

KuppingerCole Report LEADERSHIP COMPASS

by **Martin Kuppinger** and **Anmol Singh** | June 2018

Access Governance & Intelligence

Leaders in innovation, product features, and market reach for access governance & intelligence. Delivering the capabilities for managing access entitlements, always knowing the state of these, and enforcing access and SoD policies across heterogeneous IT environments on premises and in the cloud. Your compass for finding the right path in the market.



by **Martin Kuppinger**
mk@kuppingercole.com
June 2018



by **Anmol Singh**
asi@kuppingercole.com
June 2018



Leadership Compass
Access Governance
By KuppingerCole

Content

1	Introduction	7
1.1	Market Segment	9
1.2	Delivery models	12
1.3	Required Capabilities.....	12
2	Leadership.....	16
2.1	Overall Leadership.....	17
2.2	Product Leadership.....	19
2.3	Innovation Leadership	21
2.4	Market Leadership.....	23
3	Correlated View	25
3.1	The Market/Product Matrix	26
3.2	The Product/Innovation Matrix.....	28
3.3	The Innovation/Market Matrix.....	30
4	Products and Vendors at a glance	32
4.1	Ratings at a glance.....	33
5	Product/service evaluation	36
5.1	Avatier	37
5.2	Beta Systems	38
5.3	Brainwave	39
5.4	CA Technologies	40
5.5	E-Trust.....	41
5.6	EmpowerID	42
5.7	Evidian	42
5.8	Fischer International Identity	44
5.9	Hitachi ID	45
5.10	IBM	46
5.11	Micro Focus	47
5.12	Nexis	48
5.13	Omada	49
5.14	One Identity.....	50
5.15	Oracle.....	51
5.16	Pirean.....	52

5.17	RSA.....	53
5.18	SailPoint	54
5.19	SAP	55
5.20	Saviynt	56
5.21	SecureAuth + Core Security	57
5.22	Systancia	58
5.23	Tools4ever	59
6	Vendors to watch out for Access Governance	60
6.1	Atos.....	60
6.2	Avanpost	60
6.3	Cion Systems.....	60
6.4	Deep Identity	61
6.5	FSP	61
6.6	Identity Automation	61
6.7	Ilantus	61
6.8	Imprivata	61
6.9	iSM Secu-Sys.....	62
6.10	ITconcepts.....	62
6.11	ITMC Soft	62
6.12	Microsoft	62
6.13	Ogitix.....	63
6.14	OpenIAM.....	63
6.15	Propentus	63
6.16	SmartAIM.....	64
6.17	Usercube.....	64
6.18	Tuebora.....	64
6.19	WSO2	64
7	Methodology.....	65
7.1	Types of Leadership	65
7.2	Product rating.....	66
7.3	Vendor rating.....	68
7.4	Rating scale for products and vendors	69
7.5	Spider graphs	69

7.6	Inclusion and exclusion of vendors	70
8	Copyright	71

Content of Tables

Table 1: Comparative overview of the ratings for the product capabilities.....	33
Table 2: Comparative overview of the ratings for vendors	34
Table 3: Avatier major strengths and challenges.....	37
Table 4: Avatier rating	37
Table 5: Beta Systems major strengths and challenges.....	38
Table 6: Beta Systems rating	38
Table 7: Brainwave’s major strengths and challenges.....	39
Table 8: Brainwave rating	39
Table 9: CA major strengths and challenges	40
Table 10: CA rating	40
Table 11: E-Trust major strengths and challenges.....	41
Table 12: E-Trust rating	41
Table 13: EmpowerID major strengths and challenges	42
Table 14: EmpowerID rating	42
Table 15: Evidian major strengths and challenges.....	43
Table 16: Evidian rating.....	43
Table 17: Fischer International major strengths and challenges.....	44
Table 18: Fischer International rating	44
Table 19: Hitachi ID major strengths and challenges.....	45
Table 20: Hitachi ID rating.....	45
Table 21: IBM major strengths and challenges.....	46
Table 22: IBM rating	46
Table 23: Micro Focus major strengths and challenges.....	47
Table 24: Micro Focus rating.....	47
Table 25: Nexis major strengths and challenges	48
Table 26: Nexis rating.....	48
Table 27: Omada major strengths and challenges	49
Table 28: Omada rating.....	49
Table 29: One Identity major strengths and challenges	50
Table 30: One Identity rating	50
Table 31: Oracle major strengths and challenges.....	51
Table 32: Oracle rating	51
Table 33: Pirean major strengths and challenges	52
Table 34: Pirean rating	52
Table 35: RSA major strengths and challenges	53
Table 36: RSA rating	53
Table 37: SailPoint major strengths and challenges	54
Table 38: SailPoint rating	54

Table 39: SAP major strengths and challenges	55
Table 40: SAP rating	55
Table 41: Saviynt major strengths and challenges.....	56
Table 42: Saviynt rating.....	56
Table 43: SecureAuth + Core Security major strengths and challenges	57
Table 44: SecureAuth + Core Security rating	57
Table 45: Systancia major strengths and challenges	58
Table 46: Systancia rating	58
Table 47: Tools4ever major strengths and challenges	59
Table 48: Tools4ever rating.....	59

Content of Figures

Figure 1: The Status and Expected Evolution of Access Governance	11
Figure 2: The Overall Leadership rating for the Access Governance market segment	17
Figure 3: Product leaders in the Access Governance market segment	19
Figure 4: Innovation leaders in the Access Governance market segment	21
Figure 5: Market leaders in the Access Governance market segment	23
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.....	26
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.	28
Figure 8: The Innovation/Market Matrix	30

Related Research

Executive View: Beta Systems Garancy IAM Suite - 71530

Executive View: Beta Systems Garancy Recertification Center - 71315

Executive View: CA Technologies Mobile API Gateway, Mobile App Services, and App Experience Analytics - 70811

Executive View: CA Privileged Access Manager - 71264

Executive View: Evidian Identity & Access Manager - 70871

Executive View: Hitachi ID IAM Suite - 72543

Executive View: IBM Security Identity Governance and Intelligence - 71113

Executive View: IBM QRadar Security Intelligence Platform - 72515

Executive View: IBM Privileged Identity Manager - 71557

Executive View: IBM Cloud Security Enforcer - 71523

Executive View: Micro Focus Privileged Account Manager - 71314

Executive View: Nexis Controle 3.0 - 72535

Executive View: Omada Identity Suite - 70301

Executive View: Omada Identity Suite v11.1 - 70835

Executive View: One Identity Manager v7.0.1 - 70894

Executive View: RSA SecurID® Access - 70323

Executive View: RSA NetWitness Suite - 72516

Executive View: SailPoint IdentityIQ - 71319

Executive View: SailPoint SecurityIQ - 70849

Executive View: SAP HANA Platform Security - 70272

Executive View: SAP Fraud Management - 71182

Executive View: SAP HANA Enterprise Cloud – Security and Compliance - 71117

Executive View: SAP Enterprise Threat Detection - 71181

Executive View: Saviynt Identity Governance and Administration (IGA) 2.0 - 71506

Leadership Compass: Privilege Management - 72330

Leadership Compass: CIAM Platforms - 70305

Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) - 71141

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: identity provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Access Management and Federation - 70790

Leadership Compass: Access Governance - 70735

1 Introduction

The KuppingerCole Leadership Compass provides an overview of vendors and their product or service offerings in a certain 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 an 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 auditability and role governance.

Based on the adoption trends, changing customer priorities and deployment patterns, we decided to create three 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 Identity Provisioning:** This Leadership Compass focuses on solutions with strong support for identity provisioning. While we expect some baseline access governance capabilities, they are not a necessary evaluation criterion. However, we also look at complete IGA offerings if they have strong identity provisioning support.
- **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 three 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 involvement of business in the overall management of access rights across an organization's IT environment. Access governance provides necessary (mostly self-service) tools for business to manage workflows and access entitlements, run reports, access certification campaigns and SOD checks. Access intelligence 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. Many prominent security incidents during the last few years originated from poorly managed identities and prove 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 lack of proper access governance controls. Access risks can have 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. An adequate access governance framework is thus essential for the organizations dealing with constantly changing paradigm 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 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 not only identify the risk in access governance but 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

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

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.



Figure 1: The Status and Expected Evolution of Access Governance

To achieve this, features for role management, policy management, rule definition and analysis, workflows as well as additional functionality are required. Dashboards for executives and extended auditing and reporting capabilities are a part of these tools. Risk management features are recommended but are not a standard feature of products in the market yet.

To connect with target systems, access governance tools should support different types of interfaces:

- Connectors to extract access control status information out of target systems, frequently using flat file exports;
- Interfaces to provisioning systems to use their access management features for active management and, in some cases, to extract access control status information;
- Direct connectors to target systems for changing access control information in these systems;
- Interfaces to Service Request Management (SRM) tools which are used to manually provide information to target systems;
- Workflows providing manual tasks to operators. The execution of these tasks should be automatically tracked by the analysis features of the product.

An increasing number of tools are now supporting these features or building on capabilities to support them. An in-depth analysis of architectural options for access governance is provided in the KuppingerCole Advisory Note #71,039 “Access Governance Architectures”².

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 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

² http://www.kuppingercole.com/report/adnote_accessgov_7103914314

- 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 ³ /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.

³ http://www.kuppingercole.com/report/advisorynote_comprehensiveeag7110919214

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 be only based on the comparison provided by 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

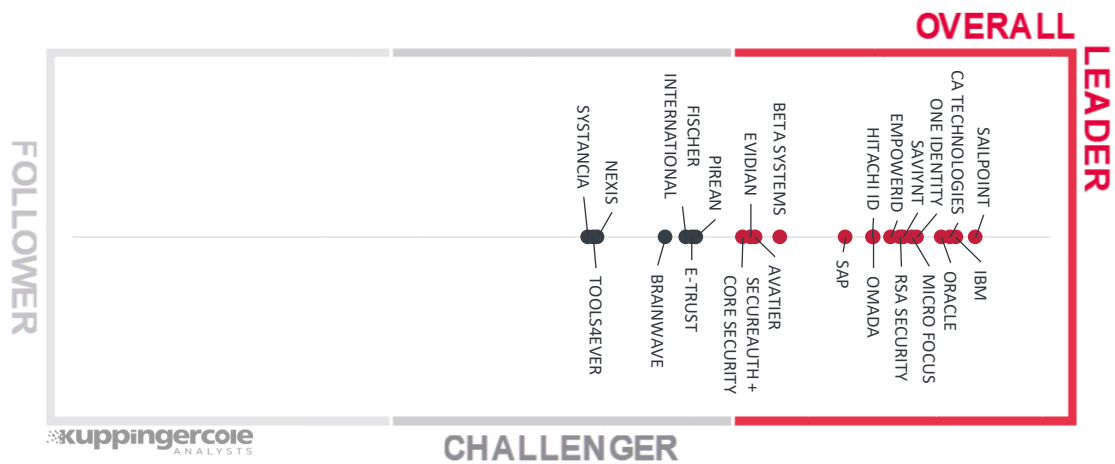


Figure 2: The Overall Leadership rating for the Access Governance market segment

When looking at the Overall Leader segment in the Overall Leadership rating, we see a picture that is common for mature market segments, where a significant number of vendors delivers solutions with a rich feature set. The market is crowded with about 25 prominent vendors that we have considered for our Leadership Compass evaluation and a few others listed in the “vendors to watch” section.

For Overall Leadership, we find SailPoint in the lead, slightly ahead of its closest group of competitors consisting of IBM, CA Technologies and Oracle. Another group of vendors follows closely, located in the same segment. This group consists, in alphabetical order, of EmpowerID, Hitachi-ID, Micro Focus, Omada, One Identity, RSA Security, SAP and Saviynt. All these vendors have an established market presence in the access governance market segment, with EmpowerID and Hitachi ID being the two least known of these vendors but both delivering comprehensive access governance capabilities, positioning them clearly in the Overall Leaders segment. Saviynt is another vendor that has earned itself a position in the Leaders segment, ahead of many established players, with its consistent execution and completeness of access governance offering.

Micro Focus also made its entry into the Overall Leader segment, after maturing and enhancing their product significantly over the past few years. Further vendors we find in this segment include Beta Systems, Avatier, Evidian, and SecureAuth + Core Security. All provide solutions which move them, in combination with their ratings on Market Leadership and Innovation Leadership, into the Overall Leader segment.

The Challenger segment is also well populated and surprisingly dominated by vendors based in Europe. GDPR and other political developments in the region have fueled the need for strong access governance in the market accelerating the innovation and creating opportunities for local vendors. The vendors in Challenger segment also provide strong offerings, which challenge the established players. Here we find a group of five vendors being close to entering the Leaders segment. These are, in alphabetical order, Brainwave, E-Trust, Fischer International and Pirean. Brainwave differs from other vendors, aside of Nexis, in their specific focus on access governance only, not delivering identity provisioning capabilities on its own but closely integrating with other identity provisioning tools.

Other vendors in the same segment include Tools4ever, that enter the market more from the SMB end but deliver an interesting product particularly for mid-sized organizations outside of the heavily regulated industries; and Systancia, a vendor that started in the Healthcare market but now delivers a solution targeted at all industry verticals. In the same cluster is Nexis, another smaller German vendor, which is focused purely on access governance and, within that on Access Review and Role Mining capabilities. Nexis makes an interesting solution to complement existing identity provisioning deployments.,

Another vendor in Challenger segment is German vendor FSP. They have a fairly limited market presence and exhibit some functionality gaps when looking at the breadth of access governance capabilities. However, they excel in offering a balanced integration of RBAC (Role Based Access Control) with ABAC (Attribute Based Access Control) model, which remains a rare but helpful feature for organizations particularly in heavily regulated industries.

There are no vendors in the Follower segment.

Overall Leaders are (in alphabetical order):

- Avatier
- Beta Systems
- CA Technologies
- EmpowerID
- Evidian
- Hitachi-ID Systems
- IBM
- Micro Focus
- Omada
- One Identity
- Oracle
- RSA Security
- SailPoint
- SAP
- Saviynt
- SecureAuth + Core Security

2.2 Product Leadership

The first of the three specific Leadership ratings is about Product Leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

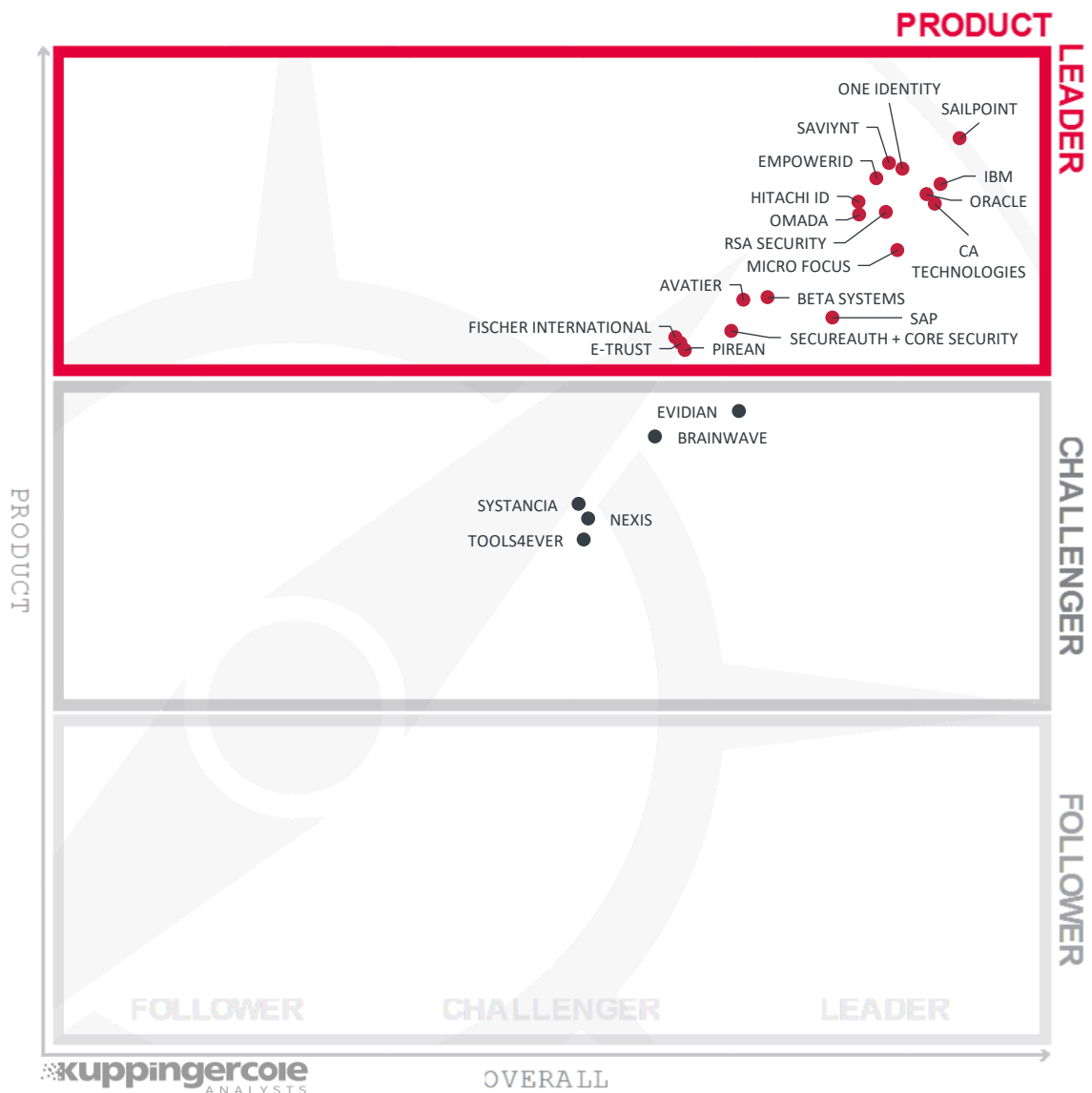


Figure 3: Product leaders in the Access Governance market segment

Product Leadership is the view where we look specifically at the functional strength and completeness of products. As access governance is an established and mature market segment, we find a significant number of vendors which qualify for the Leaders segment. Due to the specifics of the various offerings, a thorough vendor selection process for access governance is strongly recommended, starting with a thorough requirements analysis and taking into account also some of the more specialized vendors.

On top, we find a group of vendors, all placed close to each other. This group of ten vendors consists, in alphabetical order, of CA Technologies, EmpowerID, Hitachi-ID, IBM, Omada, One Identity, Oracle, RSA

Security, SailPoint, and Saviynt. All these vendors deliver leading-edge products for on premises access governance and score high in our evaluation. They differ in many details as discussed further in vendor's section, but in sum all deliver strong offerings for access governance.

With a little distance, we find Micro Focus. While Micro Focus is in the top group for identity provisioning, their overall access governance offering is good but not relatively as strong as their identity provisioning.

With some distance, but still positioned in the Leader segment, we find another group of vendors. This includes, again in alphabetical order, Avatier, Beta Systems, SecureAuth + Core Security, E-Trust, Fischer International, Pirean and SAP.

In the Challenger section, we find Evidian, lacking on a few capabilities we expect to see either in the depth or breadth of functionalities, but being close to becoming a leader. Slightly lower in the same segment is Brainwave, which is somewhat specific in being one of the few vendors that are solely focused on access governance capabilities, thus making an interesting add-on to existing identity provisioning deployments.

In the middle of the Challenger section, we find a couple of more vendors. Systancia and Nexis are positioned here. Tools4ever, entering the market from the SMB segment can be a good alternative for lightweight access governance deployments. Nexis is highly specialized on Access Certification and Role Management capabilities with strong Role Mining. Like Brainwave, it offers a complementary solution to identity provisioning vendors, that lack strong access governance.

There are no vendors in the Follower section of this evaluation.

Product Leaders (in alphabetical order):

- Avatier
- Beta Systems
- CA Technologies
- EmpowerID
- E-Trust
- Fischer International
- Hitachi-ID Systems
- IBM
- Micro Focus
- Omada
- One Identity
- Oracle
- Pirean
- RSA Security
- SailPoint
- SAP
- Saviynt
- SecureAuth + Core Security

2.3 Innovation Leadership

Another angle we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what customers require for keeping up with the constant evolution and emerging customer requirements they are facing. Innovation is not limited to delivering a constant flow of new releases, but focuses on a customer-oriented upgrade approach, ensuring compatibility with earlier versions especially at the API level and on supporting leading-edge new features which deliver emerging customer requirements.

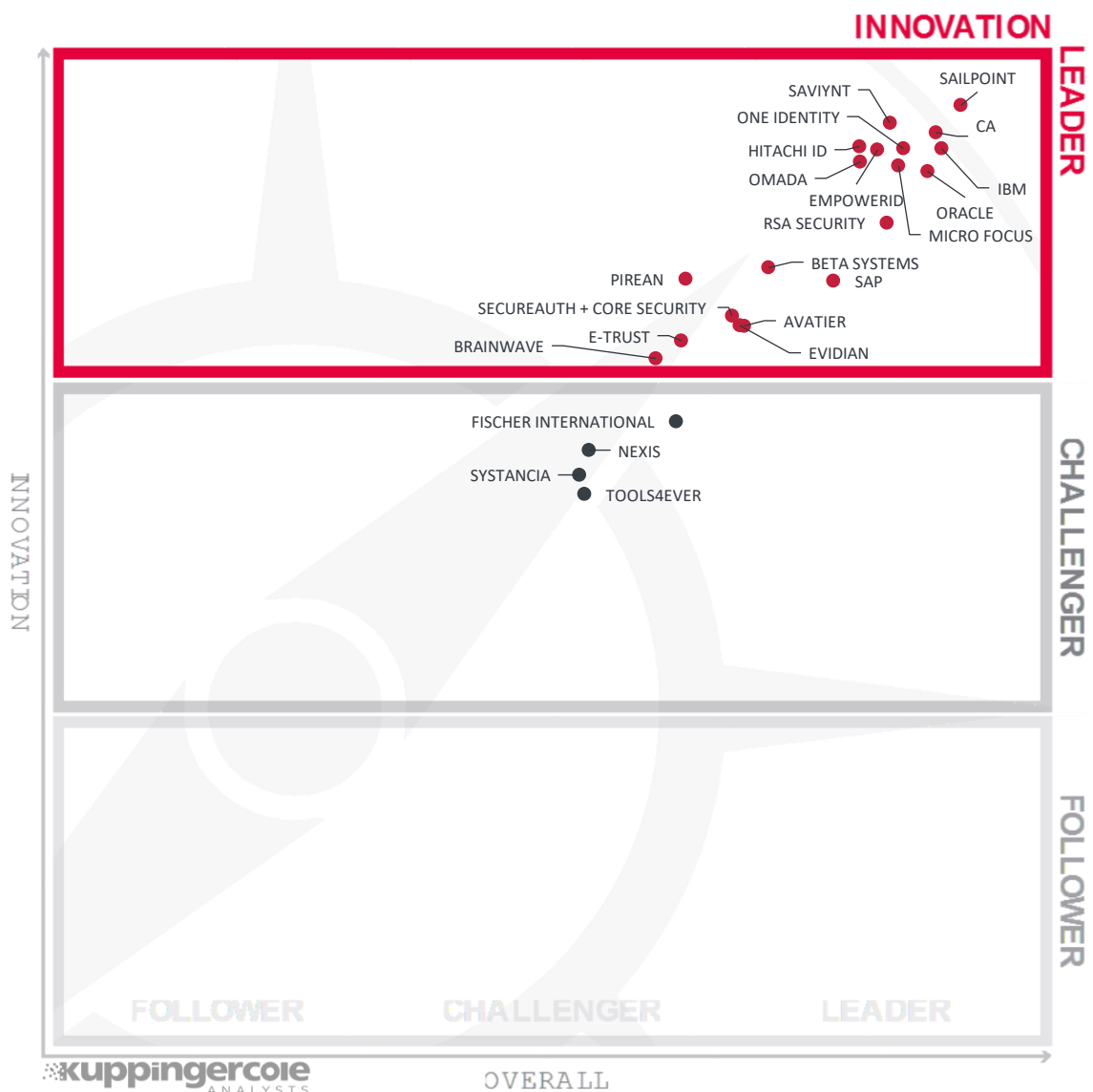


Figure 4: Innovation leaders in the Access Governance market segment

Again, we rate several vendors as Innovation Leaders in the access governance market. Given the maturity of access governance, the amount of innovation we see is somewhat limited, but vendors still try to differentiate themselves by innovating in several niche areas, from modern UIs and improved API layers to more specific areas such as improvements to Access Certification, delivering more options and more flexibility and automation. Access intelligence through analytics and deep machine learning techniques is fast becoming the new paradigm for innovation in delivering access governance.

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.

In the top group of ten vendors, we find – in alphabetical order – CA Technologies, EmpowerID, Hitachi-ID, IBM, Micro Focus, Omada, One Identity, Oracle, SailPoint, and Saviynt, followed by RSA Security at a distance. These vendors form the group of leading-edge players in the access governance market when it comes to innovation but are also strong in overall access governance capabilities. Again, they differ in many details, thus a thorough vendor selection process is essential to pick the right vendor of all the players in access governance market that fits best to customer requirements.

Aside of these vendors, we find a couple of other players that have made it into the Innovation Leader segment. Beta Systems, Pirean, and SAP are closely positioned, followed by (in alphabetical order) Avatier, SecureAuth + Core Security, E-Trust, and Evidian. All these vendors have also been able to demonstrate promising innovation in specific areas. Brainwave just crosses over the mark to make an entry into the Innovation Leaders segment.

Like other Leadership charts on this Leadership Compass, we find few vendors in the upper part of Challenger section that are close to becoming Innovation Leaders. These are, in alphabetical order, Fischer International, Nexis, Systancia and Tools4ever. Again, this is a diverse group of vendors with different focus for different access governance capabilities. We refer to the vendor pages further down in this report for more details.

There are no vendors in the Follower section.

Innovation Leaders (in alphabetical order):

- Avatier
- Beta Systems
- Brainwave
- CA Technologies
- EmpowerID
- E-Trust
- Evidian
- Hitachi ID Systems
- IBM
- Micro Focus
- Omada
- One Identity
- Oracle
- Pirean
- RSA Security
- SailPoint
- SAP
- Saviynt
- SecureAuth + Core Security

2.4 Market Leadership

Here we look at Market Leadership qualities based on certain market criteria including but not limited to the number of customers, the partner ecosystem, the global reach, and response to factors affecting the market growth. Market Leadership, from our point of view, requires global reach as well as consistent sales and service support with successful execution of marketing strategy.

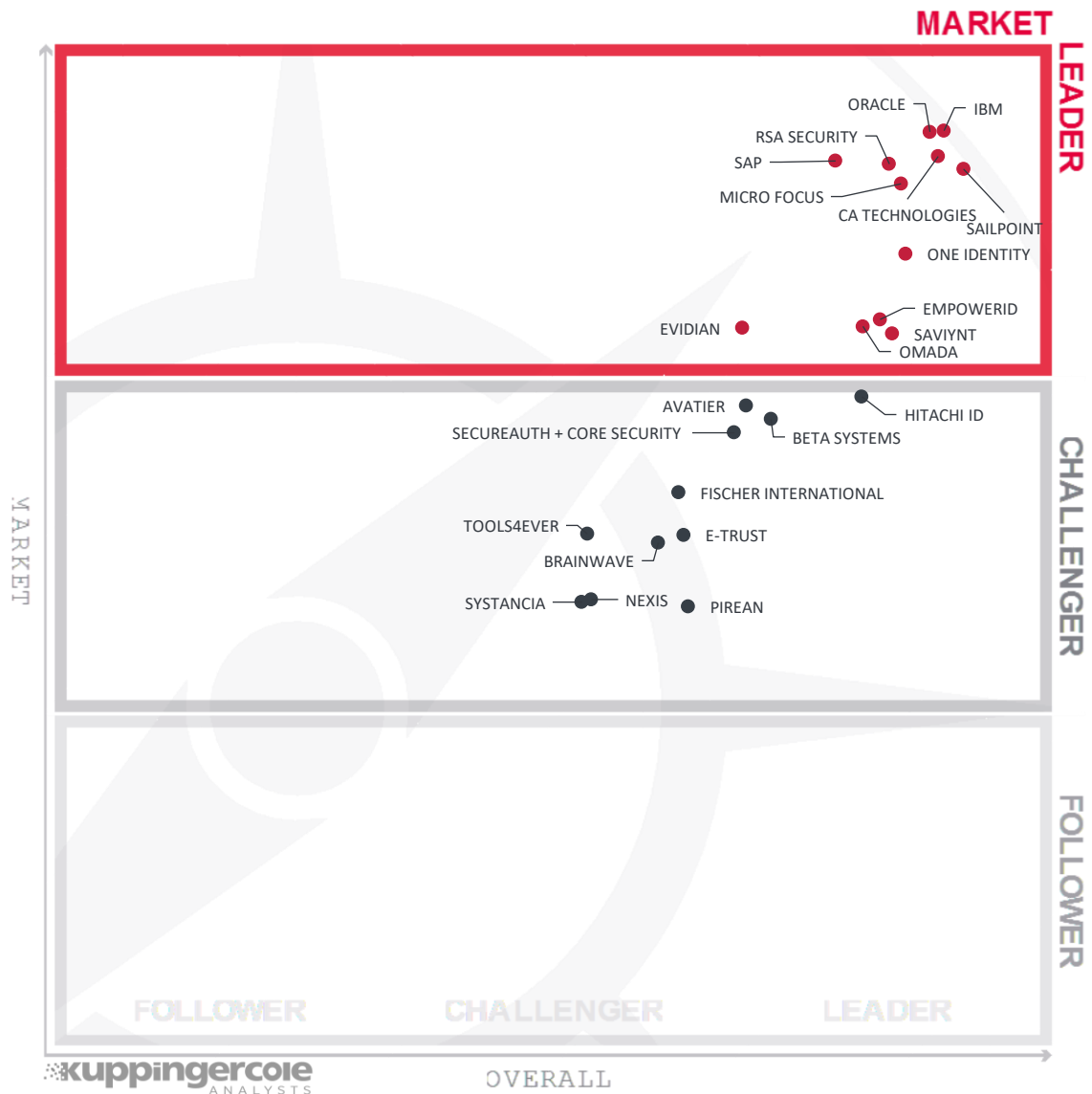


Figure 5: Market leaders in the Access Governance market segment

In the Market Leaders rating, we get a somewhat different picture. While there is a group of leading, well-established players, others are rated low, primarily for reasons such as limited market presence in certain geographies, limited industry-wide focus and relatively small customer base.

In the top right-hand corner of the Leaders segment, we find a group consisting of seven vendors. This group, in alphabetical order, consists of CA Technologies, IBM, Micro Focus, Oracle, RSA Security, SailPoint, and SAP – evidently known for a large global customer base with broader IAM portfolios which has helped them upsell access governance product

One Identity, having made some significant inroads lately in establishing itself as a market leader, now follows the cluster of long established players very closely.

EmpowerID, Evidian, Omada and Saviynt have also made it into this segment, all of them addressing market challenges aggressively than ever and working to build a stronger integration and partner ecosystem beyond their home territories.

In the Challenger section, we find Avatier, Hitachi ID, Beta Systems and SecureAuth + Core Security close to entering the Leader segment. While we count them amongst Market Leaders in other areas of the overall IGA market, their position in access governance market is affected by several factors – inadequate training and expertise of technology partners with their access governance product being one of them. .

Following these vendors closely are Fischer International, Tools4ever, Brainwave and E-Trust, all of which show considerable gaps in the specific areas we evaluate for Market Leadership, including the number of customers, average size of deployments, effectiveness of their partner ecosystem, etc.

Following from a distance are Systanica, Nexis and Pirean which are also rated as challengers due to certain limitations in executing market success as compared to their peers.

Market Leaders (in alphabetical order):

- CA Technologies
- EmpowerID
- Evidian
- 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, say, 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 deliver additional analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

The first of these correlated views looks at 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 frequently are innovative but focused on specific regions.

In the upper right segment, we find the “Market Champions”. Given that the access governance market is fast maturing, we find (in alphabetical order) CA Technologies, IBM, Micro Focus, SailPoint, Oracle, RSA Security and SAP as market champions being positioned in the top right-hand box. Of these, only SailPoint

offers a balanced view of market vs product leadership. Most others have a higher weightage for market leadership than for product leadership. One Identity presents a unique correlation with one of the strongest product functionalities amongst the market champions but somewhat lacking on relative market success in comparison.

Similarly, there are EmpowerID, Omada and Saviynt - all three positioned under the line showing their inclination for stronger product leadership in comparison to market leadership.

Evidian is the only vendor in the box to the left of market champions, clearly depicting its stronger market success over the product capabilities.

In the middle right-hand box, we see the vendors that deliver strong product capabilities for access governance but are not yet considered Market Champions. All these vendors have a strong potential for improving their market position due to the stronger product capabilities that they are already delivering. These vendors are, from top to bottom, Hitachi ID, Avatier, Beta Systems, SecureAuth + Core Security, Fischer International, E-Trust and Pirean. Amongst all these vendors, Hitachi ID and Pirean are positioned farthest from the axis depicting their stronger focus on product capabilities than market leadership. From the same group, Avatier, Beta Systems and SecureAuth + Core Security are found to have an appropriate balance of the product vs market success.

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 Brainwave, Nexis, Systancia and Tools4ever. Of this vendor group, Brainwave and Nexis are seen to offer a better balance of market success and product strength.

3.2 The Product/Innovation Matrix

The second 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 few exceptions. This distribution and correlation is typical for most markets with a significant number of established vendors plus some smaller vendors.

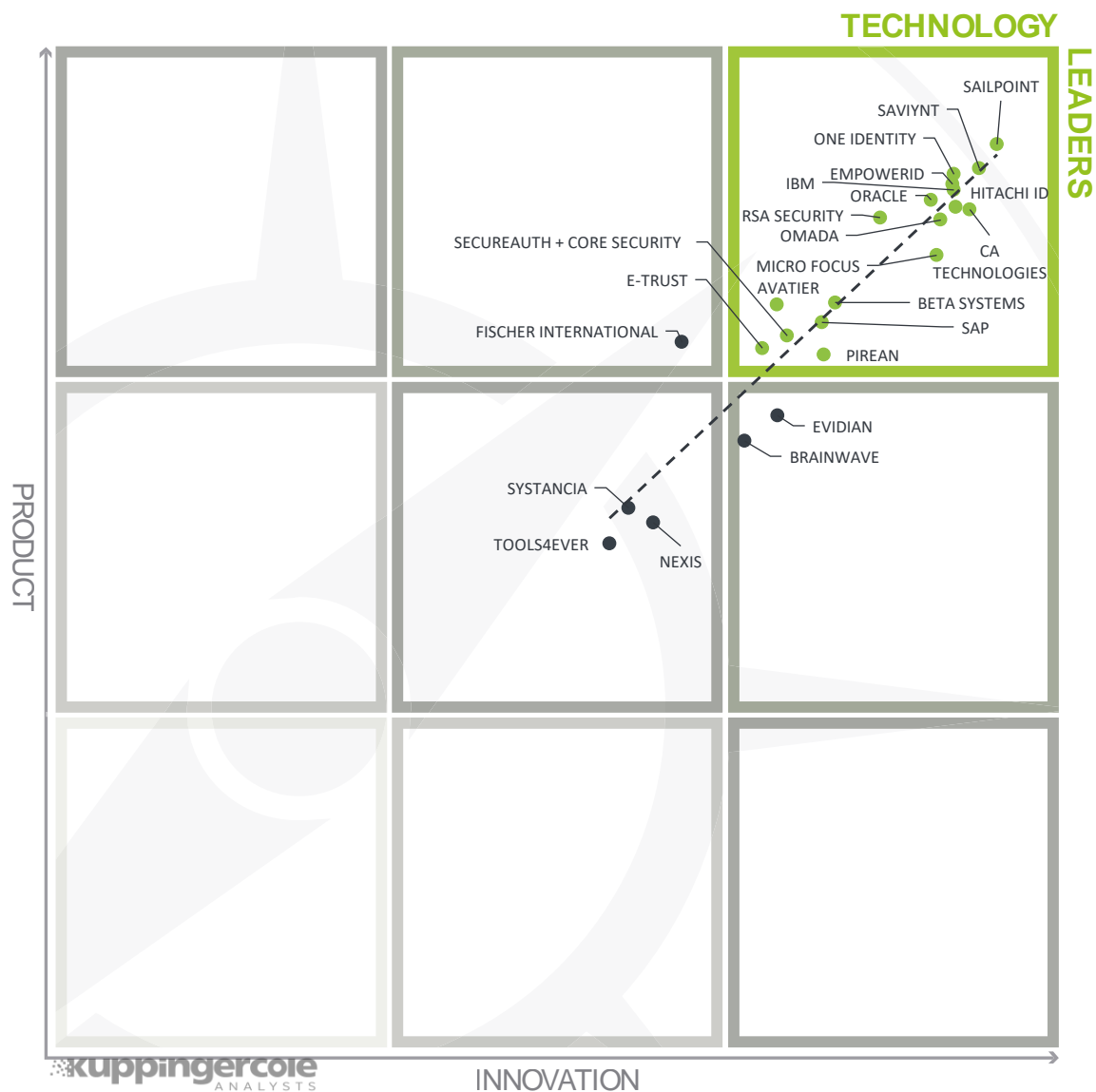


Figure 7: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we see a good correlation between the product and innovation rating, with most vendors being placed close to the dotted line. When looking at the “Technology Leaders” segment, we find the leading vendors all in the upper right corner, placed close to each other. The top-notch vendors are SailPoint, Saviynt, One Identity, , EmpowerID, Hitachi ID, Oracle, Omada, CA Technologies, and IBM. Following this

group in the Technology Leaders segment are RSA Security and Micro Focus – both having made significant positive changes to product strategy lately.

Closely following them, and also in the “Technology Leaders” box, we see Avatier, Beta Systems, SAP, SecureAuth + Core Security and Pirean. Further vendors that made it into this segment are Pirean and E-Trust.

To the left of them, we find Fischer International that is rated amongst the Product Leaders, but not the Innovation Leaders.

Evidian is positioned alone in the middle-right box, exhibiting its relatively better innovation leadership compared to overall product leadership.

The other vendors are positioned in the box to the middle of the chart, being challengers for both the product rating and the innovation rating. These are Brainwave, Systancia, Tools4ever and Nexis.

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 to 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 but might also fail, especially in the case of smaller vendors.

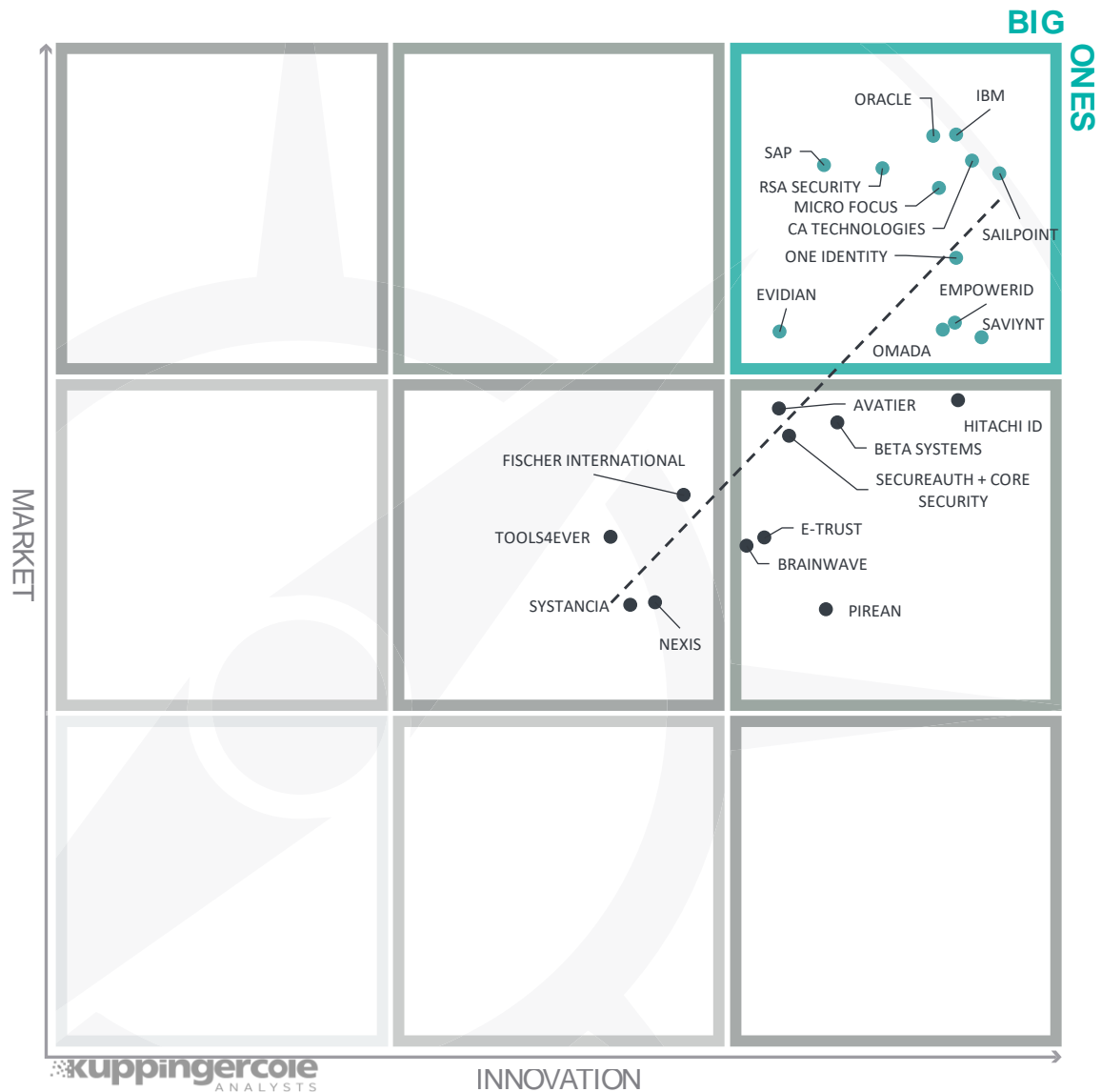


Figure 8: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relative weak 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 corner, we find the “Big Ones” in access governance, with a good number of vendors being positioned at that level. We find the large ones more on top, including (in alphabetical order) CA Technologies, IBM, Micro Focus, Oracle, RSA Security, SailPoint, and SAP.

More to the bottom of the upper right box, we see One Identity, EmpowerID, Omada, and Saviynt showcasing their higher weightage for innovation criteria than that for market success criteria. To the left, in the same box, is Evidian which makes its entry in the ‘Big Ones’ segment with its stronger market execution.

Below the “Big Ones”, in the middle-right box, we find Avatier, Beta Systems, SecureAuth + Core Security and Hitachi ID, E-Trust and Pirean, with both Hitachi ID and Pirean being the farthest from the axis implying towards their relatively strong innovation leadership in comparison to market leadership.

The segment in the middle of the chart contains the vendors rated as challengers both for market and innovation leaderships with Fischer International, Systancia, Tools4ever and Nexis.

4 Products and Vendors at a glance

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

4.1 Ratings at a glance

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

Product	Security	Functionality	Integration	Interoperability	Usability
AVATIER	positive	positive	strong positive	positive	strong positive
BETA SYSTEMS	strong positive	positive	neutral	positive	positive
BRAINWAVE GRC	positive	positive	positive	positive	positive
CA TECHNOLOGIES	strong positive	strong positive	positive	strong positive	strong positive
E-TRUST	positive	positive	positive	positive	positive
EMPOWERID	strong positive	strong positive	strong positive	positive	strong positive
EVIDIAN	strong positive	positive	neutral	positive	positive
FISCHER INTERNATIONAL	positive	positive	strong positive	positive	strong positive
HITACHI ID	strong positive	strong positive	strong positive	positive	strong positive
IBM	strong positive	strong positive	positive	strong positive	strong positive
MICRO FOCUS	strong positive	positive	positive	strong positive	strong positive
NEXIS GMBH	neutral	neutral	positive	neutral	positive
OMADA	strong positive	strong positive	positive	positive	strong positive
ONE IDENTITY	strong positive	strong positive	strong positive	positive	strong positive
ORACLE	strong positive	strong positive	positive	strong positive	strong positive
PIREAN	strong positive	positive	positive	positive	positive
RSA SECURITY	strong positive	strong positive	positive	positive	positive
SAILPOINT	strong positive	strong positive	strong positive	strong positive	strong positive
SAP	strong positive	positive	positive	positive	positive
SAVIYNT INC.	strong positive	strong positive	strong positive	positive	strong positive
SECUREAUTH + CORE SECURITY	positive	positive	positive	positive	positive
SYSTANCIA	positive	positive	positive	neutral	positive
TOOLS4EVER	positive	neutral	positive	neutral	positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
AVATIER	positive	neutral	positive	positive
BETA SYSTEMS	positive	neutral	positive	neutral
BRAINWAVE GRC	neutral	neutral	neutral	positive
CA TECHNOLOGIES	strong positive	strong positive	strong positive	positive
E-TRUST	neutral	neutral	neutral	neutral
EMPOWERID	strong positive	positive	positive	neutral
EVIDIAN	strong positive	positive	strong positive	positive
FISCHER INTERNATIONAL	strong positive	neutral	positive	neutral
HITACHI ID	strong positive	neutral	strong positive	neutral
IBM	strong positive	strong positive	strong positive	strong positive
MICRO FOCUS	strong positive	positive	strong positive	strong positive
NEXIS GMBH	neutral	weak	neutral	neutral
OMADA	strong positive	neutral	positive	positive
ONE IDENTITY	strong positive	positive	positive	positive
ORACLE	strong positive	strong positive	strong positive	strong positive
PIREAN	positive	weak	neutral	weak
RSA SECURITY	positive	positive	strong positive	strong positive
SAILPOINT	strong positive	positive	strong positive	strong positive
SAP	strong positive	strong positive	strong positive	positive
SAVIYNT INC.	positive	neutral	positive	positive
SECUREAUTH + CORE SECURITY	positive	neutral	positive	neutral
SYSTANCIA	positive	neutral	neutral	weak
TOOLS4EVER	positive	neutral	positive	neutral

Table 2: Comparative overview of the ratings for vendors

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

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

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

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

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

5 Product/service evaluation

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

5.1 Avatier

Avatier, based in California (US), has evolved from a vendor that focused primarily on providing smart user interfaces, but lacked the underlying depth of capabilities, to a vendor delivering mature identity provisioning as well as access governance capabilities. However, majority of its access governance features are limited to common governance scenarios and supporting complex requirements could be a challenge. The primary module responsible for access governance is Compliance Auditor in conjunction with Group Enforcer, Workflow Manager and Identity Analyzer.

Strengths	Challenges
<ul style="list-style-type: none"> • Innovative, user-centric approach to access governance • Easy to deploy and configure for routine governance scenarios • Flexible and strong workflow automation capabilities 	<ul style="list-style-type: none"> • Lack of full support for multi-tenancy requirements • Lack of connectors for cloud-based applications and platforms • Lack of flexibility to support advanced governance scenarios • A growing but limited partner ecosystem • A limited footprint outside of North America

Table 3: Avatier major strengths and challenges

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. Avatier is particularly strong in supporting identity lifecycle management, workflow and policy management as well as role management, primarily for Active Directory based deployments. Their focus on simplification of user interfaces offers a great abstraction of governance features for business users who are commonly unacquainted with technical details. While support for advanced access certification and access intelligence scenarios including customized reporting and dashboarding could be a challenge, Avatier IMS makes an excellent choice for access governance requirements of small to mid-sized organizations.

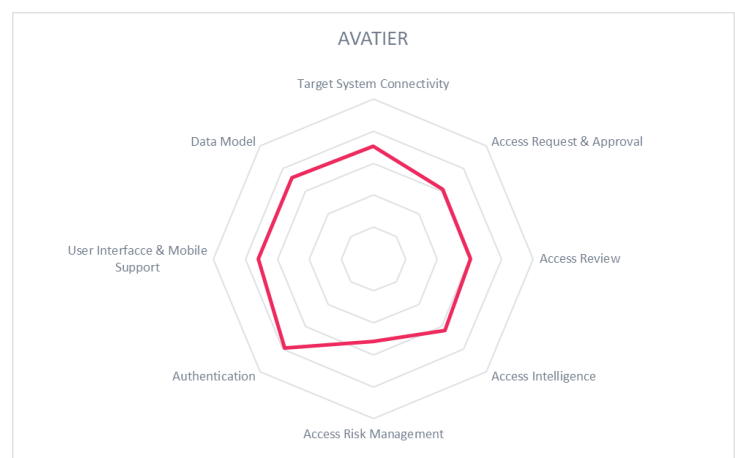
Avatier IMS though presenting an interesting alternative to the established players, leaves a few gaps in being a comprehensive access governance offering, e.g. lack of support for dynamic authorization management, multi-tenancy and RESTful APIs. Avatier with its excellent user interface and highly modular offerings is a preferred choice for customers in manufacturing and healthcare industry verticals. The biggest challenge for customers remains the small partner network and limited presence outside of North America.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 4: Avatier rating

Overall, Avatier's access governance capabilities are a good fit for customers with a focus on ease of use and reduced deployment complexity for leaner operations. For customers outside of North

America, we strongly recommend to carefully evaluate the technical and operational support that Avatier can deliver.



5.2 Beta Systems

Beta Systems, based in Germany, offers Garancy IAM suite comprising of several modules including Garancy Identity Manager for provisioning, ProcessCenter (PRC) for policy and workflow management, UserCenter (USC) for identity life-cycle management and access request workflows, RecertificationCenter (RCC) for access review and Access Intelligence Manager (AIM) for access governance. Based on business intelligence framework, Garancy Access Intelligence Manager is a full featured access intelligence product with some strong reporting and dashboarding capabilities.

Strengths	Challenges
<ul style="list-style-type: none"> Strong role management support Support for Dynamic Authorization Management Dedicated support for mainframe environments 	<ul style="list-style-type: none"> Workflow Management as an OEM component, but tightly integrated Relatively small but sufficient partner ecosystem.

Table 5: Beta Systems major strengths and challenges

Beta Systems' Garancy Access Intelligence Manager is a relatively newer component as compared to its more popular Identity Manager offering. It leverages the broad set of connectors available within its Identity Manager module to collect and analyze information. The depth of integration provided with its connectors offers a distinct advantage over its competitors. Beta Systems is one of the rare vendors offering connectors with tight application integration, allowing applications to request authorization decisions at runtime and thus enabling Dynamic Authorization Management as an integrated feature. Furthermore, they deliver a flexible approach for customizing connectors for specific applications.

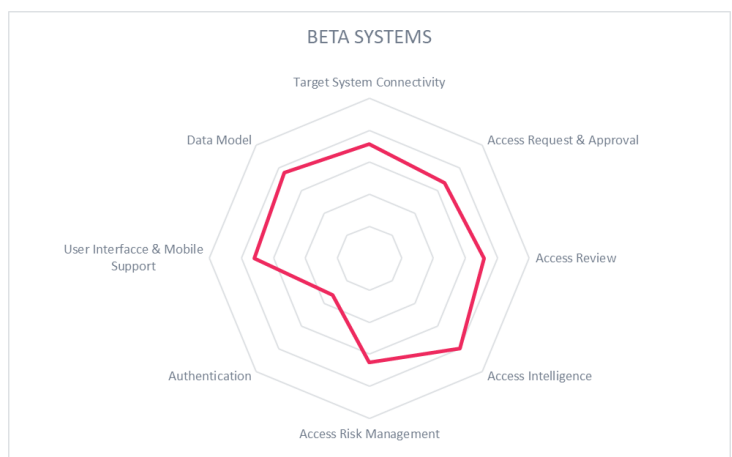
Another strength is their built-in role management capability, which allows for efficient, highly automated assignment of entitlements. The Access Intelligence module is tightly integrated with the OEM workflow management component available as an OEM component within its Identity Manager product.

Beta Systems is one of the very few vendors that offers a fixed-price implementation of its offering within defined environments and connecting to a defined set of target systems. This is a sufficient proof of their ability to rapidly deploy the product and their expertise in the market.

Security	strong positive
Functionality	positive
Integration	neutral
Interoperability	positive
Usability	positive

Table 6: Beta Systems rating

Overall, Beta Systems' Garancy Access Intelligence Manager along with other components delivers a product with rapidly evolving access governance capabilities. Beta Systems has decent presence in major markets and a small, but effective partner ecosystem in addition to a strong professional services unit.



5.3 Brainwave

Brainwave, based in France, is a relatively new entrant in the market. Founded in 2010, the company offers Brainwave Identity GRC as its primary identity provisioning and access governance product. It uses tightly integrated BIRT analytics engine at the backend for identity analytics and access intelligence capabilities. Reporting is also available through integrated BIRT's BI reporting tool. Brainwave offers a java-based access intelligence platform that is flexible and easy to customize. With a good line-up of SOD checks in place for applications with complex authorization models, Brainwave is a preferred product for small to mid-sized organizations that require flexibility to tailor workflows for internal business processes.

Strengths	Challenges
<ul style="list-style-type: none"> Flexible and easy customization Integrated SOD checks within role management Risk-based approach to governance Available integrations with prominent market players 	<ul style="list-style-type: none"> Crude but flexible user interface Growing but limited market presence outside EU A regionally confined partner ecosystem

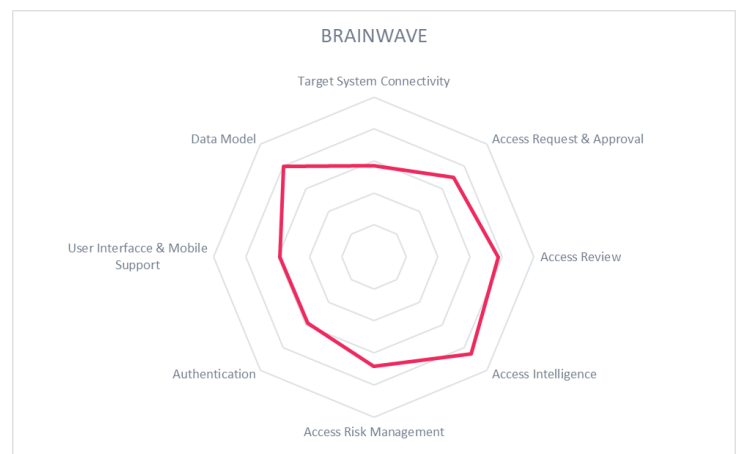
Table 7: Brainwave's major strengths and challenges

Brainwave offers a flexible risk-based approach to access intelligence that involves significant development and integration efforts at an organization's end. The workflow and policy management including configuration is offered through integrated Activiti BPM engine. It supports access intelligence features based on integrated BIRT analytics engine and can therefore cut analytics and reporting through unstructured data based on risk classification. Built on the OpenICF connector framework, it offers the flexibility for customers who demand customization of connectors based on identity attributes. Ability to support SOAP and RESTful APIs allow for extending access intelligence capabilities beyond on-premises systems to SaaS applications and other cloud platforms. This also 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.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 8: Brainwave rating

Heavily reliant on open-source platforms, Brainwave can require significant developmental 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 decision for open-source technology adoption to build an access governance platform.



5.4 CA Technologies

CA Technologies is among the largest infrastructure software vendors worldwide and offers a broad portfolio of products in the IAM market segment, including CA Identity Governance as its primary offering for access governance. Offering a range of access governance features, CA Identity Governance is a standalone product that integrates well within its identity portfolio

Strengths	Challenges
<ul style="list-style-type: none"> Feature-rich, , integrates well within CA Identity Suite Scalable and strong DevOps support OOB support for a broad range of systems and cloud applications Large global customer base Modernized, leading-edge UI Strong engineering and technical support 	<ul style="list-style-type: none"> Customizations can be complex and expensive Leans towards a closed vendor ecosystem A costly ordeal for SMBs, most product features would remain unutilized for normal deployments

Table 9: CA major strengths and challenges

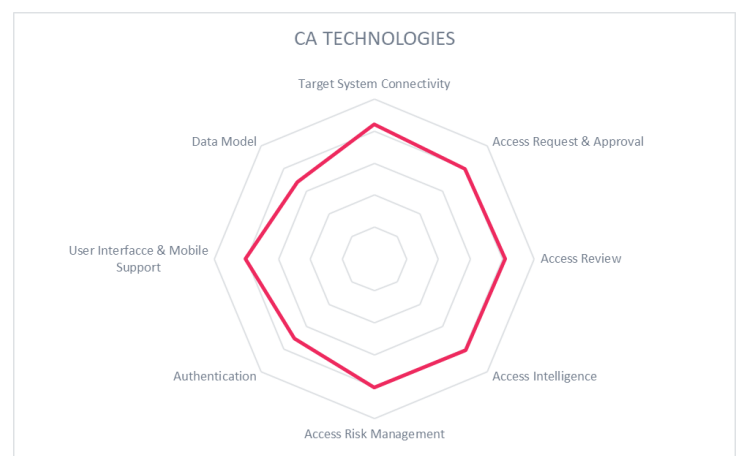
Based on the long history of the product and the market position of CA Technologies, it is no surprise that CA has several large deployments of CA Identity Governance globally. The product, fully capable of operating in silo, offers a strong line-up of access governance capabilities ranging from workflow and policy management to role management, access certification and access intelligence. Scalable by design, CA Identity Governance now offers a rapid deployment approach using DevOps policies to ease lengthy and complex product upgrades and environment releases. The overall complexity of product deployment and configuration can be a challenge for customers looking for basic access governance features. Use of separate identity repositories within CA Identity Manager and Identity Governance products reportedly leads to issues with continuous asset and attribute sync. The latest product release is based on a virtual appliance approach and is aimed at reducing installation time as well as making product upgrades easier than in past by encapsulating all the components in a virtual image thereby partly eliminating the issues with separate data stores and latency with attribute sync. While it offers support for SOD compliant provisioning, comprehensive SOD risk analysis of existing roles and access entitlements is not supported.

Support for REST and SOAP APIs enables CA Identity Governance to extend governance capabilities to SaaS applications and other cloud platforms.

Real-time analytics and machine learning offer strong access intelligence capabilities necessary for detailed risk analysis and process optimization.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 10: CA rating



Overall, CA Identity Governance is a mature and feature-rich product. CA Technologies has a global presence, but a relatively smaller number of specialized integration partners as compared to other global IAM suite vendors; however, the company has its own service offerings on a global scale.

5.5 E-Trust

E-Trust, based in Brazil, offers Horacius Identity & Governance as the common platform for identity provisioning and access governance. Also available as SaaS delivery, Horacius platform has grown overtime to be a mature product offering a spectrum of access governance functionalities. With focus on identity lifecycle management, Horacius offers a basic set of identity provisioning connectors for commonplace enterprise applications and systems, extensible for webservices using its SOA connector.

Strengths	Challenges
<ul style="list-style-type: none"> • Good identity provisioning feature set • SOA connector framework • Integrated incident management • Moderate data access governance capabilities 	<ul style="list-style-type: none"> • Limited cross-platform governance support • Lack of access intelligence capabilities • Smaller partner ecosystem mostly concentrated in South America

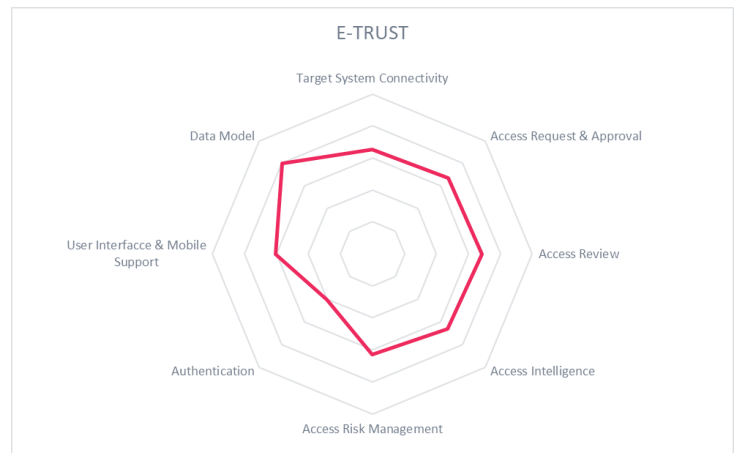
Table 11: E-Trust major strengths and challenges

E-Trust has gained some good momentum over the last few years in the identity provisioning space. Horacius Lifecycle Manager offers identity provisioning and workflow management capabilities with most basis set of connectors. Access governance include a governance platform, a compliance manager and a report manager. The governance platform module centralizes role and policy management to offer risk scoring to initiate compliance activities and lifecycle management events, while the compliance manager is responsible for access certification and policy enforcement. Access intelligence is generic and mostly dependent on reporting through the report manager component with built-in support for Microsoft PowerBI as the primary identity data analysis and reporting tool to generate on-demand reports.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 12: E-Trust rating

E-Trust is primarily an entry-level identity provisioning tool for organizations with average access governance requirements to satisfy most common identity lifecycle administration use-cases. Its customer base is concentrated in South America but is fast gaining foothold in other geographies with its simplistic approach to identity provisioning and access governance.



5.6 EmpowerID

EmpowerID, based in Ohio (US), offers EmpowerID as its primary identity provisioning and access governance product. Built on Microsoft technology, EmpowerID offers distinct integration and performance benefits for Microsoft centric organizations. Its access governance capabilities are sound but limited to common governance scenarios including role management, access certification and auditing and reporting. With separate modules for role management and access certification viz. Role Mining Manager and Compliance Manager respectively, EmpowerID supports identity analytics with built-in reporting and a risk engine to calculate risk associated with users and roles.

Strengths	Challenges
<ul style="list-style-type: none"> Strong role management and access certification capabilities Easy and flexible policy and workflow management Strong data access governance capabilities for windows environment Strong Identity Provisioning feature set 	<ul style="list-style-type: none"> Runs primarily on Microsoft platform Lack of access intelligence capabilities Smaller but selective partner ecosystem mostly concentrated across Europe

Table 13: EmpowerID major strengths and challenges

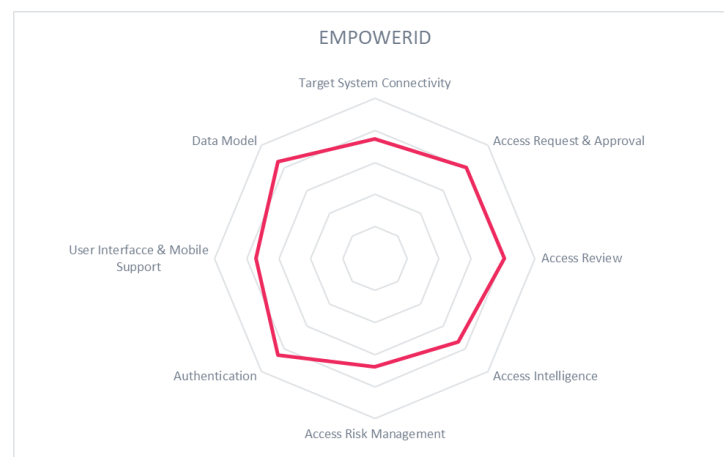
Customization of EmpowerID is very flexible, based on the architectural approach chosen by them. The product runs on the Microsoft infrastructure, which might turn out be a challenge for some companies. It delivers strong features for basic access governance scenarios in a windows environment including robust data access governance, role and group management, access certification and auditing and reporting. With missing XACML support, dynamic authorization management could be a challenge. However, support for RESTful 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 privilege management capabilities offers unique advantages over its competitors.

However, the product also delivers a broad functionality for basic Identity Provisioning requirements. We have seen a lot of progress in that area with an increased number of connectors and a very large number of out-of-the-box workflows that allow for rapid deployments.

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 14: EmpowerID rating

Overall, EmpowerID offers a comprehensive solution with strong identity provisioning and access management capabilities. Access governance features are limited but well supported on windows platform. EmpowerID makes a preferred choice of vendor for Microsoft oriented organizations looking for strong access management features with basic access governance capabilities.



5.7 Evidian

Evidian, based in France, is part of Atos which is one of the leading IT service providers in Europe. Evidian has been in the IAM business for many years. Their product, Evidian Identity Governance and Administration offers basic access governance in addition to mature identity provisioning capabilities. Evidian Analytics and Intelligence is a new launch to cater to increasing requirements of advanced access governance. Evidian Identity Governance and Administration ingests the components derived from the former Siemens DirX portfolio, which is now owned by Atos. The solution goes beyond identity provisioning and access governance to offer an integrated approach to core IAM requirements.

Strengths	Challenges
<ul style="list-style-type: none"> Established and feature-rich product sets for identity provisioning and access governance Comprehensive suite offering includes access management capabilities ATOS acquisition helps to extend global network and reach to large customers Availability as multi-tenant cloud offering 	<ul style="list-style-type: none"> Lack of full access certification capabilities Limited access intelligence capabilities Rigid reporting and dashboarding capabilities Limited scalability Limited global presence with customer base concentrated in Europe

Table 15: Evidian major strengths and challenges

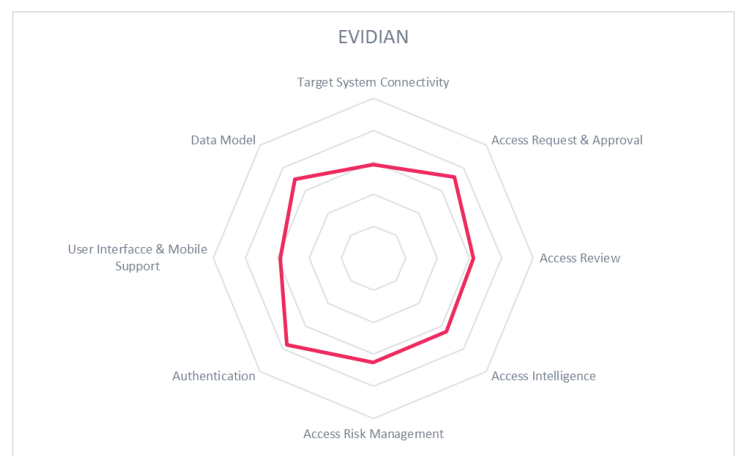
Evidian delivers an integrated IAM product which covers all major aspects of identity provisioning and access governance. It is focused on providing a consistent set of processes for users. Besides the core provisioning capability, the product is tightly integrated with the SSO (Single Sign-On) and Access Management solutions offered by Evidian. The workflow and policy management can be complex to configure for common governance scenarios. Basic access certification is supported but event-based, continuous and delta certification capabilities are missing. Advanced role management, particularly role mining could be a challenge. Access intelligence has been available through custom reporting, but the new product release of Evidian Analytics and Intelligence should address this gap while offering other access intelligence features.

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. The product also includes its own IT Service Management capabilities eliminating the need to integrate with third-party ITSM systems. In addition to basic SOD support, there is built-in support available for Dynamic Authorization Management.

Security	strong positive
Functionality	positive
Integration	neutral
Interoperability	positive
Usability	positive

Table 16: Evidian rating

Overall, Evidian delivers moderate access governance capabilities, making an interesting alternative to the leading 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.



5.8 Fischer International Identity

Fischer International offers Fischer Identity Suite comprising of several modules available as a bundled offering. Its primary module responsible for access governance is Governance and Compliance, combined with Role and Account Management. While the product is also available for on-premise deployment, the entire architecture has been defined for optimally supporting SaaS deployments, requiring only a gateway at the customer's site. This approach also suits well for on-premise deployments, giving Fischer a head-start for cloud-based deployments, having, for example, full multi-tenancy support as a logical design principle.

Strengths	Challenges
<ul style="list-style-type: none"> • Complete range of IAM capabilities in addition to basic identity provisioning and access governance • Easy to deploy and configure for basic identity tasks • Well-defined user interfaces for quick-start deployments • Cost effective delivering fair value for money • Strong multi-tenancy support 	<ul style="list-style-type: none"> • A limited set of connectors, sufficient for specific industry verticals • Workflow and policy management, though easy to configure, lack depth of functionality • Role management is basic with no support for role mining, role governance and SOD controls • Minimal access intelligence – no analytics and rigid reporting • Heavy customer focus on education vertical impedes cross industry growth

Table 17: Fischer International major strengths and challenges

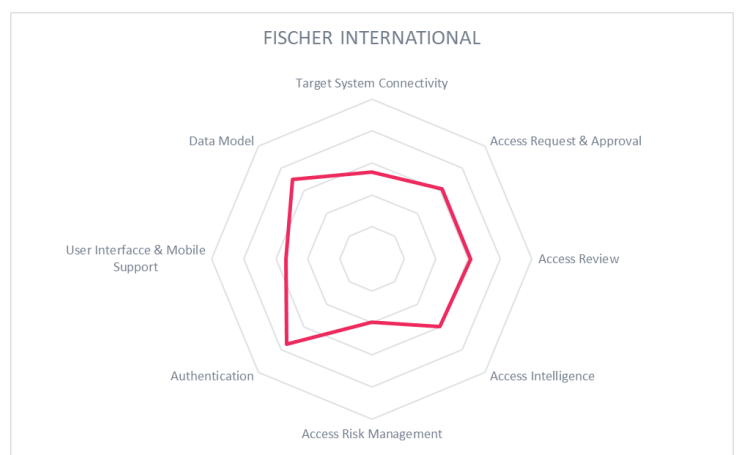
With its SaaS-ready design approach, the focus is on providing a broad set of features with standard configurations to avoid programming. There is minimal need of coding for basic scenarios, but often intensive configuration is required for advanced use-cases. Fischer has a good strategy for integration, supporting both an ETL-based approach and RESTful APIs.

Role management is adequate for identity provisioning but doesn't meet access governance criteria of role mining and governance. Access intelligence capabilities are absent with very basic and inflexible reporting used for analytics purposes. The partner ecosystem of Fischer is still somewhat limited in size but growing and based on a few global, engaged partners.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 18: Fischer International rating

Overall, Fischer provides an interesting approach to basic access governance which might not suit the needs of every customer but is suitable for small to medium sized organizations looking to kick start their identity management program with bundled features at a reasonable price. On the other hand, customization is straightforward, and the product focuses on avoiding any coding at all.



5.9 Hitachi ID

Hitachi ID provides a product named Identity Manager, which is a mature solution for managing identities and their access. It integrates access governance features, including SoD (Segregation of Duties) support and certification features. The product builds on an open, flexible architecture that also builds the foundation of other Hitachi ID IAM products. Hitachi ID provides a well-defined model for segregation of code and customizations, allowing the retention of customizations when applying release changes. However, managing changes between development, test, and production requires extracting and applying XML files from a separate revision control system.

Strengths	Challenges
<ul style="list-style-type: none"> • Broader IAM offering beyond standard access governance capabilities • Mature solution with broad connector support • Flexible workflow and policy management • Support for Active Directory Group Management 	<ul style="list-style-type: none"> • Robust but unfriendly end-user interface • Limited access intelligence capabilities • Limited footprint outside of North America • Relatively smaller partner ecosystem

Table 19: Hitachi ID major strengths and challenges

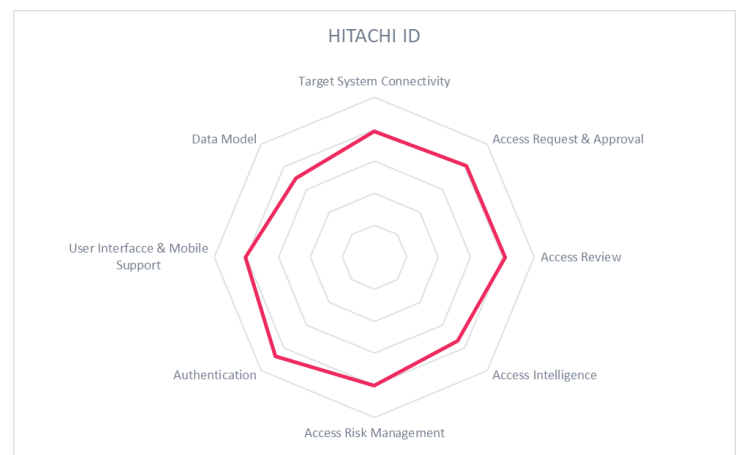
In general, the product provides a mature set of features, delivering what customers typically need. It delivers a large set of connectors. The architecture provides high flexibility and scalability and is well-thought out. There are several unique features available, plus good interoperability. Hitachi-ID also has improved the user interface, adding a variety of new capabilities. Access governance is moderately strong with flexible workflow and policy management capabilities which can support complex governance use-cases. Access intelligence, however, is heavily reliant on reporting with a wide range of built-in reports available but custom reports require additional development effort.

Other strengths of Hitachi Identity Manager include integration with Microsoft SharePoint and Windows Explorer, allowing users to directly request access to resources from these environments. The product also supports Active Directory group management

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 20: Hitachi ID rating

Overall, Hitachi ID Management Suite is an interesting 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 identity provisioning but modest access governance capabilities. The vendor still has a limited but growing footprint outside of North America and Canada.



5.10 IBM

IBM Security Identity Governance & Intelligence (ISIGI) is the successor of former 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 four years back into ISIGI and added some features to further enhance these. IBM has a very large install base, ranging amongst the top 5 vendors in the market worldwide from that aspect.

Strengths	Challenges
<ul style="list-style-type: none"> • Mature product with strong support for standard access governance capabilities • Wide range of OOB connectors • Strong support for SOD Controls • Significantly modernized by integrating into ISIGI 	<ul style="list-style-type: none"> • Complex product deployment and integration • Multi-tenancy requires multiple instances, but partners provide fully multi-tenant implementations • Early integrations tend to focus on IBM's own product portfolio, delaying integrations with other popular platforms • Lack of focus on mid-market segment

Table 21: IBM major strengths and challenges

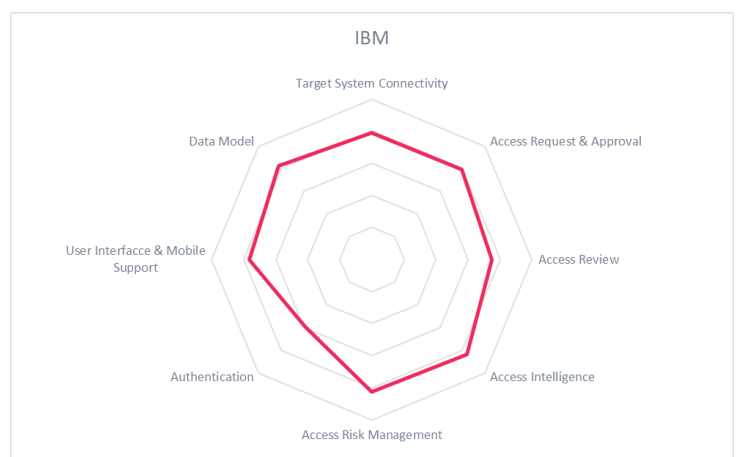
IBM Security Identity Governance & Intelligence builds on an established product supporting a broad range of different target systems with deep integration. IBM has greatly improved the usability and user interface recently, providing a good and well-integrated product now. ISIGI also provides full access governance capabilities, including support for role management and enhanced workflow capabilities. The product supports multi-tenancy for end users, but full multitenancy requires multiple instance deployments.

IBM always has been strong on the connector side, providing a wide range of connectors to virtually all types of target systems. In addition, 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.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 22: IBM rating

Overall, IBM Security Identity Governance & Intelligence is a mature offering that has undergone significant updates over last few years. It counts amongst the products that have seen the strongest evolution over the past years, making it a very competitive and interesting offering in this market. IBM also benefits from its own strong professional services and excellent partner ecosystem, plus the integration with the overall IBM Security product portfolio.



5.11 Micro Focus

UK based Micro Focus offers Identity Governance as its primary product for access governance capabilities which integrates well with Identity Manager. Micro Focus had been executing a major 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, however yet to be confirmed, are believed to offer a comprehensive security portfolio with a stronger focus on integrated IAM technologies and boost its market presence with strong HPE professional services around the globe. Micro Focus Identity Governance product offers a good range of access governance capabilities from flexible workflow and policy management to enhanced user activity reporting.

Strengths	Challenges
<ul style="list-style-type: none"> • Very large customer base and ecosystem • Strong, mature functionality covering all major aspects of identity provisioning and access governance • Flexible and scalable product architecture • Strong support for a variety of target systems • Strong support for role mining and access intelligence capabilities 	<ul style="list-style-type: none"> • Rich functionality sometimes complex to understand

Table 23: Micro Focus major strengths and challenges

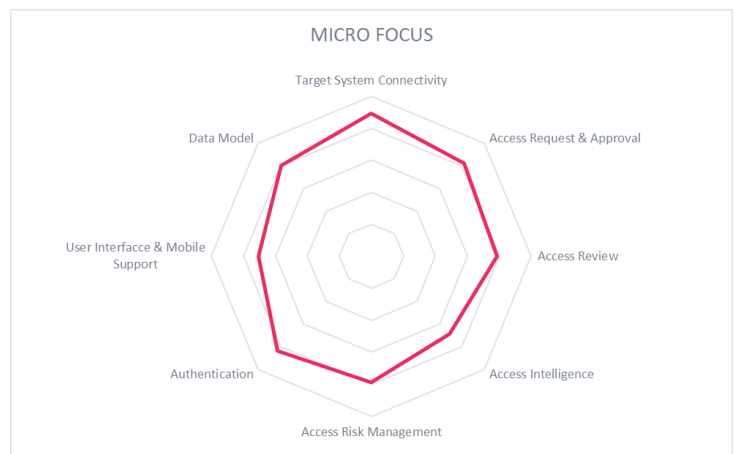
Micro Focus Identity Governance is an enhanced governance product offering mature and comprehensive capabilities with some functionality overlap to Identity Manager. Its flexible approach for workflow and policy management based on the designer tool is still widely unmatched in the industry, allowing for an 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.

The product covers almost all of the access governance features we consider instrumental for a comprehensive access governance product.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 24: Micro Focus rating

Overall, Identity Governance from Micro Focus remains a leading-edge product in the access governance market segment with its broad, mature and evolving functionality. Micro Focus also builds on an excellent partner ecosystem across the globe.



5.12 Nexis

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

Strengths	Challenges
<ul style="list-style-type: none"> • Innovative risk-based approach to role governance • Cuts through majority of access governance use-cases • Integrated SOD Controls and DAG capabilities • Hardened appliance speeds up deployment and eliminates software-based security vulnerabilities 	<ul style="list-style-type: none"> • Lack of strong identity provisioning capabilities • Limited scalability due to in-built DB component • Limited set of OOB target system connectors • Small but growing partner ecosystem • Limited presence outside of DACH region

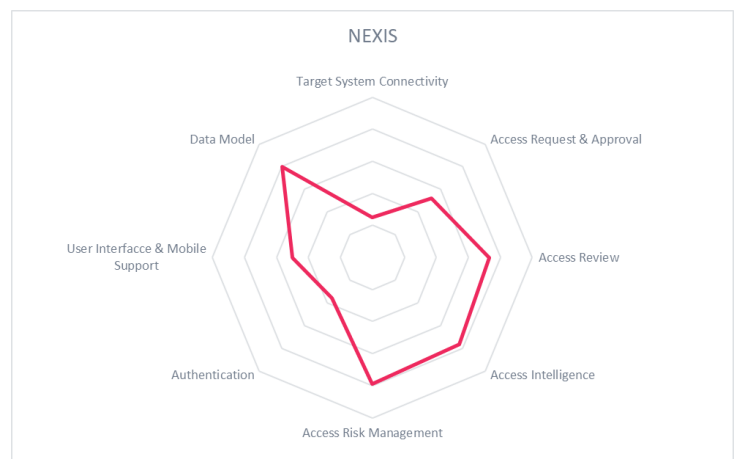
Table 25: Nexis major strengths and challenges

Nexis is one of the very few vendors that have a more mature access governance portfolio than identity provisioning. Controle offers a broad range of access governance capabilities ranging from innovative role engineering to risk-based analytics for entitlement provisioning and role mining. With common auditing and reporting capabilities, there's good support available for schema extensions and workflow customizations. Due to capacity constraints of in-built components in an appliance-based delivery model, scalability can be a challenge.

Security	neutral
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 26: Nexis rating

Nexis offers a great add-on for organizations with an existing identity provisioning tool that lacks access governance. With advanced role governance features, it makes an excellent choice for organizations that require role engineering or cleanup and prefer a quick deployment approach. Organizations that have a priority for hardware-based appliances for security reasons, particularly in highly regulated industries such as banking and telecom should evaluate Nexis. Company should strongly consider a more flexible delivery option including cloud-based service and building on its brand awareness as well as partnerships outside of the home region.



5.13 Omada

Omada, a Danish vendor, provides the Omada Identity Suite as integrated access governance and identity provisioning product. Omada focuses on making generic IGA functions such as workflow and policy management, certifications etc. more adaptable, business-centric and collaborative. It offers strong role governance, activity reporting as well as compliance and application management. During the last few years, Omada has executed a major shift in its product strategy by adding its own identity provisioning layer, instead of solely relying on integration with Microsoft Identity Manager (MIM). With that, Omada today competes in the pure-play identity provisioning market along with access governance and IGA markets.

Strengths	Challenges
<ul style="list-style-type: none"> • Mature solution with strong workflow and role management capability • Efficient approach for onboarding new applications • Good SAP connectivity features • Effective Microsoft Identity Manager governance 	<ul style="list-style-type: none"> • Good but not leading-edge support of out-of-the-box connectors • No out-of-the-box integration with Service Request Management (SRM) systems, but experience from custom integrations

Table 27: Omada major strengths and challenges

Omada Identity Suite has undergone major changes over the past few years. In addition to adding its own identity provisioning layer and removing the former dependency on Microsoft Identity Manager, Omada has re-architected the solution by changing the data model to be more flexible and massively enhancing scalability. Also, the UIs have undergone major modernization.

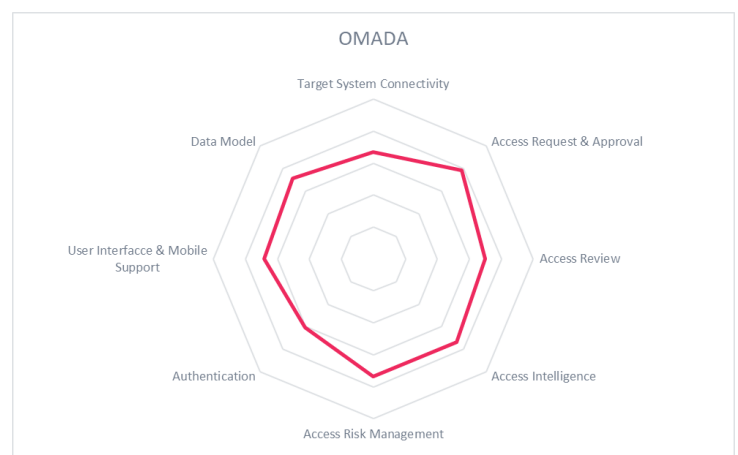
OIS delivers access governance with several in-built modules including a Role & Policy engine, Survey and Attestation engine, SOD module and a BI module for reporting and analytics – all combined in one platform. OIS leverages SSIS (SQL Server Integration Services) for custom extension of metadata and OOB connectors. It also extensively leverages SQL Server Reporting Services (SSRS) and SQL Server BI components for reporting and analytics. Built on a .NET framework, OIS has an easy deployment and configuration model but any customizations require specialized .NET programming and MS SQL expertise.

Omada shows its full strength in environments that look for both identity provisioning and access governance capabilities. It also remains an interesting option for extending Microsoft Identity Manager deployments.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 28: Omada rating

Overall, Omada Identity Suite is a very interesting solution for enterprise customers that have a need to build a governance layer on top of their Microsoft Identity Manager implementations. It has become a strong contender for the identity provisioning and access governance market segment, based on the additions Omada has done in recent years.



5.14 One Identity

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 came into the Quest portfolio through the acquisition of a German vendor Völcker Informatik, remains the core product of One Identity's IAM portfolio. One Identity Manager builds on a sophisticated, consistent concept which 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 range 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.

Strengths	Challenges
<ul style="list-style-type: none"> • Innovative, user-friendly interfaces • Strong sales and marketing execution • Very good connector support and excellent depth of integration to target systems, particularly SAP • Integrates well with its access management and privilege management capabilities • Advanced role management with strong SOD support 	<ul style="list-style-type: none"> • Process-driven approach requires some training, but is highly efficient • Inconsistent transition path and messaging for existing Dell-Quest customers • A limited but growing professional services network

Table 29: One Identity major strengths and challenges

The product is designed with some rather uncommon but useful features. While the shopping cart approach for access request has become increasingly common, features such as the ability to simulate effect of changes to access entitlements or role definitions remain fairly unique. Customizations are straightforward, mainly done through policy configurations and workflow extensions. The flexibility regarding customization and the product architecture have been greatly improved over the past few years. Cloud delivered One Identity Starling is their recent addition that offers Identity Analytics and Risk Intelligence to complement its existing access governance capabilities.

In addition, One Identity has made significant enhancements to the functional capabilities of the product to establish itself amongst the leaders in the market. The number of connectors has grown to offer one of the largest connector base. There is a broad support available for Data access governance through the Data Governance Edition.

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 30: One Identity rating

Overall the product is amongst the most interesting and intriguing offerings in the identity provisioning and access governance markets. It gets a clear recommendation for evaluation in product selections.



5.15 Oracle

Oracle Identity Governance (OIG) Suite is the on premise offering within Oracle's IAM portfolio. It includes Oracle Identity Analytics (OIA), which offers access governance capabilities but relies on integration with OIM (Oracle Identity Manager) for delivering capabilities across the access governance spectrum. Several IGA and particularly access governance capabilities have been significantly improved in the 11g R2 release, especially the integration of modules along with the ease of their deployment. With an improved integration strategy, Oracle attempts to eliminate the overlap of several functionalities that existed in previous versions. Oracle remains a preferred vendor for organizations that have substantial investment in Oracle Fusion Middleware and require high flexibility for customizations to accommodate complex business processes.

Strengths	Challenges
<ul style="list-style-type: none"> • Mature, feature-rich product focused on identity provisioning • Significant improvements for deployment and customization • Very broad support for different environments and enterprise-level architectures • Global customer base with strong channel partner network 	<ul style="list-style-type: none"> • Long and complex product deployment and upgrade cycles • Depending on use cases, there exist some dependencies between various components of the Oracle IAM portfolio; however, for identity provisioning only when adaptive authentication is required

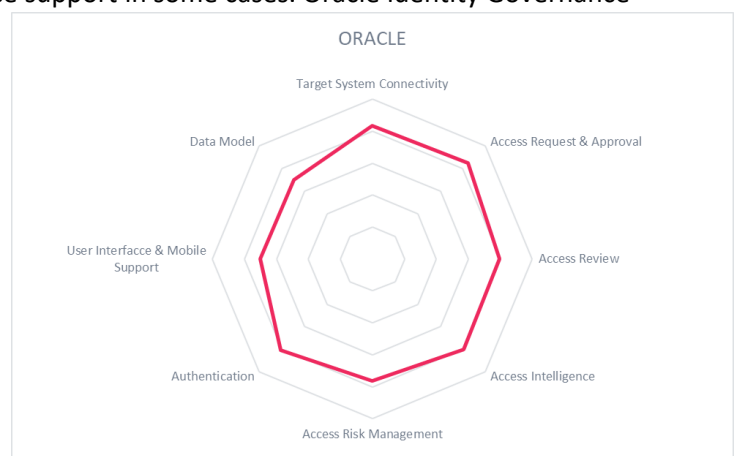
Table 31: Oracle major strengths and challenges

Oracle delivers mature identity provisioning capabilities, including a broad set of connectors to a wide variety of on premises systems, business applications as well as SaaS applications. Recent product releases bring several important and useful changes including an extensible data model and API enablement to make the product more agile. 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. Given that few connectors are still offered by third parties leads to issues regarding implementation and maintenance support in some cases. 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.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 32: Oracle rating

Overall, Oracle Identity Governance Suite counts amongst the leading products in the access governance market. It provides a broad set of features focused on identity provisioning and access governance with good support for enterprise-level architectures, including external workflow systems. OIG makes an excellent choice for large implementations requiring scalability and flexibility to support complex IAM scenarios.



5.16 Pirean

Pirean is a UK-based software company that is not yet well-known outside of their home market but shows strong potential. Their Access:One offering combines a variety of capabilities, from identity provisioning for the workforce to strong user self-service capabilities leading to support common CIAM (Consumer IAM) use cases, including authentication and SSO capabilities.

Strengths	Challenges
<ul style="list-style-type: none"> Well-architected and well-integrated IAM suite Strong support for use cases beyond workforce IAM Strong self-service interfaces Modern UI 	<ul style="list-style-type: none"> Still relatively small vendor, limited visibility outside of UK, but expanding to APAC and Central Europe Weak marketing messaging and sales support Lack of SOD controls and access intelligence features Still small partner ecosystem on global scale Good but not leading-edge connector framework

Table 33: Pirean major strengths and challenges

While most identity provisioning tools remain primarily focused on employees and contractors, the focus of Pirean Access:One is providing a unified platform across all types of identities, from the employee to the consumer and, in B2G (Business to Government) use cases. That sets them apart from most other offerings in the market.

From a feature perspective, Pirean Access:One is feature rich with respect to the core identity provisioning capabilities but limited access governance features. It comes with a modern UI including mobile apps, a broad range of self-service interfaces and flexible workflow management. Pirean offers limited role governance and access intelligence capabilities with basic auditing and reporting capabilities.

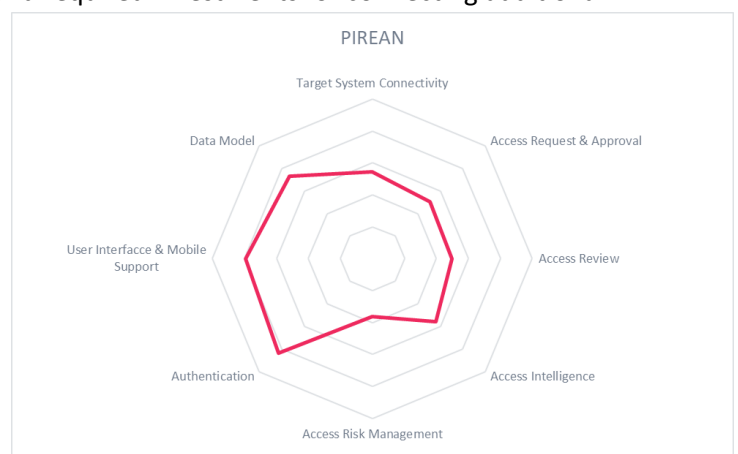
The set of connectors is sufficiently broad covering the most common systems including several SaaS applications. Its ability to support access governance in customer environments must be carefully evaluated to understand the existing challenges and required investments for connecting additional systems.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 34: Pirean rating

With moderate identity provisioning and lifecycle management support, Pirean makes a good choice for small to mid-sized IAM deployments that have a need for managing consumer identities with common access

management requirements including authentication and SSO. Their biggest challenge remains minimal access governance and a lack of visibility outside of the UK with a small partner ecosystem. Pirean is investing to grow in APAC and EMEA regions, however, due to their specific strengths for consumer identity use-cases, we recommend considering Pirean in evaluations.



5.17 RSA

RSA, a leading provider of security solutions, offers RSA Identity Governance and Lifecycle as its combined offering for both identity provisioning and access governance. Built on Aveksa IAG platform, RSA Identity Governance and Lifecycle is the new and enhanced version of RSA Identity Manager and Governance. RSA IGL takes a risk-based business friendly approach to access governance. With a broad range of target system connectors, RSA IGL works in conjunction with RSA Archer GRC solution to consume user and policy metrics to dynamically determine application risk-ratings which in turn influence request and approval workflows to drive access governance.

Strengths

- Strong risk-based access governance
- Offers cloud-based delivery under MyAccessLive brand
- Integration with RSA Archer GRC, NetWitness and SecurID Access
- User-friendly interfaces
- Well functioning strong partner ecosystem
- Global presence across all industry verticals

Challenges

- Effects of recent acquisitions and spun-offs with EMC and then Dell on product strategy is unclear
- Limited flexibility, customizations can be complex

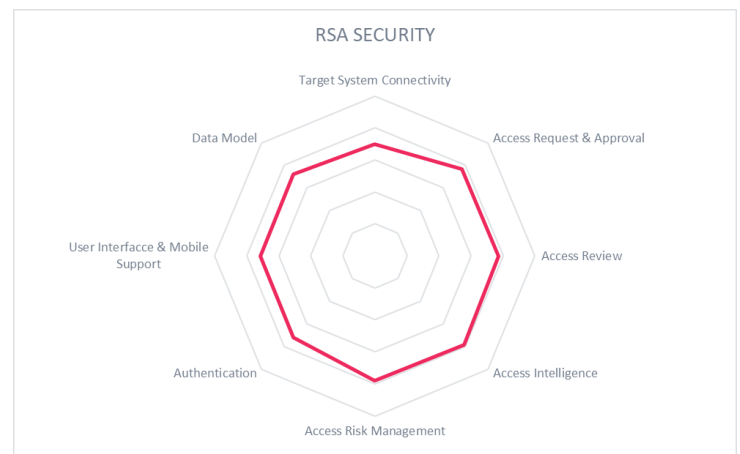
Table 35: RSA major strengths and challenges

RSA IGL offers strong policy and role management capabilities due to support for granular entitlements with extensive role meta-data. Custom extensions to metadata, however, can be complex and not recommended. Tight integrations with RSA Archer GRC and NetWitness enables risk-based monitoring and event detection and response in real time. RSA IGL also offers easy integration with RSA SecurID Access Suite to deliver integrated access management capabilities for its customers.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	positive

Table 36: RSA rating

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. RSA IGL makes an excellent choice for organizations that have existing deployments of RSA security products and require identity automation and heavy access governance without much customizations.



5.18 SailPoint

SailPoint originally started as a vendor specialized in access governance. However, since 2010 they have made strategic personnel and technology investments in the identity provisioning market that have accelerated the capabilities of their flagship product, IdentityIQ. The SailPoint IdentityIQ product now is a solution that integrates access governance and identity provisioning capabilities into a single product, i.e. a full IGA solution. SailPoint has enhanced its provisioning support massively over the past years.

Strengths	Challenges
<ul style="list-style-type: none"> • Strong integrated identity provisioning and access governance capabilities • Integration capabilities with other provisioning systems and SRM out-of-the-box • User-friendly interfaces • Strong and effective governance focused marketing messaging • A large and effective channel partner network 	<ul style="list-style-type: none"> • Lack of SOD controls • Lack of focus on mid-market segment • No multi-tenancy support, but provides separate multi-tenant cloud solution IdentityNow

Table 37: SailPoint major strengths and challenges

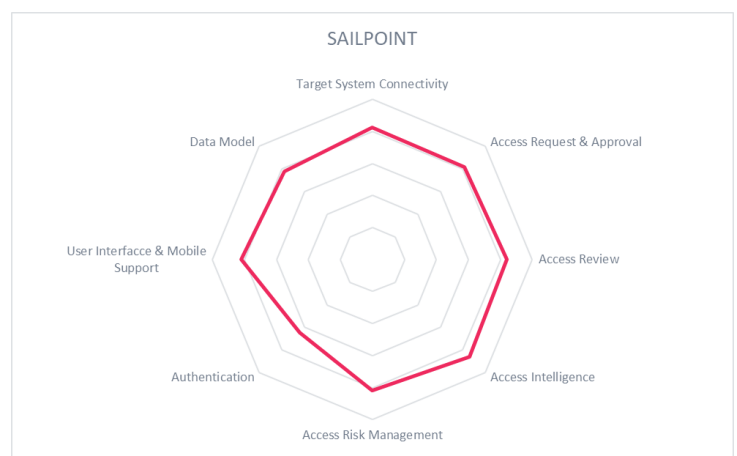
Due to its origin in the access governance market, the IdentityIQ user interfaces are geared towards business users. The approach in general is very much business-driven and less technology-focused than what some of the “classical” vendors in that market provide. The user interfaces are quite flexible and configurable.

With strong role governance and access intelligence capabilities, SailPoint has made significant progress to build stronger identity provisioning capabilities. 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. Their recent partnership with Okta will help SailPoint to leverage Okta’s access management capabilities for cross-sell opportunities. SailPoint also partners with Microsoft to offer access governance capabilities currently absent in MIM (Microsoft Identity Manger). Among the shortcomings is the lack of multi-tenancy support.

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	strong positive

Table 38: SailPoint rating

SailPoint has been a leading-edge vendor in the access governance market. They provide a feature-rich and increasingly mature solution. In addition, they have built an excellent support for identity provisioning capabilities as part of the offering. SailPoint’s early recognition for 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 access governance.



5.19 SAP

SAP has established a considerable IAM portfolio over the past years and its recent acquisition of Gigya shows its continued commitment to grow and compete in the space. It consists of both on premises tools and cloud services. Access governance capabilities are delivered primarily through the SAP Access Control suite in conjunction with its flagship identity provisioning product, SAP Identity Manager. SAP Identity Manager is well-integrated with SAP Access Control and SAP Business Suite to provide excellent access governance capabilities for SAP as well as other applications.

Strengths	Challenges
<ul style="list-style-type: none"> • Excellent integration into SAP environments, including SAP access control • Strong identity provisioning feature set • Integrates identity virtualization • Good role management capabilities 	<ul style="list-style-type: none"> • Strong connectors for many systems, but some gaps particularly for non-SAP business applications • Some gaps in baseline access governance, but covered by other SAP offerings • Costly and complex product deployment and upgrades

Table 39: SAP major strengths and challenges

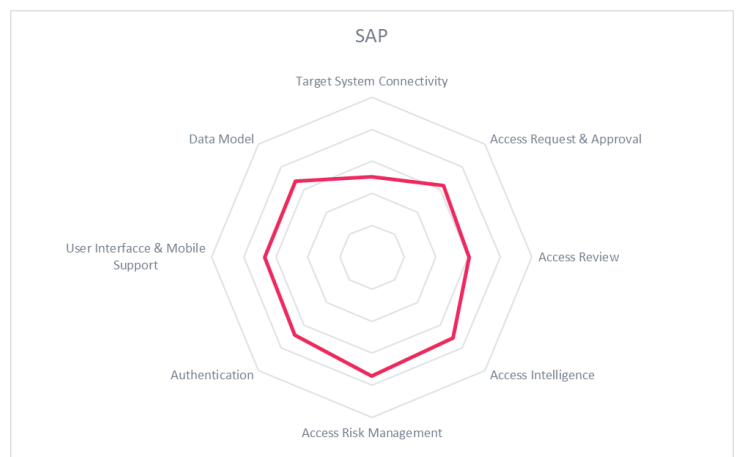
SAP has made significant progress with its SAP Identity Management offering over the past few years, including product re-architecture to expose a comprehensive set of APIs for simplified customization and integration. The product comes with standard access governance capabilities, including flexible workflows, support for automated assignment of entitlements based on roles, approval processes, and self-service functionalities. It also delivers good reporting and auditing capabilities.

One of the challenges is the relatively small set of connectors, when compared to other leading products in the market. While there is good support for common target systems such as LDAP, Microsoft AD and SAP's own products, the support for non-SAP business applications and several other systems for e.g., mainframe systems is lacking. The access governance capabilities are limited to role management and auditing with more complex requirements such as SoD controls served by SAP Access Control. While SAP Access Control has excellent support for role management and access governance across SAP and SAP-like applications with complex role structures, it is often criticized for associated maintenance overheads both in terms of cost and deployment complexity.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 40: SAP rating

SAP remains a leading product in the market with detailed access governance capabilities for SAP and other ERP applications. In its current state, SAP Identity Manager with Access Control suite is a strong contender in the access governance market, particularly for organizations with significant investments in SAP software.



5.20 Saviynt

Saviynt, based in California (US), offers Saviynt Security Manager as its combined offering for identity provisioning and access governance. Relatively a new vendor, Saviynt has quickly established itself as a key player in the market demonstrating timely response to market trends and quality innovation. Saviynt offers a strong lineup of access governance features including risk-based policy and workflow management, role governance, access certification and intelligence across a wide range of applications and infrastructure. Saviynt also offers granular data access governance and cross-application SOD risk management capabilities.

Strengths	Challenges
<ul style="list-style-type: none"> • An innovative integrated risk-based approach to access governance • Strong role engineering and governance • Flexible policy and workflow management • Mature DAG and SOD risk management • OOB integrations with a wide range of SaaS applications • An effective and growing partner ecosystem 	<ul style="list-style-type: none"> • Pricing is in the higher end of the spectrum • Competes against established market players with broader channel reaches • Inconsistent delivery and quality of professional services • Weak brand awareness in regions outside NA

Table 41: Saviynt major strengths and challenges

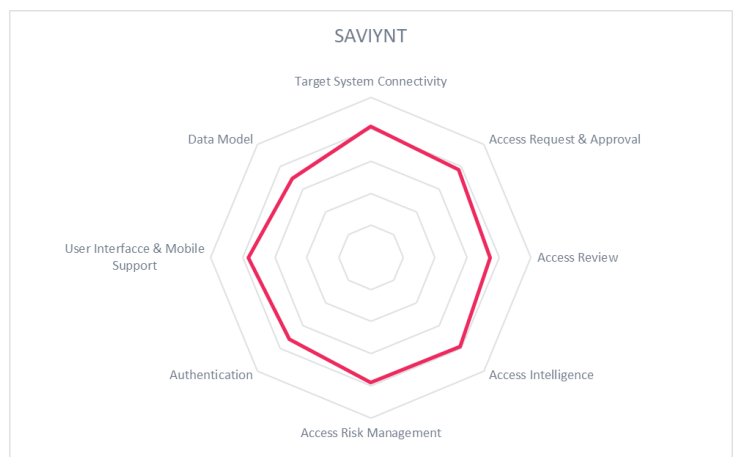
A feature-rich identity provisioning and access governance platform, Saviynt Security Manager offers OOB integration with a broad range of target systems and enterprise applications including SaaS applications. Leveraging on a combination of homegrown and OpenICF connector framework to integrate with target systems, Saviynt offers a Java SDK for connector development. Besides flexible entitlements management enabling effective role governance, Saviynt also offers one of the most comprehensive access certification capabilities in the market. Access intelligence is backed by strong analytics and built-in reporting capabilities. Connector configuration or workflow customizations, however, require specialized development skills in-house or professional services support.

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.

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 42: Saviynt rating

Saviynt with its market responsiveness and strong execution is poised to lead in the identity provisioning and access governance market. Customers looking for an integrated risk-based approach to access governance across the range of on-premise and cloud-based applications should consider evaluating Saviynt. Saviynt has a limited but growing partner ecosystem in APAC and EMEA regions.



5.21 SecureAuth + Core Security

SecureAuth + Core Security, based in Atlanta, is the newly formed entity from the merger of SecureAuth, Courion and SecureReset. Core Security has evolved from supporting specific problems especially around password synchronization to a company offering a suite covering major areas of IAM today. The Core Security Access Insight (AI) is their primary access governance offering which integrates with Core Access Assurance Suite to deliver broader IAM capabilities. From the various products it offers, only the access governance capabilities delivered by Access Insight product along with the Visual Identity Suite's (VIS) Role Designer product and the Core Compliance module from Access Assurance Suite (AAS) are evaluated for its representation in this Leadership Compass.

Strengths	Challenges
<ul style="list-style-type: none"> • Broad support of access governance and identity provisioning capabilities • Innovative, risk-based approach to access governance • Modular but well integrated access governance features • Modern and intuitive UI • Delivers industry contextualized, best practice workflow templates out-of-the-box 	<ul style="list-style-type: none"> • Still limited footprint in the market outside of North America • Lack of integrated workflow and policy management across Access Insight and Access Assurance product suite • Lack of basic SOD controls for risk analysis and compliant provisioning • Heavy focus on healthcare and manufacturing industry verticals constraints growth and market outreach

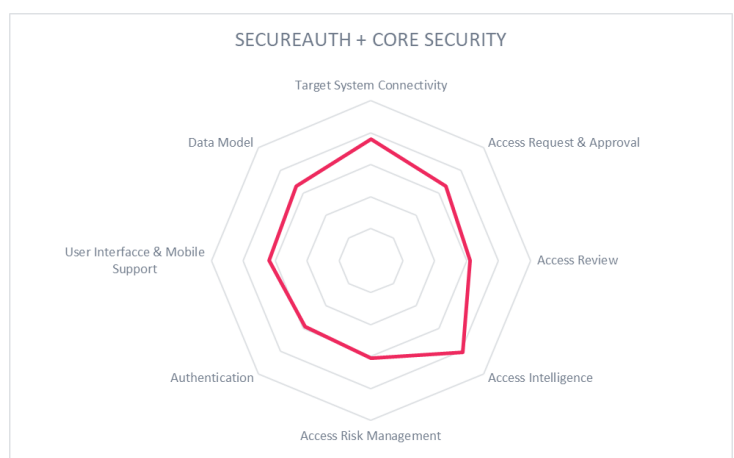
Table 43: SecureAuth + Core Security major strengths and challenges

Access Insight uses an analytics engine to perform predictive analytics on identity and access data gathered from various sources. It offers continuous governance capabilities built upon on-demand micro certifications and an automated policy management by evaluating access risks, used as an aid to make policy decisions in real time. Use of heat maps to visualize identity correlations and access violations enables an interactive view of environment for the business. The VIS Role Designer is a separate product aimed at providing advanced role management capabilities, including role mining and role redesign, which uses data visualization techniques to simplify the Role Based Access Control (RBAC) implementations. The Core Compliance module, a part of Access Assurance, offers access certification and detailed compliance reporting capabilities. However, a lack of SOD controls, integrated remediation workflows and governance support for cloud-based applications can be challenging for some customers.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 44: SecureAuth + Core Security rating

Overall, SecureAuth + Core Security has an innovative and business friendly approach to access governance, offering a range of features. Their major challenge remains a weak partner ecosystem resulting in a limited footprint outside of the North American market. Their existing customer base is mostly composed of healthcare, financial and manufacturing industries limiting cross industry exposure.



5.22 Systancia

Systancia is a France based IT security company that originally started as an identity provisioning provider for healthcare industry. They recently merged with a France based e-SSO (Enterprise Single Sign-On) vendor, Avencis. Systancia offers Hpliance as its identity provisioning product. Recent developments have enhanced the identity provisioning capabilities delivered by Hpliance across the industry verticals and not just limited to the healthcare industry.

Strengths	Challenges
<ul style="list-style-type: none"> • Tight integration with the the Systancia SSOX product for E-SSO • Well thought-out approach to managing access controls of users • Can simulate forthcoming changes • Specific capabilities for the healthcare market 	<ul style="list-style-type: none"> • Connector set is only average, with specific capabilities in healthcare environments • Limited access governance • Limited global reach and still relatively small partner ecosystem

Table 45: Systancia major strengths and challenges

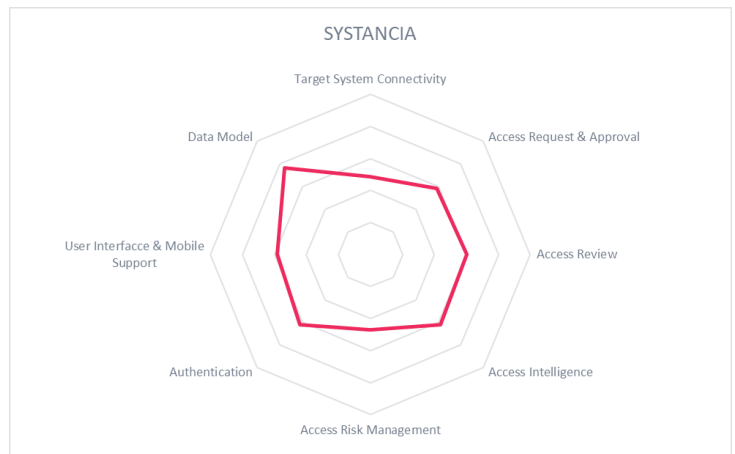
The Hpliance IAM solution has evolved to be a considerably mature offering. It supports the standard requirements in identity provisioning and has a well-thought-out approach to managing entitlements of users. However, the connector set is only average, lacking the breadth compared to its peers. Given that its initial target market had been the healthcare industry, Systancia offers strong support for this industry. The connectors, however, have been adapted to work out equally well for organizations in other industry verticals too. Its workflow capabilities have been expanded to meet the common expectations of the market but still lack support for workflow standards and integration with external workflow tools. Access governance capabilities are currently limited to basic reporting but Systancia is working to develop machine learning for advanced access management and intelligence capabilities at the time of this evaluation.

We see a strong potential for the product through its integration with the SSOX solution, offering the customers authentication and access controls as add-ons.

Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	positive

Table 46: Systancia rating

Systancia has evolved overtime to extend its reach beyond the healthcare industry, for which the solution counts amongst the leading vendors. Given the overall feature set of the product, it offers good potential for deployments within other industry verticals as well.



5.23 Tools4ever

Tools4ever is a Dutch software company that started in the SMB market segment but has grown its portfolio to a level where it can also serve the IAM requirements of larger organizations. Their main offering for identity provisioning is Identity & Access Manager, which covers the major features we expect to see in this market segment.

Strengths	Challenges
<ul style="list-style-type: none"> Lean solution for identity provisioning Overall good feature set Well-thought-out approach for delegating tasks to service desks Good baseline support for access governance 	<ul style="list-style-type: none"> Small vendor with limited partner ecosystem Good, but not leading-edge set of connectors, but straightforward customization based on standard connectors

Table 47: Tools4ever major strengths and challenges

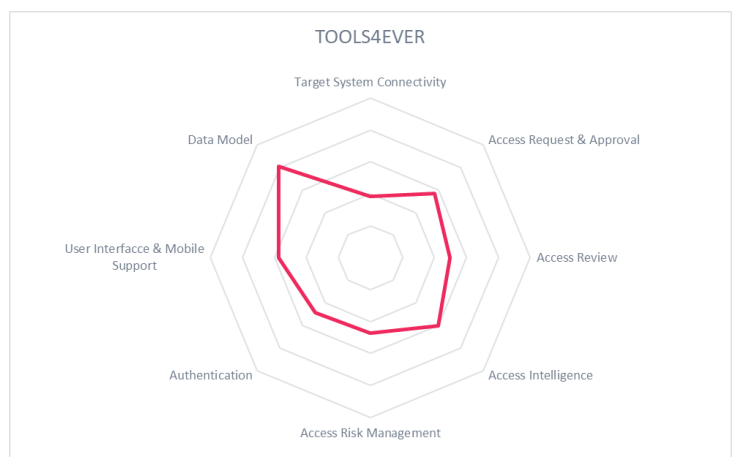
Tools4ever provides a solution that covers all major areas of identity provisioning, from a good set of connectors, also supporting integration to several HR systems, over password self-services, a good baseline access governance functionality to workflow management capabilities. In all these areas, it comes with some good but not yet leading-edge features. A specific strength is their support for delegating tasks to the helpdesk (or other users) in a flexible way. Thus, routine tasks can be distributed efficiently and in a well-managed approach. Furthermore, the solution is lean, compared to some of the more heavy-weight offerings in the market. On-premise and cloud solutions are offered.

While we'd love to see more out-of-the-box connectors, the number and range of connectors provided is overall good. Furthermore, custom connectors can be developed efficiently based on standard connectors for common protocols and interfaces.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 48: Tools4ever rating

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



6 Vendors to watch out for Access Governance

Besides the vendors covered in details in this Leadership Compass document, we come across some other vendors in the market that also offer credible access governance capabilities in the market. A few of these vendors have decided not to participate in this KuppingerCole Leadership compass for own reasons, but because we find them interesting and worth a mention, we decided to include them here. These vendors may not fully fit into the market segment of access governance or do not meet our eligibility criteria to be considered in this evaluation. We provide short abstracts for these vendors below. Notably, several vendors in the broader IGA market that are primarily targeting the identity provisioning functionalities are covered in the **KuppingerCole Leadership Compass on identity provisioning**.

6.1 Atos

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

DirX Identity has been a proven legacy solution for directory synchronization, but Atos has significantly enhanced the tool to make it a competent IGA solution in the market today. Amongst these areas are the depth of connectors, the underlying support for identity attributes based on a flexible meta-directory approach, the high availability and fail-safe configurations, and strong identity and life-cycle fulfilment capabilities.

From a feature perspective, DirX Identity comes as an offering that delivers a comprehensive set of identity provisioning capabilities, with significant improvements made over the past years regarding the ease of customization and the overall flexibility of the offering. However, it still lacks strong access governance capabilities. DirX Identity counts amongst the strong identity provisioning products in the IGA market.

6.2 Avanpost

Avanpost, based in Russia, primarily offers identity provisioning capabilities as part of its IAM product, but only limited access governance features. Their primary strength remains the support for a broad range of authentication technologies, including integration with physical access control solutions. Avanpost's presence is confined to home region and has limited partner reach outside of Russia and CIS countries, but this is changing as Avanpost gains recognition outside of Russia solely based on its strong technical abilities, an efficient product architecture and easy product deployment.

6.3 Cion Systems

Cion Systems offers a range of identity provisioning and access governance tools aimed at Active Directory. They have multiple components serving specific IGA needs of Microsoft environment. These include separate components for Multi-factor Authentication, identity provisioning, AD policy management and Data access governance for Windows platforms and O365 applications. They also offer a cloud-based IGA service targeted primarily at managing AD accounts. Deep Identity

6.4 Deep Identity

Singapore-based Deep Identity, a part of Temesak Management Services group of companies, offers several IAM products with Deep IACM (Identity Audit and Compliance Manager) as its primary access governance offering. Deep Identity Manager is aimed at identity provisioning offering identity lifecycle management and access request management. Their Data Governance Manager product offers data governance capabilities that add to completeness of their access governance portfolio. Deep Identity also offers a privilege management component, Deep PIM, that's well integrated with their IGA portfolio. Deep Identity's presence is limited to SEA (South East Asia) but is trying to expand in other Asian regions as well as in Europe.

6.5 FSP

FSP, based in Germany, provides an integrated IGA solution named "IGA Suite ORG". As an integrated suite, the product covers both identity provisioning and access governance, with its strengths being more in the access governance area and the integrated support for both role-based and attribute-based access control. However, the product also comes with required baseline support for identity provisioning. As one of the fewer vendors in the market offering the right mix of RBAC with ABAC, FSP lacks role mining and advanced role governance where it plans to offer integration with Nexis. Using BIRT analytics engine for common reporting across all components, FSP currently lacks access governance for SaaS applications.

While FSP IGA Suite ORG makes a good alternative to global vendors in the home region, the company is challenged by its very small partner ecosystem, which limits its ability to provide services to customers outside of the German-speaking countries. The company is actively working on expanding its partner ecosystem.

6.6 Identity Automation

Identity Automation is another system integrator turned identity software provider. Based on the experience and expertise from the integration business, Identity Automation has developed its own software product, RapidIdentity, aimed at offering IAM capabilities for SMB market through a well-integrated range of individual modules for identity provisioning, access governance, Access Management and even Privilege Management. .

6.7 Ilantus

India based Ilantus Technologies is a specialized vendor in the IAM domain. Originally a system integrator and a managed IAM service provider, it has started to offer an IDaaS (Identity-as-a-Service) offering of its own specializing in enterprise-grade access management capabilities. While still offering white-labelled IAM services for its partners, Ilantus is fast gaining a strong foothold as an IDaaS provider in the region offering limited access governance but certain other competitive advantages to established players in Asia. Its core focus has now moved to be a pure-play IDaaS provider focusing on SSO and other B2E access management requirements.

6.8 Imprivata

Imprivata, a provider of healthcare access management solutions acquired Caradigm, which is a GE healthcare company focused on delivering identity life-cycle management targeted at the healthcare industry. With the acquisition, Imprivata now has one of the most comprehensive IAM capabilities to

address the unique IAM challenges of the healthcare industry. In addition to few overlapping access management features such as Single Sign-On and multifactor authentication, Caradigm adds strong identity provisioning and access governance capabilities for healthcare IT systems to the Imprivata's IAM portfolio, making it a preferred choice for healthcare organizations looking for vendors with the knowledge and expertise of managing industry-specific IAM challenges.

6.9 iSM Secu-Sys

iSM Secu-Sys, based in Germany, offers bi-cube with a focus on identity provisioning capabilities. In addition to common workflow and policy management, bi-cube offers integrated SOD and DAG (Data access governance) capabilities. Also available in SaaS delivery format, iSM bi-cube makes a good choice for small to mid-sized organizations with requirements of detailed identity provisioning integrated with access governance for common scenarios focused at SOD and DAG. iSM Secu-Sys has limited visibility beyond the local markets but is investing considerably in building awareness and a stronger partner ecosystem beyond home territory.

6.10 ITconcepts

ITconcepts leverages Cognitum as a development platform for IAM solutions that allows organizations to quickly create IAM solutions, based on own requirements of connectivity to target systems and integrated policy and workflow management. Cognitum is based on the former BMC Calendra product. Based on Cognitum, ITConcepts offers a standardized IAM solution targeted at SMB market segment, allowing for rapid deployment of a standardized IAM solution. This is named go: Identity and offers limited access governance features. While Cognitum itself is attractive as a complementary tool for all IAM deployments, the standard solution is primarily targeted on SMBs.

6.11 ITMC Soft

Founded by a group of IAM experts, ITMC offers IDM365 as its primary offering focused at ease of use and reduced deployment complexity. Delivering a strong set of out-of-the-box concepts and processes combined with a modern UI help customer reduce the need for long-running, costly IAM implementations. With its current feature set, the product fits well into the identity provisioning and access governance market segments.

6.12 Microsoft

Microsoft's offering in the identity provisioning market segment is the Microsoft Identity Manager 2016 (MIM). The product is an upgraded and integrated version of Microsoft FIM (Forefront Identity Manager). The former access governance capabilities, which were based on assets acquired from BHOLD, have been discontinued. On the other hand, Microsoft Identity Manager comes with some specific add-on capabilities such as built-in Privilege Management features for domain administration as well as keys and certificate management. In sum, MIM follows a relatively technical approach to identity provisioning with a focus on synchronization than on workflows.

Microsoft Identity Manager 2016 still relies on the technical foundation of its predecessors. On the other hand, Microsoft has integrated some of the formerly isolated features such as the key and certificate management. Furthermore, the solution is increasingly complemented by Azure-based offerings such as

password management in integration with Microsoft Azure Multi Factor Authentication (MFA) and Azure-based reporting capabilities.

A shortcoming of MIM is that it requires coding in many situations, more frequently than many other products in the market. Besides this, due to its concept, simple user interfaces and workflow-driven approaches are often implemented by either customization or using 3rd party products. The native set of connectors is good, but not leading-edge. Several partners deliver additional connectors if required.

Microsoft Identity Manager is not part of this evaluation due to the fact that it is positioned less as a stand-alone access governance offering. Its partnership with SailPoint last year to deliver access governance capabilities including access certification, SOD policy and role management for Azure AD wasn't a great success for reasons of certain functional overlap and lack of available guidance on integration opportunities by the vendors.

6.13 Ogitix

Ogitix is a German company that provides an IAM solution targeted at the SMB market, with focus on the local market. It provides some interesting capabilities but is not yet at the level of enterprise solutions in the area of identity provisioning. However, Ogitix makes a good candidate for further evaluation by SMBs as a lean alternative to established players.

6.14 OpenIAM

OpenIAM counts amongst the lesser known vendors in the IAM market with a limited but growing market potential. Offered primarily in hardware appliance form, the product has two distinct components: OpenIAM Identity Manager delivering identity provisioning and auditing capabilities, and the OpenIAM Access Manager delivering access management including identity federation, web-based access management and SOA security. Access governance capabilities are limited and insufficient for a standalone access governance deployment due to the lack of role governance and SOD controls management capabilities. Based on an open source IAM framework, OpenIAM deployments generally require significant development efforts often leading to considerable customization for configuring basic IAM scenarios. Overall, OpenIAM makes a good choice of vendor for organizations with a demand for common identity provisioning and access management platform with good flexibility imbibed from an open source model. OpenIAM's product architecture is also suitable for organizations considering a microservices approach to IAM delivery.

Overall, OpenIAM is a relatively smaller vendor that faces the challenges of a limited partner ecosystem and growing unwillingness of organizations to adopt open source software options for security.

6.15 Propentus

Propentus, a Finnish software vendor offers Propentus United Identity which takes an HR-based approach to identity and access management. With a strong HR focus, Propentus offers limited identity provisioning and access governance capabilities. Majority of Propentus's customers are in the Nordics but the company plans to expand operations in Europe. It makes a good fit for small to mid-size organizations looking for an HR-driven approach to identity and access management.

6.16 SmartAIM

SmartAIM is a Dutch vendor offering SmartAIM Authorization Management Suite with several optional modules covering most identity provisioning and access governance capabilities. SmartAIM Identity Manager, Provision and Password Self-Service modules deliver identity provisioning capabilities while Audit and Authorization Workflow modules are core to its access governance capabilities. SmartAIM's customer base is relatively small and limited to home country but it might soon become a vendor that meets all the evaluation criteria for inclusion in the KuppingerCole Leadership Compass for access governance.

6.17 Usercube

Usercube is a French software company that primarily offers an identity provisioning solution built on .NET framework. With user intuitive interface for access requests and approvals, it offers a decent range of provisioning connectors. While its access governance capabilities are few and limited, with the proficiency and pace of development, it might make a strong contender for inclusion in the next edition of KuppingerCole Leadership Compass for identity provisioning.

6.18 Tuebora

Tuebora, based in California, offers Tuebora Governance as its provisioning and governance product. 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. In addition to delivering a cloud-based service, Tuebora also offers a white-labelled deployment approach with its service partners like HCL, Wipro and Happiest Minds. While Tuebora has a good presence in Asia, it continues to expand its presence in Europe and Middle East. It makes a good choice for organizations looking for risk-based access governance capabilities. It equally appeals to managed IAM service providers considering to offer a 'white-labelled' service in partnership.

6.19 WSO2

WSO2, headquartered in Palo Alto, California offers a platform for securing IT infrastructure and applications based on SOA (Service Oriented Architecture) framework. The SOA approach to IAM provides WSO2 a strong market differentiator by delivering capabilities that support complex event processing and a service oriented IAM implementation. WSO2 Identity Server provides identity life-cycle management capabilities, including flexible identity provisioning features. An Identity API and development platform, WSO2 Identity Server is targeted at customers integrating IAM and other adjacent IAM capabilities into customer's solution. Primarily focused at connecting businesses with partners and customers, their out-of-the-box support for on-premise identity provisioning and access governance requirements is somewhat limited. WSO2 is a preferred choice for customers looking for an API-driven IAM platform. Organizations looking for a developer friendly API driven approach to basic IGA functions should evaluate WSO2 for its proven flexibility and scalability.

7 Methodology

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.

7.1 Types of Leadership

We look at four types of leaders:

- **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 area, 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 best choice for specific use cases and customer requirements but are of limited value in other situations.

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

7.2 Product rating

KuppingerCole as an analyst company regularly does 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 on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Interoperability
- Functionality
- Usability
- Integration

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management⁴). 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.

⁴ http://www.kuppingercole.com/report/mksecnario_understandingiam06102011

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 insure 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. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy⁵) for more information about the nature and state of extensibility and interoperability.

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 is 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.

⁵ http://www.kuppingercole.com/report/cb_apieconomy16122011

7.3 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 over all 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.

7.4 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.

7.5 Spider graphs

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

Connector Breadth	The number of connectors and the breadth of target systems, including e.g. directory services, business applications, mainframe systems, and others. Also, broad support for common cloud services is rated here.
Connector Depth	Capabilities of connectors, in particular when it comes to connecting to complex target systems such as SAP environments or mainframes. This rating also looks at customization capabilities for connectors through connector toolkits.
Baseline access governance	Integrated access governance capabilities, including baseline Access Review, Role Management, and SoD (Segregation of Duties) controls.
Self-Service & Mobile Support	User self-service interfaces and support for secure mobile access to selected capabilities.
Workflows	Advanced workflow capabilities, including graphical workflow configuration, for supporting the various requirements of access governance.

Authentication	Support for strong and adaptive authentication for both administrators and end users accessing the service.
Auditing & Reporting	Extensive auditing and reporting capabilities, including analytical capabilities for analysing the current state of entitlements.
Data Model	Flexible but centralized data model that allows customization by the customer for its specific need.

The spider graphs add an extra level of information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas, while being strong in other areas. These might 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 decisions on IDaaS.

7.6 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 about vendors not covered and their access governance offerings in chapter Vendors . In that chapter, we also look at some other interesting offerings around the access governance market and in related market segments.

8 Copyright

© 2018 Kuppinger Cole Ltd. All rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice.

The Future of Information Security – Today

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

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact clients@kuppingercole.com