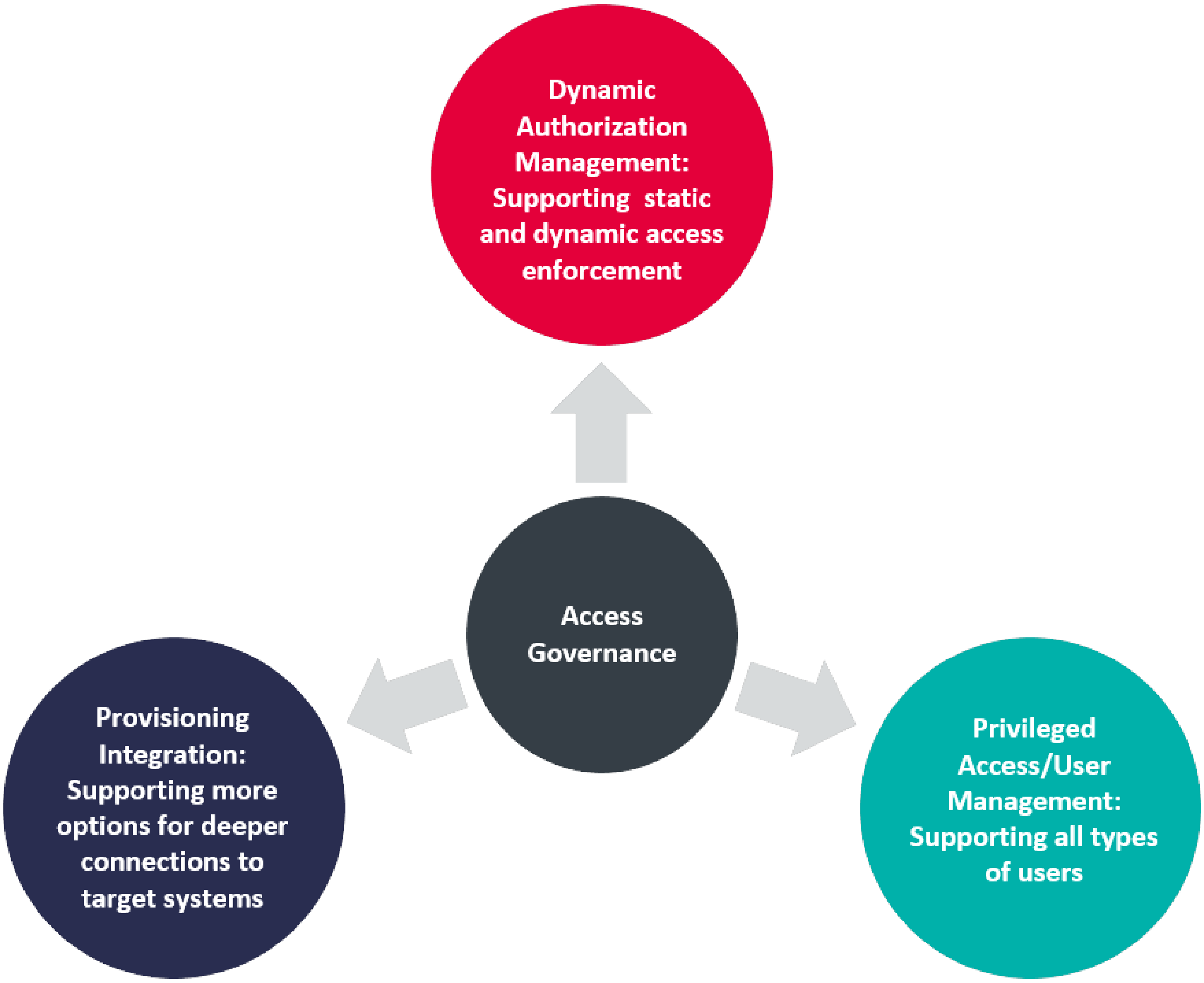

Dynamic Authorization Management: Supporting static and dynamic access enforcement
Access Governance
Provisioning Integration: Supporting more options for deeper connections to target systems
Privileged Access/User Management: Supporting all types of users

Figure 1: The Status and Expected Evolution of Access Governance

1.2 Delivery models

This Leadership Compass is focused on products that predominantly run on-premises, either at the customer site or hosted by a Managed Service Provider (MSP) at their site. We do not include Identity as a Service (IDaaS) delivery that consists of hosting and managing of the product by the vendor itself, as part of our current evaluation of access governance focused vendors in this Leadership Compass.

Please refer to KuppingerCole Leadership Compass on IDaaS, including IDaaS B2E, focused on solutions for supporting IGA for hybrid environments, delivered as a service.

1.3 Required capabilities

When evaluating the products, we look at various aspects, including:

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- traditional core features of identity provisioning

Within the area of functionality, the required capabilities are centered around the key components listed above:

- Workflow support for request and approval processes
- Workflow support for role lifecycle 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.
- SPML/SCIM support
  Support for SCIM (System for Cross-domain Identity Management) is preferred over traditional SPML (Service Provisioning Markup Language) for federated as well as on-prem provisioning. However, we evaluate support for both the standards depending on specific use-cases.
- Deployment models
  Supporting multiple delivery options such as hard/soft appliances and optional MSP services gives customer a broader choice.
- Customization
  Systems that require little or no coding and that support scripting or, if programming is required, SDKs or support for a range of programming languages, are preferred. We here also look for transport mechanisms between IT environments (e.g., development, test, and production), and the ability of keeping customizations unchanged after upgrades.
- Mobile interfaces
  Secure apps providing mobile access to certain key capabilities of the product such as access request approvals etc.
- Authentication mechanisms
  We expect 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 pretty popular for simplifying the access request management process by using shopping cart paradigms familiar to the users.

- Standards
  Support for industry standards for direct provisioning including well known protocols like HTTP, Telnet, SSH, FTP etc.
  Support for industry standards for federated provisioning, including OpenID Connect, OAuth and SCIM.
- Analytical capabilities
  Analysis of identity and entitlement data to support capabilities like role management, access requests and policy management. Advanced analytical capabilities beyond reporting, using standard BI (Business Intelligence) technology or other advanced approaches such as deep machine learning for automated reviews are becoming increasingly important.
- Role and risk models
  Especially in access governance, what counts is the quality and flexibility of role and risk models. These models not only need to look nice, there needs to be a strong conceptual background and sufficient flexibility to adapt to the customer's need. Unfortunately, not every tool that looks nice at first glance is sophisticated enough to cover all needs of customers. But it is not the customer adapting to the tool, it should be the tool adapting to the customer.
- EAG[2] /Data Governance
  Support for Entitlement and access governance (EAG), i.e. the ability to also analyze entitlements at the level of underlying systems such as SAP, Windows file servers, etc.
- Role/SoD concept
  Should be able to analyse 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've also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other offerings available in the market.

2 Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

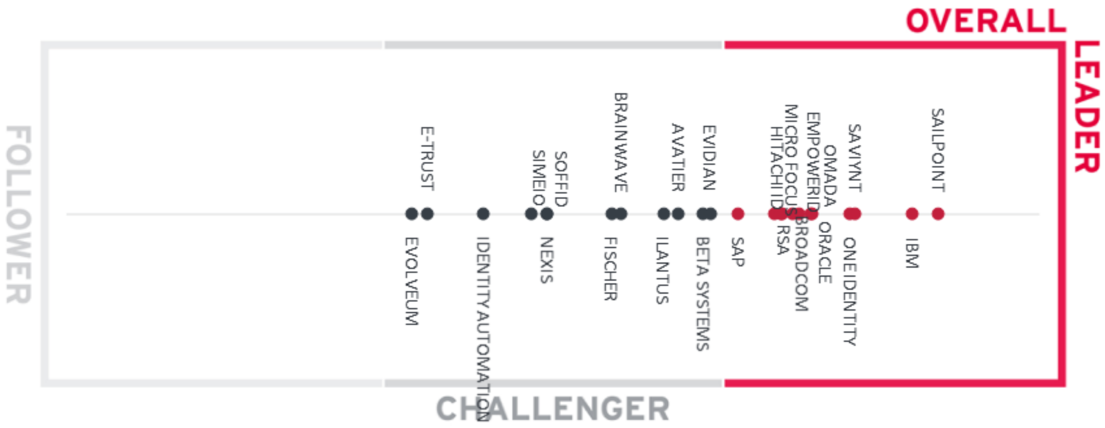


Figure 2: The Overall Leadership rating for the Access Governance market segment

When looking at the Leader segment in the Overall Leadership rating, we see a picture that is a typical representation of mature markets, where a considerable number of vendors deliver feature-rich solutions. The market continues to remain crowded, with 24 vendors we chose to represent in our Leadership

Compass rating with a few other vendors that did not meet our basic evaluation criteria listed in the "vendors to watch" section or which declined participation in this year's edition.

SailPoint retains its leadership position in the Overall Leadership evaluation of the Access Governance (AG) market closely followed by IBM. Next is Saviynt and One Identity. A group of vendors is following, including (in alphabetical order) Broadcom, Hitachi ID, Omada, Oracle, Micro Focus, EmpowerID, and RSA. This group of vendors is a mix of established and emerging players, some being stronger in their market position, and others in innovativeness. We strongly recommend further, detailed analysis of the information provided in this document for choosing the vendors that are a best fit to your requirements.

Another vendor in the Overall Leaders segment for AG is SAP near the bottom boarder – which pushed into the Overall Leader segment with its improved ratings for market and innovation evaluation criteria.

The Challenger segment is as populated as the Leaders segment and features both established vendors, frequently being more regional focused, and several niche vendors with fit-for-purpose AG capabilities and preferred by many organizations over the established players. Leading in this segment are Evidian, and Beta Systems closely followed by Avatier, and Ilantus. Brainwave, and Fischer Identity appear close together with Soffid, Simeio, Nexis and Identity Automation follow with some distance. Near the bottom boarder of the Challenger segment is E-Trust and Evolveum, all good products with varying levels of AG capabilities, market presence throughout the world or other market niche focus.

No vendors appear in the Follower segment.

Overall Leaders are (in alphabetical order):

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

2.2 Product Leadership

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

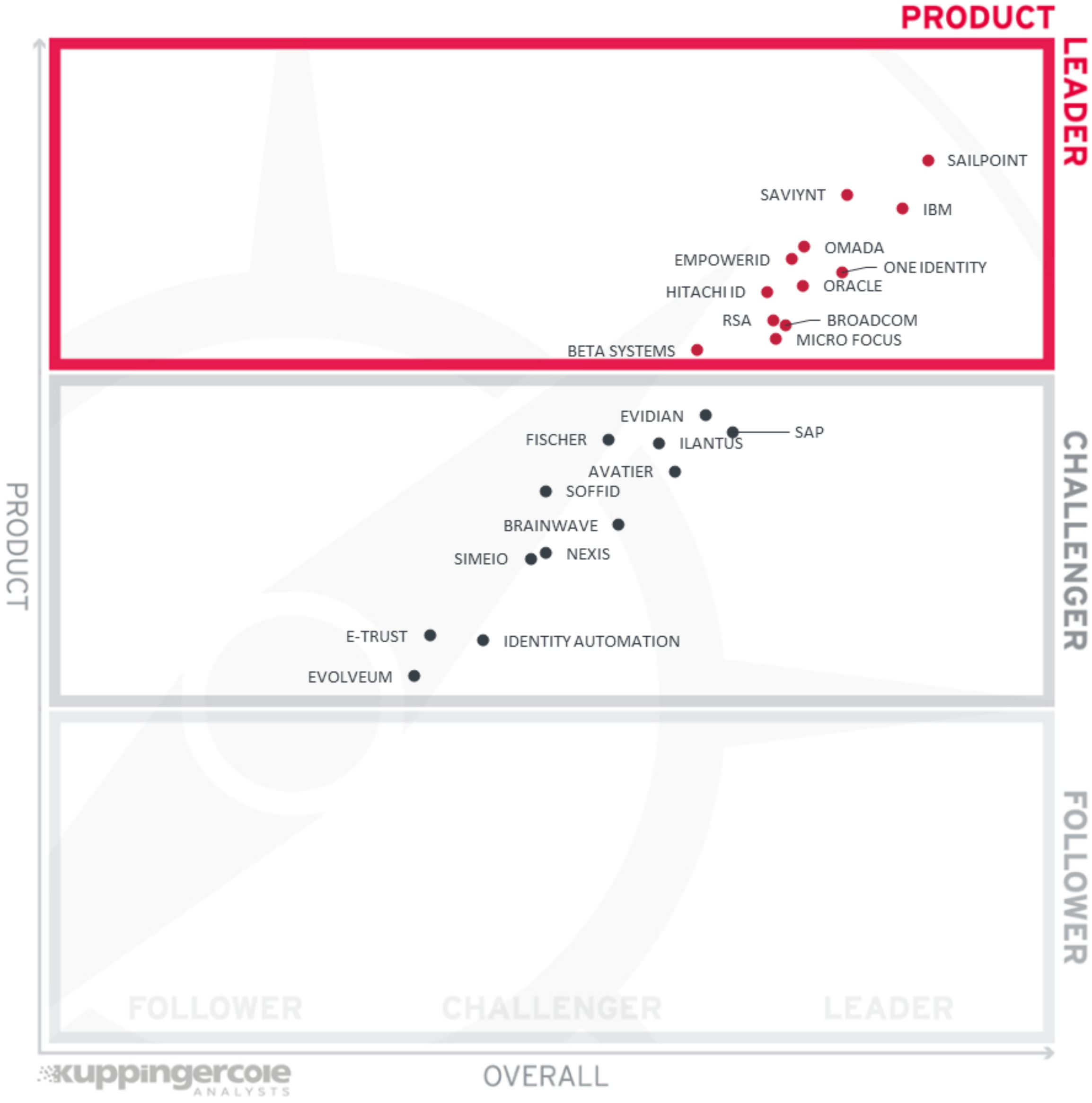


Figure 3: Product Leaders in the Access Governance market segment

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 a number of vendors qualifying for the Leaders segment as well as a number of 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 IBM. Omada and EmpowerID takes a position in the upper range of the Leader's segment, followed by a group of vendors including (in alphabetical order) Hitachi ID, and One Identity, 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. RSA Security, Broadcom, Micro Focus and Beta Systems are positioned next as leaders in the product leadership segment, trailing the others from a close distance in the completeness of product leadership qualities.

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

No vendors appear in the Follower segment.

Product Leaders (in alphabetical order):

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

2.3 Innovation Leadership

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

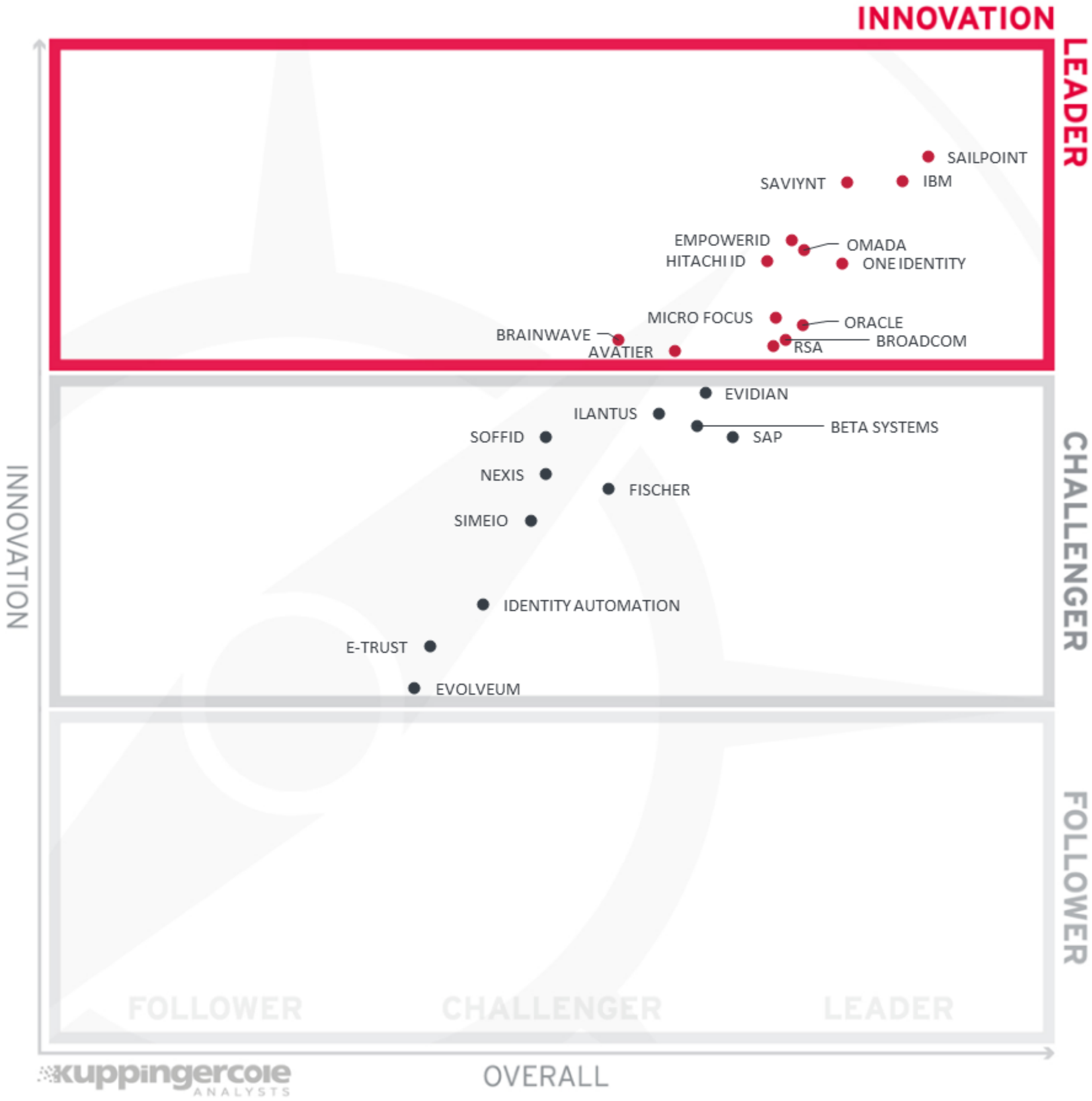


Figure 4: Innovation Leaders in the Access Governance market segment

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

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

SailPoint continues to lead the Innovation Leadership evaluation, very closely followed by IBM, and Saviynt. EmpowerID, Hitachi-ID, Micro Focus, Omada, and One Identity (in alphabetical order) are next on the chart and continue to strengthen their AG leadership position with constant innovation. Ranked next are Avatier, Brainwave, Broadcom, Micro Focus, Oracle, and RSA Security (in alphabetical order) that have made significant changes to their AG product portfolio to be in-line with other innovative vendors in the market. These vendors differ in many details when it comes to innovation and balancing it with overall product leadership, and therefore a thorough vendor selection process is essential to pick the right vendor of all the AG players that best fit the customer requirements.

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

No vendors appear in the Follower segment.

Innovation Leaders (in alphabetical order):

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

2.4 Market Leadership

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

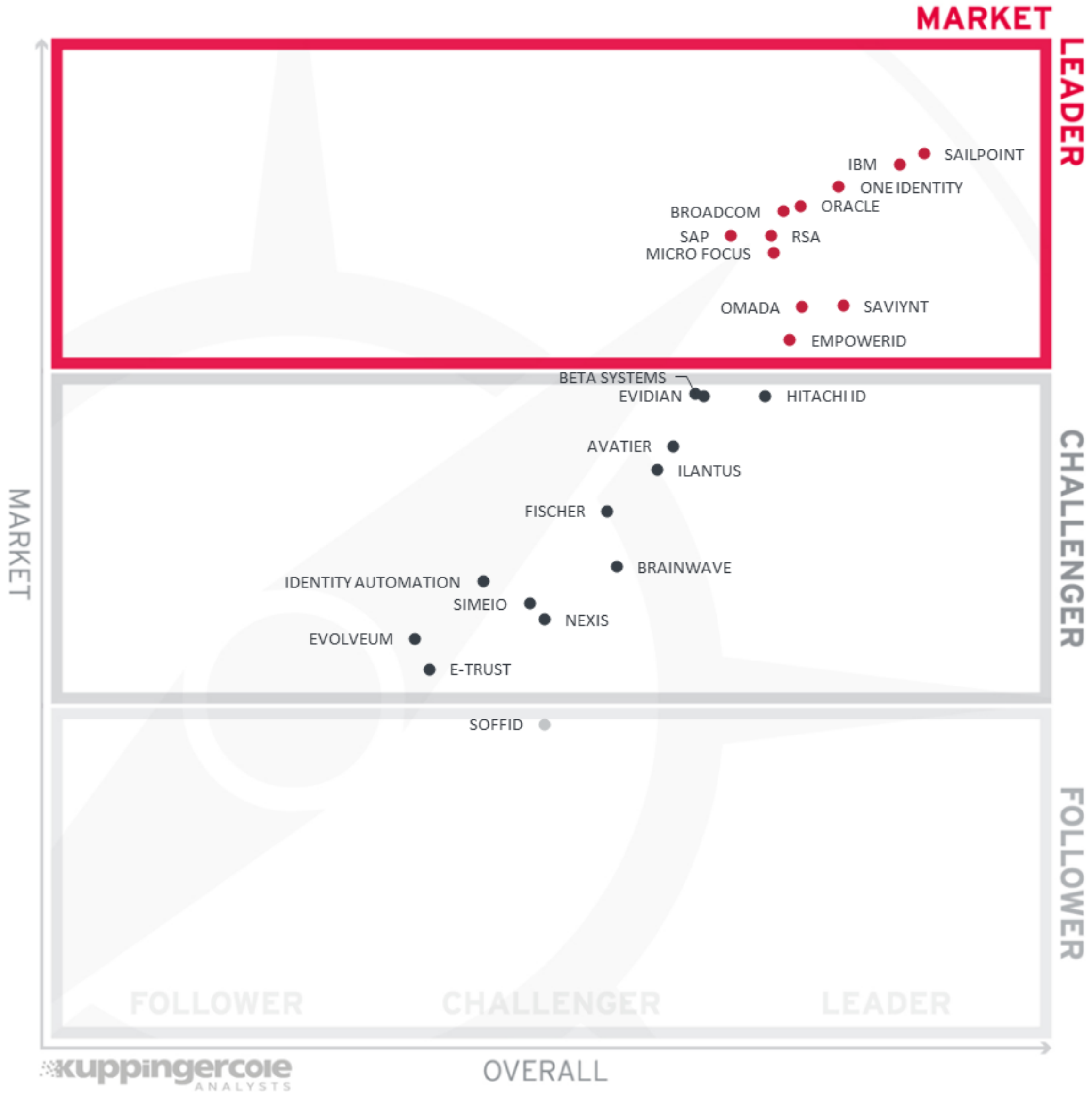


Figure 5: Market Leaders in the Access Governance market segment

The Market Leadership evaluation paints a different picture of vendors. With a group of leading, well-established Access Governance (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 relatively smaller customer base.

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

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

In the Follower segment, we find Soffid - 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):

- Broadcom
- EmpowerID
- IBM
- Micro Focus
- Omada
- One Identity
- Oracle
- RSA Security
- SailPoint
- SAP
- Saviynt

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

3.1 The Market/Product Matrix

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

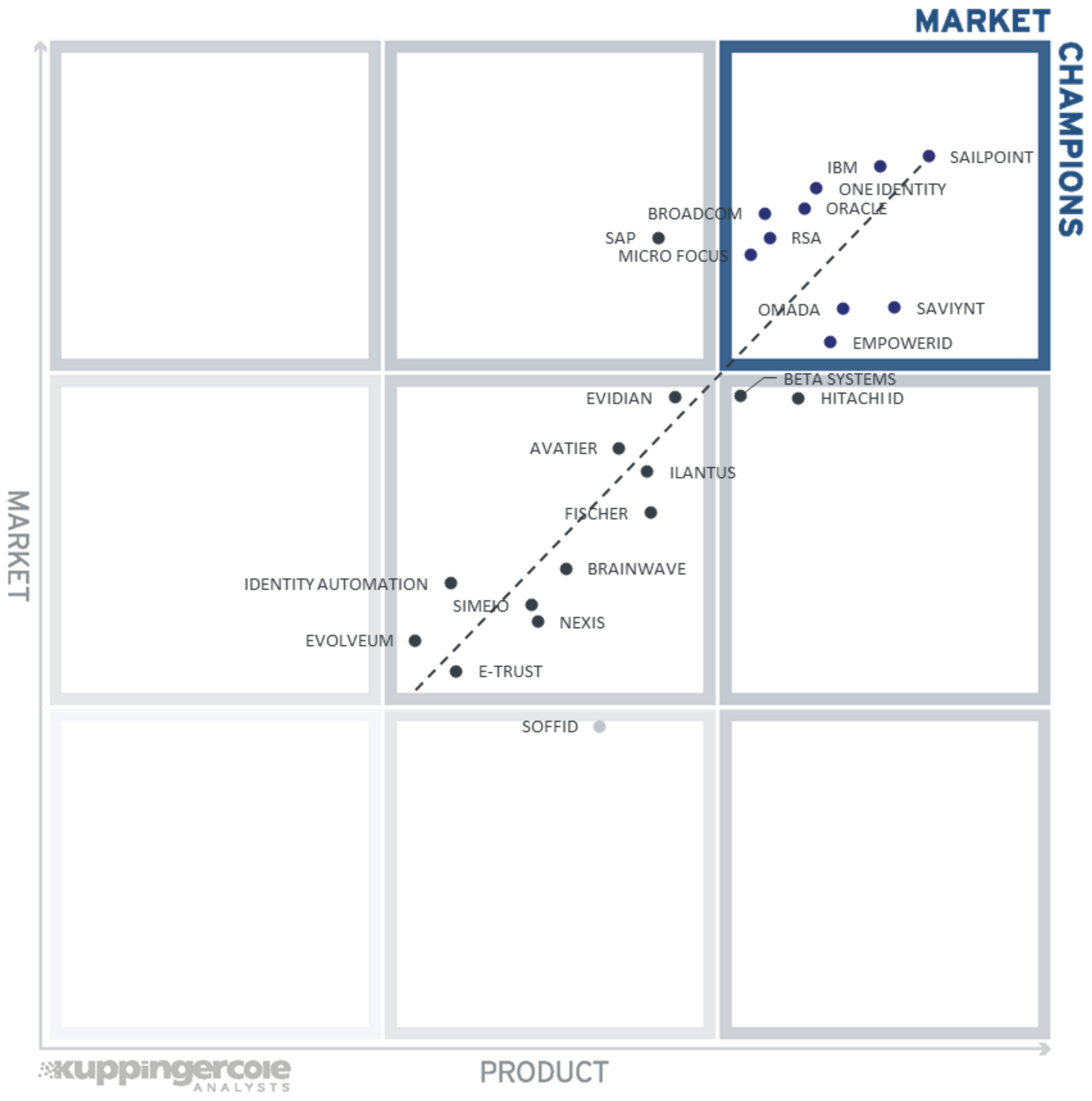


Figure 6: The Market/Product Matrix

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

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

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

EmpowerID, Omada, and Saviynt are positioned under the axis representing their inclination for stronger product leadership in comparison to the market leadership 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 two vendors that deliver strong product capabilities for AG but is not yet considered Market Champions. Beta Systems and Hitachi ID have a strong potential for improving its market position due to the stronger product capabilities that they are already delivering.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not Market Leaders as of yet. They also have average market success as compared to market champions. These vendors include (in alphabetical order) Avatier, Brainwave, E-Trust, Evidian, Evolveum, Fischer Identity, Identity Automation, Ilantus, Nexis, and Simeio.
Finally, in the bottom middle box is the remaining vendor, Soffid, with less market visibility than product strength.

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

3.2 The Product/Innovation Matrix

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

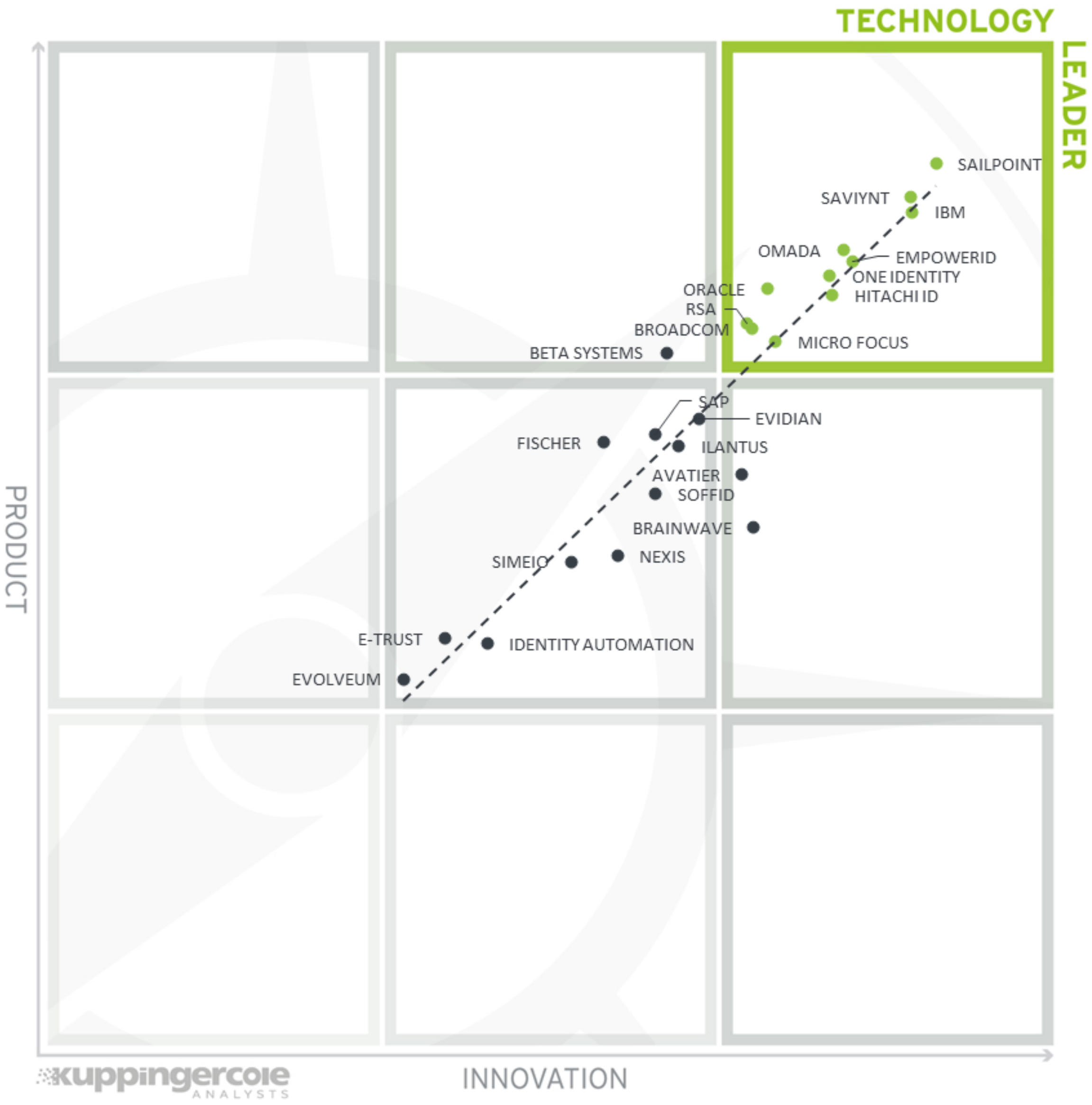


Figure 7: The Product/Innovation Matrix

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

Here, we see a good correlation between the product and innovation rating, with most vendors being placed close to the dotted line indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find most of the leading vendors in the upper right corner, scattered throughout the box. The top-notch vendor is SailPoint closely followed by Saviynt, and IBM– with both placing close to the axis depicting a good balance of product features and innovation.

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

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

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

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

3.3 The Innovation/Market Matrix

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

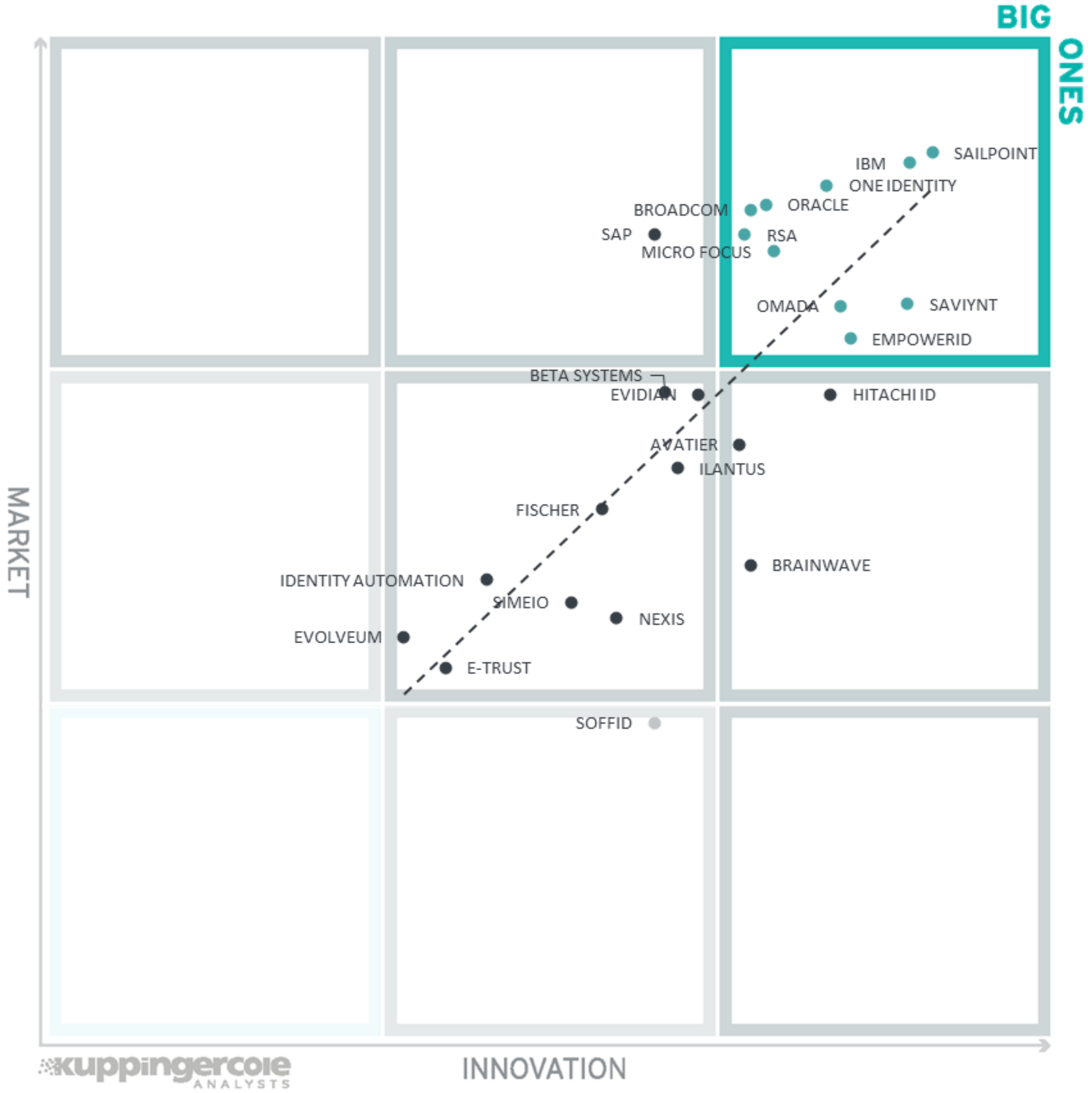


Figure 8: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relatively weaker position in the Innovation Leadership rating, while vendors below the line show, based on their ability to innovate, the biggest potential for improving their market position.

In the upper right-hand corner box, we find the “Big Ones” in the Access Governance market. We see the large ones more on top, including (in alphabetical order) Broadcom, IBM, Micro Focus, One Identity, Oracle, RSA, and SailPoint. Omada, Saviynt and EmpowerID are placed in the same box, more towards the bottom, indicating that they haven’t yet reached the same market position as the established players.

Three vendors, Avatier, Brainwave, and Hitachi ID appear in the middle right box showing good innovation with slightly less market presence than the vendors in the "Big Ones" category.
In the box at the middle top, we find SAP with a strong market position but not scoring as much in Innovation Leadership.

The segment in the middle of the chart contains the vendors rated as challengers both for market and innovation leaderships, which includes (in alphabetical order) Beta Systems, Evidian, Ilantus, Fischer Identity, Identity Automation, Simeio, Nexis, Evolveum, and E-Trust.

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

4 Products and Vendors at a glance

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

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

Product	Security	Functionality	Interoperability	Usability	Deployment
Avatier Identity AnyWhere	🟢	⚫	⚫	🟢	⚫
Beta Systems Garancy IAM Suite	🟢	⚫	🟢	⚫	⚫
Brainwave Identity GRC Platform	⚫	⚫	⚫	⚫	⚫
Broadcom Symantec Identity Governance and Adminstration (IGA)	🟢	⚫	🟢	🟢	⚫
E-Trust Horacius	⚫	⚪	⚫	⚫	⚫
EmpowerID	🟢	🟢	🟢	🟢	⚫
Evidian IGA	🟢	⚫	⚫	🟢	⚪
Evolveum midPoint	⚫	⚪	⚫	⚪	⚫
Fischer International Identity Suite	🟢	⚫	⚫	⚫	🟢
Hitachi ID Identity Manager	🟢	⚫	🟢	🟢	🟢
IBM Security Identity Governance & Intelligence	🟢	🟢	🟢	🟢	⚫
Identity Automation RapidIdentity	⚫	⚪	⚫	⚫	⚫
Ilantus Compact Identity	🟢	⚫	⚫	⚫	🟢
Micro Focus Identity Manager Suite	🟢	🟢	🟢	🟢	⚫
Nexis Controle	⚫	⚫	⚪	⚫	⚫
Omada Identity	🟢	🟢	⚫	🟢	⚫
One Identity Manager	🟢	🟢	🟢	🟢	⚫
Oracle Identity Governance	🟢	🟢	🟢	🟢	⚫
RSA SecurID Suite	🟢	🟢	⚫	🟢	⚫
SailPoint Predictive Identity Platform	🟢	🟢	🟢	🟢	⚫
SAP Access Control & Identity Access Governance	🟢	⚫	⚫	⚫	⚫
Saviynt Security Manager	🟢	🟢	🟢	🟢	🟢
Simeio Identity Orchestrator	🟢	⚫	⚫	⚫	⚫
Soffid IAM	🟢	⚫	⚫	⚫	⚫
Legend	🟠 critical	🔴 weak	⚪ neutral	⚫ positive	🟢 strong positive

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Avatier	⚫	⚫	⚫	⚪
Beta Systems	⚫	⚫	⚫	⚫
Brainwave GRC	⚫	⚪	⚪	⚪
Broadcom Inc.	⚫	🟢	🟢	🟢
E-Trust	⚪	⚪	⚪	⚪
EmpowerID	🟢	⚫	⚫	⚫
Evidian (was acquired by Atos)	⚫	⚫	🟢	⚫
Evolveum	⚪	🔴	⚪	⚫
Fischer International Identity	⚪	⚪	⚫	⚪
Hitachi ID Systems	🟢	⚫	🟢	⚫
IBM	🟢	🟢	🟢	🟢
Identity Automation	⚪	🔴	⚪	⚪
Ilantus Technologies	⚫	⚪	⚫	⚫
Micro Focus	⚫	🟢	🟢	🟢
Nexis	⚫	⚪	⚪	⚪
Omada	🟢	⚫	⚫	⚫
One Identity	🟢	🟢	🟢	🟢
Oracle	⚫	🟢	🟢	🟢
RSA Security	⚫	⚫	🟢	🟢
SailPoint	🟢	🟢	🟢	🟢
SAP	⚫	🟢	🟢	🟢
Saviynt	🟢	⚫	⚫	🟢
Simeio Solutions	⚪	⚪	⚫	⚪
Soffid	⚫	🔴	⚪	⚪
Legend	🟠 critical	🔴 weak	⚪ neutral ⚫ positive	🟢 strong positive

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

In Innovativeness, this rating is applied if vendors provide none or very few of the more advanced features we have been looking for in that analysis, such as providing access intelligence using analytics, AI/ML, role discovery or mining, assistance in incident analysis and/or remediation, risk-based analysis of identity events, user activity monitoring, or support for container-based microservice related deployment model as examples.

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

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

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

5 Product/service evaluation

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

Spider graphs

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

- Target System Connectivity
  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 others. Broad support for standard cloud services is also considered. The depth of connector capabilities is analyzed too, in particular, 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, Approval & 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 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
  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.
- Access Policy & Workflow 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.
- Governance UI & Mobile Support
  This is the extent to which the access under governance control can be viewed in a consolidated or single-pane view, such as in a dashboard format, as well as features and controls it provides. Also evaluated is support for secure mobile access to selected AG capabilities.

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

5.1 Avatier Identity AnyWhere

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

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

Identity Anywhere is comprised of several modules catering to a broad spectrum of Access Governance functionalities, which includes Workflow Manager, and Identity Analyzer. Avatier supports both SPML and SCIM for provisioning/de-provisioning, and has a broad set of connectors available for a variety of systems. 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. Although good access and risk intelligence capabilities are given, more advanced features such as user activity monitoring (UAM) that can detect abuse of user privileges through abnormal activity pattern analysis is not.

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

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

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

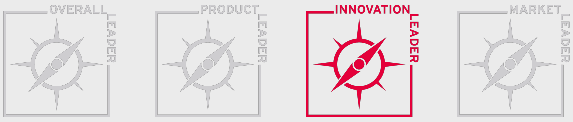
Strengths

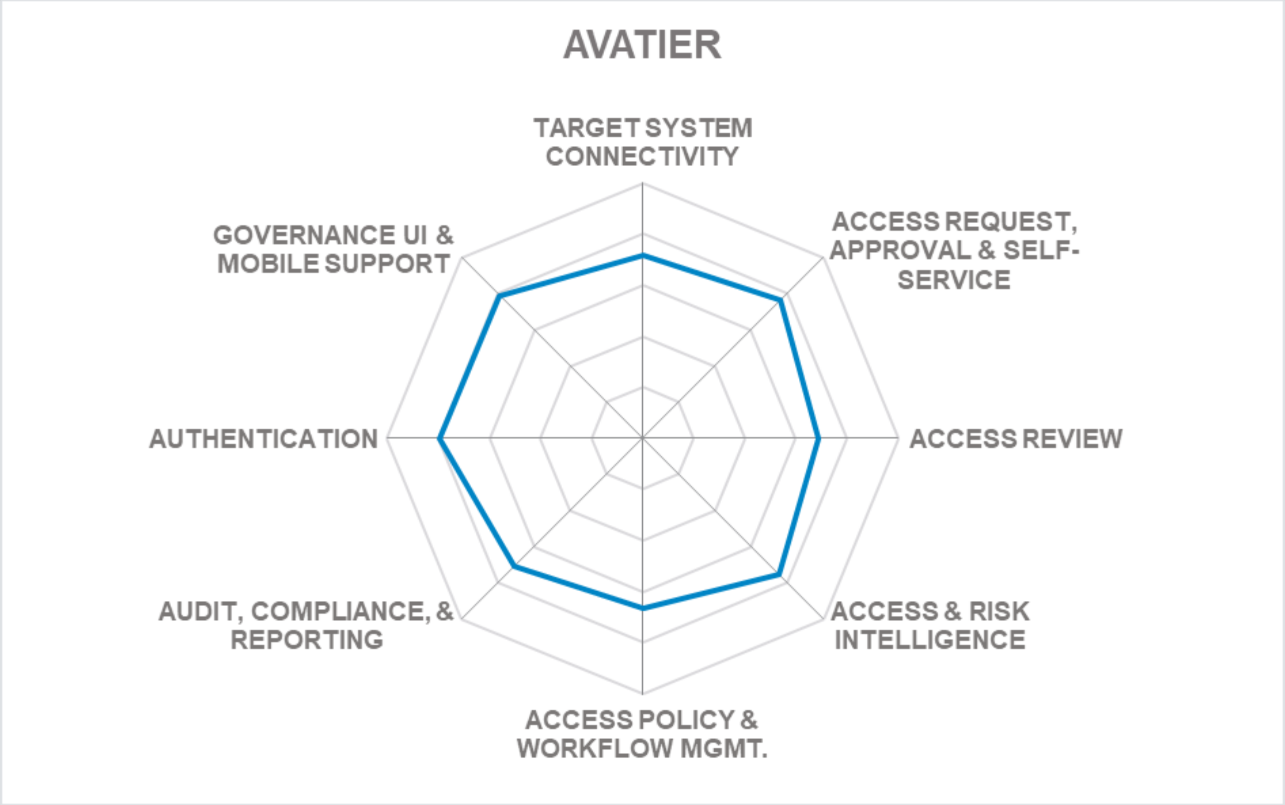
- Fully containerized governance platform
- Innovative, user-centric approach to AG
- Depth & breadth of OOB connectors to both on-premises and SaaS systems
- Strong authentication option support
- Access & risk intelligence
- Role management
- Flexible workflow automation capabilities
- Good reporting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

Challenges

- A growing but limited partner ecosystem
- A limited footprint outside of North America
- Limited marketing visibility
- Missing user activity monitoring (UAM) support

Leader in




AVATIER
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.2 Beta Systems Garancy IAM Suite

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

Beta Systems is one of the few vendors offering connectors with full application integration, allowing applications to configure and request authorization decisions at runtime and therefore enabling dynamic authorization management as an integrated feature within the base product. Garancy Process Center enables customization of connectors for applications and non-standard target systems while offering a business-friendly approach to create and configure authorization workflows.

The built-in role management capability allows for the efficient and automated assignment of entitlements, although role mining capabilities are not available. 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 solution. Access intelligence is given, providing strong reporting and dashboarding capabilities, although only basic support for SOD risk analysis is given and there is some room for improvement regarding outlier detection intelligence.

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

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

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

_betasystems

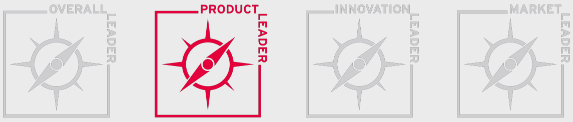
Strengths

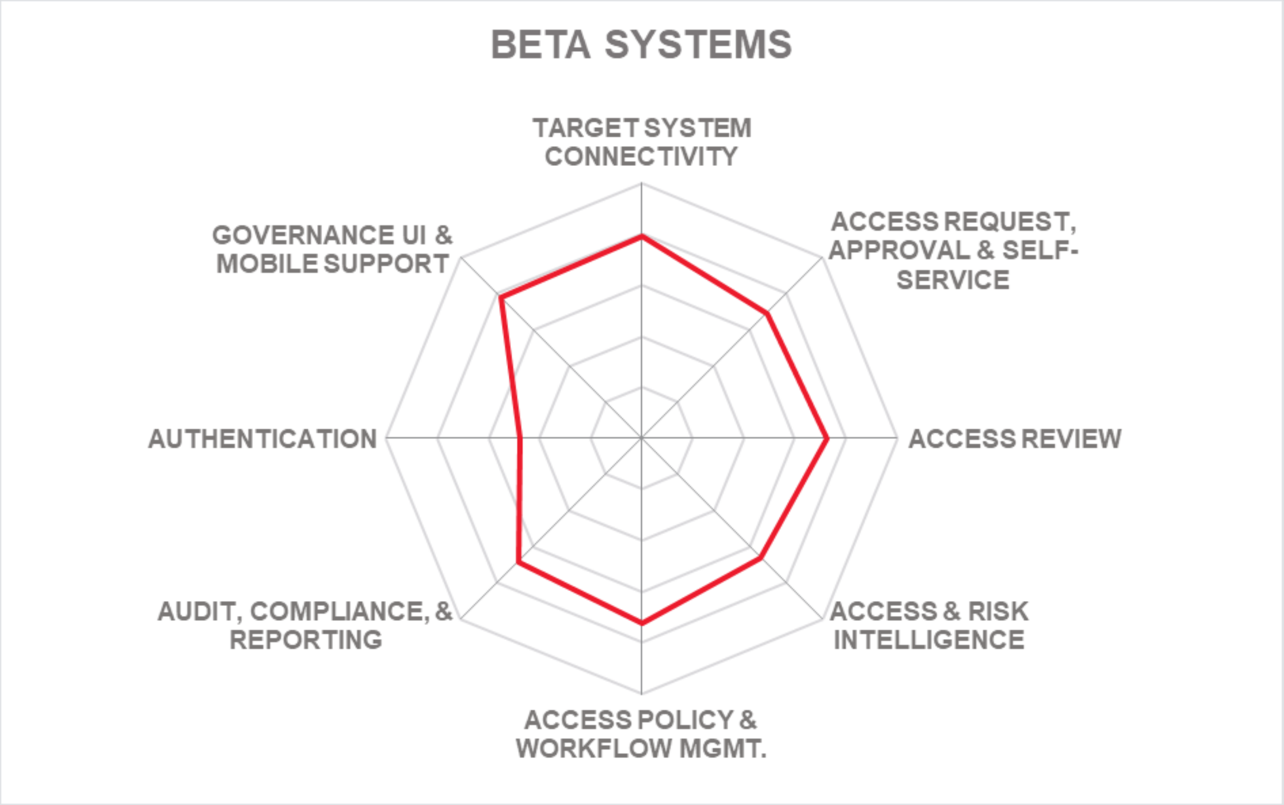
- Breadth of OOB connectors
- Ease and flexibility of workflow customization
- Support for Dynamic Authorization Management
- Governance UI and mobile support
- Supports granular Data Access Governance
- Dedicated support for mainframe environments

Challenges

- Primarily focused in the EMEA region
- Somewhat small but growing functional partner ecosystem
- Basic user and admin authentication options
- Some room for improvement regarding OOB connector support for SaaS applications
- Some room for improvement for outlier detection intelligence

Leader in




BETA SYSTEMS
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.3 Brainwave Identity GRC Platform

Brainwave, based in France, was founded in 2010. The company offers Brainwave Identity GRC as its core analytics based GRC solution. An extension to IGA 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.

Brainwave supports on-premises and private cloud deployment models that can be delivered as SaaS or software deployed to a server. A managed service is possible in a single-tenant dedicated cloud environment. The solution runs within a Linux environment with a database dependence in which PostgreSQL, Microsoft SQL Server or Oracle databases are supported. 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 alerting is given. SDK support is limited to Server-Side JavaScript.

Built on the OpenICF connector framework, it offers the flexibility for customers who demand customization of connectors based on identity attributes. Good out-of-the-box connector support is given for on-premises target applications, although slightly less support to SaaS target systems. Very little support for user self-service is available. Good Access Governance related reports that include access risks, accounts, attestations, groups, roles, users, and privileged access, as well as reports related to SoD, unstructured data, PAM, and IAS are given. Also, strong support for out-of-the-box reports for major compliance frameworks is available. 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 does include a BPMN 2.0 workflow engine with templates for other governance processes. Authentication options for user self-service are not available, although good authentication support is available administration access.

Brainwave Identity GRC uses a tightly integrated BIRT analytics engine at the backend for identity analytics and access intelligence capabilities. This enables Brainwave to conduct SOD risk analysis beyond SAP ERP platforms into hybrid ERP platforms that support RESTful APIs for identity and access entitlements exchange. 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 at an organization's end, although Brainwave can provide training and technical assistance to implement the solution. 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.

Heavily reliant on open-source platforms, Brainwave can require significant development efforts to achieve common access governance tasks. With specialized java development skills inhouse, 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	● ● ● ● ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

Brainwave GRC

Strengths

- 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
- Available integrations with prominent market players
- User activity monitoring (UAM) support

Challenges

- Growing but limited market presence outside the EU
- Missing user self-service support
- Authentication options apply to administrative access only
- A regionally confined partner ecosystem

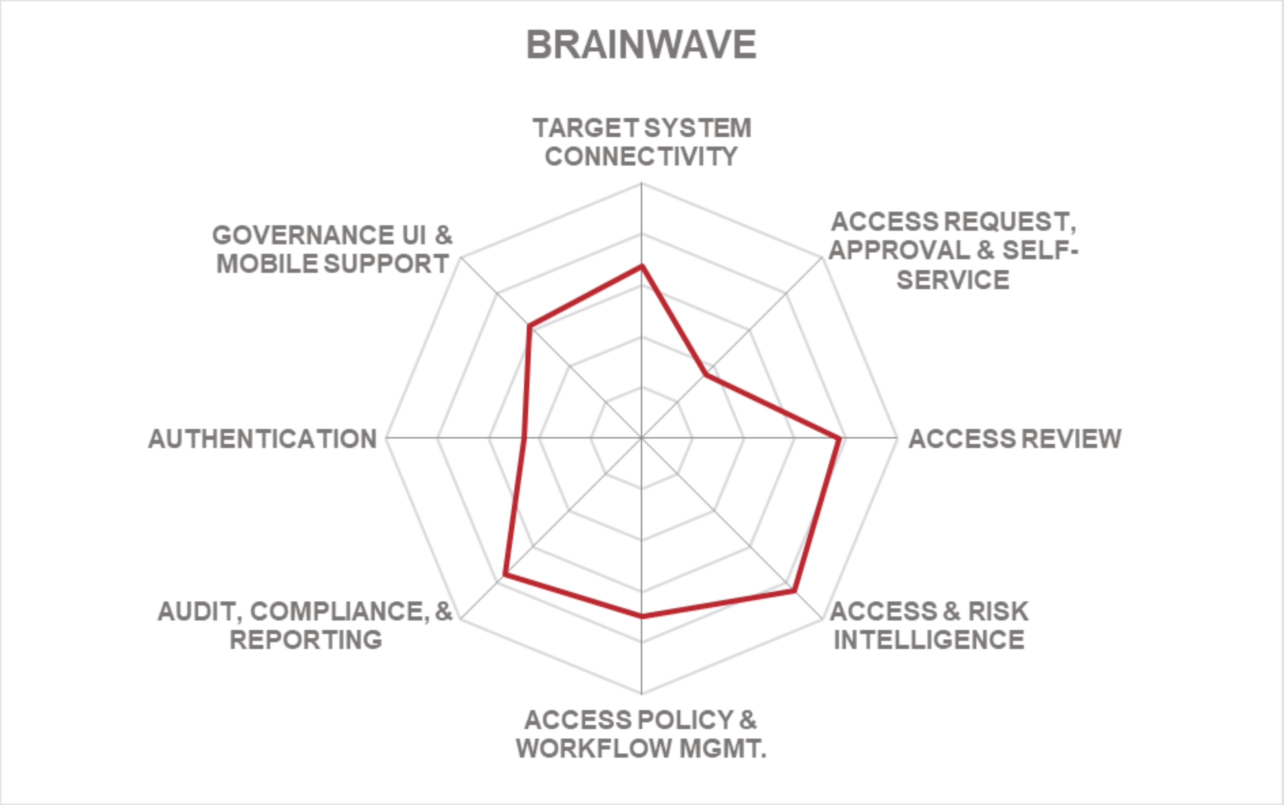
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


BRAINWAVE
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.4 Broadcom Symantec Identity Governance and Adminstration (IGA)

Broadcom, an American manufacturer of semiconductor and infrastructure software products company, acquired CA Technologies in late 2018 and acquired the Symantec Enterprise business in late 2019. The former CA Security business is now part of the Symantec Enterprise Division of Broadcom. Broadcom's Symantec Enterprise portfolio includes Symantec Identity Governance and Administration (IGA), which consists of Identity Manager, Identity Governance, and the Identity Portal. Today, Broadcom Symantec IGA maintains a well-integrated platform providing the range of Access Governance features to be expected from an established market player.

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

Good support for role management is given which includes role discovery and mining capabilities. Although entitlement outlier detection is available, other access and risk intelligence is missing such as access modeling, anomaly and role outlier detection. Support for access certification is also given, but recertification triggers such as access risks or SoD violations are not. User activity monitoring (UAM) is supported, but requires the addition of the Symantec PAM solution.

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

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

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

BROADCOM

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

Strengths

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

Challenges

- Customization is better than in past but could easily grow complex and expensive
- Relatively smaller technology partner ecosystem in comparison to other established players in the market
- Limited product delivery options
- Some access & risk intelligence limitations

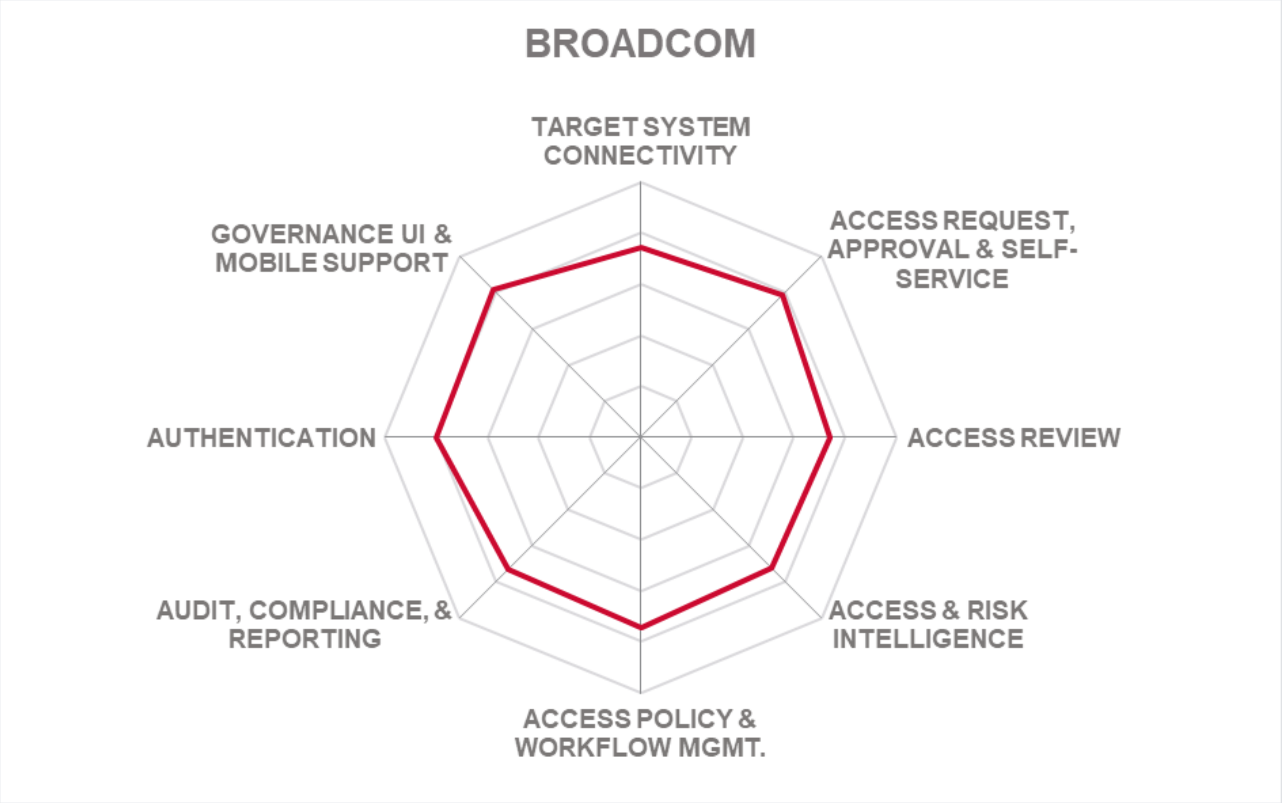
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


BROADCOM
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.5 E-Trust Horacius

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

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

E-Trust offers Horacius as a common platform for identity provisioning and access governance. The Horacius platform has grown over time to be a mature product offering a spectrum of access governance functionalities. Horacius is capable of handling automated user provisioning, access reviews & attestations, orphan account monitoring, or employee and third-party contract termination use cases, to name a few. Horacius offers good breadth with some depth with out-of-the-box connectors for on-premises systems, with less breadth regarding out-of-the-box connectors to SaaS systems. Horacius does provide REST and SOAP APIs to connect to third-party solutions for encapsulated identity requests, access functionality, as well as connecting to external AI, Analytics or fraud services for additional functionality. SDKs for major programming languages are not supported.

Their web user interface can include scorecard tiles for identities that are managed, active, as well as managed profiles or pending tasks. Graphical widgets can also show graphs over time for automatic access grants, revocation, or password resets as some examples. Navigation through their functional screen is laid out in a user-friendly way. Horacius does provides good audit and compliance reporting support that include major compliance frameworks such as GDPR, HIPPA, SOX, and Brazil Central Bank (BACEM).

E-Trust has gained good momentum over the last few years. E-Trust customers are primarily small to mid-market, although making inroads into some enterprise-level businesses. E-Trust is a good fit for organizations with average access governance requirements to satisfy the most common identity lifecycle administration use-cases with customer-focused in the North and South American regions.

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

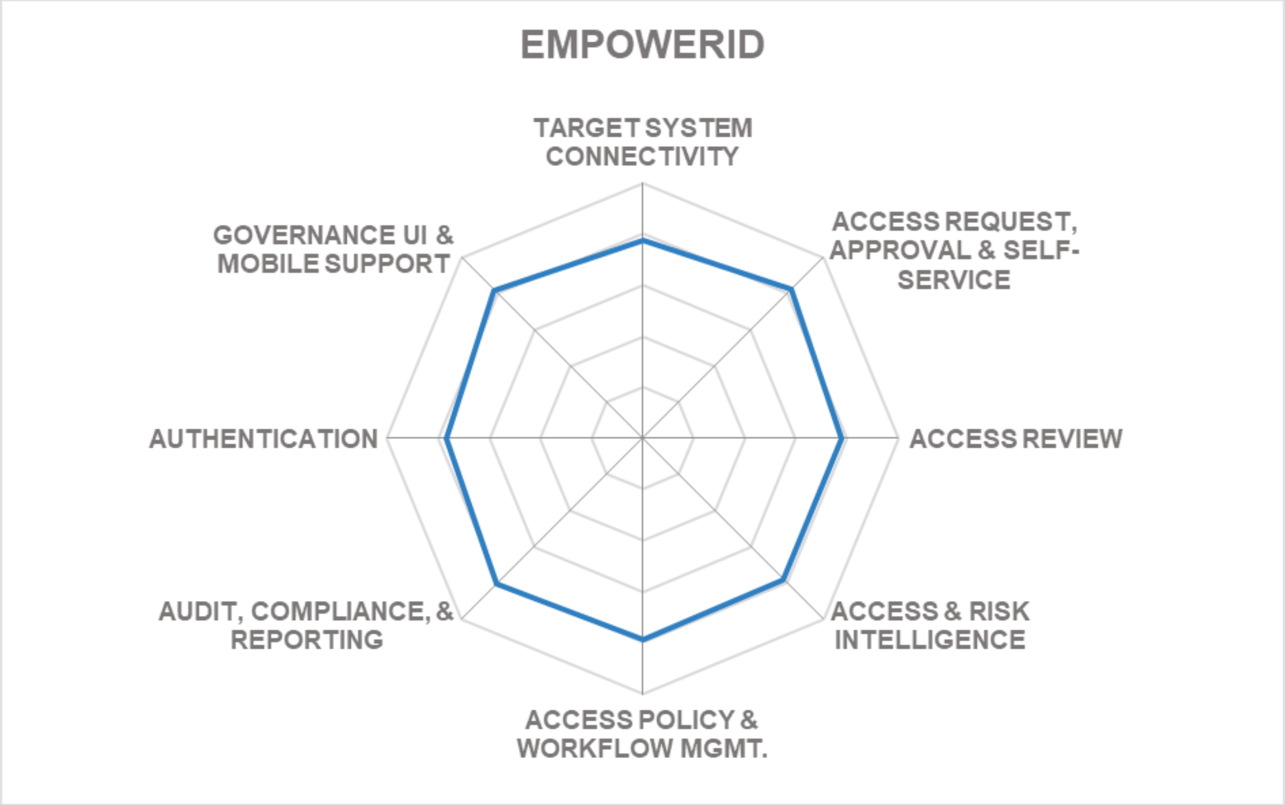
HORACIUS

Strengths

- Connectors to on-premises systems
- Centralized governance UI
- Good access governance reporting
- Provides REST & SOAP APIs to functionality and services

Challenges

- Smaller partner ecosystem mostly concentrated in South America
- Some limitations of OOB connectors to SaaS systems
- Some limitations of workflow capabilities
- Missing SDKs for major programming languages


EMPOWERID
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.6 EmpowerID

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

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

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

Access Governance capabilities are limited to common governance scenarios, including role management, access certification, auditing, and reporting. However, EmpowerID provides strong role governance features that support role design and SOD compliance. Advanced governance features such as access analytics and intelligence support risk-based analysis of identities, role mining, recertification recommendations, as well as various outlier detections. EmpowerID workflow customization offers great flexibility in policy and workflow management, as well as giving good out-of-the-box reporting options. User activity monitoring (UAM) capability through Privileged Session Management is limited.

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

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

empowerID

Strengths

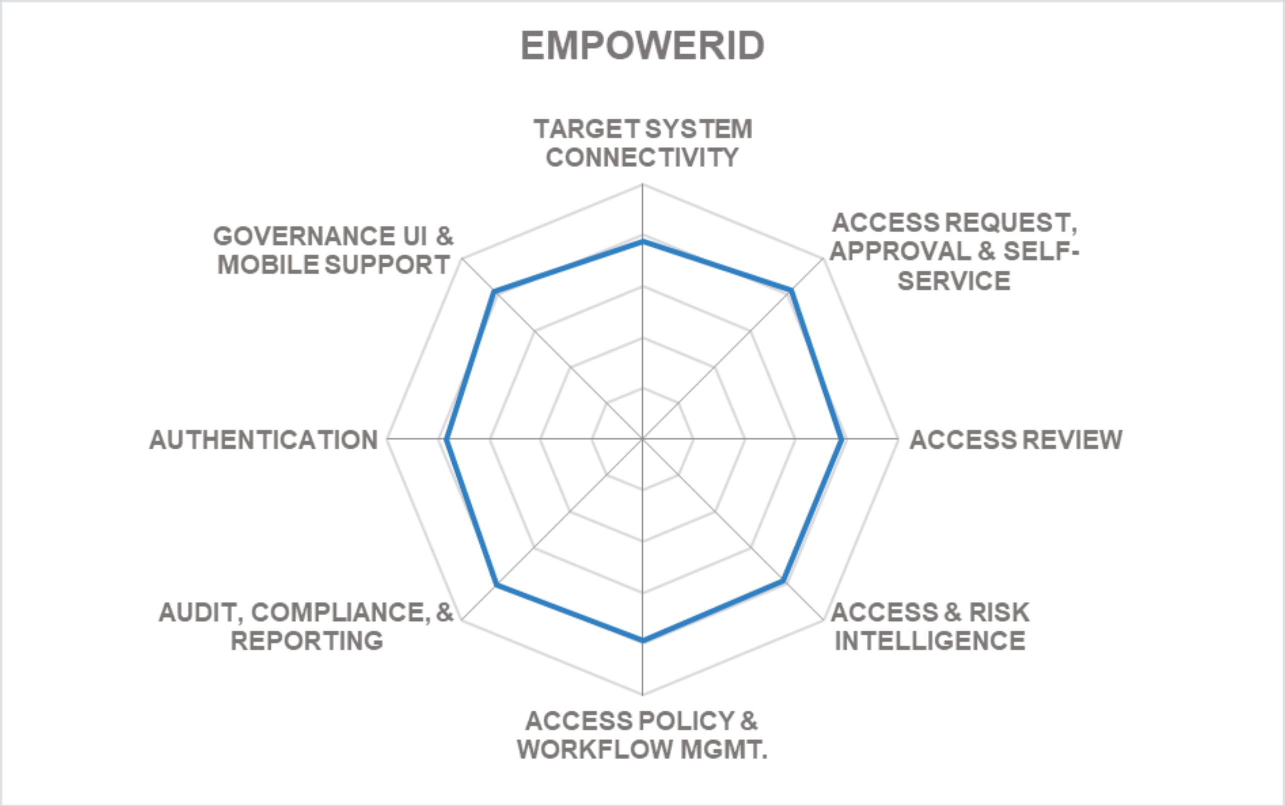
- Strong role management and access certification capabilities
- Easy and flexible policy and workflow management
- Strong Data Access Governance capabilities for windows environment
- Both depth & breadth of OOB connectors to systems
- Well thought out and modern UI

Challenges

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

Leader in

OVERALL LEADER PRODUCT LEADER INNOVATION LEADER MARKET LEADER


EMPOWERID
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.7 Evidian IGA

Based in France, Evidian is a dedicated business branch of the ATOS group within their Cybersecurity division since 2015, which is one of the leading IT service providers in Europe. Evidian has been in the IAM business for many years and has more than 900 customers with over 5 million users within the Finances Services, Manufacturing, Retail, Transport, Telecom, Media, Utilities, and Public Health sectors.

Their product, Evidian Identity Governance and Administration (IGA) offers basic Access Governance in addition to mature Identity Provisioning capabilities. Although there is good out-of-the-box support for on-premises systems, there is a somewhat limited set of out-of-the-box connectors to SaaS systems. Evidian Analytics and Intelligence (A&I) was introduced in 2017 to meet the increasing requirements of advanced Access Governance. Evidian IGA audit and compliance reporting is well supported that include major compliance frameworks such as GDPR, HIPPA, and SOX. Evidian A&I uses TIBCO Jaspersoft for its reporting capabilities giving Evidian the ability to provide good A&I dashboard capabilities. Evidian IGA ingests the components derived from the former Atos DirX portfolio. The solution goes beyond Identity Provisioning and Access Governance to offer an integrated approach to core IAM requirements. Evidian delivers an integrated IAM product which covers all major aspects of IGA. Besides the core provisioning capability, the product is tightly integrated with the SSO (Single Sign-On) and Access Management solutions offered by Evidian. While it supports risk-based access, continuous and event-based delta certification capabilities are currently not supported. Advanced role management, particularly role mining could be a challenge.

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

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

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

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

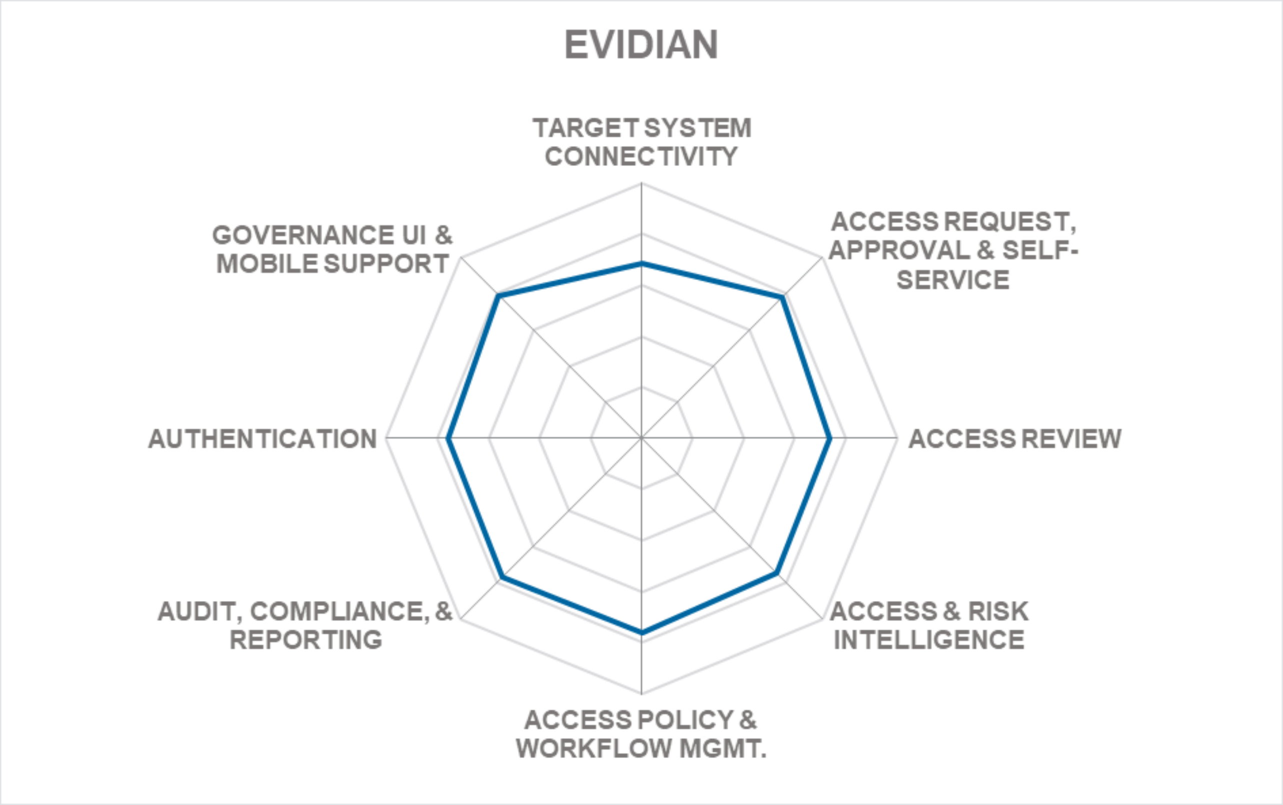
Evidian

Strengths

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

Challenges

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


EVIDIAN
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.8 Evolveum midPoint

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

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

Evolveum’s midPoint access governance features include a centralized role management that includes role discovery support, but role mining that can create or modify entitlement groups or roles is not supported. 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, for example. Evolveum deliberately removed its workflow engine recently in favor of a workflow-less approval process that is entirely driven by policies. For instance, for approval, policy rules are applied to roles, then the approval engine will compute the approval process. Some access governance intelligence such as access modeling is available, although more advanced anomaly or types of outlier detection is not.

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

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

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

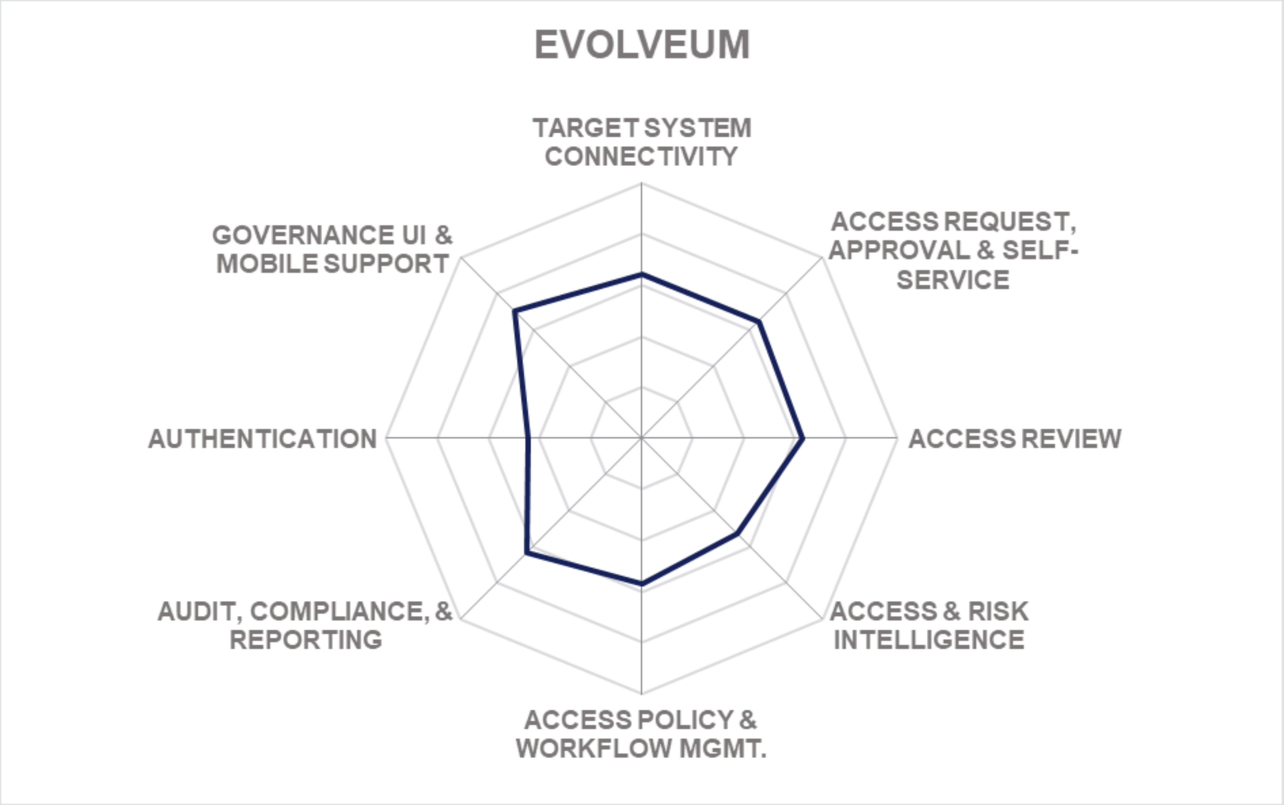
Evolveum

Strengths

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

Challenges

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


EVOLVEUM
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.9 Fischer International Identity Suite

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

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

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

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

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

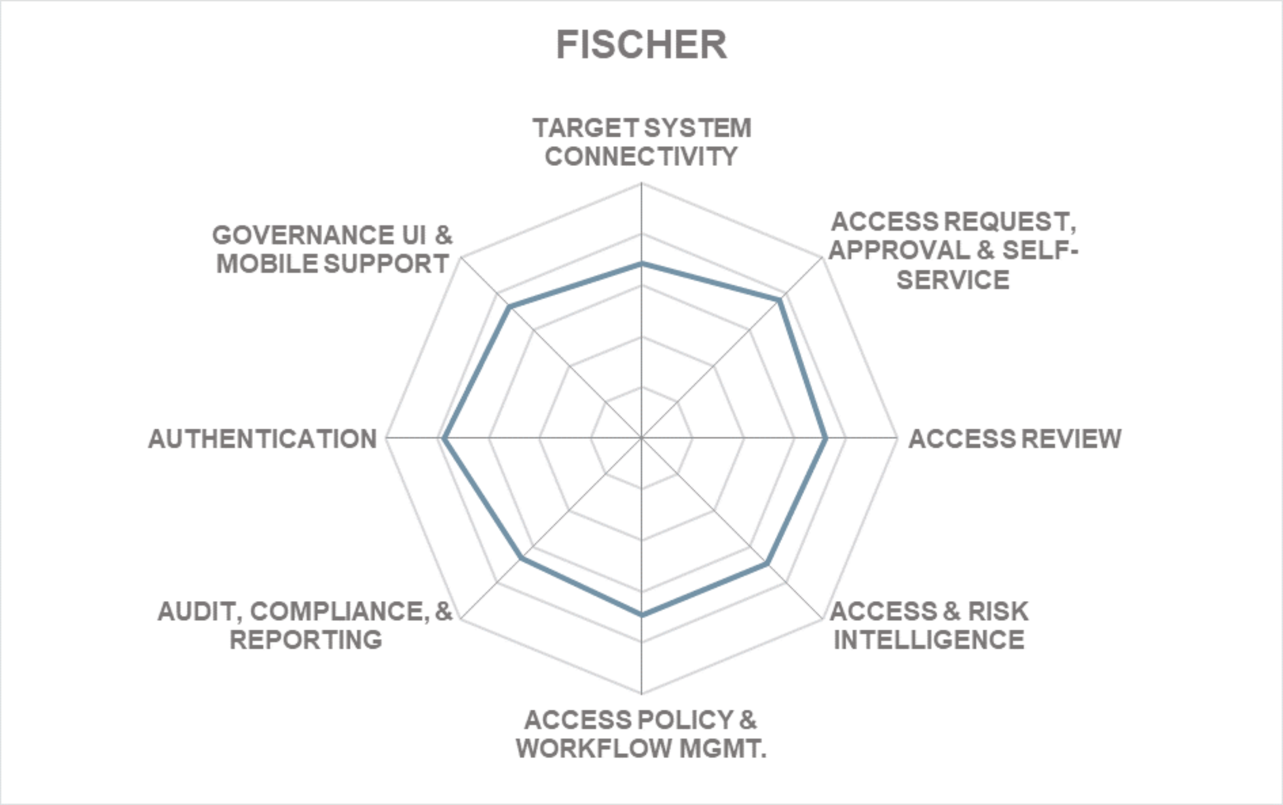
FISCHER IDENTITY

Strengths

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

Challenges

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


FISCHER
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.10 Hitachi ID Identity Manager

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

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

In general, the product provides a mature set of IGA features, delivering what customers typically need. It offers a wide range of provisioning connectors. Access Governance is moderately strong with flexible workflow and policy management capabilities, which can support complex governance use-cases. Analytic features include outlier detection, recommendation level indicators, as well as role mining. Access modeling and anomaly detection are not given. However, some intelligence capabilities can detect data quality issues, and corrections can trigger a recalculation of user entitlements and automatically generate access change requests. Hitachi ID Identity Manager supports real-time control of user behavior in accessing resources principally through its Persistent Discovery solution. Changes to accounts, groups, and attributes can be discovered and imported into Hitachi ID Suite in real-time either natively or via other third-party tools, such as STEALTHBits, which is a provider of data access governance solutions.

Strong support for reporting, as well as major compliance framework reporting, is available out-of-the-box. Another strength of Hitachi Identity Manager includes integrations with Microsoft SharePoint and Windows Explorer, allowing users to request access to resources from these environments directly. The product also supports group lifecycle management in which users can create new and manage existing groups through the system. At no additional cost, Hitachi ID Identity Manager includes additional governance features such as the Hitachi ID Access Certifier for periodic review and clean-up of security entitlements, and Hitachi ID Group Manager that performs self-service management of security group membership.

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

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

Hitachi ID

Strengths

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

Challenges

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

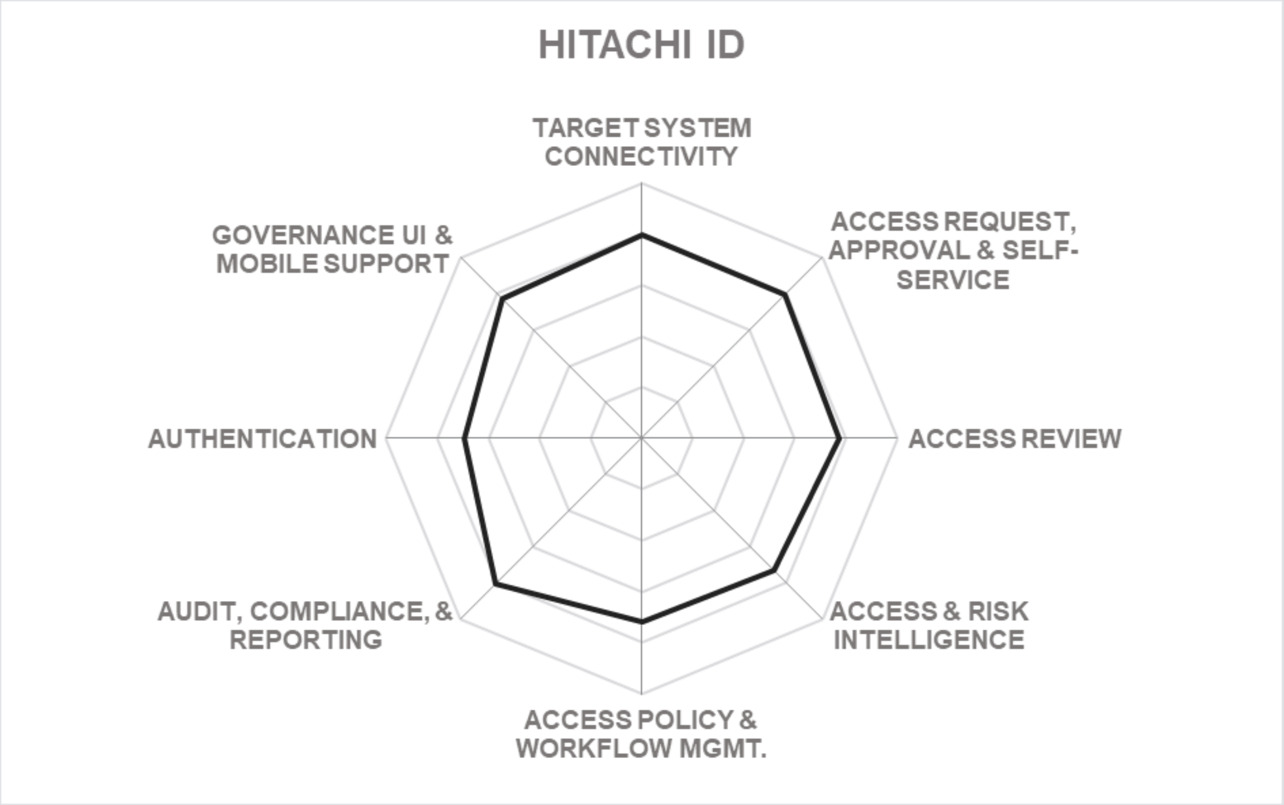
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


HITACHI ID
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.11 IBM Security Identity Governance & Intelligence

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

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

IBM Security Identity Governance & Intelligence builds on an established product supporting a broad range of different target systems with deep integration. IBM has dramatically improved the usability and user interface recently, providing a good and well-integrated product now. ISIGI also provides full Access Governance capabilities for access review and certification as well as automated access revocation fulfillment, least privilege policy configuration and validation. SoD analysis and mitigation policies can also be defined. Flexible workflows are given for role management, access request, identity data synchronization as well as account, entitlement provisioning/de-provisioning as well as access request workflow is supported. Limited supports are given for more advanced analytical functions/business intelligence features such as access intelligence, although good out-of-the-box access risk management and access risk analytics support is available. User activity monitoring (UAM) is supported, but requires the addition of the IBM Security QRadar UBA offering.

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

This makes ISIGI a good fit for customers looking for a comprehensive package of overall Access Governance and security.

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

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

IBM

Strengths

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

Challenges

- Product configuration and customization can be complex, although some assets and features are available to help simplify the process
- The user interface has been redesigned in recent releases but still has limited flexibility to customize
- User activity monitoring (UAM) requires additional IBM product integration
- Lack of focus on mid-market segment

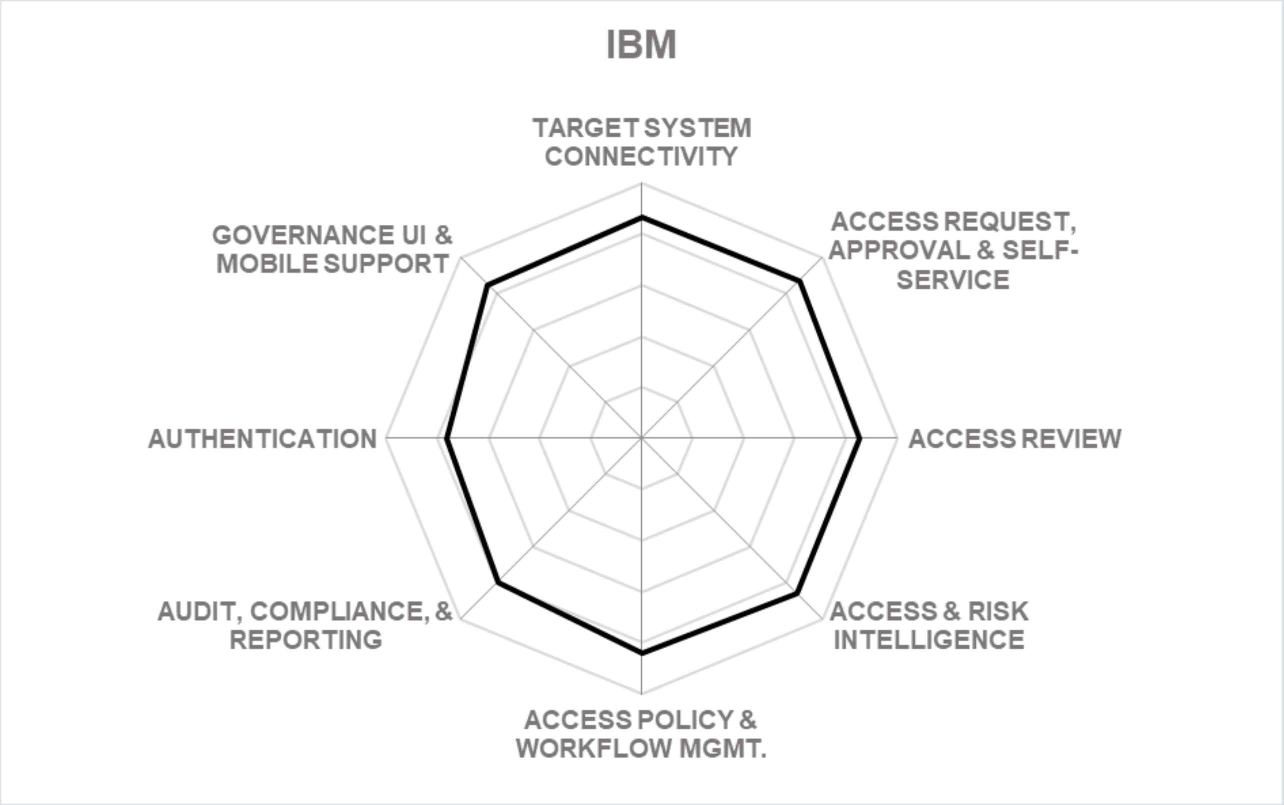
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


IBM
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.12 Identity Automation RapidIdentity

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

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

Identity Automation offers full Access Governance capabilities. The breath of on-premises provisioning connectors covers most major enterprise target applications out-of-the-box. Also, supported out-of-the-box are provisioning connectors for SaaS systems that include most of the better-known applications. Access policies can be defined for use cases such as account termination, role modification, access exception approval, rights delegation, SoD analysis & mitigation as examples. Support for role management is given which includes role discovery and mining capabilities. Support for access certification, including event-based micro certification are available. Triggers for recertification can be based on access risks, SoD violations, and schedules as examples.

Good reporting capabilities are available to support compliance audits. Reports for major compliance frameworks are available out-of-the-box include SOX, HIPAA, NIST SP 800-53, and PCS DSS. Access Governance related reports out-of-the-box include groups (members, owners, etc.), roles, users, and privileged access as examples. Reports related to access risks, accounts, or attestations are not given.

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

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

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

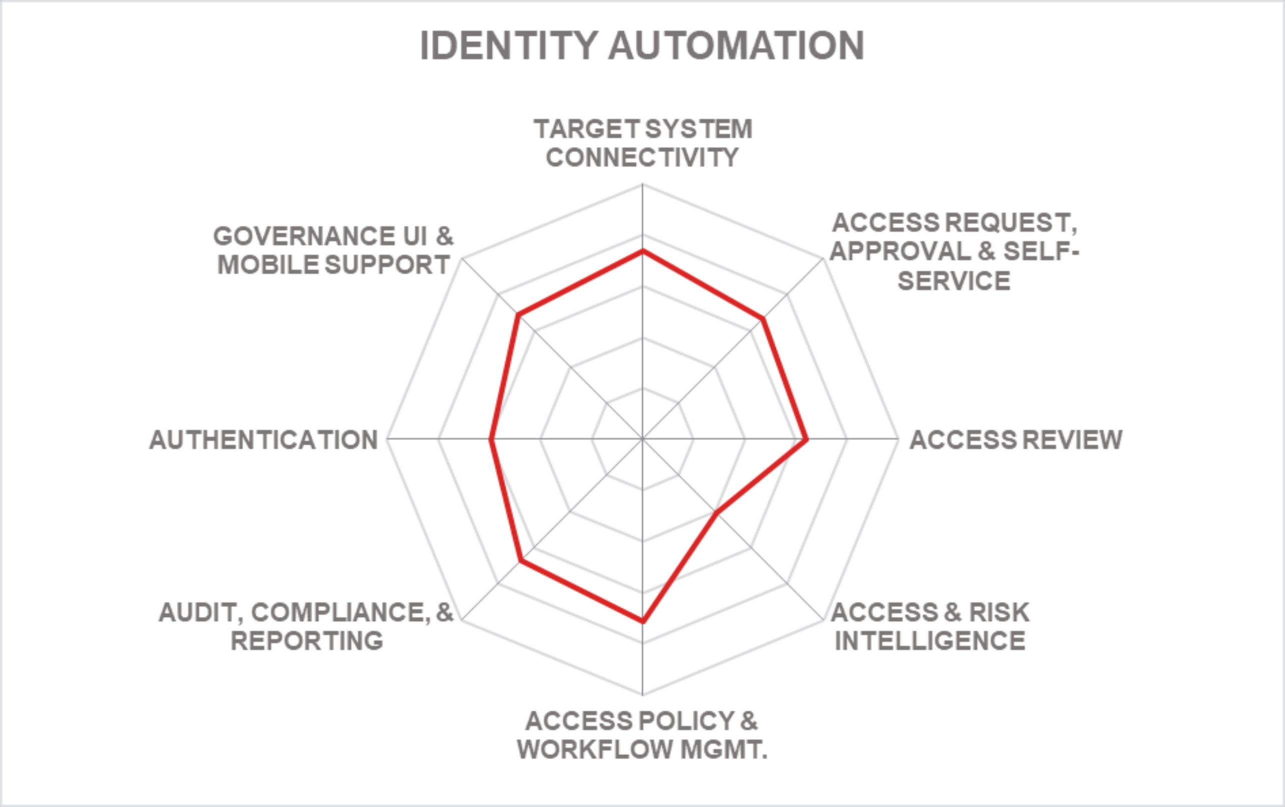
IDENTITY AUTOMATION

Strengths

- Target system connectivity support
- Certification campaign support
- Delegation support
- Good workflow features
- Reporting capabilities
- Focus on automation

Challenges

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


IDENTITY AUTOMATION
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.13 Ilantus Compact Identity

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

In 2017, Ilantus merged all of its product offerings into one single IDaaS platform. For cloud deployments, Ilantus provides an on-premise agent with connections to their cloud platform. Alternatively, they can deploy their cloud solution to customers on-premises data-centers and private clouds.

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

For Access Governance, Ilantus delivers standard Access Review support, including multi-level campaigns, but also additional Access Intelligence capabilities. It also offers Robotic process automation (RPA) capabilities integrated with SSO and user lifecycle management connectors. The workflow capabilities are flexible and support a basic registration workflow as well as access request and approval workflows, with many additional workflows on the roadmap, although Compact Identity falls short in the case of access exception approvals as well as rights and registration delegation. Also, only basic user access self-service capabilities are available, although all functions related to access requests are supported in a mobile app. Centralized role management is given although role discovery and role mining support is not. Access intelligence features rely on Microsoft Analytics & Power BI, which supports access modeling, anomaly detection, and outlier detection that includes entitlements, identities and roles.

Ilantus continues to add innovative features now and on their roadmap, such as identity analytics that supports anomaly and other types of detections, as well as robotic process automation (RPA) capabilities integrated for SSO and user lifecycle management activities.
Ilantus is currently serving mid-market companies in North America, Europe and the APC regions, as well as their partner ecosystem. Ilantus continues to move in a positive direction with the completion of future capabilities on its roadmap.

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

ilantus

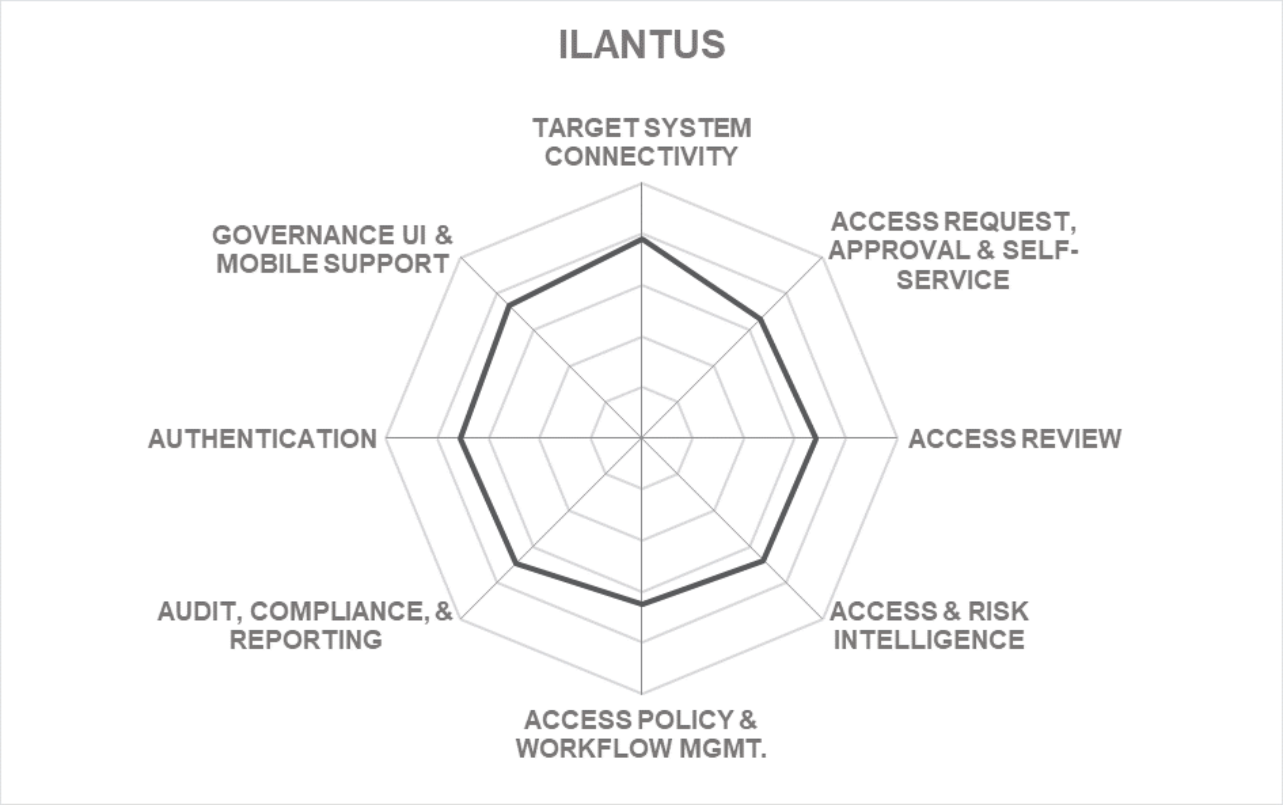
The Identity Management People

Strengths

- Depth and breadth of connectors
- Access & risk intelligence
- Flexibility for customization including policy and workflow customizations
- Reporting capabilities
- Innovative list of capabilities on roadmap

Challenges

- Customer presence is still primarily focused on the US and few Asian countries, still low in EMEA
- Missing out-of-the-box reporting for major compliance frameworks
- Somewhat limited user access self-service
- Missing role mining capabilities


ILANTUS
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.14 Micro Focus Identity Manager Suite

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

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

Micro Focus Identity Manager is a robust product for Identity Provisioning with mature and comprehensive capabilities for identity lifecycle management and fulfillment. Micro Focus Identity Governance is an enhanced governance product offering mature and in-depth capabilities with some functionality overlap to Identity Manager. Its flexible approach for workflow and policy management based on the designer tool is still widely unmatched in the industry, allowing for efficient and easy management of complex environments. Integrated role mining, adaptive access certification, and risk-based analytics are some of its distinct and improved governance features.

Identity Intelligence provides analytics and reporting capabilities for IGA data. Vertica is a behavioral analytics platform that was acquired through the HPE acquisition, in which IGA capabilities of Vertica are packaged into their Identity Intelligence offering. More recently, Micro Focus acquired Interset for their machine learning and AI capabilities, although currently not integrated with their governance solution. For data mining and analytics, Micro Focus gives identity correlation and user profiling, anomaly detection, risk scoring, and role mining as some examples.

Identity Tracking gives the capability to monitor user activity in real-time and can detect the abuse of user privileges through abnormal activity pattern analysis. The products combined offer a comprehensive IGA platform that offers good flexibility and scalability.
Overall, Identity Manager and Governance products from Micro Focus remain leading-edge products in the IGA market space with its broad, mature, and evolving Access Governance functionality. Acquisitions of analytics and AI platforms set the stage for identity and access governance intelligence now and in the future. Also, Micro Focus is building on an excellent partner ecosystem on a global scale.

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

MICRO FOCUS®

Strengths

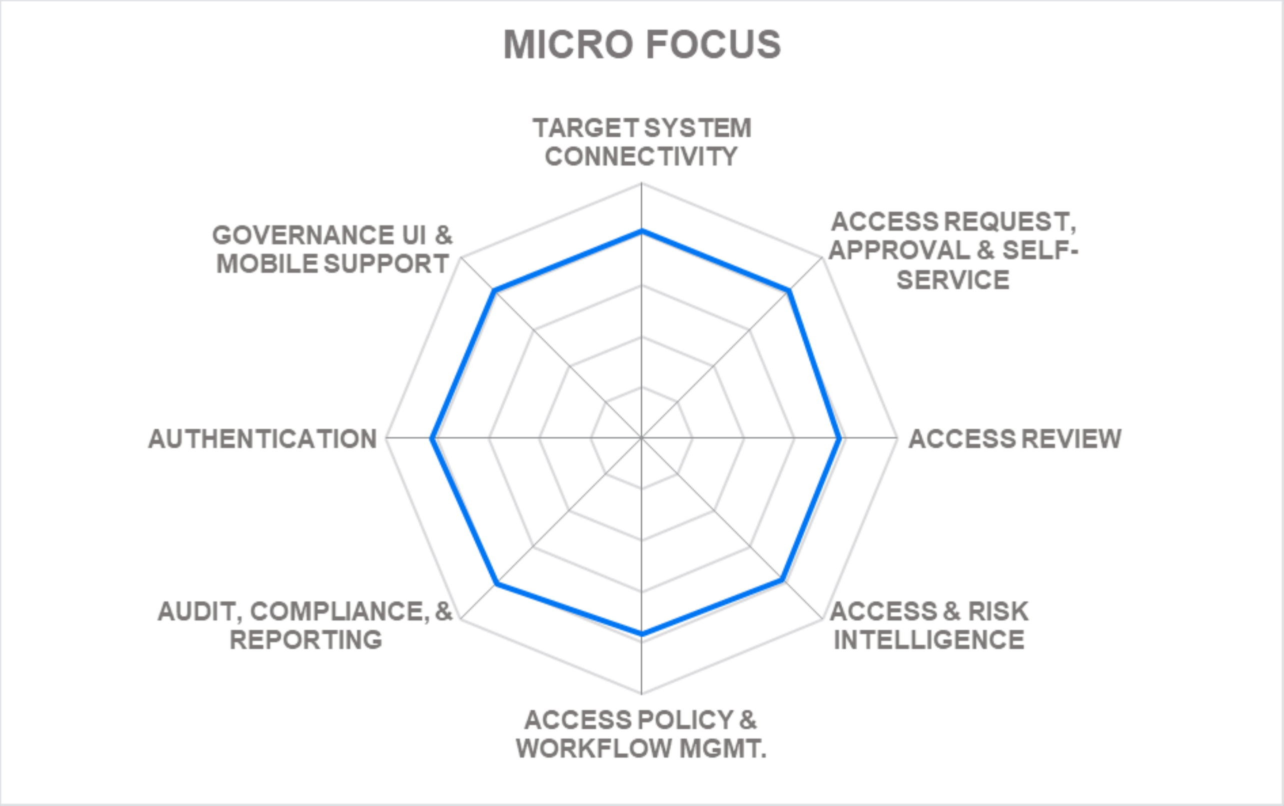
- Strong, mature functionality covering all major aspects of Access Governance
- Aggressively moving to a more modernized and flexible architecture
- Strong support for a variety of target systems
- Strong support for access & risk intelligence
- User activity monitoring (UAM) support
- Very large customer base and strong partner ecosystem

Challenges

- Rich functionality sometimes complex to understand and implement
- Powerful analytics platform, although requires a separate containerized component deployed before consuming data from the IGA system
- The merger with HPE created some uncertainties with certain security product functionality overlap, although the acquisition of Vertica through HPE showed some benefit
- Weaker marketing messaging and execution compared to competitors

Leader in

OVERALL LEADER PRODUCT LEADER INNOVATION LEADER MARKET LEADER


MICRO FOCUS
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.15 Nexis Controle

Nexis, based in Regensburg, Germany, offers Nexis Controle as its Access Governance offering. Controle, first released in 2014, builds on an innovative plug and play approach to access governance, which remains its core focus. Nexis Controle provides a stand-alone solution with a specific focus on risk & entitlement analyses and (re-) modeling governance capabilities that can close deficiency gaps of some existing IAM-solutions. Nexis Controle itself is not considered a full IAM suite but gives Access Governance with Identity Analytics, Role Modeling & Optimization, Compliance, SoD Management, and Data Cleanup capabilities positioned as an add-on to existing IAM products on the market and therefore doesn't come with its own provisioning engine, but instead delivers standard connectors to the existing IAM provisioning tools. A stand-alone software option is also available for Access Governance.

Controle supports on-premises, public, and private cloud environments. The solution can be delivered as SaaS (e.g., on Azure, AWS), virtual appliance, or software deployed to a server with Windows or Linux OS. A hardware appliance is also possible when required by customers. For cloud delivery, Nexis does support full multi-tenancy. Most of the solution's capabilities are available via SOAP or REST APIs. SDKs for Java and scripting via JavaScript are also available. Support for functionality access via CLI and a developer portal with documentation, tutorials, examples, etc. are not available.

Controle provides good access certification support that includes event-based micro certifications and recertifications based on triggers based on access risks, schedule, SoD violation, or other types of triggers such as the number of unauthorized access attempts. Also, Controle can detect changes to access entitlements in a role and trigger role certification. Nexis rule-based policy management comes with full lifecycle processes and is capable of role discovery or mining. Policies can be defined for account termination, role modifications, access exception approval, rights delegation, and SoD mitigation. Strong workflow support is given with 150 fully customizable (no coding required) workflows available out-of-the-box. Currently, SoD checks are detective, and not preventive, although SoD checking in the workflows is on Nexis near-term roadmap. Also, an additional dedicated SoD check for handling SAP Auth Profiles is available.

Nexis Controle gives access and risk intelligence that includes access modeling, current and future state comparisons, anomaly, entitlement, and role outlier detection. Also, many Access Governance reports are available out-of-the-box that include access risks, accounts, trend analysis, attestation

related, delegated access, group, privileged access, user and role-related, although reports for major compliance frameworks are not given.

Nexis customers cover Germany, Austria, and Switzerland markets supporting mid to enterprise organizations. For customers in these regions, Nexis Controle offers an Access Governance solution that complements rather than replace existing IAM implementations.

NEXIS Controle

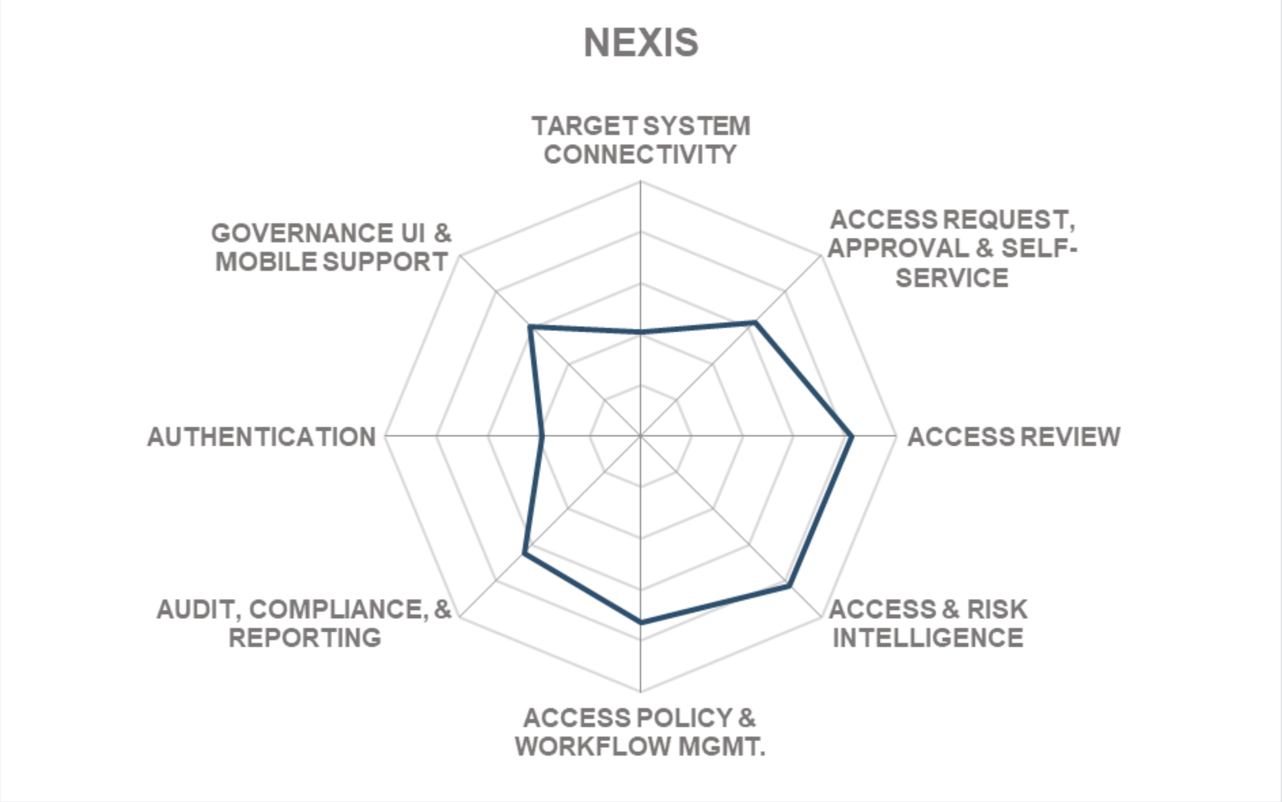
Security	● ● ● ● ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

Strengths

- Innovative risk-based approach to role governance
- Supports the majority of access governance use-cases
- Access certification support
- Integrated SOD Controls capabilities
- Workflow capabilities
- Access and risk intelligence

Challenges

- Lack of identity provisioning capabilities, although connectors to provisioning tools are available
- Limited user and admin authentication options
- Limited set of OOB target system connectors
- Small but growing partner ecosystem
- Limited presence outside of DACH region


NEXIS
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.16 Omada Identity

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

Omada Identity has undergone significant changes over the past years. Aside from adding its Identity Provisioning layer and removing the former dependency on Microsoft Identity Manager, Omada has also re-architected the solution, changing the data model to be more flexible and scalable. The solution can be delivered as SaaS or software deployed to customer owned infrastructure. When delivered as software, Omada Identity requires Microsoft Windows Server and Microsoft SQL Server. Managed services are available via MSP/CSP partners. With both Omada Identity and Omada Identity Cloud options, on-premises, cloud, and hybrid deployment models are supported. The majority of Omada functionality is available via its OData (REST) and/or SOAP APIs. Access to functionality via CLI is not supported. A .NET SDK is available for customizations.

Omada offers good Access Governance features such as workflow and policy management that can support AG use cases Access certification is supported as well as event-based micro certification and certification campaigns. Recertifications can be triggered based on access risk, or SoD violations as examples. It also offers strong role governance that includes role discovery and mining. Omada support of out-of-the-box connectors to on-premises and SaaS target systems is somewhat limited, although supported OOB connectors cover major Microsoft services, SAP ERP, and Oracle DB, as well as ServiceNow and Workday as examples. A flexible set of configurable template connectors are available for standard protocols, e.g. REST, SOAP, and SCIM. Good user self-service functionality is also available, although very limited authentication options are given. Good Access Governance related reporting that includes access risks, accounts, attestations, groups, roles, users, and privileged access. Out-of-the-box report for major compliance frameworks is not support.

Access & risk intelligence includes access modeling, anomaly, entitlement and role outlier detection capabilities. Omada's Control Policy feature includes automated compliance capabilities that can detect non-compliant situations that can automatically react (e.g. terminate risky access, send alerts, trigger recertifications, etc.). Role mining is based on the Microsoft analytics platform.

Omada serves customer in mid to enterprise size organizations that primarily reside in the EMEA region, although growing in North America and the APAC region. Omada Identity is an interesting IGA solution for enterprise customers that need to build a governance layer on top of their Microsoft Identity Manager implementations. With recent enhancements to its product capabilities, such as delivering an enterprise AG (IGA) solution as a cloud service, Omada is a strong
contender to traditional players in the IGA and Access Governance market segments.

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

Omada

Strengths

- Mature solution with strong workflow and role management capability
- Efficient approach for onboarding new applications
- Good SAP connectivity features
- Good audit & compliance reporting support
- Effective Microsoft Identity Manager governance

Challenges

- Limited support of out-of-the-box connectors to on-premises and SaaS systems, although configurable template connectors are available for standard protocols
- Limited authentication options for user self-service and administrative access
- On-premises deployments has required dependencies on Microsoft platforms
- Customer presence is still primarily focused on the EMEA, although growing in North America and the APAC regions

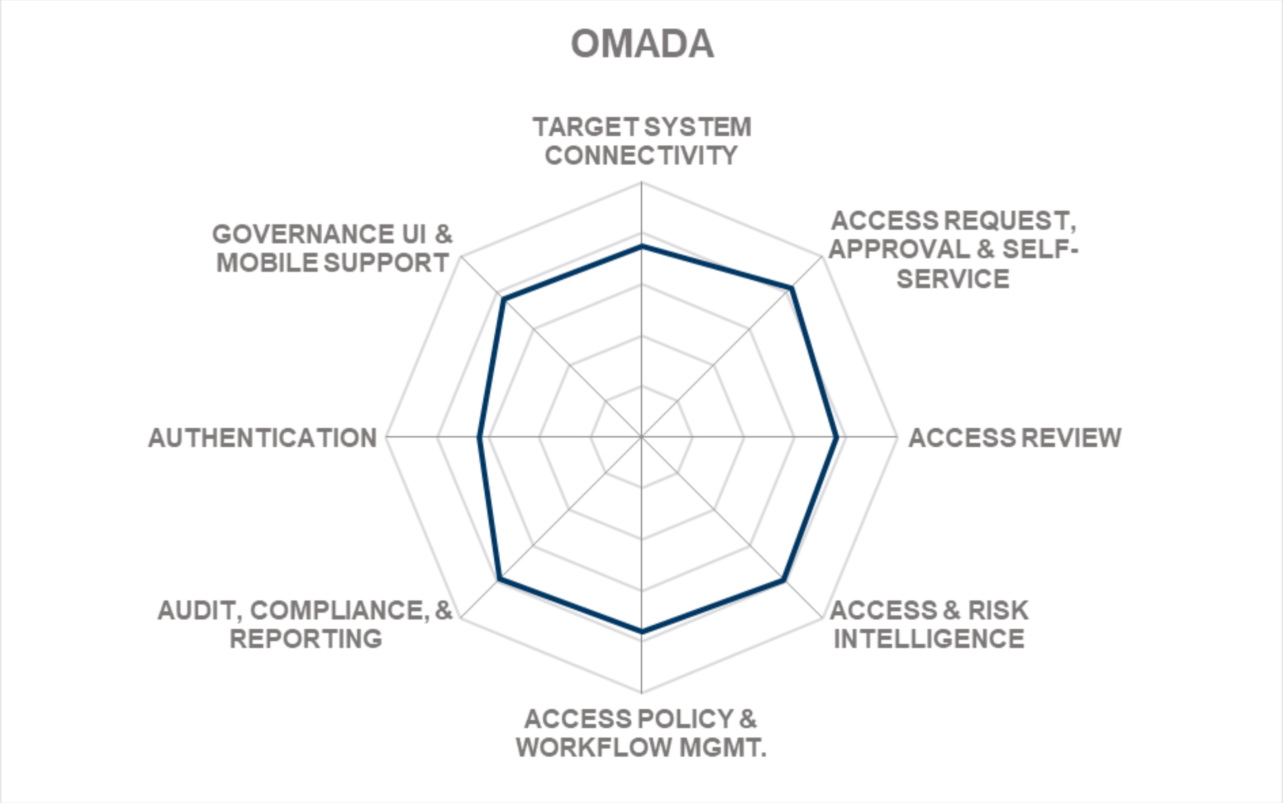
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


OMADA
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.17 One Identity Manager

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

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

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

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

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

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

ONE IDENTITY™

Strengths

- Strong connector support to target systems
- Innovative, user-friendly interfaces
- User self-service support
- Reporting capabilities
- Strong sales and marketing execution
- Integrates well with its access management and privilege management capabilities
- Advanced role management with strong SOD support

Challenges

- Process-driven approach requires some training, but is highly efficient
- Missing some more advanced authentication options for administration access
- A limited but growing professional services network

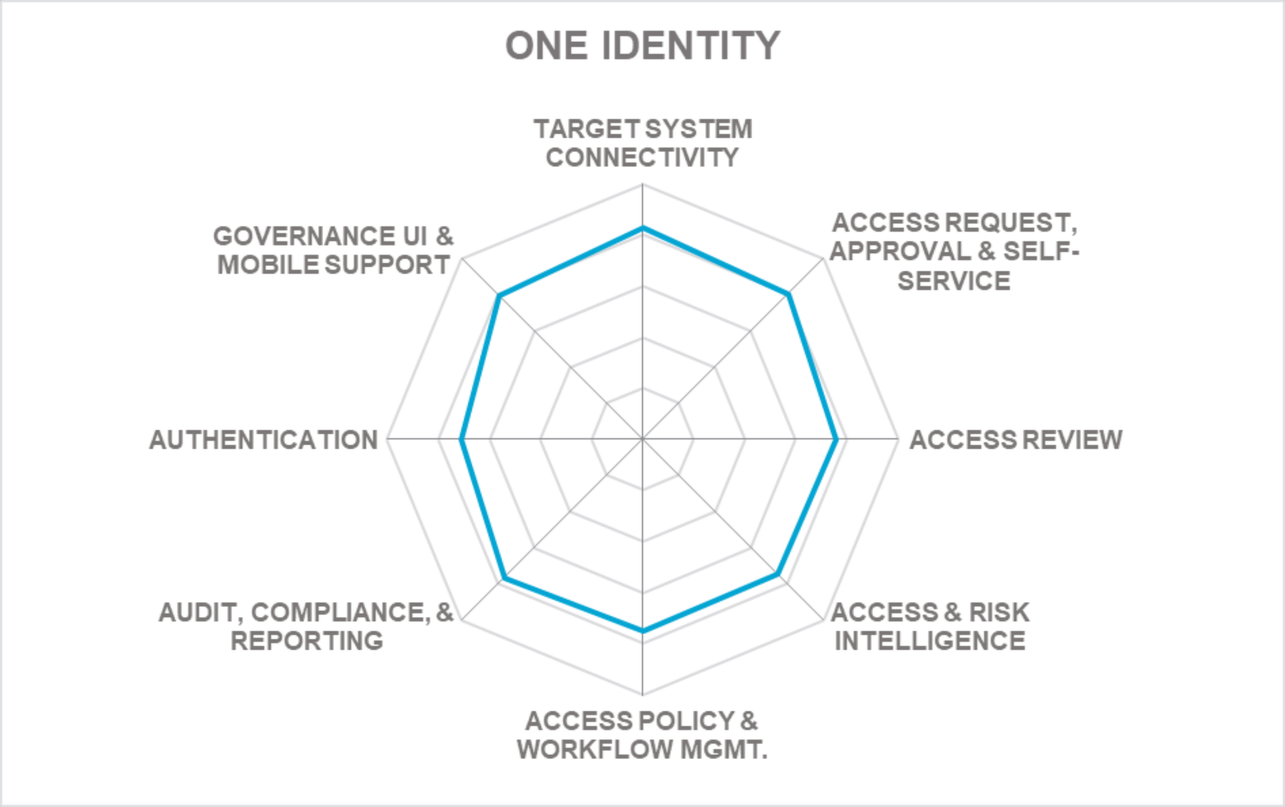
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


ONE IDENTITY
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.18 Oracle Identity Governance

Oracle Identity Governance (OIG) Suite is the on-premise offering within Oracle’s IAM portfolio. Oracle Identity Governance is Oracle's primary IGA offering that includes Oracle Identity Manager and Oracle Identity Analytics. Several IGA and particularly Access Governance capabilities have been significantly improved in the 12c release, especially the integration of modules along with the ease of their deployment. Oracle remains a preferred vendor for organizations that have a substantial investment in Oracle Fusion Middleware and require high flexibility for customizations to accommodate complex business processes.

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

Access Governance features include good user self-service access request support and profile management, access certification, automated provisioning and reconciliation, policy management, as well as for access intelligence that includes access modeling, anomaly, entitlement, and role outlier detection. Oracle has a particular strength in role management, which includes role discovery and mining capabilities. Good authentication options are available for both user and administrative access, although some options will require further integrations with Oracle products such as Oracle Access Manager. Out-of-the-box reports for major compliance frameworks are available for GDPR, HIPPA, and SOX as well as other Access Governance related reports that include access risks, accounts, attestations, groups, roles, users, and privileged access. Customizations can be done without extensive coding in most situations and are clearly segregated from Oracle code. Features like shopping cart approaches have been implemented to improve the UX.

Oracle Identity Governance Suite cuts across its competition through its enhanced UIs, recent pricing adjustments, enterprise-level design, support for modern architectural concepts, and an extensive partner network.

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

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

ORACLE®

Strengths

- Strong connector support to target systems
- Good reporting capabilities
- Role management
- Access & risk intelligence
- Significant improvements for deployment and customization
- Very broad support for different and modern environments with an enterprise-level architecture
- Global customer base with strong channel partner network

Challenges

- Can be complex to upgrade in some environments
- Dependence on an Oracle database
- Depending on use cases, there exist some dependencies between various components of the Oracle IAM portfolio

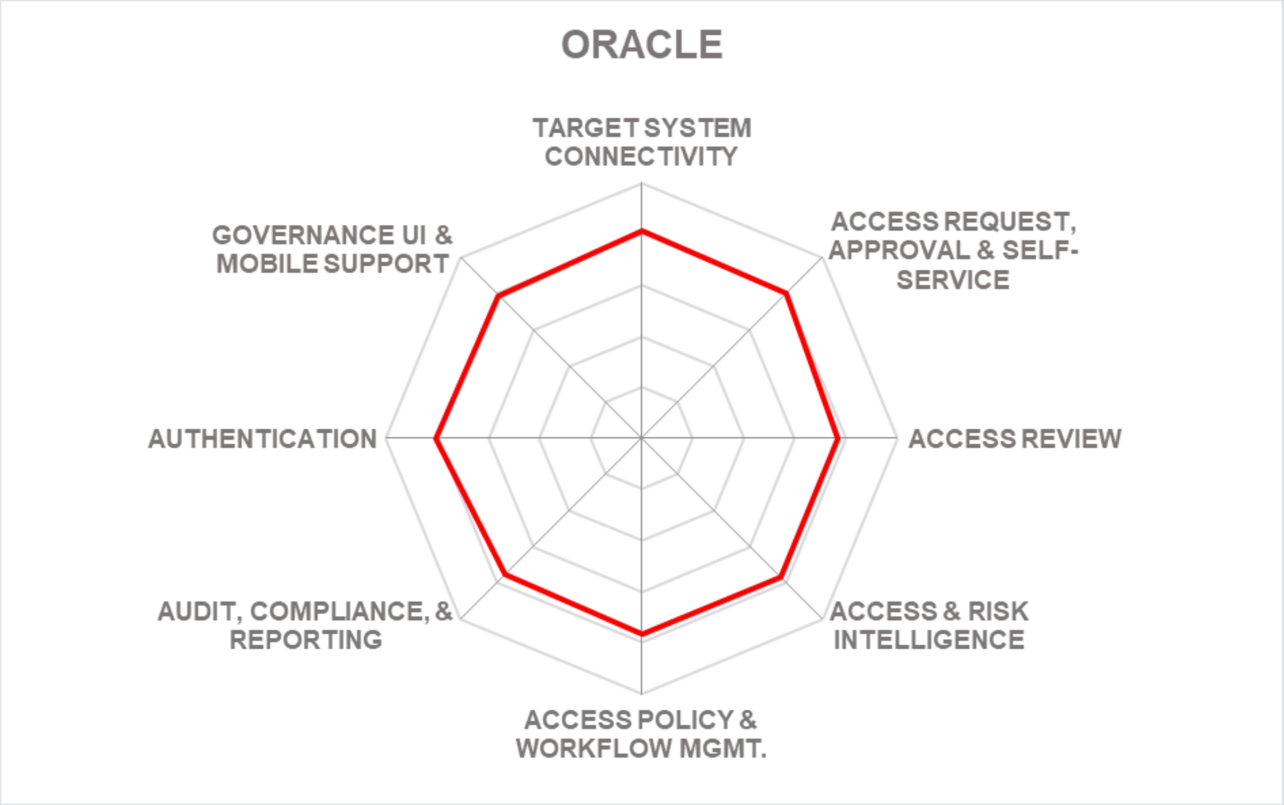
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


ORACLE
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.19 RSA SecurID Suite

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

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

For Access Governance, RSA IGL offers strong policy and role management capabilities due to its native support for granular entitlements with an elaborate role meta-data. Access requests and certification management are also given. Custom extensions to metadata, however, can be complex although extensions to object schema, metadata and attributes can be performed through the user interface. Tight integrations with RSA Archer Suite and RSA NetWitness Platform enable risk-based monitoring and event detection and response in real-time. RSA IGL provides identity and access analytics with insights into access patterns and peers analytics as examples, which allows for intelligent prioritization and guidance to those in the governance role. Although good access and risk intelligence capabilities are given, more advanced features such as user activity monitoring (UAM) that can detect abuse of user privileges through abnormal activity pattern analysis is limited.

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

With a substantial customer base around the globe, RSA's dominance of GRC and authentication markets has helped RSA to cross and upsell RSA IGL for IGA. RSA IGL makes an excellent choice for organizations that have existing deployments of RSA security products and have primary IGA requirements for identity task automation, strong Access Governance, and identity & access intelligence while avoiding extensive customizations.

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

RSA®

Strengths

- Strong risk-based Access Governance
- User-friendly interfaces
- User self-service support
- Access & risk intelligence capabilities
- Strong partner ecosystem
- Flexible deployment options including cloud-based and hosted offerings
- Useful user community forum (RSA Link)

Challenges

- Some limitations on SDK programming language options and access to product functionality via the SDK
- Advanced risk-based monitoring, detection, and response may require integration with other products in the RSA portfolio
- Limited user activity monitoring (UAM) support

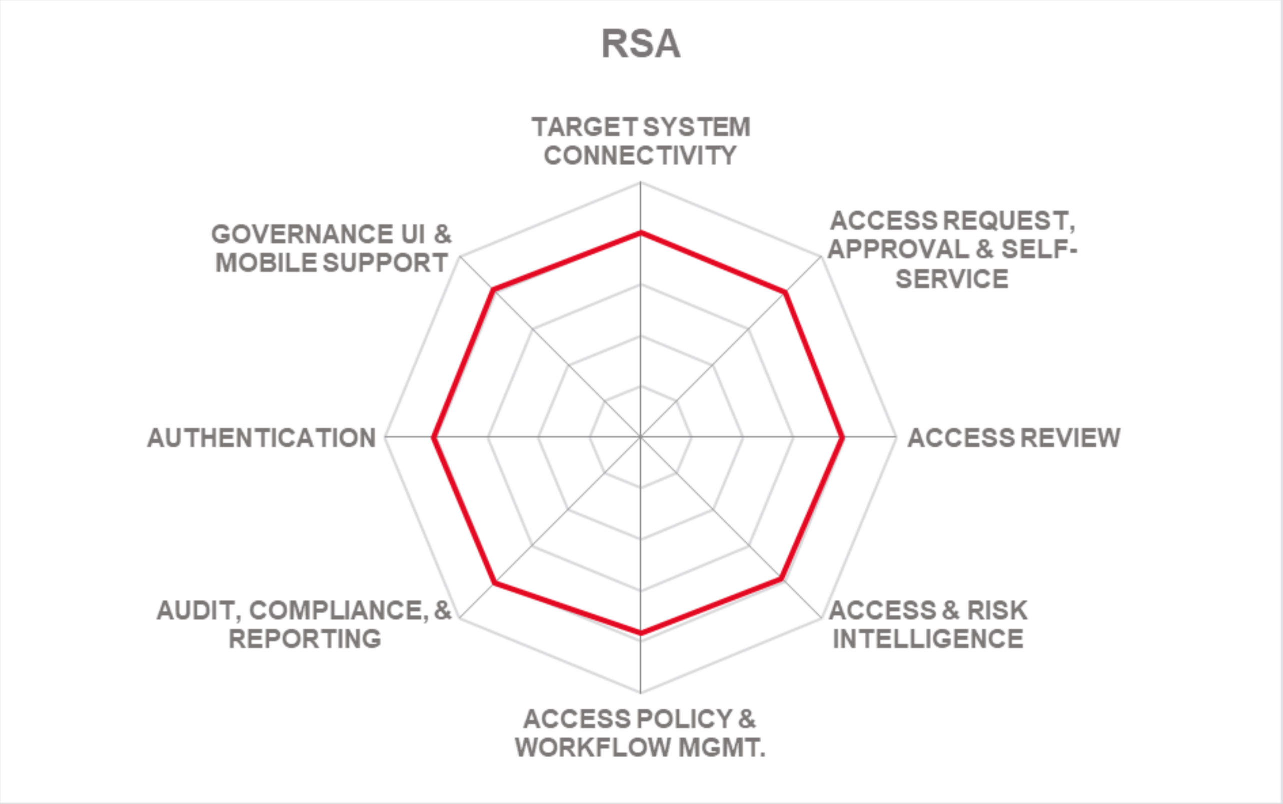
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


RSA
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.20 SailPoint Predictive Identity Platform

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

The base on-premises deployment of IdentityIQ is a Java application server model that can also be delivered in the cloud as container-based, or managed service. For cloud delivery, the product does not support full multi-tenancy. All of the product's functionality is exposed via SOAP or REST APIs, as well as the majority of the functionality is accessible via CLI. SDKs expose nearly all functionality and can be extended via the Java programming interface as well as JavaScript, Angular, and jQuery options. The solution supports both SPML and SCIM for identity provisioning/de-provisioning. Support for different identity types such as Bot/RPAs is also given.

Beyond the core governance capabilities such as access certification, SoD, provisioning, and self-service access request and password management, SailPoint also brings strong support to Access Governance audit and compliance reporting which includes access modeling, anomaly, entitlement and role outlier detection as well as stale data indication, role change and membership suggestions. Leveraging SailPoint's SaaS big data repository improves reporting via its business intelligence and Access History interfaces that can give a complete timeline of user access. Also, basic to advanced authentication options are available for both user self-service and administration access. SailPoint also supports user activity monitoring natively via File Access Manager as well as activity collection via configurable activity aggregations. Full reporting support is available, as well as out-of-the-box reports for major compliance frameworks.

Due to its origin in the Access Governance market, the user interfaces are geared towards business users. The approach, in general, is very much business-driven and less technology-focused than what some of the “classical” vendors in that market provide. The user interfaces are well laid out and user-friendly with some superior dashboard graphics. Regarding out-of-the-box connectors to on-premises and SaaS systems, they have not only extended the number of connectors, but also the depth of various connectors such as the one for SAP systems to meet governance requirements of complex scenarios. Besides supporting connectivity to target systems via identity provisioning, the product also directly supports integration with ITSM (IT Service Management) tools.

SailPoint has been a leading vendor in the IGA market, providing strong Access Governance capabilities. In addition, SailPoint has built excellent support for Identity Provisioning and role lifecycle management as part of the IGA offering with an increased focus on identity and access intelligence. SailPoint’s early recognition of Access Governance requirements in heavily regulated industries such as banking combined with strong marketing messaging and execution has led it to be one of the most evaluated vendors for IGA and Access Governance.

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

SailPoint

Strengths

- Strong Access Governance capabilities
- Strong support for access & risk intelligence
- Well thought out and user-friendly interfaces
- Good user self-service
- Audit & compliance reporting support
- Good authentication options
- User activity monitoring (UAM) support
- A large and effective channel partner network

Challenges

- Lack of SOD controls for transaction monitoring and emergency access management
- Lack of focus on small to mid-market segments
- Lack of multi-tenancy support for IdentityIQ concerns IAM professional service providers offering managed IGA services

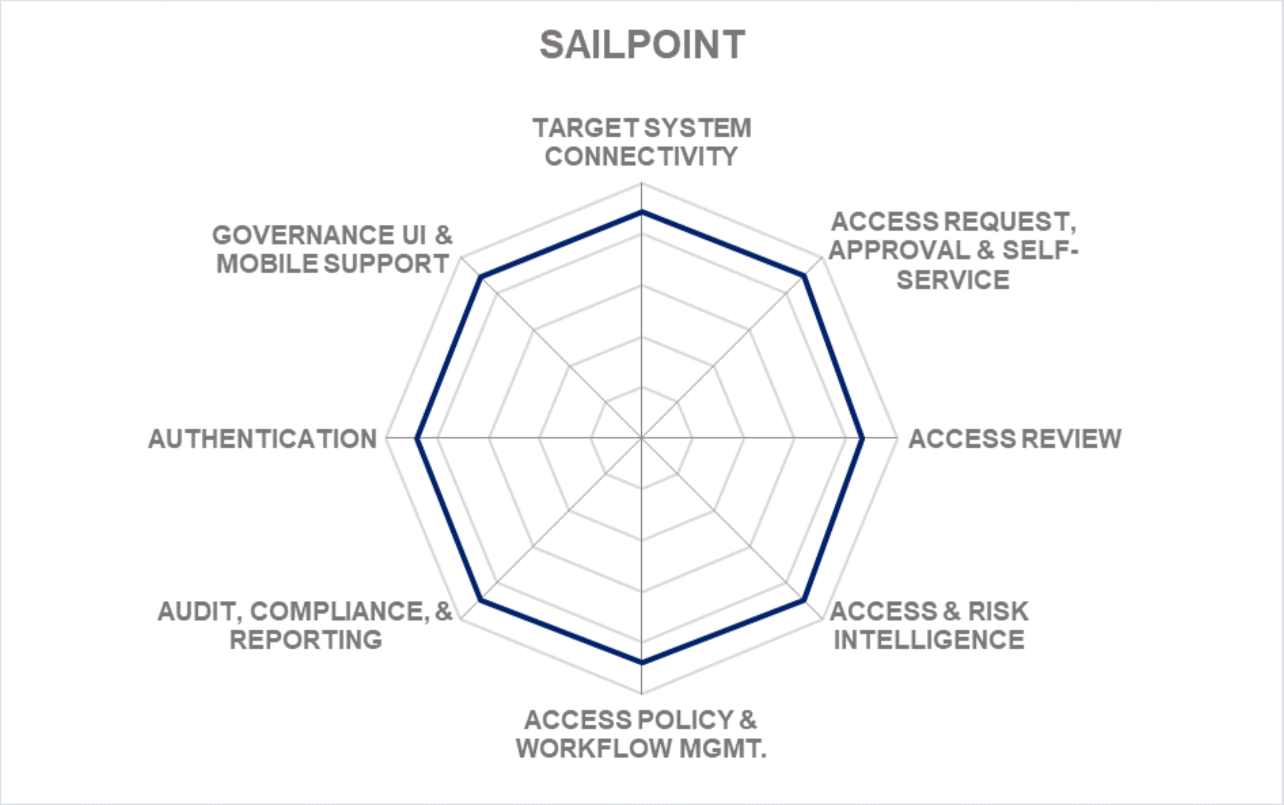
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


SAILPOINT
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.21 SAP Access Control & Identity Access Governance

SAP has established a considerable IAM portfolio over the past few years, and its recent acquisition of Gigya shows its continued commitment to grow and compete in the space. SAP offers the SAP Access Control and SAP Identity Access Governance products as an IGA solution, which is well-integrated with other SAP solutions such as SAP Business Suite to provide excellent Access Governance capabilities for SAP and few other ERP applications.

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

SAP has made significant progress with its offerings over the past few years, including product re-architecture, to expose a comprehensive set of APIs for simplified customization and integration. The product comes with standard Access Governance capabilities, including flexible workflows, support for automated assignment of entitlements based on roles, approval processes, and self-service functionalities. Support for user self-service requests via a mobile device is also given. Good access governance visibility is made available through its administrative UI. Role management also includes role discovery and mining capabilities. Using its integrated policy engine, policies can be defined to address account termination, role modification, access exception approval, rights delegation, or SoD analysis and mitigation use cases as examples. It also delivers good reporting and auditing capabilities which includes access risks, accounts, analytics trend analysis, attestations, groups, roles, users, and privileged access, although less support of out-of-the-box reports for major compliance frameworks. More advanced features such as access & risk intelligence for entitlements, identities and roles are supported, which includes access modeling, anomaly, and outlier detection.

A primary challenge has been the relatively small set of connectors when compared to other offerings in the market. SAP gives good support for out-of-the-box provisioning connectors for on-premises systems, with comprehensive support for SAP cloud business applications including Ariba, SuccessFactors, and S4 Hana. While SAP Access Control has excellent support for role management and Access Governance across SAP and SAP-like applications with complex role structures, it is often criticized for associated maintenance overheadsuch as deployment complexity. SAP Access Control is used to help define business functions, rules, and policies within business processes, which is a differentiator from other solutions that simply administer roles and assignments.

SAP maintains a significant customer base in EMEA followed by North America, with less presence in other regions. We rate SAP Identity Management as a strong contender in the IGA market and a preferred vendor for organizations with significant investments in SAP software.

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

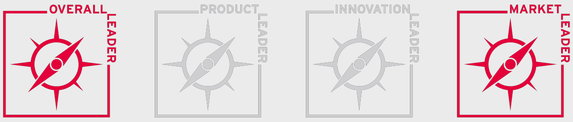
Strengths

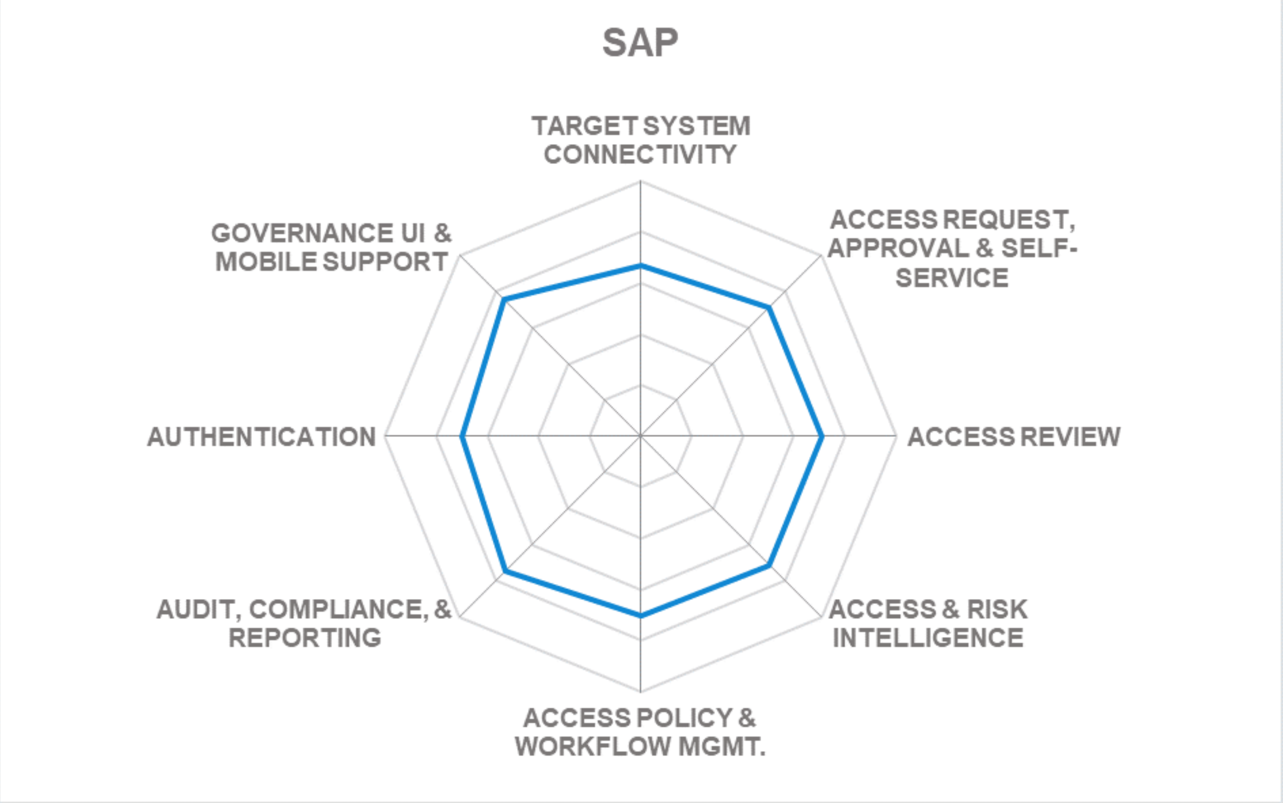
- Excellent integration into SAP environments, including SAP Access Control
- Good role management capabilities
- Audit & compliance reporting support
- Access & risk intelligence capabilities
- Access governance visibility
- Self-service capability with mobile self-service support
- Support for hybrid cloud and on-premise environments

Challenges

- Strong connector support for on-premises systems, but some gaps particularly for non-SAP business applications and SaaS applications
- Complex product deployment and upgrades, although efforts are being made to address this by providing more options to customers
- Primary IAG customer base is focused in EMEA, with less of a foot print in the North America, followed by a presence in other regions of the world.

Leader in




SAP
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.22 Saviynt Security Manager

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

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

Saviynt offers a strong lineup of IGA, application GRC, a cloud security analyzer, and cloud PAM. More recently, Saviynt added ID Risk Exchange and the Saviynt Exchange products to their portfolio, which is a collaborative platform with their customers to exchange insights.

Strong Access Governance support is given throughout a number of capabilities. Good user self-service support is given, although with limited authentication options available. Workflow management with a drag-and-drop feature is also 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. Intelligent access request capabilities are available to allow more ways to request access, such as through Slack or MS Teams, for example. Saviynt has also added a built-in connector RPA Bot that can be deployed on-premises for a hybrid deployment. It can be used to onboard and convert disconnected applications to connected applications for automated reconciliation, provisioning, and account management. More advance capabilities such as User Activity Monitoring (UAM) is accomplished through JRM (Job Rule Management) and Entitlement Usage and Controls. In addition, privileged activity monitoring and approval is also supported.

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

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

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

SAVIYNT

Strengths

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

Challenges

- Limited self-service and administration authentication options
- Still limited but growing brand awareness in regions outside North America

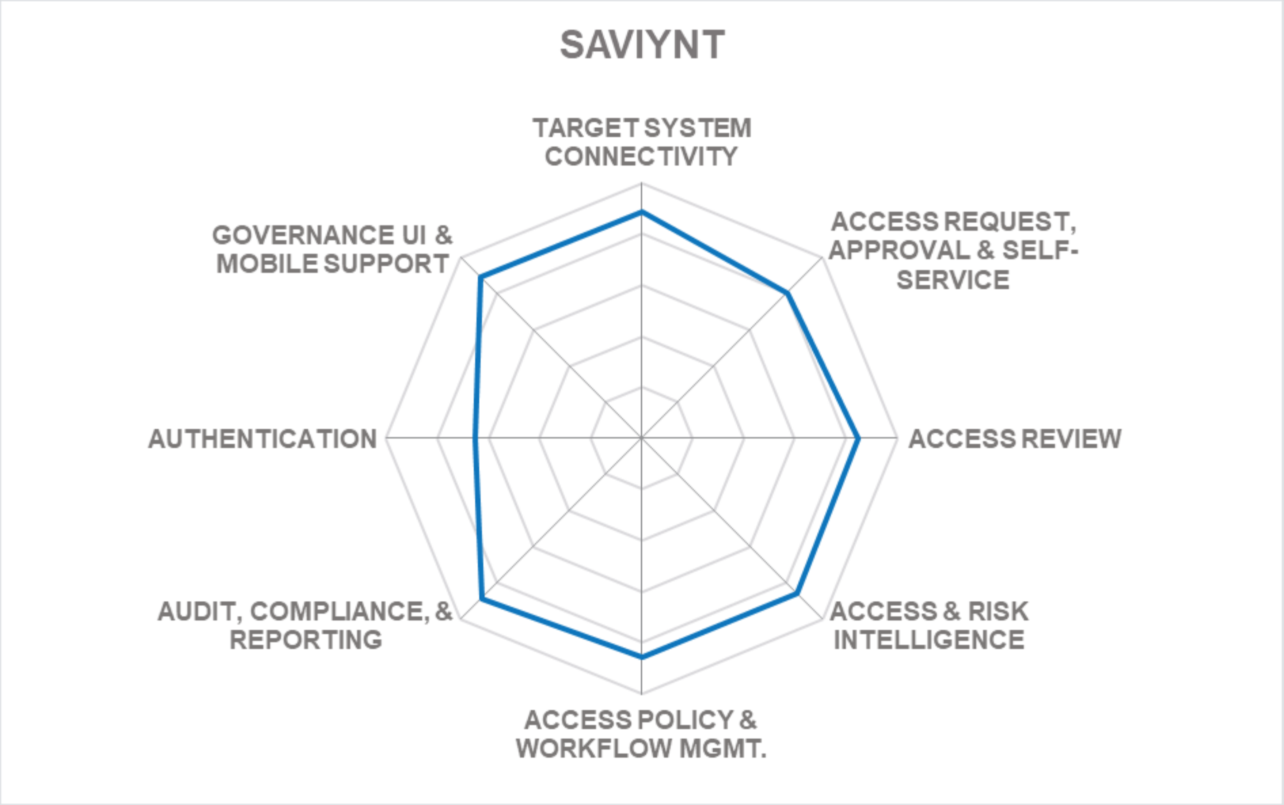
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


SAVIYNT
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.23 Simeio Identity Orchestrator

Founded in 2007, Simeio Solutions witnessed significant growth when shifting from its IAM system integration business into a full-fledged IDaaS service provider over the past years. Previously offering dedicated hosted services underpinned by other IAM vendor's products, Simeio enters the mainstream IDaaS market with Simeio IDaaS. Simeio Identity Orchestrator is its primary IGA service, although the Access Governance component of that service are 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 3rd party functionality such as Splunk integration and certified integrations with commercial solutions like BeyondTrust and CyberArk as examples. Simeio Identity Orchestrator (IO) gives clients the ability to access their entire IAM infrastructure within a single platform. Although Simeio has a focus on providing a SaaS, it also offers hardware and virtual appliance, and software deployed to servers and container-based options for on-premises delivery.

Simeio IO Access Governance features include a self-service access request & approval workflow with a shopping cart-based approach to select and request access as well as roles. Basic and somewhat limited audit & compliance reporting support is available, although out-of-the-box SOX and attestation related reports are given. Also, certification, password management, delegated administration, and privileged check-out is included. Simeio provides most out-of-the-box connectors to major on-premises and SaaS applications. Both basic and some more advanced authentication options are given to user self-service and administration access. Support for policies that give flexible entitlement models using attributes is primarily focused on roles and organizations. Some access and risk intelligence are shown through capabilities such as role discovery and mining, as well as access modeling. SoD risk analysis is conducted across all roles. Access risk is shown through high, medium, low indicators.

Interfaces to Simeio IO includes a web UI, mobile application, and REST APIs options. All the functionality available via the UI is available using the REST APIs, although CLI an SDK support to that functionality is not given. SOAP service APIs are not supported. Its mobile app interface provides the ability to the user to conduct activities such as access request approvals and access certifications.

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

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

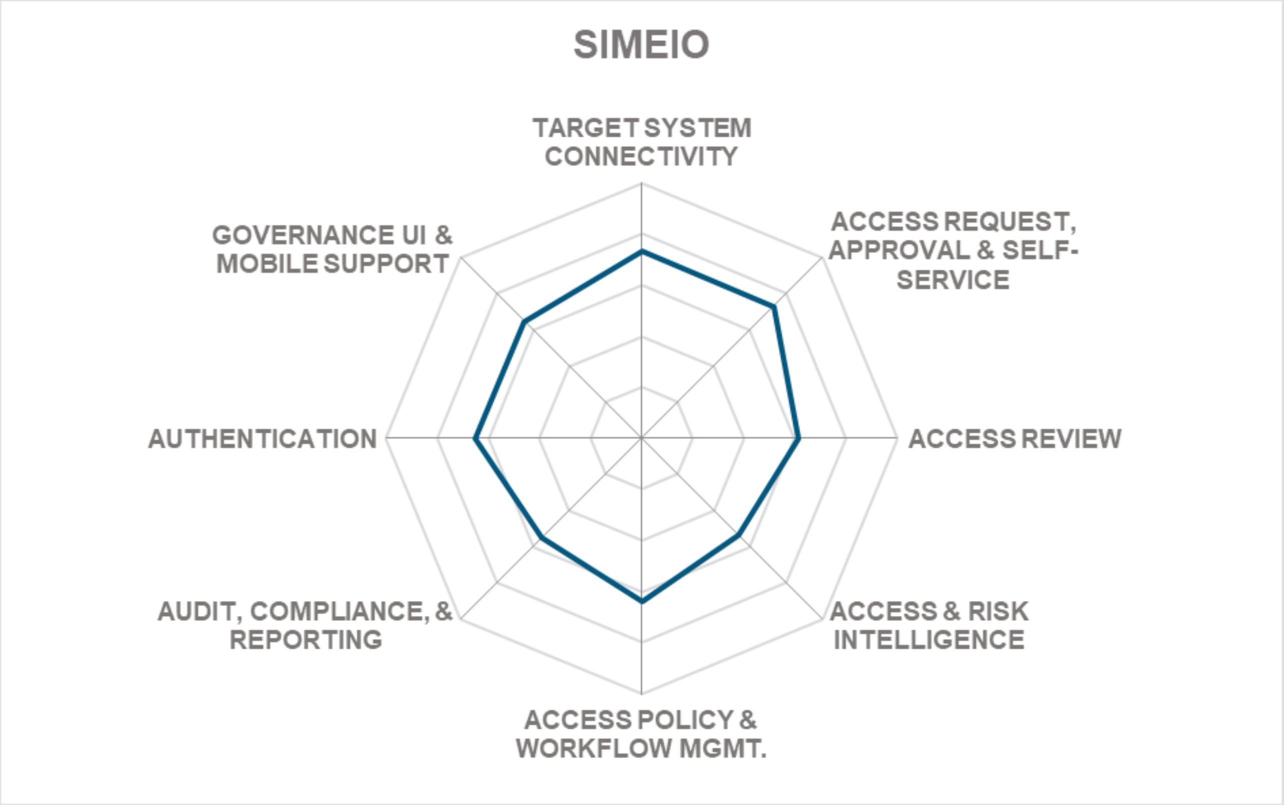
simeio

Strengths

- Core AG features
- Breadth of OOB connectors to on-premises and SaaS systems
- Basic with some advanced authentication options available
- User self-service and mobile support
- Innovative mobile application
- Flexible deployment options

Challenges

- OOB AG reporting options are moderately limited, but improvements on roadmap
- SDK support to functionality is missing, although REST APIs are available
- Somewhat limited access intelligence
- Good ability to execute in North America, but limited system integrator partner network on a global scale The wide-spread reputation of primarily being only a global SI vendor


SIMEIO
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

5.24 Soffid IAM

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

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

Regarding Access Governance, Soffid IAM offers good user self-service capabilities such as a shopping cart approach to access requests including roles and privileged access as well as approval workflows. All access request management is available from a mobile device. Password and policy management capabilities are also given. 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. In addition, Soffid IAM provides SSO and the capability to record sessions and keystrokes. Additional features include a workflow web editor, recertification capabilities, and adaptive authentication with biometrics. An XACML policy editor and PEP configuration tools are also given.

Soffid provides a functional dashboard with the ability to customize dashboard widget based on customer requirements. Some access & risk intelligent features include access modeling, anomaly, entitlement and role outlier detection and are shown through status and risk indicators. Additionally, role mining and discovery capabilities are also available.

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

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

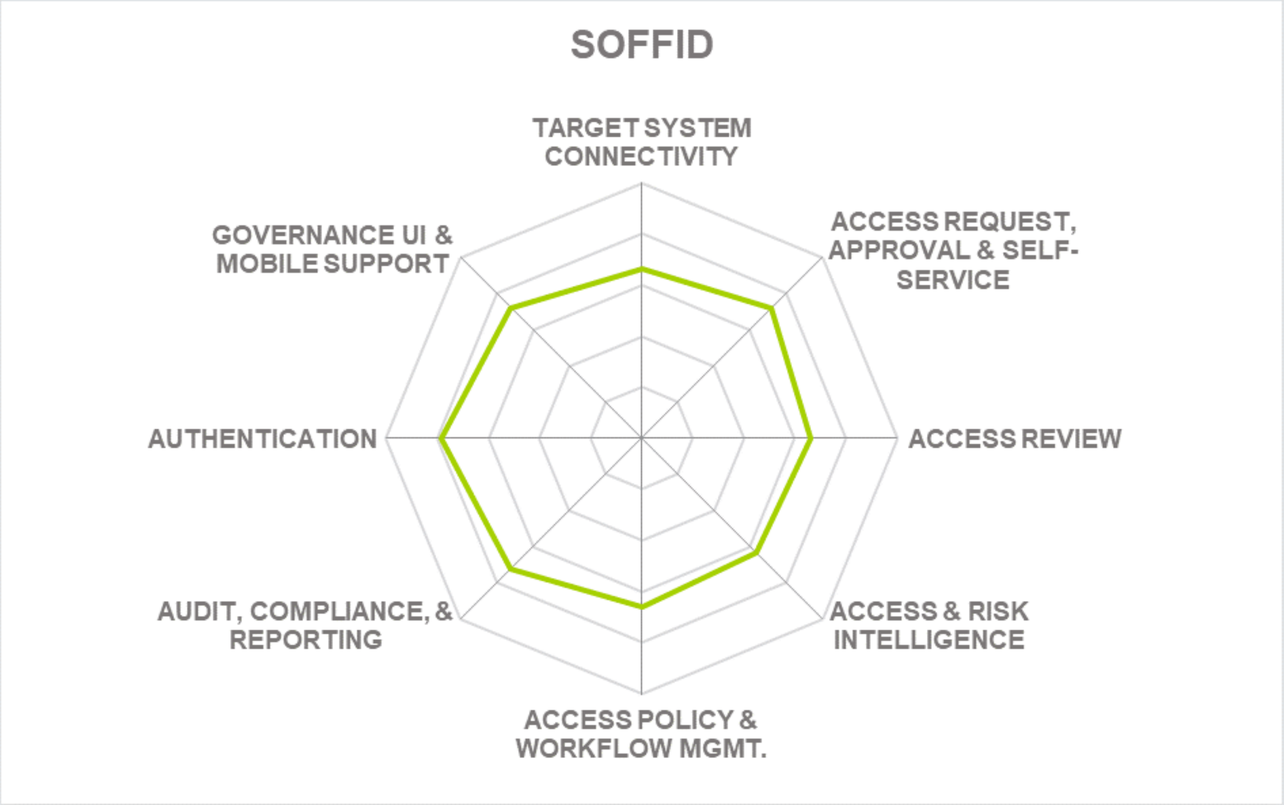
soffid

Strengths

- Breadth of OOB connectors to on-premises systems
- Good self-service & administration access authentication options
- All functionality exposed via APIs
- Access & risk intelligence
- AG related reporting support
- Dynamic authorization management

Challenges

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


SOFFID
TARGET SYSTEM CONNECTIVITY
ACCESS REQUEST, APPROVAL & SELF-SERVICE
ACCESS REVIEW
ACCESS & RISK INTELLIGENCE
ACCESS POLICY & WORKFLOW MGMT.
AUDIT, COMPLIANCE, & REPORTING
AUTHENTICATION
GOVERNANCE UI & MOBILE SUPPORT

6 Vendors and Market Segments to Watch

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

6.1 Imprivata

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

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

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

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

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

6.2 Kleverware

Kleverware is a French software company that started in 2005 and based in Paris, France. Kleverware customer base is primarily located in the EMEA region, focusing on delivering a lean, targeted solution for Identity & Access Governance (IAG). Kleverware IAG does not provide the full set of capabilities of IGA, but rather focuses on the governance aspects, while less on the administrative aspects of the technologies. Kleverware IAG is delivered as software deployed to a Windows Server 2016+ with an SQL Server in either on-premises or private cloud environments. Although not currently supported, full REST API support is on Kleverware's roadmap.

Since Kleverware focuses on Access Governance, instead of full IGA capabilities, including Identity Provisioning, integration with the IT systems across the landscape, including cloud services, is rather straightforward. Data collection is done agentless, by using either export formats such as CSV files supported by the various IT systems, or standard interfaces including LDAP and others. The data is consolidated into the Kleverware IAG Warehouse, which is based on an in-memory database. Kleverware then analyzes that data and delivers reports, access review campaigns, and other types of analytics. Good Access Governance-related reporting is available that gives visibility into access risks, accounts, analytics trend analysis, attestations, groups, roles, and privileged access.

Although Kleverware doesn't support full access governance capabilities such user access self-service, OOB connectors to on-premises systems or authentication support, Kleverware does provide some interesting features such as access intelligence, consolidated view of access entitlements of users across the entire IT landscape, identifying and highlighting SoD and other policy violations, and enabling simple and focused access review processes.

6.3 N8 Identity

N8 Identity was founded in 200 and headquartered in located Burlington, Ontario, Canada. N8 Identity offers an Identity and Access Management/Governance (IAM/IAG) solution that runs in the cloud (IDaaS) called TheAccessHub. Although TheAccessHub is cloud-based and can run on Microsoft Azure or AWS. With TheAccessHub host in the cloud, it can connect to on-premise systems via an API gateway to a customer's on-premise gateway. TheAccessHub can also be hosted within the customer's data center using the same API gateway mechanism.

N8 Identity TheAccessHub Enterprise provides four modules. The Activ8 module focuses on integration with HR and other authoritative source systems for onboarding and offboarding. The Orchestr8 module also performs onboarding, offboarding, and provisioning as well as request management, workflows, analytics, and reporting capabilities. The Remedi8 module supports access certification and governance. The fourth module, Valid8, is targeted towards the healthcare industry and provides patient check-in/out capabilities through an integration with Microsoft FaceAPI.

6.4 SecurEnds

Founded in 2017, SecurEnds is a mid-size company with its headquarters in Atlanta, GA. SecurEnds security product portfolio includes Credential Entitlement Management, Identity Lifecycle Management, and Identity Risk & Analytics. The SecurEnds Identity Management Platform is container-based for on-prem, cloud, and SaaS offerings. The SecurEnds Identity Management Platform is cloud-based but can extend to on-premises through the use of an agent that connects on-prem applications to the SecurEnds cloud service. In cases where the SecurEnds cloud service cannot be used, SecurEnds provides a Docker container of its software that can be deployed on-premises and connect to the on-prem applications. Both REST and SCIM APIs are available as well.

The SecurEnds dashboards of its Identity Risk & Analytics solution provide interesting real-time graphics of user data that maps the user to their applications, credentials, and entitlement. SecurEnds matches identities with user credentials across the enterprise using pattern matching fuzzy logic and behavior analytics from various sources. For example, it shows the identity risks, anomalies, inliers, and outliers. SecurEnds Identity Management Platform provides a wide range of connectors to many popular applications. It also provides a Flex Connectors based on OpenAPI which can connect to databases, FTP folder to consume data, web APIs (e.g., REST), or even upload a JAR file or script to connect to an application and retrieve user entitlements as well as provisioning & de-provisioning. SecurEnds is also capable of managing access requests, access notifications, access reviews, and certifications. Although SecurEnds provides full IGA capabilities, many of its customers can start with SecurEnds Access Governance features.

6.5 Tuebora

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

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

6.6 Usercube

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

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

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

7 Related Research

Executive View: Atos DirX Identity - 80166
Executive View: Avatier Identity Management Suite - 71510
Executive View: Beta Systems Garancy IAM Suite – 71530
Executive View: EmpowerID - 70297
Executive View: Evidian Identity & Access Management - 70872
Executive View: Hitachi ID IAM Suite – 72543
Executive View: Kleverware IAG - 80042
Executive View: Nexis Controle 3.0 - 72535
Executive View: Nexis contROLE - 71502
Executive View: Omada Identity Suite - 70301
Executive View: Oracle Identity Governance - 80157
Executive View: RSA® Identity Governance and Lifecycle - 71052
Executive View: SailPoint SecurityIQ - 70849
Executive View: Saviynt Security Manager for Enterprise IGA - 80325
Executive View: Simeio IAM for SMB - 79071
Leadership Compass: Identity Governance & Administration (IGA) - 80063
Leadership Compass: Access Management and Federation - 71147
Leadership Compass: IDaaS Access Management - 79016
Leadership Compass: Identity API Platforms - 79012
Leadership Compass: Identity as a Service (IDaaS) IGA - 80051
Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) - 71141
Leadership Compass: Identity as a Service (IDaaS B2E) - 70319
Leadership Compass: Identity Provisioning – 71139
Whitepaper: A Lean Approach on Identity & Access Governance - 80048
Whitepaper: SailPoint: Governance for all data: Get a grip on unstructured data - 79046

Endnotes

[1] http://www.kuppingercole.com/report/advisorynote_comprehensiveeag7110919214

[2] http://www.kuppingercole.com/report/advisorynote_comprehensiveeag7110919214

Methodology

About KuppingerCole's Leadership Compass

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

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

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

Types of Leadership

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

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

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

- **Leaders**: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular areas.

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

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

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

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

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

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

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

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

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of

these areas will only result in increased human participation in deploying and maintaining IT systems.

- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

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

Vendor rating

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

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

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

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

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

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

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

Rating scale for products and vendors

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

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

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

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

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

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

Inclusion and exclusion of vendors

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

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

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

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

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

Content of Figures

Figure 1: The Status and Expected Evolution of Access Governance

Figure 2: The Overall Leadership rating for the Access Governance market segment

Figure 3: Product Leaders in the Access Governance market segment

Figure 4: Innovation Leaders in the Access Governance market segment

Figure 5: Market Leaders in the Access Governance market segment

Figure 6: The Market/Product Matrix

Figure 7: The Product/Innovation Matrix

Figure 8: The Innovation/Market Matrix

Copyright

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

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

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