KuppingerCole Report

LEADERSHIP COMPASS

By Martin Kuppinger
March 30, 2021

Leadership Compass Identity Fabrics

This report provides an overview of the market for Identity Fabrics, comprehensive IAM solutions built on a modern, modular architecture, and provides you with a compass to help you to find the solution that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing solutions that serve customers best in building their Identity Fabrics.

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

Content

1 Introduction

The term “Identity Fabrics” stands for a paradigm of a comprehensive set of Identity Services, delivering the capabilities required for providing seamless and controlled access for everyone to every service. They support various types of identities such as employees, partners, consumers, or things. They deliver the full range of identity services required by an organization.

Identity Fabrics are not a single technology, tool, or cloud service, but a paradigm for architecting IAM within enterprises. Commonly, the services are provided by a set of tools and services. However, most organizations that are using this paradigm as a foundation for the evolution of their overall IAM tend to build on a strong core platform for delivering major features and complementing this by other solutions.

In this Leadership Compass, we evaluate solutions that can serve as a foundation for customers creating their own Identity Fabrics by delivering a wide range of capabilities in a modern architecture.

Thus, this Leadership Compass analyzes which of the IAM offerings in the market are best suited to form the foundation for an Identity Fabric, in delivering

- a broad range of IAM capabilities, at minimum including a good level in both IGA (Identity Governance and Administration) and Access Management (Identity Federation, Multi Factor Authentication, etc.)
- by providing a comprehensive set of APIs for consuming these services, beyond the admin and end user UI/UX
- this in a modern architecture, following paradigms such as microservices architectures and container-based deployments
- support for different deployment models, serving the needs of customers for options in their operating models
- support for all types of identities, including employees, business partners, customers and consumers, connected things, devices, and services

In sum, solutions must not only deliver functionality and support for all types of identities, but also meet our requirements regarding the architecture, deployment model, and their interoperability with traditional applications, cloud services, and new digital services.

1.1 Market Segment

Digital business has evolved from simple e-commerce websites from the 90s. Modern digital business models are complex, distributed, multidimensional and involve many parties in a variety of roles. This has a direct impact on how communication takes place, how people work together and how services and goods are created and delivered to customers.

Employees, partners, service providers, customers, devices, and processes use and provide services. Access is made from and to any conceivable location to services that are somewhere between on-premises data centers, the cloud, mobile systems.

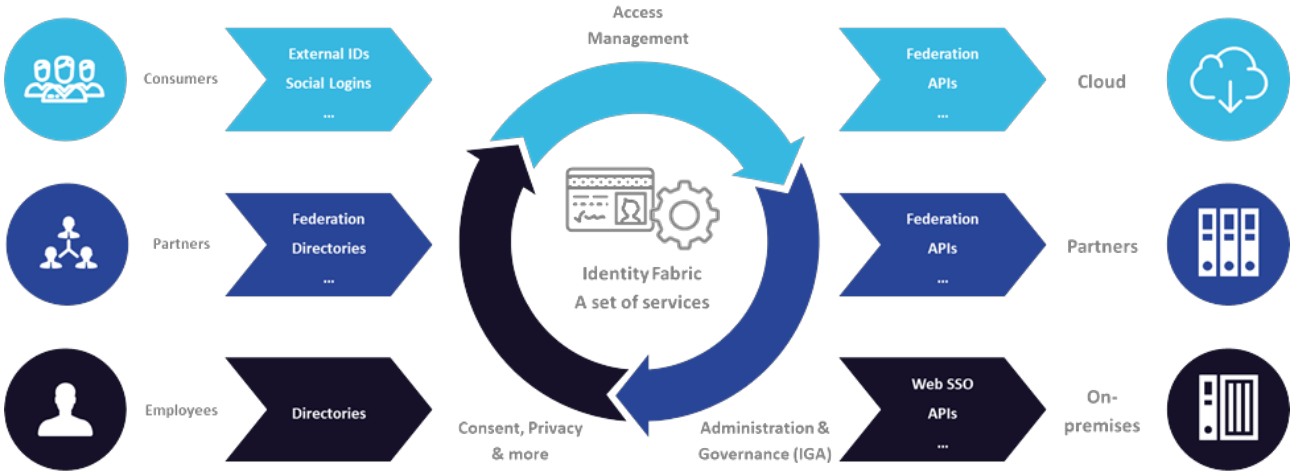


Figure 1: Identity Fabrics are a set of services that support all users in gaining seamless yet controlled access to all services they require.

The formerly classic corporate network with clearly defined "inside" and "outside" has given way to a massively hybrid, new IT reality. IAM (Identity and Access Management) is the essential security infrastructure for this and at the same time a facilitator of these new services, models and forms of cooperation.

To make this possible, IAM must be transformed. It needs to be converted into a consolidated portfolio of isolated but corresponding services that enable to connect anything and anyone via a comprehensive architecture, and to make services available to all users everywhere: secure, scalable and without losing control.

“Identity Fabric” refers to a logical infrastructure for enterprise Identity and Access Management. It is conceived to enable access for all, from anywhere to any service while integrating advanced features such as support for adaptive authentication, auditing capabilities, comprehensive federation of services, and dynamic authorization capabilities.

Digital technologies influence and change all areas of an organization, and this fundamentally shapes the way communication takes place, how people work together and how value is delivered.

IT architectures, in turn, are undergoing profound structural changes to enable and accelerate this gradual paradigm shift. This evolution reflects the transformation resulting from the changing challenges facing virtually every organization worldwide for a long time in different contexts. They affect processes and systems alike and the underlying architectures.

In order to remain competitive in this charged environment, companies strive to be as flexible as possible by adapting and modifying business models and, last but not least, opening up new channels of communication with their partners and customers. With the rapid growth of cloud and mobile computing, businesses are becoming increasingly networked. The very idea of a company's outer boundary, the concept of a security perimeter, has practically ceased to exist.

The assumption that previously independent identities (employees, customers, partners, mobile devices, etc.) in an enterprise can be regarded as isolated is no longer valid.? The management of identities and permissions in digital transformation is the key to security, governance and audit, but also to system usability and user satisfaction. The demands on a future-proof IAM are complex, diverse and sometimes even conflicting. These include:

- Different types of identities (first and foremost, consumers) must be integrated quickly and securely in user-friendly processes.
- At the same time, users should be able to retain control over their identities by bringing their own identities with them (BYOID).
- Employees (internal and external) should be able to use the devices they prefer.
- Secure access to working environments must be possible no matter where users and systems are located.
- Zero Trust such as continuously verifying access must be part of the capabilities.
- Identities must be linked to reflect relationships within teams, companies, families, or partner organizations.
- Identities maintained in trusted organizations should be directly and reliably integrated and authorized in each organization’s IAM.
- Identities should be able to do business and execute payments.
- All relevant laws and regulations must be observed.
- At the same time, KYC processes are to be optimized, enabling rather than deterring visitors from using the service.
- Existing data should be usable by analytics and artificial intelligence applications.
- All this must apply to all possible identities, beyond people, so that devices, services and networks

are integrated into our next generation IAM infrastructure.

- New digital services must be able to consume the identity services, building on a consistent set of services e.g., for onboarding and authenticating users.

Today's IAM systems meet, if at all, only a fraction of current requirements. In many cases these IAM infrastructures stem from traditional enterprise IAM systems, sometimes extended with an additional customer identity system, most probably siloed. At the same time, they are often monolithic in design and implementation, making it difficult to break them down into individual components.

Unfortunately, this is exactly one of the central challenges. In many situations, the path to an identity fabric will pass along the challenge of unambiguously isolating individual functional components and exposing their interfaces through secure and accessible APIs. This applies to source systems that provide identities and enforce permissions, but also to all target systems. And in individual cases it can also apply to one or more legacy IAM systems if a replacement is difficult or not possible in a timely manner.

If organizations need to seamlessly give access to all users, wherever they are accessing from, and provide any digital service to these users, the Identity Fabric must be able to securely mediate that very connection between user and service.
To achieve this, we are shifting away from isolated, singular systems to a logical platform that provides and orchestrates a set of required IAM services and related functions. The way these services are delivered can vary: they may involve existing as-a-service offerings or might be based on existing on-premises services.

These services can be located in a public cloud, they can be web applications with or without support of federation standards, they can be exclusively back-end services only accessible via REST APIs, or even legacy applications encapsulated by some kind of middleware. At the same time, it might be even valid to integrate redundant services for different usage scenarios.

What they all have in common is that they are always part of a consistent framework of services, capabilities and building blocks as part of a well-defined, loosely coupled overall architecture that is ideally delivered and used homogeneously via secure APIs.

However, the agility of the digital journey requires IT to provide seamless access to all these services while maintaining control and security. In parallel, all requirements for scalability, performance and resilience must be met.

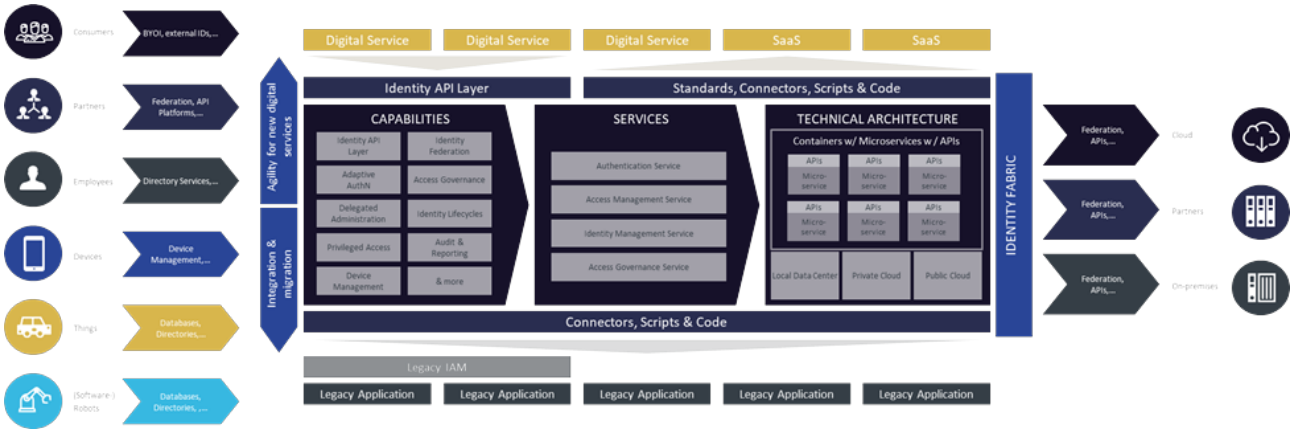


Figure 2: A sample high-level, conceptual architecture for an Identity Fabric. The set of capabilities and services provided depends on the specific requirements of the organization.

Identity fabrics are not an entirely new concept. They are based on the challenges of a modern workplace and digitalization, which is responsible for almost everything. The resulting tasks, which cannot be solved with traditional IAM paradigms, must be mastered.

They combine current and proven IAM concepts, supplemented by security by design and APIs, a service-oriented IT concept (which can certainly be implemented in microservices) and modern delivery concepts for cloud, hybrid infrastructures, containers and their orchestration or serverless infrastructures.

The way towards the implementation of an Identity Fabric as a strategic, hybrid IAM platform is a company-specific challenge, because the actual requirements and the individual starting points are company-specific.

KuppingerCole recommends the following strategic approach, which should be mapped to meaningful technical, conceptual and project planning measures.

- Define a comprehensive and efficient target architecture, based on microservices architecture and container-based deployment, and work towards its implementation in well-organized individual projects.
- Proceed consistently, step by step and in an integrated manner.
- Provide your company with all the necessary services it needs for its current and strategic identity needs.
- Offer consistent backend services and develop an identity API platform as the foundation.
- Define a clear architecture layer model. Reuse and encapsulate whatever and whenever you can.
- Organically add missing functionality to your target architecture when needed.
- Replace inappropriate components along the way, but if possible, later.

This transformation of your IAM infrastructure into an Identity Fabric does not need to be and is not meant to

be disruptive by any means. It can be executed in a way that allows for stable and reliable continuous operations without any kind of “big bang” while augmenting new functions and enabling new categories of access paths, ideally driven by changing corporate demands.

Required technological and architectural building blocks are already available and proven reliable. However, choosing the right components to enable support for individually required new authentication and authorization use cases with stepwise extended platform capabilities demands strict strategic oversight and management.

To clarify it once again: There is no “standard Identity Fabric”. An Identity Fabric is based on the required capabilities and services for digital identities an organization has. These commonly involve certain key capabilities but will always differ slightly. Also, the implementation of an Identity Fabric commonly builds on very few (one or two) main technical components for IGA and Access Management, but is complemented by additional components that provide further services and capabilities. There might be even some level of redundancy, either in migration or for technical or organizational reasons. However, the concept of Identity Fabrics serves well for designing and implementing a modern IAM that is modular, flexible, and provides the capabilities required, including a consistent Identity API layer that allows digital services to consume the identity services.

1.2 Delivery models

Identity Fabrics are, generally speaking, agnostic to the deployment model. Ideally, various components can be deployed in different types of deployments, including instance of components running in different locations such as a public cloud and on the edge of the on-premises infrastructure.

However, this also includes support for some level of IDaaS capabilities. This defines IAM solutions that are delivered in an as-a-service model. In our definition, IDaaS includes

- Multi-tenant public cloud services
- Single-tenant public cloud services if updates, patches, etc. are deployed by the service provider across all tenants with full automation, which requires adequate software architectures (segregation of customizations and data from application code)
- Single-tenant services that can operate in various deployment models, i.e., in private or public clouds or even on-premises, as long as they can be operated in a full as-a-service model if updates, patches, etc. are deployed by the service provider across all tenants with full automation, which requires adequate software architectures (segregation of customizations and data from application code)

Furthermore, delivery must meet the expectations regarding licensing models (pay-per-use), elasticity and scalability, i.e. flexible scaling of the service. Beyond that, as mentioned above, we expect modern software architectures, which are anyway the foundation for flexibility in deployment.

We thus prefer solutions that can be deployed and orchestrated flexibly, supporting a variety of deployment models. This gives customers the choice for a gradual migration to the cloud, but also enables support for more complex scenarios such as geographically dispersed deployments and hybrid scenarios.

This Leadership Compass looks at solutions that are traditionally deployed on-premises but can be deployed and operated as a service by Managed Service Providers (MSPs) as well as pure-cloud solutions.

1.3 Required capabilities

Identity Fabrics must support a good baseline level in both IGA and Access Management but could add further capabilities such as integrated directory services, PAM (Privileged Access Management), and other IAM capabilities that are commonly required by customers.

IGA covers two broad functional areas

- Identity Lifecycle Management/Identity Provisioning
- Access Governance, including Access Reviews and Access Intelligence

The focus of this report is on solutions that cover both aspects of IGA and are not solely limited to either Identity Provisioning or Access Governance.

Main capabilities of IGA solutions are

- Automated User Provisioning
- Connectors to both cloud services and on-premises applications
- Toolkits for customizing connectors
- Integration and/or synchronization to directory services
- Self-services for credentials and user profiles
- Access Request & Approval
- Entitlement Management, including Role Management
- SoD Controls Management & Enforcement
- Access Certification
- Identity and Access Analytics

- Auditing, Reporting & Dashboarding

We expect solutions to cover a majority of these capabilities at least at a good baseline level.

Access Management also consists of various capability areas such as

- Identity Federation and Web Access Management
- Multi-Factor Authentication and Adaptive Authentication (risk-/context-based)

Again, we expect support for both areas.

Main capabilities in Access Management include but are not limited to

- Support for inbound and outbound federation
- Support for all major Identity Federation standards, including SAML and OAuth
- Web Access Management capabilities for integrating applications without built-in federation support
- User onboarding and registration
- Self-services for credentials and user profiles
- Integration and/or synchronization to directory services
- Support for federated provisioning
- Auditing, Reporting & Dashboarding
- Support for a broad range of authenticators
- Toolkits for adding additional authenticators
- Support for 2FA/MFA
- Step-up authentication
- Risk- and context-based authentication

As mentioned above, we also expect a comprehensive set of APIs, exposing capabilities via APIs and not just UI/UX, a modern architecture, and support for a broad range of deployment models.

Included in this Leadership Compass are solutions that serve both IGA and Access Management, provide a comprehensive set of APIs (plus traditional UI/UX), follow modern architectural paradigms, and support flexible deployment models and thus can form the foundation for customers building their own Identity Fabric.

Excluded from this Leadership Compass are:

- Vendors that only cover IGA or Access Management will not be considered. We expect at least good baseline capabilities in both areas and appreciate seeing additional IAM capabilities. On exception, we considered vendors covering only one of these areas, but delivering strong capabilities in another field of IAM such as PAM.
- Vendors that have multiple products with heterogeneous architectures and no or little integration regarding deployment, operations, architecture, UI/UX, APIs etc., will not be considered.
- Vendors that don't meet the definition of IDaaS will not be considered for this Leadership Compass. This includes pure MSP (Managed Service) deployments as well as solutions without a pay-per-use licensing model.
- Vendors without active deployments at customers (e.g., start-ups in stealth mode) will not be considered.
- Solutions with a traditional architecture, not supporting modern deployment models such as container-based deployments, but only traditional installs, will not be considered.
- Solutions that lack a comprehensive set of APIs will not be considered.
- Solutions that are targeted at either only employees/business partners or at customers/consumers will not be considered.

However, there are no further exclusion criteria such as revenue or number of customers. We cover vendors from all regions, from start-ups to large companies.

Based on that, we have a list of evaluation criteria for the products and services covered in this Leadership Compass:

Functionality	Weightage
Key Capabilities	
Automated User Provisioning	High
Connectors to both cloud services and on premises applications	High
Toolkits for customizing connectors	High
Integration and/or synchronization to directory services	High
Self-services for credentials and user profiles	High
Access Request & Approval	High
Entitlement Management, including Role Management	High
SoD Controls Management & Enforcement	High
Access Certification	High
Identity and Access Analytics	High
Auditing, Reporting & Dashboarding	High
Support for inbound and outbound federation	High

Functionality	Weightage
Support for all major Identity Federation standards, including SAML and OAuth	High
Web Access Management capabilities for integrating applications without built-in federation support	High
Support for federated provisioning	High
Support for a broad range of authenticators	High
Support for 2FA/MFA	High
Risk- and context-based authentication	High
Step-up authentication	High
Comprehensive set of APIs	High
Flexible, modern software architecture & deployment	High
Additional Capabilities (Selection)	
Standards support	High
Automated reconciliation	High
Out-of-the-box processes, e.g., JML and beyond	High
Mobile support	Medium
Extended Service Catalogues	Medium
Delegated Administration	High
SoD Controls Management (in-depth) for Business Applications, e.g., SAP	Medium
Password Synchronization	Medium
Workflow capabilities	High
Policy management	High
Flexible approaches for access reviews	High
Toolkits for adding additional authenticators	Medium
Privileged Access Management capabilities	Medium
Enterprise Single Sign-On capabilities	Low
Innovative Capabilities (Selection)	
ITSM Integration (e.g., ServiceNow)	High
Applied AI/ML for Identity and Access Analytics	Medium
Applied AI/ML for Adaptive Authentication	High
Data Access Governance	Medium
API Management and Security	Medium
Privacy & Consent Management	Medium
BYOD support	High
Developer support/capabilities	Medium

The list of functionalities is not complete but intended to give an overview of our expectations regarding functionality in the Identity Fabrics market segment. Certain capabilities of high weightage will be rated higher than others.

2 Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

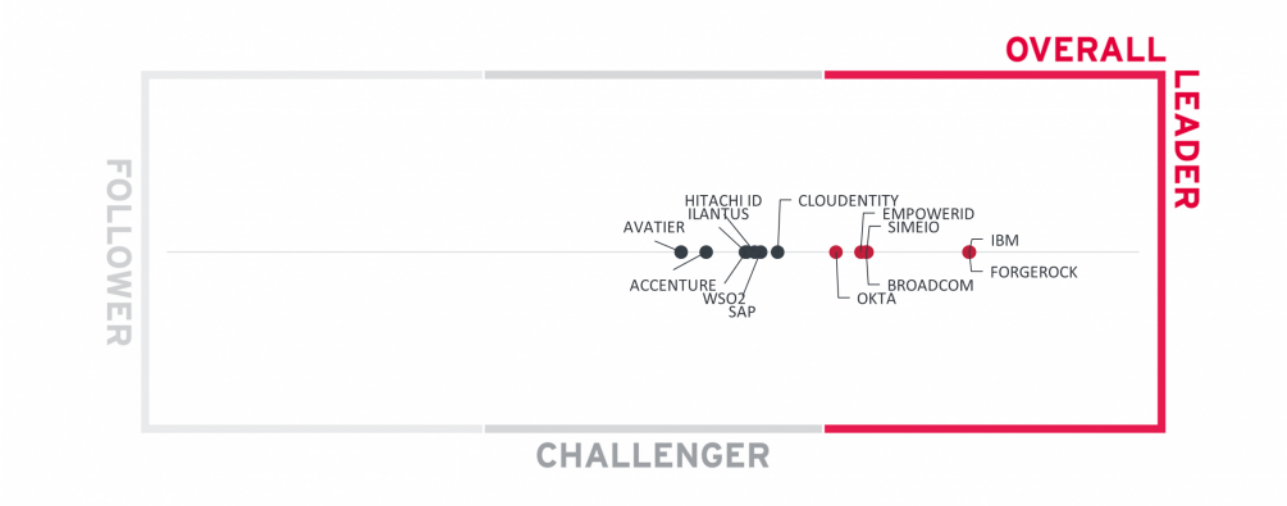


Figure 3: The Overall Leadership rating for the Identity Fabrics market segment

In the overall rating, we see IBM and ForgeRock head-to-head, both at the same level. IBM has invested significantly into their IBM Security Verify platform, building a new, modern identity service that can be operated in a range of deployment models. This new platform utilizes the established IBM Security solutions in certain areas, but increasingly provides services directly from that platform. ForgeRock, on the other hand, has its ForgeRock Identity Platform as a combined solution that integrates products such as the

ForgeRock Identity Manager and ForgeRock Access Manager into a unified solution, which also can operate from the cloud. While both differ in their approaches, these solutions provide a strong set of capabilities in a modern architecture and thus can serve well as the foundation for an Identity Fabric, delivering a strong set of core services.

In the next group, we find, in alphabetical order, Broadcom, EmpowerID, and Simeio. These three vendors take very different approaches on delivering an Identity Fabric. Broadcom also has constructed a new, cloud-based identity platform, Symantec Identity Security, which comprises a range of capabilities derived from the former portfolios of CA Technologies and Symantec. The products aren't yet fully integrated but can be deployed and operated in as-a-service models and deliver a wide range of capabilities. EmpowerID, on the other hand, is a provider of a unified IAM suite that covers most of the IAM capabilities in a unified solution. While being delivered as a unified solution following current architecture models, some few of the components are not yet modernized. Last but not least, Simeio has constructed their own IAM platform, Simeio Identity Orchestrator. While this originally was an orchestration platform for existing legacy IAM solutions, it now delivers many IAM capabilities directly, while still supporting the integration of a wide range of existing solutions. Together with the fact that Simeio also acts as the MSP (Managed Service Provider), this makes Simeio Identity Orchestrator an interesting solution for building an Identity Fabric while integrating existing legacy IAM solutions.

Amongst the Overall Leaders, we also find Okta. Okta is a pure public cloud SaaS offering that has evolved beyond the Access Management and Single Sign-On focus of its early days. While Access Management capabilities still dominate the features, Okta has added strong workflow capabilities, leading-edge support for an Identity API Platform and thus providing an Identity API layer, and is also adding User Lifecycle Management and further capabilities.

In the Challenger section, we find Cloudentity, which take a different approach on Identity Management, focusing on a central identity and authorization plane plus excellent API support. This makes them a strong vendor in areas such as Access Management, API support, and the support of a broad range of identity types, but with major gaps in IGA and the support of legacy IAM systems. However, they might become a cornerstone in constructing a modern Identity Fabric.

Closely following them, we find a group of three vendors, which are, again in alphabetical order, Hitachi ID, Ilantus, SAP, and WSO2. Again, these vendors take quite different approaches on IAM. Hitachi ID has a suite of proven IAM solutions that can be delivered in a range of deployment models, backed by the IT services provided by their parent company. . Ilantus is a vendor focusing more on the mid-market segment, providing an integrated IAM solution as a service that covers the main capabilities. As for some of the other challengers, they lack some of the more advanced capabilities, but can be an interesting alternative for medium-sized to mid-market companies. SAP, on the other hand, has a growing range of cloud-based IAM services plus a number of established products, that can deliver a wide range of IAM capabilities, with specific strengths in SAP environments. WSO2 again takes a different approach. They provide platforms for Enterprise Integration, API Management, and Identity Management, specifically Access Management. These platforms are targeted more at developers, but can serve well as a cornerstone of an Identity Fabric due to their modern architecture and strong API support, even while falling short in IGA capabilities.

Following these, we find Accenture and Avatier. Accenture provides their Memority solution as a full-featured Identity Fabric with B2E and B2B focus, but also coming with strong IoT support. They have overall good capabilities and a high degree of flexibility in configuration, while lacking some of the more advanced features other vendors provide, including integration to other platforms or advanced reporting capabilities. Memority also benefits from the comprehensive services that Accenture can provide in implementation projectsAvatier also provides a good set of IAM capabilities and shows strong innovation in certain areas, including their user experience, but in few areas such as adaptive authentication lacks the depth and breadth of capabilities provided by some of the other players in the market. Furthermore, they still have limited global presence, affecting their rating for Overall Leadership.

There are no vendors in the Follower section.

Overall Leaders are (in alphabetical order):

- Broadcom
- EmpowerID
- ForgeRock
- IBM
- Okta
- Simeio

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

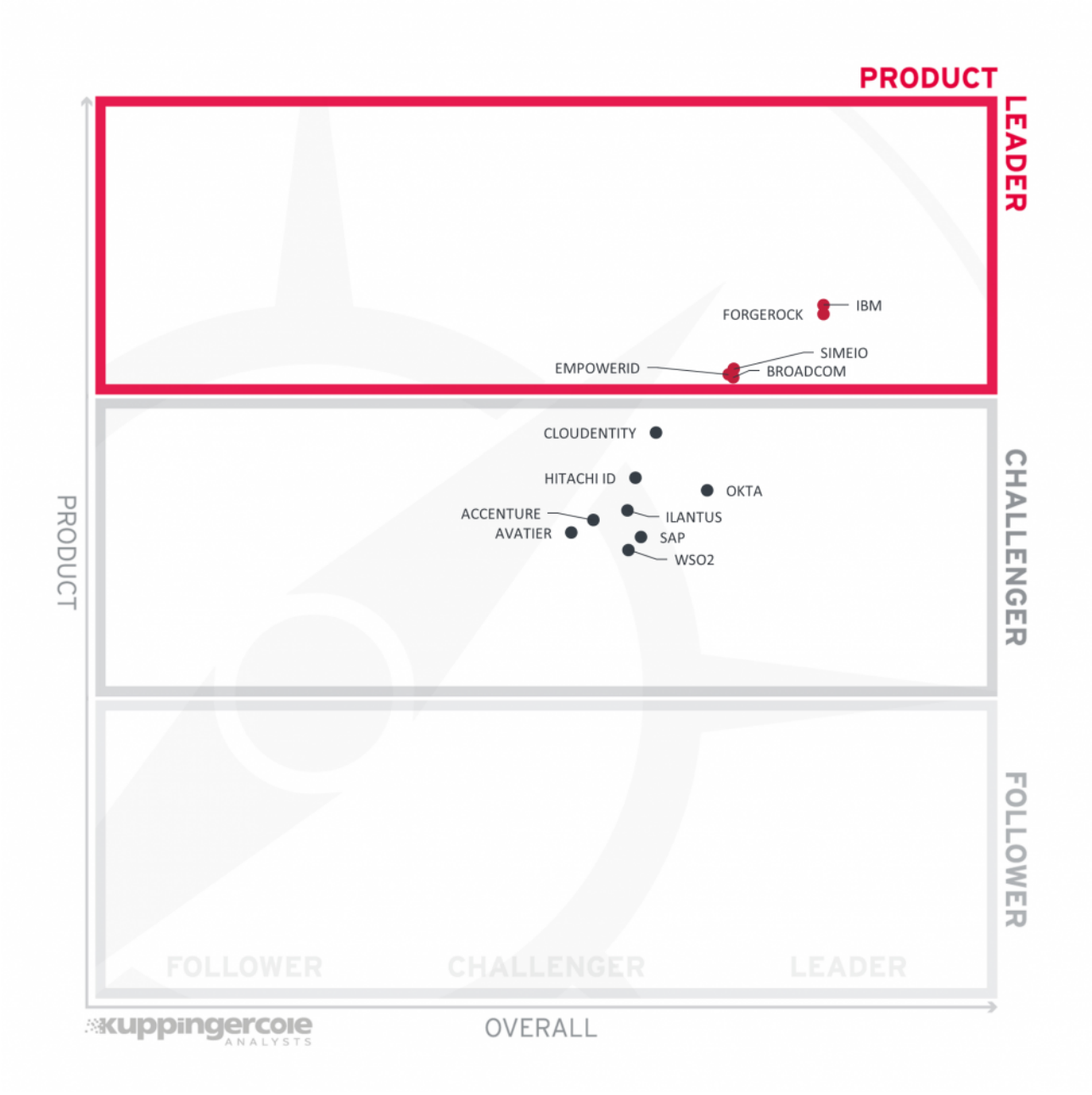


Figure 4: Product Leaders in the Identity Fabrics market segment

Product Leadership is where we examine the functional strength and completeness of services. For Identity Fabrics, this covers a range of areas such as the breadth and depth of functionality, but also the architecture and deployment models. The Leadership section is still rather empty, with only four vendors being at a level that grants them a rating as a Product Leader. This is due to the broad range of requirements beyond functionality, which are hard to meet by a single vendor. As explained previously, we expect most implementations of Identity Fabrics to build on few core products, but complement these by additional solutions.

In the lead, we see IBM, very closely followed by ForgeRock. Both have strong offerings, which are modern

in architecture and deliver both breadth and depth in features. They are ahead of other the other vendors in the IAM market and can well serve as the foundation for organizations building their Identity Fabric.

The other three vendors that we rate as Product Leaders are Simeio, Broadcom, and EmpowerID, which just passed the bar to the Leader section. All three have interesting offerings with good capabilities and modern architectures that make a good foundation for an Identity Fabric.

All other vendors are in the Challenger section. First, we findCloudentity, which score with their strong capabilities in API Management and Access Management.

Hitachi ID and Okta are next, with Hitachi ID having a strong set of features in both breadth and depth, specifically around IGA and PAM, and Okta being amongst the established leaders in Access Management. Okta lacks more advanced IGA capabilities to score better, even while their highly innovative workflow management provides some interesting alternatives to common approaches on IGA.

In the next group we find, in alphabetical order, Accenture, Avatier, Ilantus, SAP, and WSO2. Accenture provides a broad set of features, while sometimes lacking the depth. The solution is supporting multi-tenancy and flexible deployment models, building on a microservices architecture. The same holds true for Avatier, which are especially strong in user experience. Ilantus also provides a wide range of features, while sometimes lacking the depth found in other products. SAP excels in certain areas, specifically around IAM for SAP environments, while not being overly strong in the support for other target systems. WSO2 has strengths in API Management and Access Management, while being weaker in IGA. All of these solutions also might be considered when looking for the core building blocks of a modern Identity Fabric.

Product Leaders are (in alphabetical order):

- Broadcom
- EmpowerID
- ForgeRock
- IBM
- Simeio

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

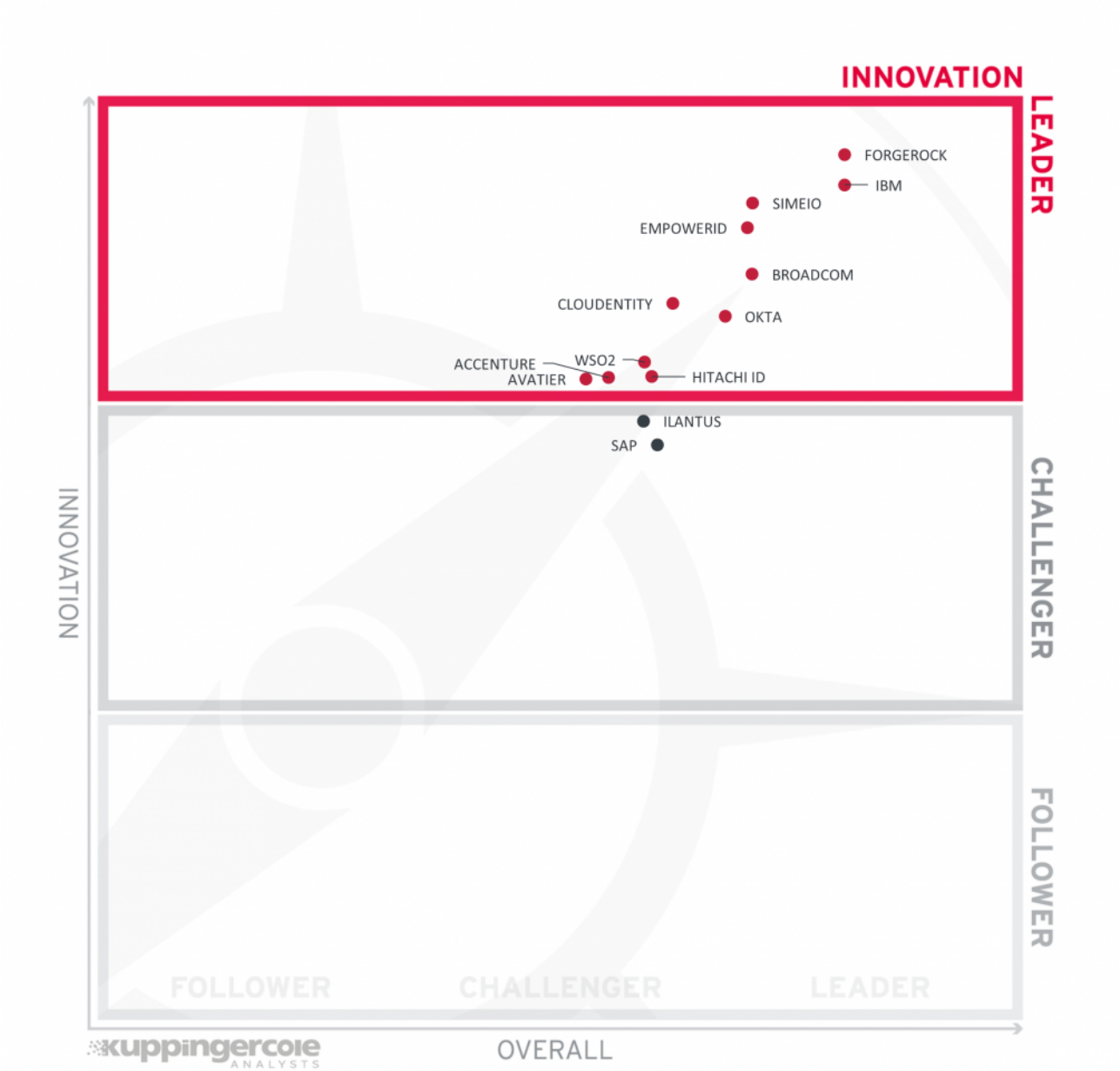


Figure 5: Innovation Leaders in the Identity Fabrics market segment

While the Leader segment for Product Leadership is quite empty, we see a lot of vendors in that segment when it comes to Innovation Leadership. This is quite common for emerging market segments, where we set a lot of innovation, while the breadth and depth of capabilities is still sometimes missing. Furthermore, the majority of vendors participating in this Leadership Compass rating already have invested significantly in modernizing their architectures (or creating new offerings) and API support, which both score high in the rating for Innovation Leadership.

Again, we find ForgeRock, IBM, Simeio, and EmpowerID in front, slightly ahead of other vendors. All four vendors have distinct strengths that we count as innovative. ForgeRock excels with its flexibility and the

support for complex, high-scalability use cases. IBM has successfully created a new, modern platform that on the other hand integrates well with other IBM offerings. Simeio is benefiting from own capabilities and their strengths in orchestrating existing legacy IAM services, which make them an interesting pick for Identity Fabrics. EmpowerID has a range of well-thought-out, innovative capabilities such as their SCIM-based, centralized integration with SaaS services.

The next group of vendors is formed by Broadcom, Cloudentity, and Okta. Broadcom has various innovative features amongst the broad set of capabilities provided, while not excelling in a certain area. Cloudentity is especially strong around API Management and authorization. Okta finally is amongst the leading-edge vendors in Access Management, but also delivers highly innovative workflow capabilities.

The four other vendors rated amongst the Innovation Leaders are WSO2, Hitachi ID, Accenture, and Avatier. WSO2 is strong in API Management and the overall architecture, while Hitachi ID shows its strengths more in the field of comprehensive capabilities across all areas, plus increasingly good IoT support. The latter counts also as a strength of Accenture Memority, which also shows strong support for complex use case scenarios. Avatier is strong in innovation around user experience, but still has some gaps around full API support and adaptive authentication.

In the Challenger segment, we only find two vendors, which are SAP and Ilantus. SAP also has some innovative features, but also some gaps due to their focus on SAP environments. Ilantus is overall good and close to becoming an Innovation Leader, but still catching up with some of the other vendors in both breadth and depth of capabilities, thus not showing that many innovative features.

Innovation Leaders are (in alphabetical order):

- Accenture
- Avatier
- Broadcom
- Cloudentity
- EmpowerID
- ForgeRock
- Hitachi ID
- IBM
- Okta
- Simeio
- WSO2

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the

partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

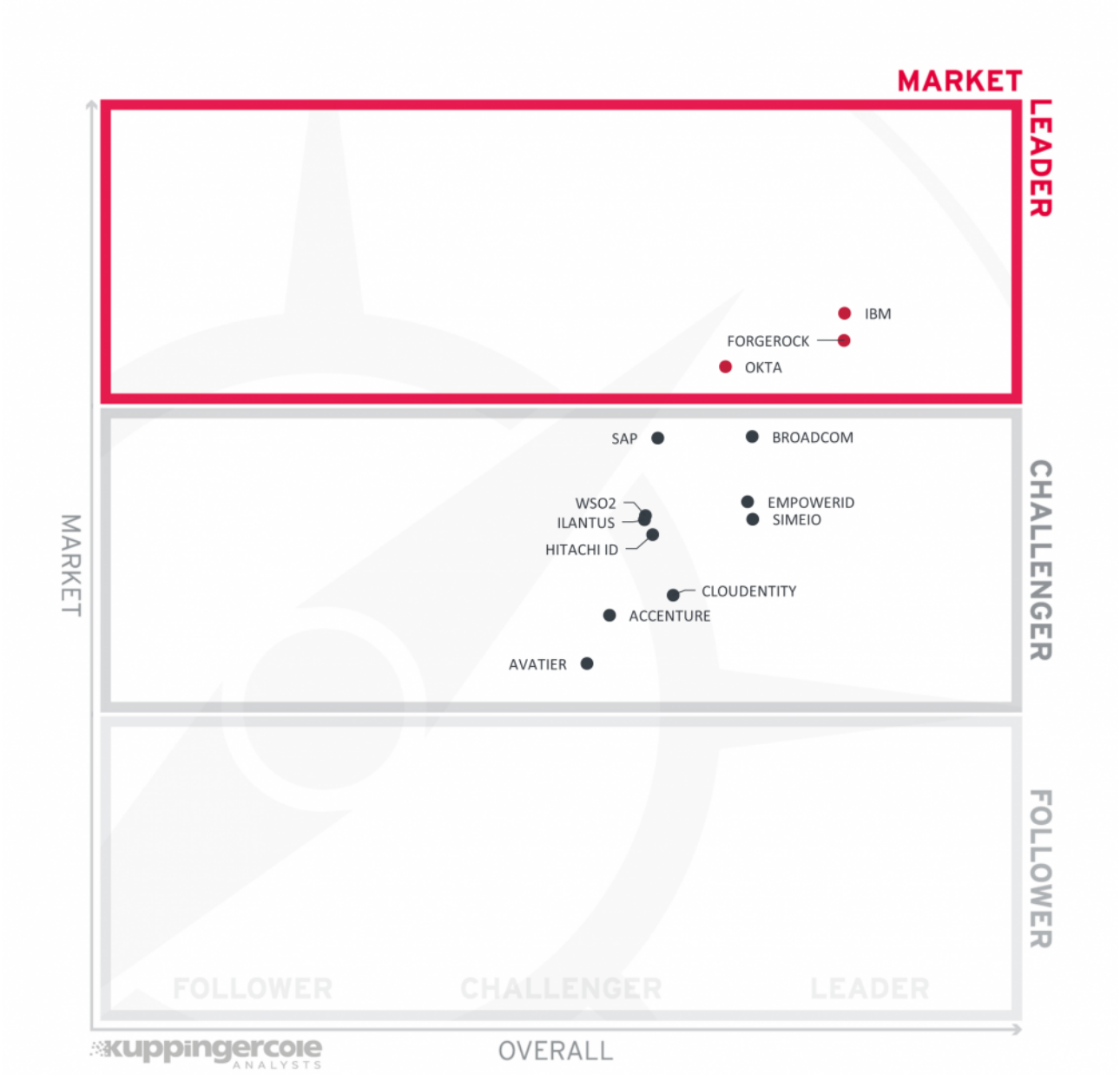


Figure 6: Market Leaders in the Identity Fabrics market segment

With Identity Fabrics still being a rather new market segment, we don't see that many specific implementations with a focus on delivering a modern, comprehensive infrastructure for future IAM to organizations. Thus, most vendors are still rated as Challengers, with only few that are included in the Leader segment.

The three Market Leaders are IBM, ForgeRock, and Okta. Both IBM and ForgeRock already provide comprehensive platforms and address the market with these offerings. Okta, on the other hand, has its weaknesses in User Lifecycle Management, but a strong momentum in other areas. All three vendors have a global partner ecosystem and a significant number of customers.

Following them, we find SAP and Broadcom, which both count amongst the leading global software vendors. With their global presence and partner ecosystem, both are close to entering the Market Leader segment.

Following them, we see a group of vendors including (in alphabetical order) EmpowerID, Hitachi ID, Ilantus, Simeio, and WSO2. Amongst these, EmpowerID and Hitachi ID are still relatively small with respect to the number of customers. WSO2 also has a strong global presence, while Ilantus still has a limited presence in EMEA, and Simeio still being focused on the North American market.

Cloudentity is still a relatively young vendor, lacking a comprehensive global presence and ecosystem. Accenture has only a limited number of customers, but some very large installations. Furthermore, while benefiting from the own global presence, their partner ecosystem outside of Accenture is very limited. Last not least, Avatier has a good number of customers, but many of these mid-market customers with some large enterprises, and lacks a global presence, being mostly active in North America.

Market Leaders are (in alphabetical order):

- IBM
- ForgeRock
- Okta

3 Correlated View

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

3.1 The Market/Product Matrix

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

Figure 7: The Market/Product Matrix.

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

This graphic shows a state of the market that reflects the fact that this is a still emerging market, with relatively few offerings having reached the state of maturity and completeness making them Product Leaders, and still few vendors that are perceived as Market Leaders.

In the upper right corner, we only find IBM and ForgeRock, which are both rated as Product Leaders and

Market Leaders. They are offering overall comprehensive solutions and deliver these as integrated platforms to the market, also having a significant market share and strong global presence and ecosystem.

Left to these two, we find Okta, which also performs strong in the market, but still lack some of the capabilities that would make them a Product Leader, specifically around User Lifecycle Management and Access Governance. However, we see a strong potential of Okta evolving further towards Product Leadership as well.

In the segment at the middle right, we find Broadcom, EmpowerID and Simeio, all having already reached a state of maturity that places them amongst the Product Leaders, while not being Market Leaders. We see a good potential for them to further grow, based on their strong technology offerings.

All other vendors are found in the center of the graphic, being challengers regarding both market and product leadership. Some of them are close to entering the upper right segment of being leader in both market and product ratings. Overall, all vendors in this analysis show strong potential for delivering to the emerging Identity Fabrics paradigm and market and being a cornerstone in the Identity Fabrics of end-user organizations.

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

3.2 The Product/Innovation Matrix

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

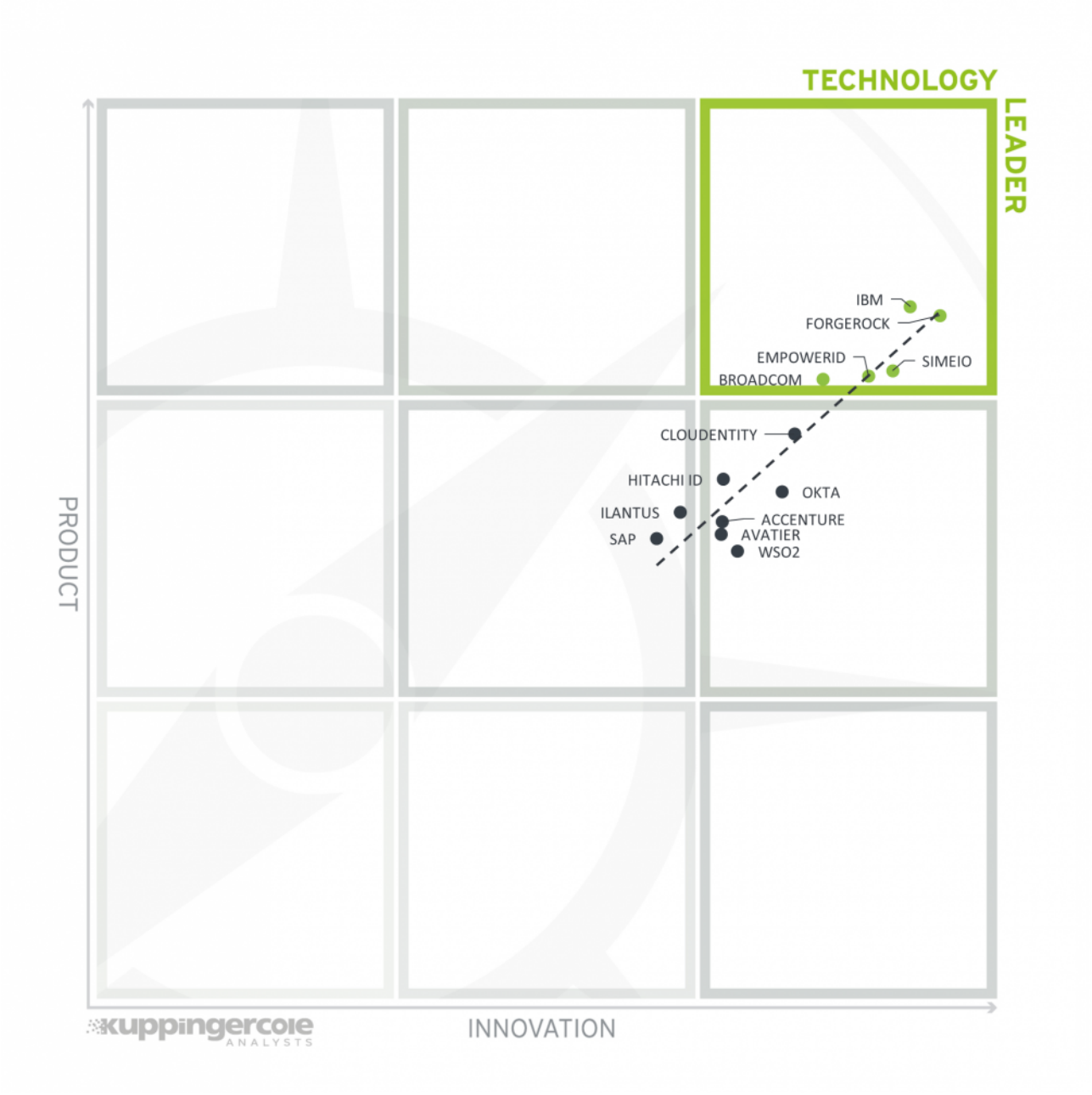


Figure 8: The Product/Innovation Matrix.

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

While there is a strong correlation between the two ratings, the graphic for the market segment of Identity Fabrics still looks uncommon, compared to many other market segments. The line of vendors is placed more to the right of the graphic, showing a high degree of innovation, while overall product maturity and completeness is lower. However, this is a typical representation for an emerging market segment such as Identity Fabrics, where we find a lot of innovative solutions that haven't yet reached the level of completeness and maturity making them Product Leaders. For Identity Fabrics with the broad range of

requirements on functionality and architecture, the bar for becoming a Product Leader is high, but we expect several of the vendors passing this soon.

In the upper right segment, we find, in alphabetical order, Broadcom, EmpowerID, ForgeRock, IBM, and Simeio. While these vendors all take different approaches for delivering a foundation for an Identity Fabric, all perform well in both the current product offering and the innovation they demonstrate.

Below them, to the middle right, we find – again in alphabetical order – Accenture, Avatier, Cloudentity, Hitachi ID, Okta, and WSO2. These vendors excel by the degree of innovation there are showing and are likely candidates for becoming Product Leaders in a future version of this Leadership Compass.

Last but not least, we find two vendors in the segment to the center, which are Ilantus and SAP. While they have their specific strengths in certain areas, they remain at a Challenger level in both product and innovation ratings.

Overall, we see a strong momentum in the market for delivering modern, comprehensive IAM solutions that enable customers building their own Identity Fabric. There are many offerings to choose from, plus a wide range of additional IAM solutions in other market segments to add to such cornerstones of an Identity Fabric.

3.3 The Innovation/Market Matrix

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

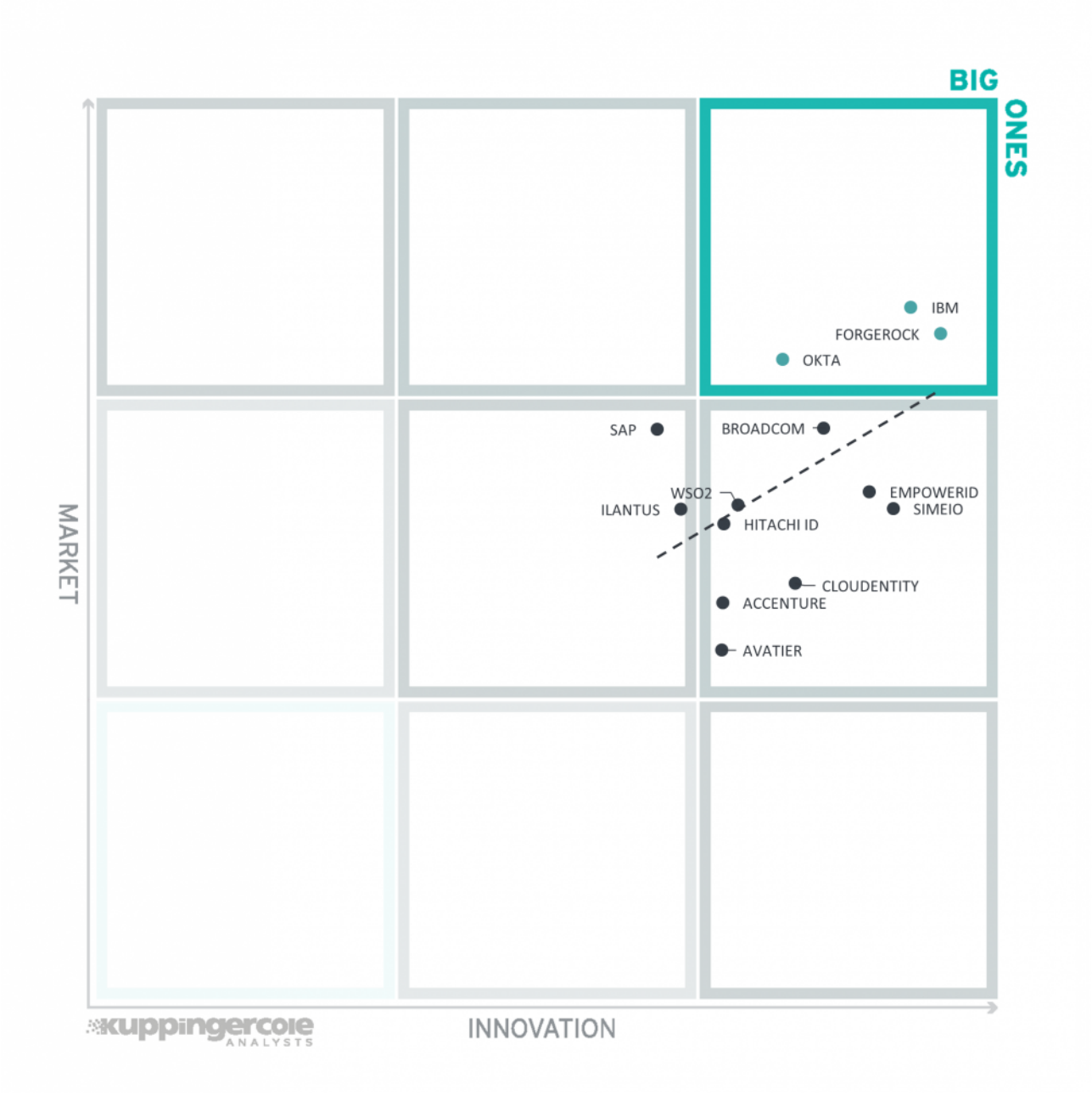


Figure 9: The Innovation/Market Matrix.

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

This graphic also shows a somewhat uncommon picture of a market, which is typical for emerging market segments with few Market Leaders, but many vendors showing strong innovation. In the upper right segment, we find ForgeRock, IBM, and Okta, which are rated as Leaders in both innovation and market. They have a strong potential in further increasing their position in the Identity Fabrics market.

Below them, to the middle right, we find – in alphabetical order again – several vendors that have been rated

as Innovation Leaders, but not yet as market leaders. Some of them are more to the bottom, showing that they still have some longer way to go in becoming market leaders, while others such as Broadcom are close to becoming a Market Leader. The vendors in this segment are Accenture, Avatier, Broadcom, Cloudentity, EmpowerID, Hitachi ID, Simeio, and WSO2.

Finally, there are two vendors in the center segment, which are challengers in both innovation and market leadership. Here, we find Ilantus and SAP.

4 Products and Vendors at a glance

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

4.1 Ratings at a glance

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

Product	Security	Functionality	Interoperability	Usability	Deployment
Accenture Security Memority	●	●	●	●	●
Avatier Identity AnyWhere	●	●	●	●	●
Broadcom Symantec Identity Service	●	●	●	●	●
Cloudentity Digital Identity Plane and Authorization Control Plane	●	●	●	●	●
EmpowerID	●	●	●	●	●
ForgeRock Identity Platform	●	●	●	●	●
Hitachi ID Bravura Security Fabric	●	●	●	●	●
IBM Security Verify	●	●	●	●	●
Ilantus Compact Identity	●	●	●	●	●
Okta Identity Cloud	●	●	●	●	●
SAP	●	●	●	●	●
Simeio Identity Orchestrator	●	●	●	●	●
WSO2 Identity Server	●	●	●	●	●
Legend		● critical	● weak	● neutral	● positive	● strong positive

Table 2: 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
Accenture Security	positive	neutral	strong positive	neutral
Avatier	positive	neutral	positive	neutral
Broadcom Inc.	strong positive	positive	strong positive	positive
Cloudentity	positive	neutral	neutral	neutral
EmpowerID	strong positive	positive	positive	positive
ForgeRock	strong positive	strong positive	positive	strong positive
Hitachi ID Systems	positive	positive	strong positive	positive
IBM	strong positive	strong positive	strong positive	strong positive
Ilantus Technologies	neutral	positive	positive	positive
Okta	positive	strong positive	positive	strong positive
SAP	positive	positive	strong positive	strong positive
Simeio Solutions	strong positive	positive	positive	neutral
WSO2	positive	positive	positive	positive
Legend	critical	weak	neutral	positive	strong positive

Table 3: Comparative overview of the ratings for vendors

5 Product/service evaluation

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

Spider graphs

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

- Architecture & Deployment
  This category represents the combination of the architecture and the deployment options. In architecture, we look at the type of architecture and focus on modern, modular architectures based on microservices. This also affects deployment, given that container-based deployments provide good flexibility. For deployment, supporting a range of models including as-a-service deployments is preferred.
- Customization & APIs
  This category is related to the architecture but focuses more on the comprehensiveness of APIs and the simplicity of customization. Our expectation on modern solutions for Identity Fabrics is that all custom code can be segregated into separate modules/microservices and is not affected by release updates. This also requires stable APIs. APIs furthermore build the foundation for providing an Identity API Layer to digital services and for orchestration with other services.
- Identity Types
  In this category, we focus on a broad support for different identity types including employees, partner, customers, and consumers, but also devices, things, and services. Supporting a broad variety of different types of identities allows Identity Fabrics to provide seamless yet controlled and secure access for everyone and everything to every service.
- Identity Lifecycles
  Here, we look at the baseline capabilities for Identity Lifecycle Management and User Provisioning as part of the IGA capabilities within Identity Fabrics. Features such as flexible workflows and a broad range of connectors to both traditional systems and cloud services add to this rating.

- Access Governance & Risk
  As the second part of IGA, Access Governance and Access Risk Management, including Access Analytics, are represented by this axis of the spider charts.
- Access Management
  In this area, we rate the Access Management capabilities such as Identity Federation support, Adaptive Authentication, and support for flexible, policy-based authorization. This is one of the main categories, given that Access Management is at the core of every Identity Fabric.
- Legacy IAM Support
  Given that organizations rarely can implement a green field approach in IT, supporting existing applications and integrating the legacy IAM is essential for a migration towards a modern Identity Fabric at the pace of the customer. Thus, supporting legacy IAM and legacy applications is an essential element in our rating of solutions that deliver to Identity Fabrics.
- Extended IAM Capabilities
  These include features beyond Access Management and IGA, such as PAM (Privileged Access Management) and others, as long as these are part of the offering of the vendor.

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

5.1 Accenture Security

Accenture is one of the largest consultancies globally. Part of their offering is Accenture Memority, an integrated solution that supports most areas of IAM, specifically IGA and Access Management. The unit of Accenture developing Memority is based in France, as most of the current customers using Memority are. Accenture has some very large installations of Memority deployed.

From a feature perspective, Memority covers a broad range of features, but lacks the depth of capabilities found in some of the leading-edge products in certain areas. This is specifically true for Access Governance, where Memority only has baseline capabilities. On the other hand, Memority excels with strong IoT support and a proven high scalability. Focusing on IGA and Access Management, there is no support for extended IAM capabilities such as PAM. Customers would need to rely on 3rd party vendors here. However, Memority supports segregating administrative accounts from regular user accounts, thus enabling applying separate security policies and management by 3rd party tools to these.

Being a relatively young product, Memority has a modern, modular architecture and provides a

comprehensive set of APIs. Deployment is flexible. On-premises installations are supported, as well as managed services can be provided by Accenture, and as Memority can run in public clouds. Commonly, Accenture itself is involved into deployment and customization. This is beneficial in that Accenture provides global services. However, Memority as of now has no external partners supporting customers in deployment and customization.

Accenture positions Memority as an Identity Fabric solution, which is valid given the architecture and breadth of supported features. Accenture with its services and practices can support in adapting Memority to specific needs of certain industries.

In sum, Accenture Memority is an interesting solution in the area of Identity Fabrics, specifically with respect to the ability of Accenture in supporting industry-specific solution and global deployments and operations. There is a buy-in into Accenture services as a logical consequence of opting for Memority.

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

accenture

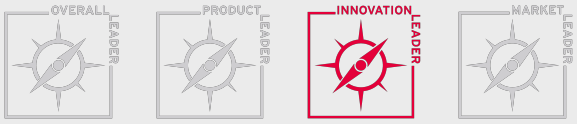
Strengths

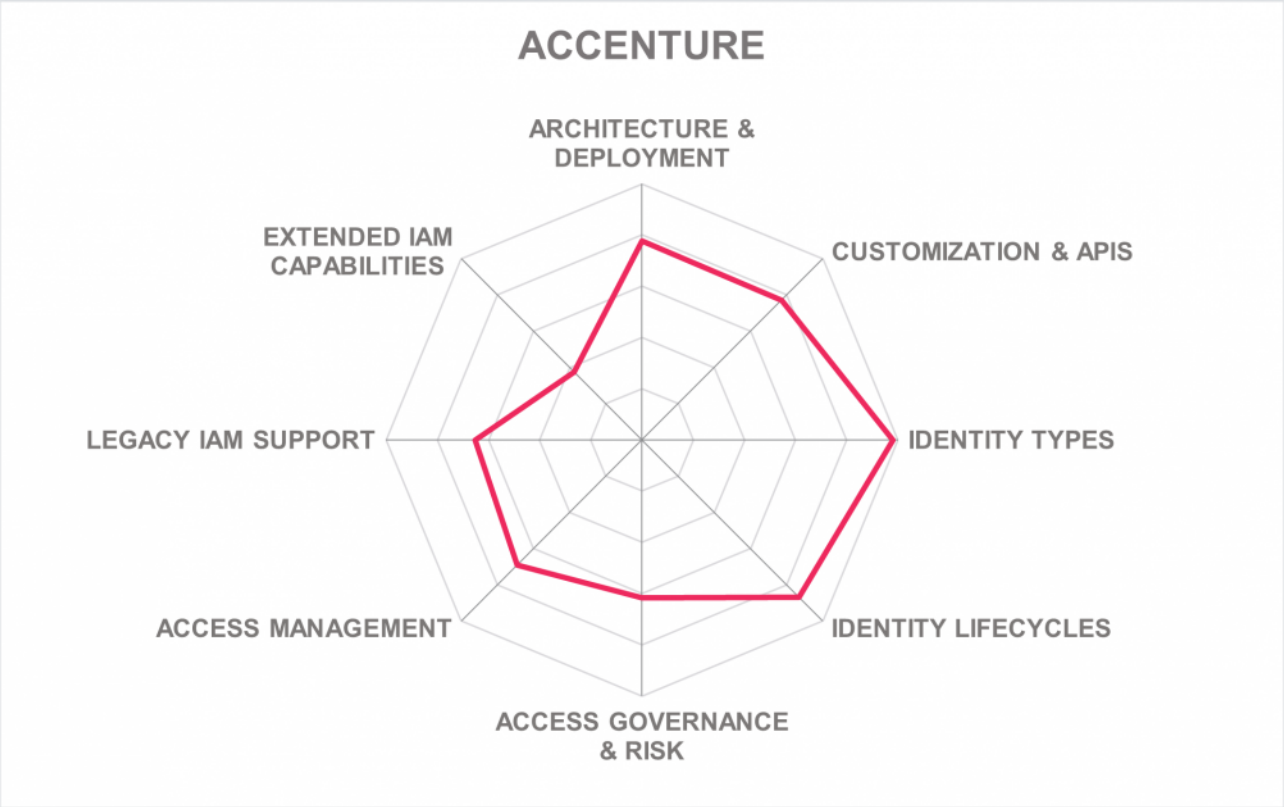
- Integrates IGA and Access Management capabilities into a unified offering
- Comprehensive set of APIs
- Modern, modular architecture
- Excellent support for a broad range of identity types, including connected things
- Ability to deliver industry-specific implementations based on Accenture practices
- Commitment to supporting modern standards

Challenges

- Only baseline Access Governance capabilities
- Broad set of capabilities, but sometimes lacking the depth found with other providers, e.g. for reporting
- No partner ecosystem outside of Accenture
- Still relatively low number of customers and presence focused on central Europe

Leader in





5.2 Avatier

Avatier is an U.S.-based vendor that provides a suite of IAM solutions, Identity Anywhere. This suite supports a range of capabilities, including IGA and Access Management. Most of the customers of Avatier are mid-market companies, with some large enterprise customers. A specific strength of Avatier is their strong focus on delivering modern, innovative user experience.

Avatier Identity Anywhere comes with a good breadth of features and depth in certain areas such as Identity Lifecycle Management. On the other side, we see gaps in the depth of capabilities in some areas such as Access Management or the full breadth of support for identity types such as things or consumers. Identity Anywhere also does not deliver support for extending IAM capabilities such as PAM. Overall, the solution delivers a good foundation for building an Identity Fabric, specifically for the requirements of mid-market companies.

Deployment of Avatier Identity Anywhere is container-based, which allows the solution to be operated in a range of deployment models. However, the as-a-service offerings are limited, also due to the relatively low number of partners Avatier has and the lack of a global presence. Most of Avatier's business is still focused on North America.

As mentioned above, Avatier always had a focus on providing modern, innovative user experience. They provide e.g., integrations into ServiceNow based on ServiceNow apps, but also chat bots, Microsoft Teams integration, and strong mobile support, which provides easy access to the capabilities.

Avatier is an interesting alternative to the established vendors, specifically for mid-market companies in North America. If Avatier manages to extend their global ecosystem, that solution will also become of more interest to organizations in other regions.
Technically, it provides good capabilities, while lacking the depth of features in certain areas that some other offerings in the market provide.

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

AVATIER

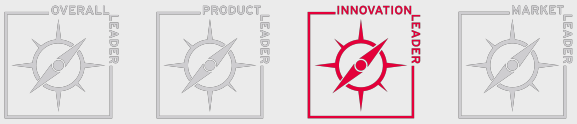
Strengths

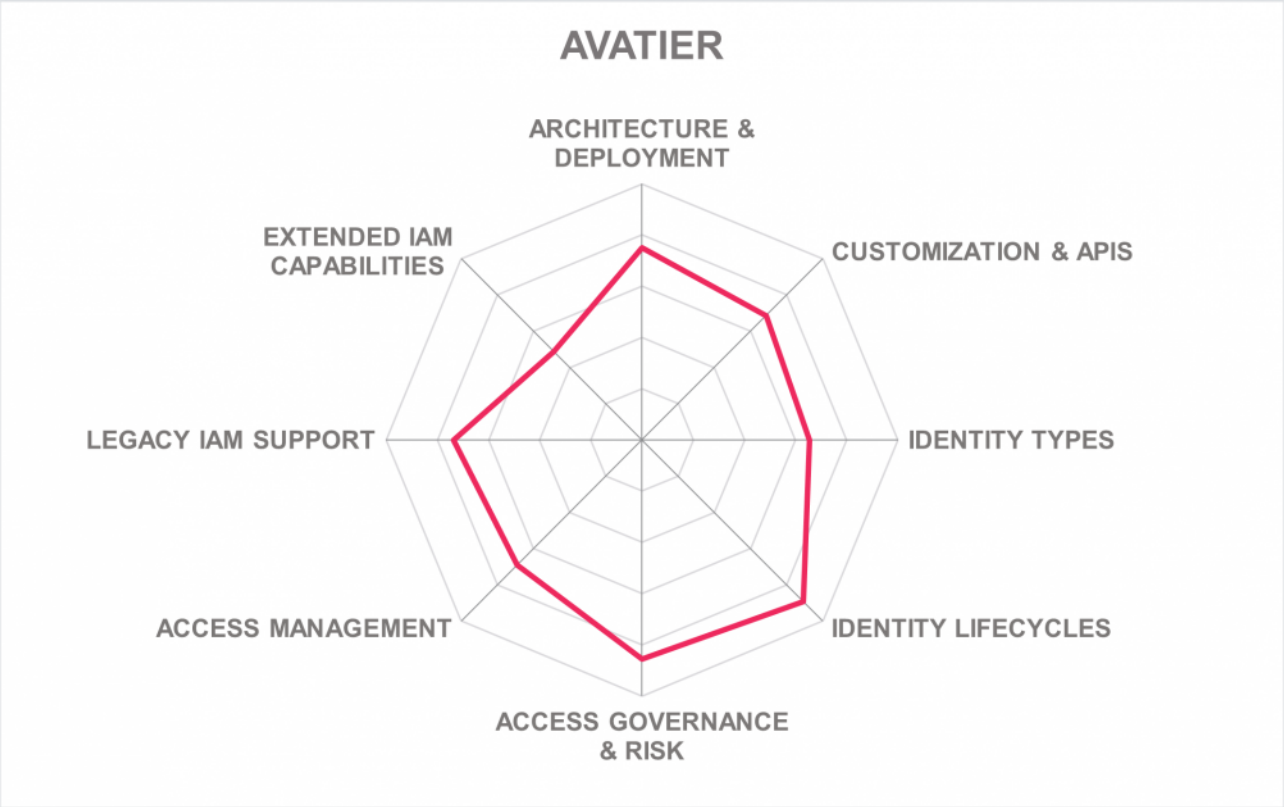
- Good set of capabilities for IGA and Access Management
- Established vendor with a long-standing presence in the market
- Modern, innovative user experience and strong mobile support
- Out-of-the-box integration into ServiceNow
- Out-of-the-box integration into hundreds of applications for Access Management
- Container-based deployment

Challenges

- Lacks depth of features in certain areas, such as adaptive authentication
- No support for extended IAM capabilities such as PAM
- Very limited presence and partner ecosystem outside of North America
- Limited options for managed service and as-a-service deployments

Leader in





5.3 Broadcom Inc.

Broadcom and the Symantec Identity Service have emerged following the mergers of Broadcom, CA Technologies, and Symantec. The Symantec Identity Service thus comprises multiple solutions for Access Management, Authentication, IGA, and Privileged Access Management. These are based on several existing products such Symantec SiteMinder, Symantec IGA, Symantec Directory, Symantec VIP, and Symantec PAM. These products are all integrated via open standards, with deeper level integrations provided where they add value above a standards-based approach.

Based on that broad set of technologies, the Symantec Identity Service delivers both breadth and depth in capabilities across all major areas of IAM. This includes legacy support in both integrating with existing IAM services and integrating with legacy applications. All components within the solution are mature, while having undergone significant modernization and improvements over the past years.

On the other hand, the Symantec Identity Service is a set of components with different roots, lacking a common architecture, and with most components not being fully modernized. Positively, the Symantec Identity Service supports a range of deployment options as well as good support for standards and comprehensive APIs. However, due to the different legacies of the components, while there are comprehensive APIs, there is no consistent API layer yet.

It also is proven to scale well in large installations. Broadcom is targeting such large customer installations, which are, together with the service offerings, better able to handle the complexity inherent to such a bundle

of established products.

Broadcom positions itself as a provider of enterprise solutions for large businesses. In that context, the Symantec Identity Service is an interesting option as a foundation for an Identity Fabric, despite some need for further modernizing components of that service. Backed by a global ecosystem, the company can deploy such solutions. Furthermore, there are strong integrations, both technical and in licensing, to the security portfolio of Broadcom, which might be of interest to enterprise customers.

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

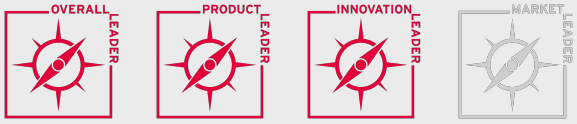
Strengths

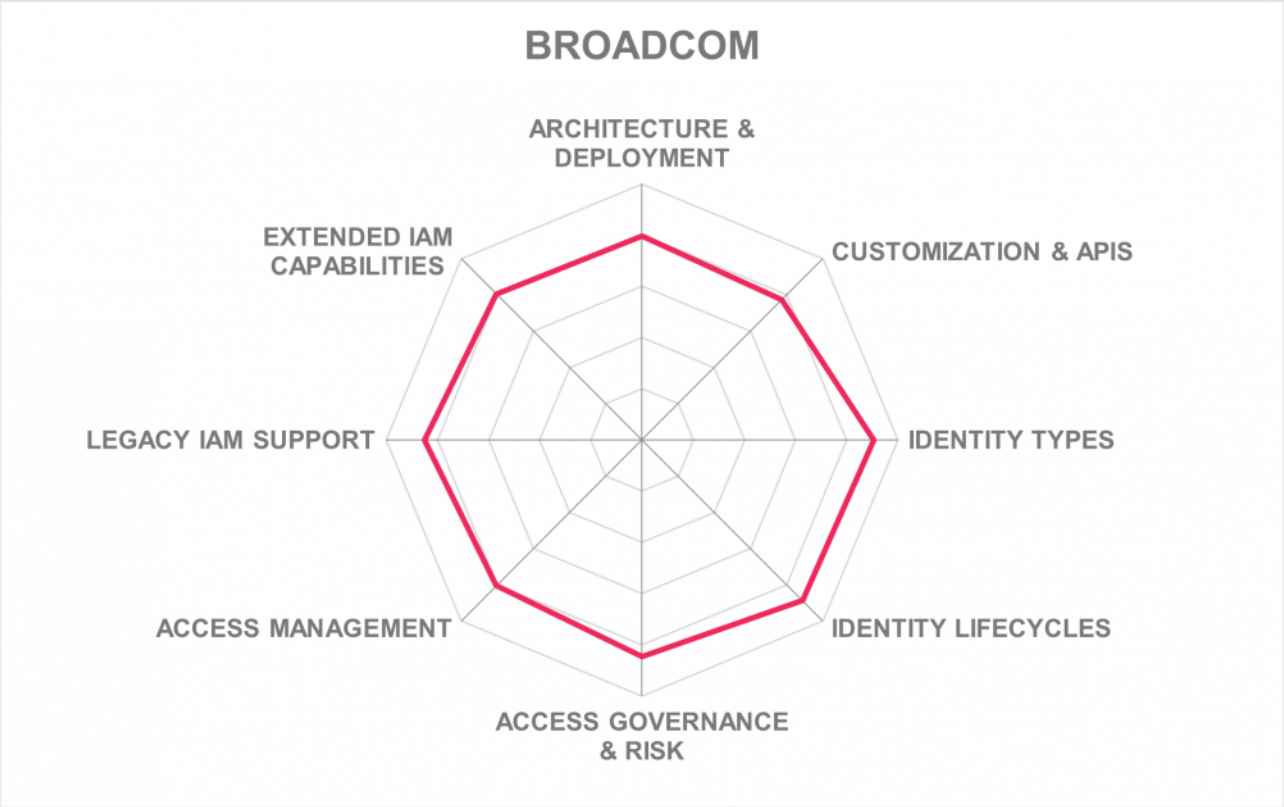
- Proven set of solutions bundled and integrated into a common service
- Broad range of managed service offerings
- Comprehensive set of capabilities comprising IGA, Access Management, and PAM
- Global ecosystem and ability to scale for large enterprise deployments
- Integration with the security portfolio of Broadcom

Challenges

- Not all components are already fully migrated into a microservices architecture
- Not well-suited for mid-market and SMB organizations
- Will require significant amounts of professional services in deployment and customization

Leader in





5.4 Cloudentity

Cloudentity is a relatively young vendor in the broader IAM market that delivers solutions for managing identities and controlling authorization at the API level. That makes them an interesting vendor for future Identity Fabrics, delivering strong Access Management capabilities, providing a modern architecture, and providing full control on the APIs and their authorization.

Cloudentity's unique approach focuses on building an Identity Fabric that bridges clouds, existing IdPs and APIs through the usage of Identity Authorization by normalizing data and authorization across application endpoints. Key features include automated discovery of applications and services, automated onboarding of applications and automated protection through NIST and industry specific policy packs. The Cloudentity platform is built as a set of highly scalable, distributed microservices that can be delivered in a SaaS or managed SaaS model providing customers with flexible deployment options for cloud and edge protection.

The first product in scope is Cloudentity Authorization Control Plane. This product focuses on context-aware authorization at the API level. It provides capabilities such as API Discovery and Catalog, Consent Management, Authorization Policy Governance, and several more. This component provides strong capabilities for exposing a common set of identity APIs and thus creating an Identity API Layer as part of an Identity Fabric. Cloudentity also provides a specialized API Security solution named MicroPerimeter.

The second main product we looked at is Cloudentity Identity Plane. This solution focuses on Access Management and covers capabilities such as user registration, MFA, SSO and BYOD support, and

delegated administration. While the main focus of the solution is on B2C and B2B use cases, it also can support other types of services. Furthermore, in combination with the other components, there is strong support for other identity types such as services.

With this focus, Cloudentity scores well in some of the areas we are looking for in our Identity Fabrics evaluation. While there are gaps when it comes to supporting legacy IAM and IGA, Cloudentity's focus is not to replace existing IAM and IGA infrastructure, but to enhance and expand customers' existing infrastructure. This provides a bridge from legacy solutions to modern hybrid, multi-cloud ecosystems. Cloudentity's "Bring Your Own IdP" and "Bring Your Own Gateway" approach should complement other vendor products or services needed for delivering a comprehensive Identity Fabric.

Cloudentity, being a rather young vendor, has a still relatively small global partner ecosystem, compared to many of the other vendors. On the other hand, Cloudentity is very innovative and provides a modern solution that fits well to the architecture requirements of a modern Identity Fabric.

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

CLOUDENTITY™

CUSTOMER IDENTITY AT CLOUD SPEED

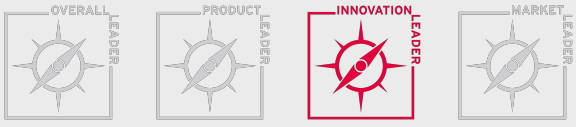
Strengths

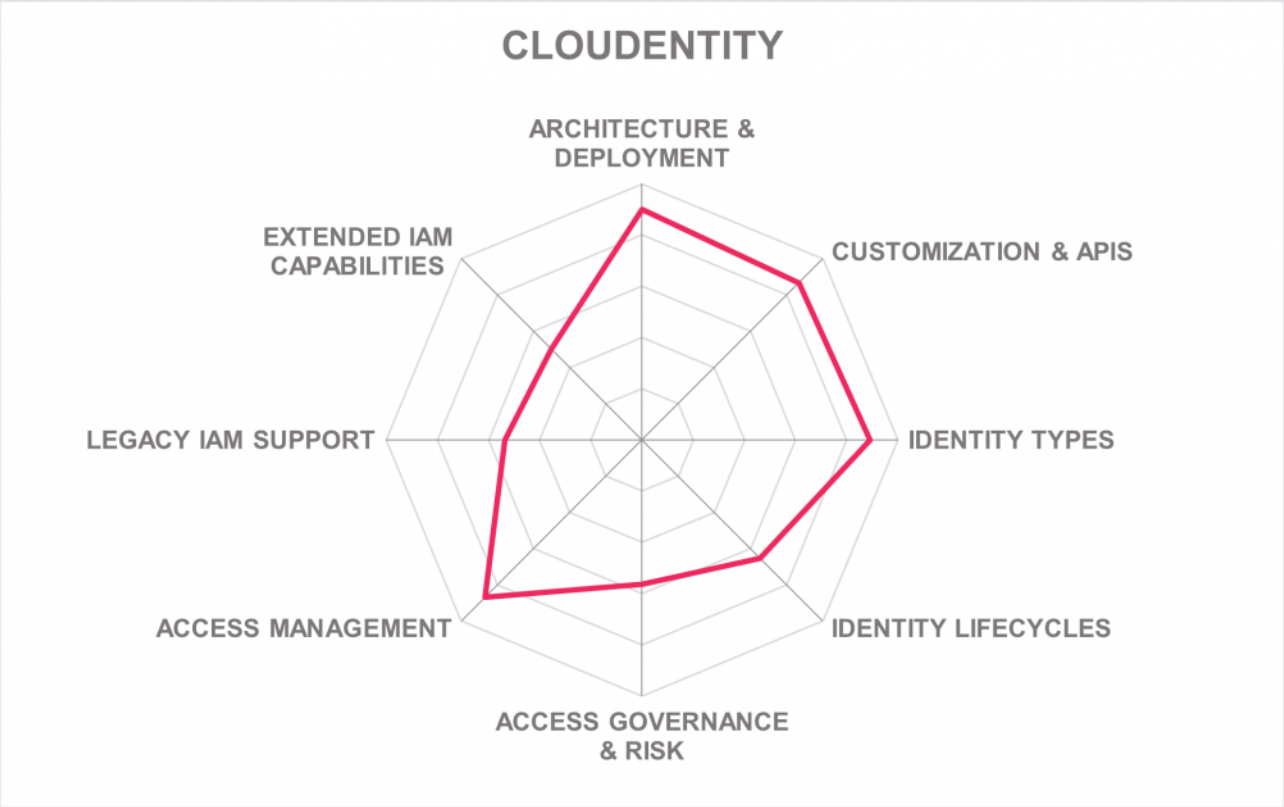
- Strong API Management and API Security capabilities
- Excellent foundation for exposing, managing, and securing a consistent Identity API Layer
- Central management of authorizations at the API level, including API Governance
- Might complement existing legacy IAM and other vendor's IAM solutions in an IAM Fabric with additional services
- Strong Access Management capabilities, specifically for B2C and B2B use cases
- Modern architecture

Challenges

- Limited capabilities in IGA, specifically Access Governance
- No support for extended IAM capabilities such as PAM
- Still a relatively young vendor with a limited number of customers
- Small but growing global partner ecosystem

Leader in





5.5 EmpowerID

EmpowerID with its set of modules for IAM is one of the very few vendors in the market that provide a comprehensive, integrated solution for all areas of IAM. While there is a focus on IGA, the solution also covers Access Management and PAM. It also integrates well with Microsoft Azure Active Directory, utilizing the Access Management capabilities and extending the IGA and other services.

EmpowerID always has focused on providing an integrated IAM stack that covers all major capabilities. Some of these such as PAM (Privileged Access Management) are more baseline capabilities, while EmpowerID provides leading-edge IGA features, including strong workflow capabilities and well-thought-out integration capabilities for modern SaaS services based on a unified SCIM connector that is easy to adapt for different SaaS services.

From an architecture perspective, EmpowerID benefits from its approach for providing an integrated set of solutions. The vast majority of modules within the solution has been modernized over the past years and suits our requirements for a modern, microservices-based architecture. Additionally, EmpowerID comes with a consistent set of APIs that allow for efficient and proven customization and orchestration. The solution also provides a good standard integration to ServiceNow.

EmpowerID supports various deployment models, from traditional on-premises deployments to SaaS deployments, either on an IaaS platform or operated by managed service partners. EmpowerID has a growing number of partners, including some of the very large consultancies, across the regions.

EmpowerID, despite still being a relatively small vendor, has demonstrated its ability to serve customers in different geographies and at different scale. With its integrated approach, it is an interesting foundation for building an Identity Fabric specifically for mid-market companies, but also larger organizations looking for an integrated approach with a strong set of capabilities.

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

empowerID

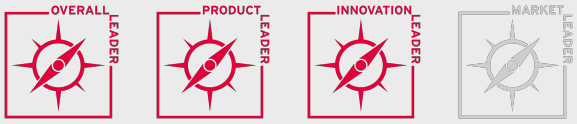
Strengths

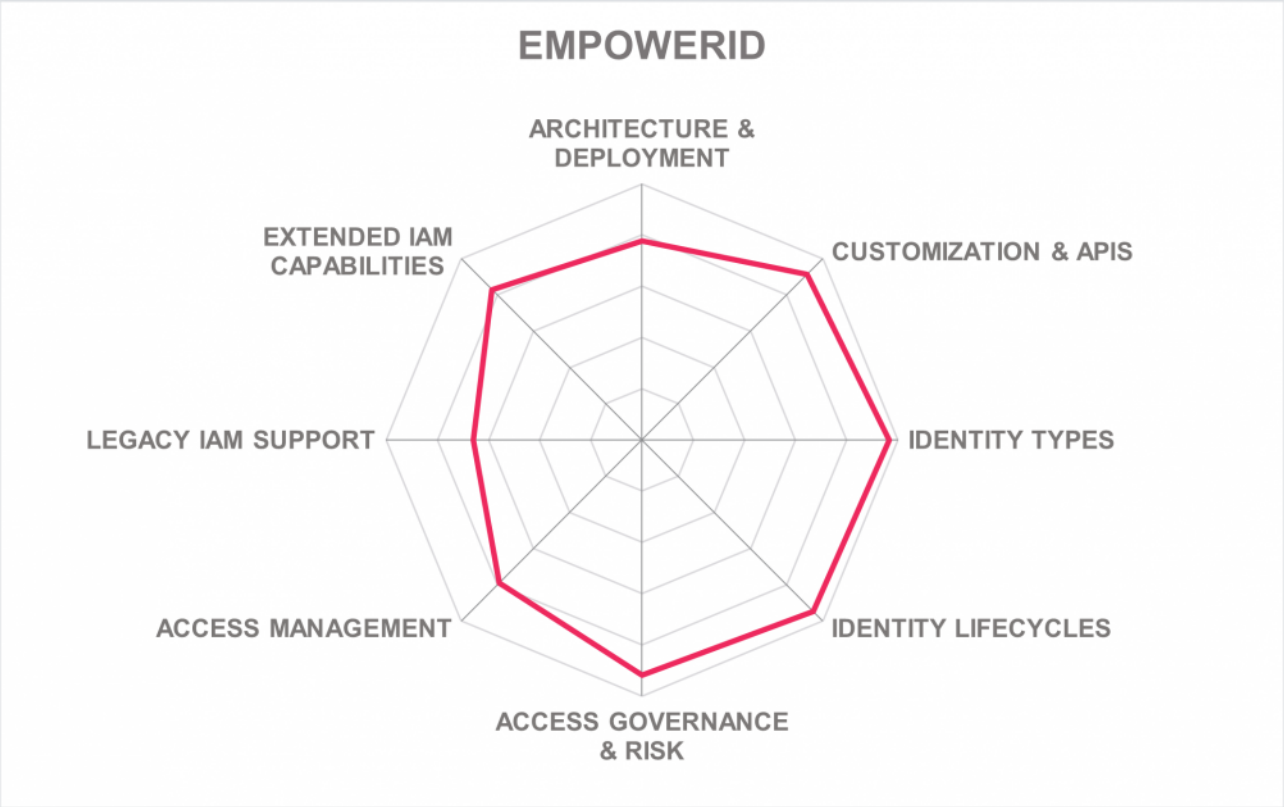
- Integrated suite, covering all major areas of IAM including PAM
- Good breadth and depth of features, specifically for IGA and Access Management
- Integrates neatly with Microsoft Azure Active Directory for Access Management
- Various innovative features, such as for connecting to SaaS services
- Broad set of APIs for flexible customization and orchestration with other services
- Out-of-the-box integration with ServiceNow
- Modern architecture

Challenges

- Still a relatively small vendor, but with some very large customers
- Global partner ecosystem is growing, but still not very large
- Some few components still need modernization

Leader in





5.6 ForgeRock

The ForgeRock Identity Platform unifies the various IAM solutions provided by ForgeRock, such as the Identity Manager, Access Manager and other components including Directory Services. These solutions are well-established and can be deployed in a broad range of deployment models from on-premises deployments to SaaS.

At the core of the Identity Platform are the Access Management capabilities, supporting a wide range of features including flexible authentication flows for Adaptive Authentication. For IGA, ForgeRock is traditionally strong in User Lifecycle Management and Identity Provisioning.. ForgeRock also has added Access Governance capabilities at a good baseline level, which now are complemented by leading-edge AI-based services that help in analyzing risks, automating managing access entitlements, and augmenting users.

From a platform perspective, ForgeRock is an excellent fit for the Identity Fabrics market segment, delivering a modern, modular solution with an extensive set of APIs and the ability to manage these APIs. ForgeRock always has been targeted at delivering platforms for IAM infrastructures and customizing these to specific business demands, including supporting Digital Transformation needs.

In contrast to some of the other vendors, ForgeRock does not deliver extended IAM capabilities such as Privilege Management. On the other hand, they deliver a very strong portfolio around the core disciplines of IGA and Access Management, making them a Leader in the market for Identity Fabrics and an interesting

foundation for organizations building their own Identity Fabric.

With the breadth and depth of functionality and the architecture, ForgeRock positions itself as one of the leaders for delivering the foundation of an Identity Fabric. ForgeRock has a global partner ecosystem and presence, and has proven its ability of satisfying very complex, high scalability requirements.

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

FORGEROCK

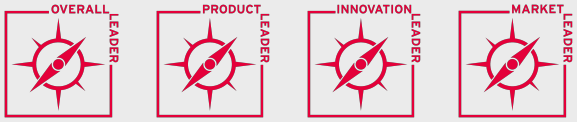
Strengths

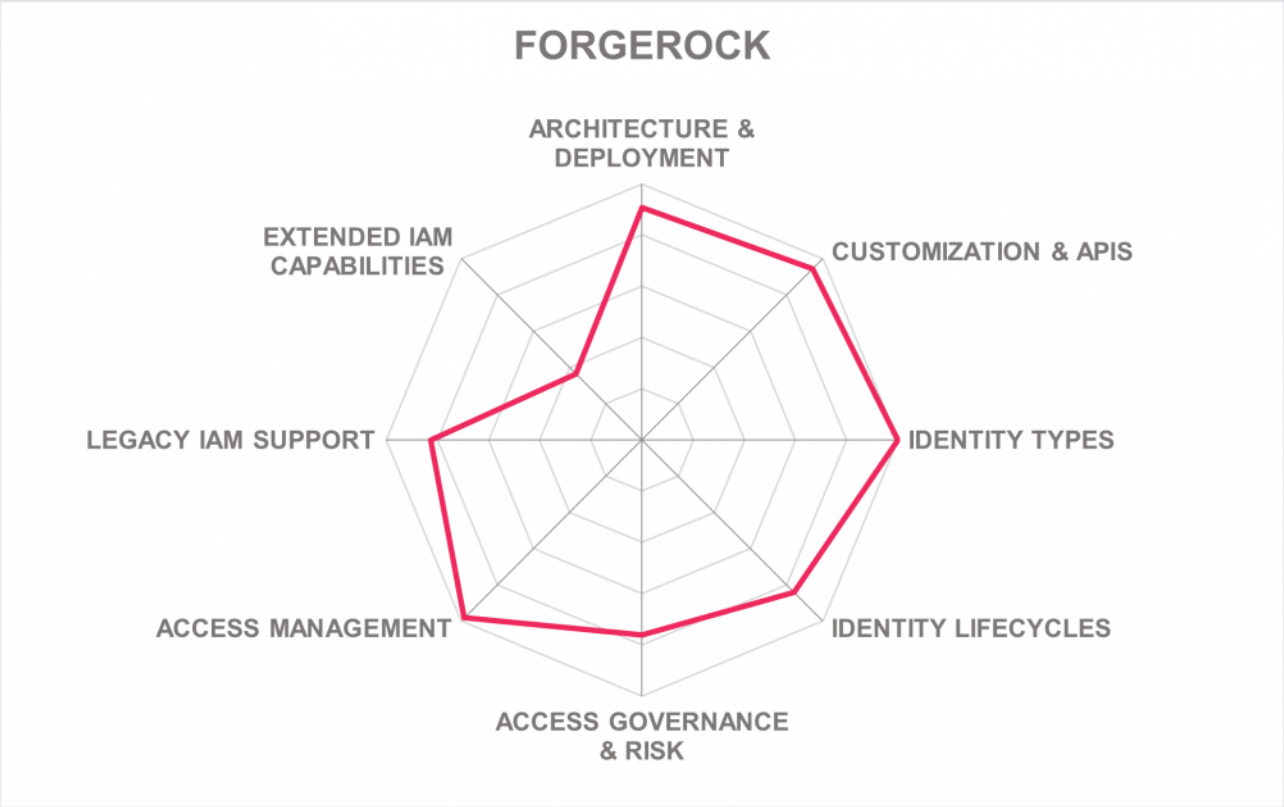
- Leading-edge Access Management capabilities, including strong features for Adaptive Authentication
- Strong features for User Lifecycle Management and Identity Provisioning
- Innovative AI-based capabilities for augmenting users in managing access requests
- Modern architecture with a comprehensive set of APIs
- Broad range of deployment models supported
- Proven scalability

Challenges

- Standard Access Governance capabilities are at good baseline level
- No support for extended IAM capabilities such as PAM
- Somewhat developer-centric, but demonstrating significant increase in user experience, e.g. with their user journey tree framework (intelligent access)

Leader in





5.7 Hitachi ID Systems

Hitachi ID is an established player in the IAM market, backed by Hitachi as the parent company. Hitachi ID recently has restructured and renamed its portfolio, and has extended it by adding a threat detection layer. The overall solution is named Hitachi ID Bravura Security Fabric, with the IAM components Bravura Identity (IGA), Bravura Privilege (PAM), and Bravura Pass (Authentication and Access Management). The concept of the Security Fabric aligns well with the Identity Fabric paradigm.

Of the three core components of the Hitachi-ID Bravura Security Fabric, which are complemented by Hitachi ID Bravura Group for Group Management and Hitachi ID Bravura Discover for Risk and Threat Asssessment, the Bravura Identity and Bravura Privilege are the two most mature components. Both are delivering proven capabilities in their respective areas, providing both the breadth and the depth of features required.

Bravura Pass has evolved from a password and authentication solution towards a more comprehensive Access Management offering, supporting SAML-based logins to other systems. While this solution is very strong in the support of authenticators, there are gaps when it comes to connecting to target systems, due to a weak support for modern standards such as OIDC (Open ID Connect), and for traditional Web Access Management capabilities in connecting back to legacy systems not supporting federation standards.

While Hitachi ID supports a wide range of deployment models, the architecture of the various components is still more traditional. We expect to see some major modernization of the underlying platform in the future,

but this might be considered a limiting factor when building an Identity Fabric.

Hitachi ID benefits from its parent company, which also can provide extensive services for deploying and operating the Bravura Security Fabric. Aside of that, Hitachi ID has an acceptable level of global partner ecosystem. Hitachi ID is a solid option in this market segment, despite the need of further modernizing and extending (specifically around Access Management) the solutions.

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

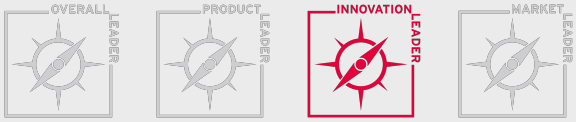
Strengths

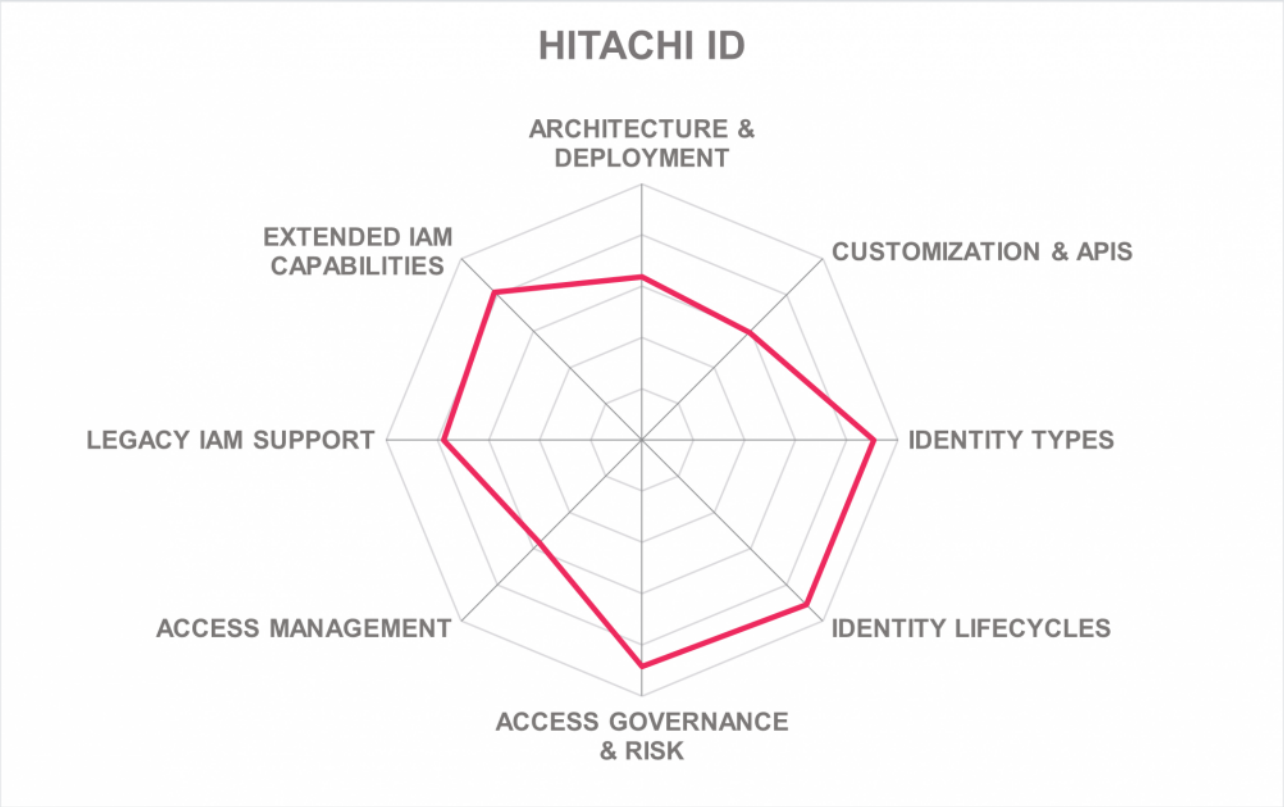
- Strong IGA capabilities, both in breadth and depth of features
- Strong PAM capabilities
- Conceptually following a “Fabric” approach in integrating a comprehensive solution
- Excellent capabilities for managing authentication
- Good support for various deployment models and own system integrator services
- Backed by large parent company

Challenges

- Relatively weak in Access Management capabilities, specifically Identity Federation and Web Access Management
- Solution needs some modernization and increased modularity
- Still relatively small but growing partner ecosystem

Leader in





5.8 IBM

IBM over the past years has developed a modern IAM solution that is provided as-a-service, but also supported in other deployment models. With IBM being a cloud provider, but also a leading system integrator, they can support a variety of options for their customers. IBM Security Verify is the solution formerly named IBM Security Cloud Identity.

From a feature perspective, IBM Security Verify counts amongst the most comprehensive offerings in the market, making them a leader amongst the solutions that can become the foundation of an Identity Fabric. IBM Security Verify supports Access Management, IGA, and – via their OEM relationship with Thycotic – also PAM capabilities.

Most features are provided via the modern IBM Security Verify product. However, for supporting legacy applications and some extended capabilities beyond the good standard capabilities within IBM Security Verify, the solution can seamlessly integrate with Verify Governance (previously ISIGI, IBM Security Identity Governance and Intelligence) and Verify Access (previously ISAM, IBM Security Access Manager). Which set of components is chosen will depend on the specific capabilities required. From a deployment perspective, a combined roll-out and operation of IBM Security Verify together with Verify Governance and Verify Access is somewhat more complex, but well-supported by standard deployment and operation schemes.

IBM also benefits from its integration to other IBM services such as IBM QRadar, adding additional

capabilities. As aforementioned, aside of having a strong global partner ecosystem, IBM also can deploy and operate the solution based on its own services, i.e., not relying on other IaaS providers for a SaaS-style deployment of the solution.

With the significant investment IBM has made over the past years into building a new, cloud-native IAM platform, IBM Security Verify, IBM positions itself as a leader in the IAM space and provides and interesting, feature-rich, and modern solution for customers that intend to build their own Identity Fabric.

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

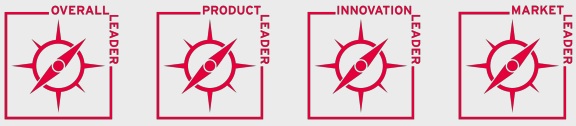
Strengths

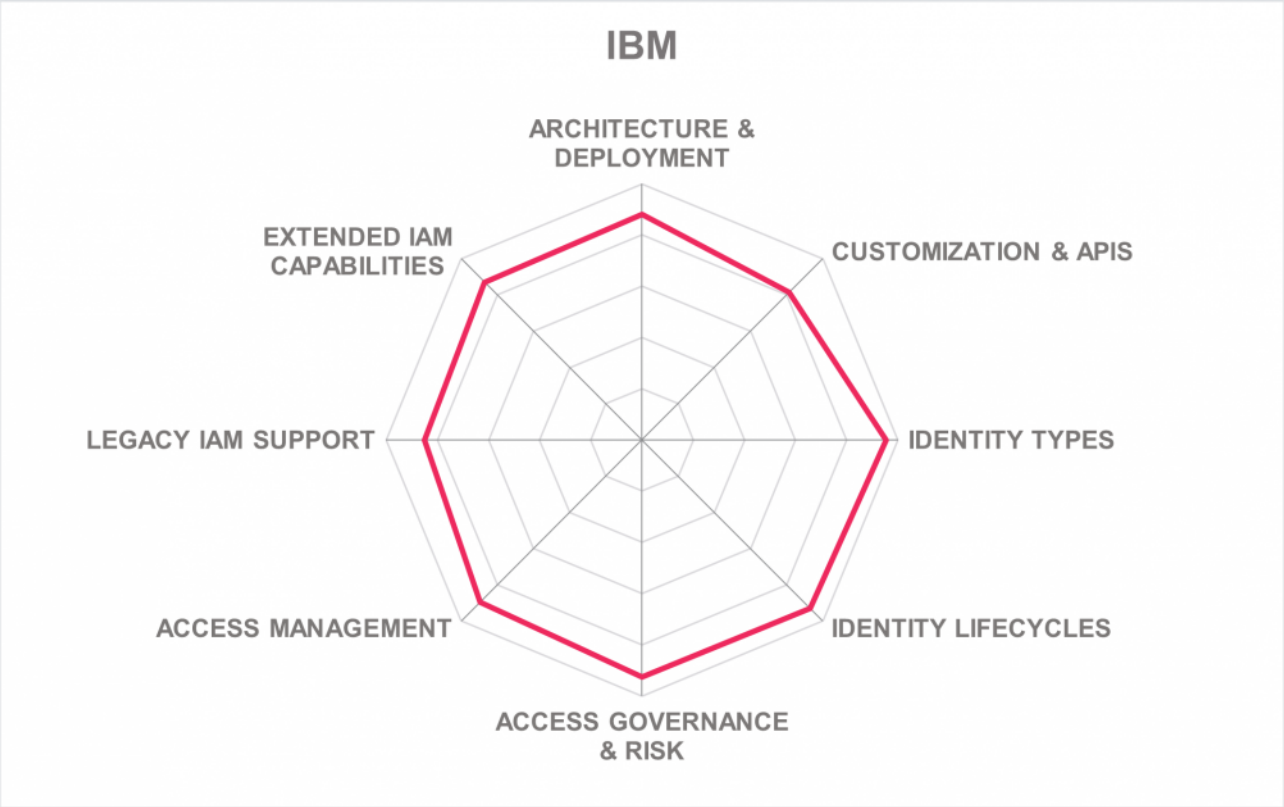
- Very broad set of capabilities across Access Management, IGA, and PAM
- Modern architecture, developed as cloud-native solution
- Own cloud services and professional services
- Strong legacy support, both directly and via integration to Verify Governance (previously ISIGI) and Verify Access (previously ISAM)
- Integrates with a range of other IBM offerings such as IBM QRadar
- Strong global partner ecosystem
- Proven scalability

Challenges

- PAM component is an OEM product, provided by Thycotic
- Advanced legacy integration might require ISIGI (now Verify Governance, included in SaaS entitlement) and ISAM (now Verify Access), adding some complexity in deployment and operations
- Advanced features provided by other IBM solutions come at extra cost

Leader in





5.9 Ilantus Technologies

Ilantus , which started as a system integrator, has moved fast to provide offerings targeted at different types of customers. Their solution Compact Identity focuses on delivering IGA and AM capabilities from a single codebase that can meet more complex requirements on IGA. Additionally, Ilantus has offerings that cover the IDaaS and Access Management requirements in the market. Compact Identity also integrates a PAM solution, and with an integrated Web Access Management capability covers all aspects on the IAM stack.

Ilantus's Compact Identity product features cover identity administration, access management through authentication, SSO, authorization, password management, and access governance, but also offers PAM, some specific CIAM capabilities, and Identity Risk Analytics capabilities as well. The solution is provided as an IDaaS service, with options for other deployment types.

Ilantus Compact Identity differs from many of the other offerings in the IAM market in both the flexible deployment options, and the breadth of supported capabilities. It comes as a full IAM package, covering IGA, Access Management, PAM, and other capabilities that businesses require. While some of the capabilities are more at the baseline level, for both IGA and Access Management comprehensive capabilities are supported that will be sufficient for most businesses.

Ilantus continues to add innovative features now and on their roadmap, such as Identity Analytics that supports anomaly and other types of detections, as well as Robotic Process Automation (RPA) capabilities integrated for SSO and user lifecycle management activities.

Ilantus Compact Identity is an interesting alternative to the established offerings in the IAM market, specifically for mid-market companies and SMBs looking for an integrated offering servicing all major areas of IAM. However, even large businesses, in particular outside of the very heavily regulated industries, might benefit from the integrated approach and the flexible deployment options.

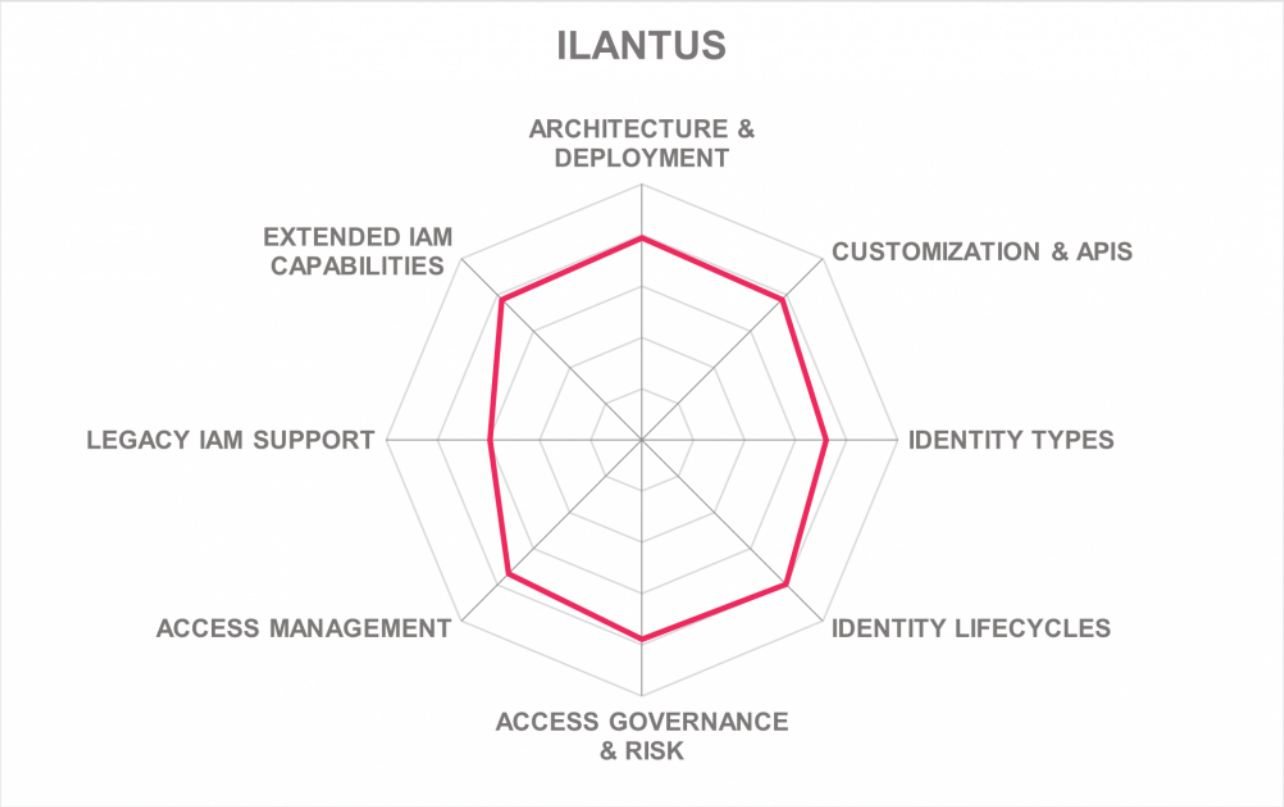
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●○

Strengths

- Service bundle tailored to meet the mid-market and, increasingly, large enterprise IDaaS requirements
- Good OOB support for enterprise-level cloud applications in addition to common on-premises systems
- Flexibility for customization of policies and workflows
- Good support for in-built MFA with contextual attributes
- Modern widget-based dashboarding
- Increased focus of enhancing user and administrative experience
- Designed to deliver quick application on-boarding and support lean IAM operations
- Innovative list of capabilities on roadmap

Challenges

- Customer presence is still primarily focused on US and a few Asian countries, still low but growing in EMEA
- Out-of-the-box reporting for major compliance frameworks just recently added
- Access Governance capabilities are good but not exceptional



5.10 Okta

Okta has, over the past years, grown to one of the leading providers of IDaaS (Identity as a Service) solutions. The Okta Identity Cloud has emerged beyond a service for providing SSO (Single Sign-On) to SaaS services towards an increasingly comprehensive platform covering different types of identities such as workforce and customers, and providing capabilities beyond the Access Management features.

While Access Management remains the key capability of Okta Identity Cloud, other capabilities include Directory Services, API Security, and Lifecycle Management. Additionally, Okta has recently added leading-edge workflow and orchestration capabilities that go well beyond what is commonly found in IGA solutions. Okta's workflow features allow for building workflows for multiple purposes and integrating all types of applications that expose REST APIs. Thus, they support Identity Lifecycle Management, but also integration to ITSM (IT Service Management) solutions.

In the area of Access Management, Okta has the well-known strong capabilities in Single Sign-On, Adaptive Authentication and MFA (Multi-Factor Authentication), but also provides an Access Gateway that supports in integrating with legacy applications that don't support modern federation standards.

For IGA, Okta provides good capabilities targeted at SaaS applications and some other common services such as Microsoft Active Directory, but lacks the breadth and depth of capabilities found in other IGA solutions, specifically around Access Governance and support for legacy applications. Furthermore, there is no integrated support for extended IAM capabilities such as PAM.

Due to the strong Access Management features, the modern approach to workflows, and with good capabilities for User Lifecycle Management to SaaS services, Okta Identity Cloud is an interesting option as a foundation for an Identity Fabric, either complemented by specialized IGA solutions for legacy environments and other services, or for customers that have low requirements in legacy integration. In contrast to most other vendors, Okta delivers its solution only as SaaS service and does not support other deployment models. There is support for Access Management to legacy applications through the Okta Access Gateway.

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

okta

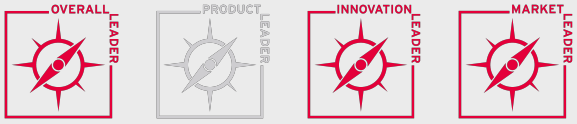
Strengths

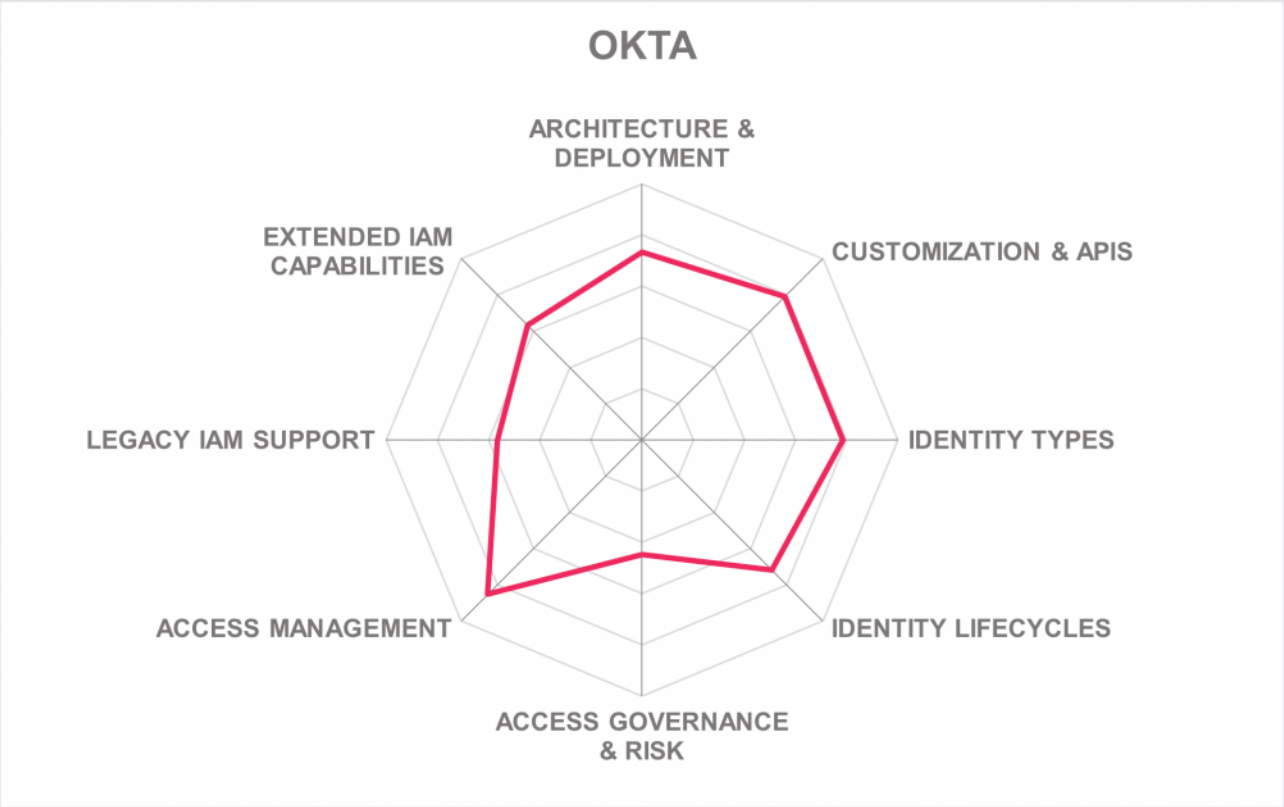
- Leading-edge Access Management capabilities
- Strong support for Adaptive Authentication and MFA
- Access Gateway to connect legacy applications
- Innovative, feature-rich workflow capabilities
- Integrates API Security
- Excellent support for connecting to SaaS applications
- Global partner ecosystem
- Lean deployment as SaaS service

Challenges

- Limited in Access Governance, but good User Lifecycle Management and Identity Provisioning to SaaS applications
- No support for advanced IAM capabilities, but some level of PAM capabilities
- Deployment limited to SaaS only

Leader in





5.11 SAP

SAP, as one of the leading global software vendors, has a number of IAM-related solutions in its portfolio, some specifically targeting the SAP environment, while others have a broader focus. The SAP portfolio for IAM comprises the following solutions: SAP Cloud Identity Access Governance, SAP Cloud Identity Authentication, SAP Cloud Identity Provisioning, SAP Identity Management, SAP Single Sign-on, SAP Dynamic Authorization Management, and SAP Access Violation Management.

At the core of the offerings that build the foundation for an Identity Fabric are the ones listed first, specifically the cloud-based offerings of SAP. IGA is covered by SAP Cloud Identity Access Governance and SAP Cloud Identity Provisioning, while SAP Cloud Identity Authentication delivers the Access Management capabilities. The other solutions complement these with additional support, either for traditional SAP environments, for on-premises targets, or with added capabilities such as SAP Dynamic Authorization Management.

Based on the range of solutions SAP is delivering, most common capabilities we expect to see in such solutions are provided, including Privileged Access Management (PAM) targeted on SAP environments. The two main challenges we see are the facts that various solutions are required for a comprehensive solution, and that the integrations to non-SAP systems still are limited, compared to other vendors. At least SAP is increasingly relying on open standards such as SCIM to expand its reach towards non-SAP solutions.

For customers that need to protect SAP business applications including SaaS services and that follow an

SAP-centric strategy, these solutions provide a good foundation for building the own Identity Fabric, while they are somewhat limited in supporting environments with a broad range of heterogenous systems, specifically legacy applications and legacy IAM services of other vendors.

SAP has a global partner ecosystem and presence that help in delivering their solutions. Furthermore, they can add other capabilities such as CIAM (Consumer IAM) as part of the SAP Customer Data Cloud, beyond core IAM capabilities. For organizations that broadly utilize SAP solutions, the SAP IAM solutions are an interesting option for building their Identity Fabric.

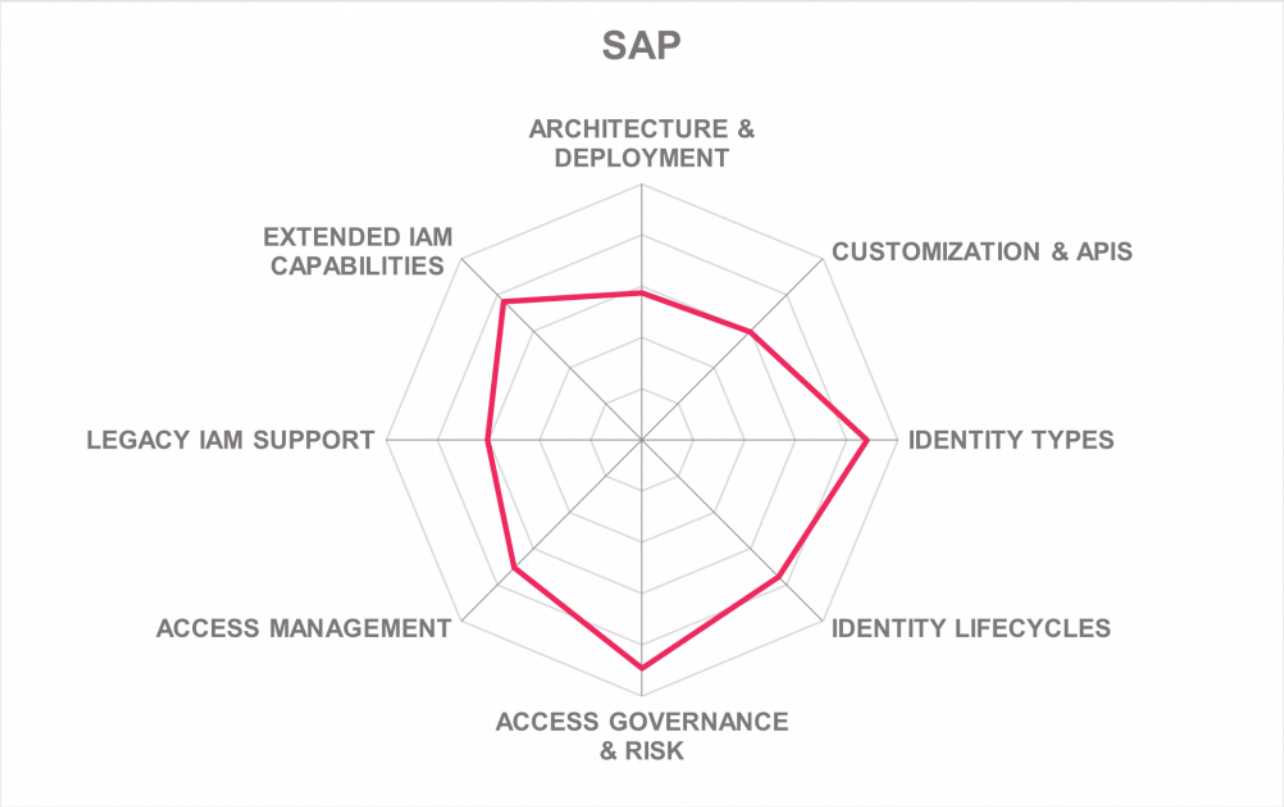
Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ○
Deployment	● ● ● ○ ○

Strengths

- Broad range for solutions for IAM
- Set of modern, cloud-based services for IGA and Access Management
- Additional solutions for many specific requirements such as Dynamic Authorization Management
- Increasingly good support for open standards such as SCIM, extending the reach to non-SAP applications
- Excellent coverage of specific requirements in SAP environments
- Strong global partner ecosystem and presence

Challenges

- Solution comprises a range of products, resulting in more complex deployment and operations
- Not all features/functions available via APIs across all solutions
- Support for non-SAP environments somewhat limited, specifically for legacy applications



5.12 Simeio Solutions

Simeio is a US-based vendor in the IAM market, delivering their Simeio Identity Orchestrator as a solution that supports customers in orchestrating IAM solutions that they have in place or that they deploy in addition to their current solutions. Thus, while Simeio Identity Orchestrator (IO) delivers a good set of IAM capabilities on its own, it also – as the name indicates – is an orchestration platform to integrate other IAM solutions. Moreover, Simeio IO adds a range of capabilities beyond what standard solutions provide.

Simeio is distinguished from other vendors that offer integration platforms or, more commonly, integrated offerings spanning multiple IAM tools, in both the breadth of their own capabilities provided, and in the breadth and number of IAM solutions supported. Simeio IO comes with integration capabilities for about one dozen IAM vendors, covering all major areas including IGA, Access Management, and PAM.

Notably, implementation of Simeio IO still will require system integrator work and customization, but Simeio has extensive experience in dealing with the rapid orchestration of a significant number of leading IAM solutions in the market.

Simeio not only provides the technology but also acts as the operator as well. Thus, deployment can be part of a managed services package, with existing solutions still running on-premises and Simeio acting as MSP (Managed Service Provider). Simeio can also operate all services as cloud-delivered IDaaS on behalf of customers. In these models, as is common practice, Simeio provides SLAs for availability, response time, resolution time, and performance.

Simeio IO follows a well-thought-out approach for adding a centralized layer on top of existing IAM solutions. This enables orchestration amongst multiple solutions by abstracting these functions. However, Simeio goes beyond merely integrating existing solutions and adds a range of their own capabilities in a modern microservices architecture. This makes Simeio IO an interesting option for building an own Identity Fabric.

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

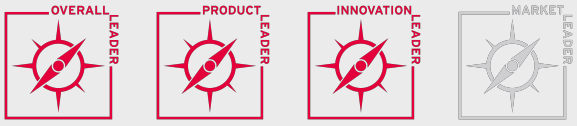
Strengths

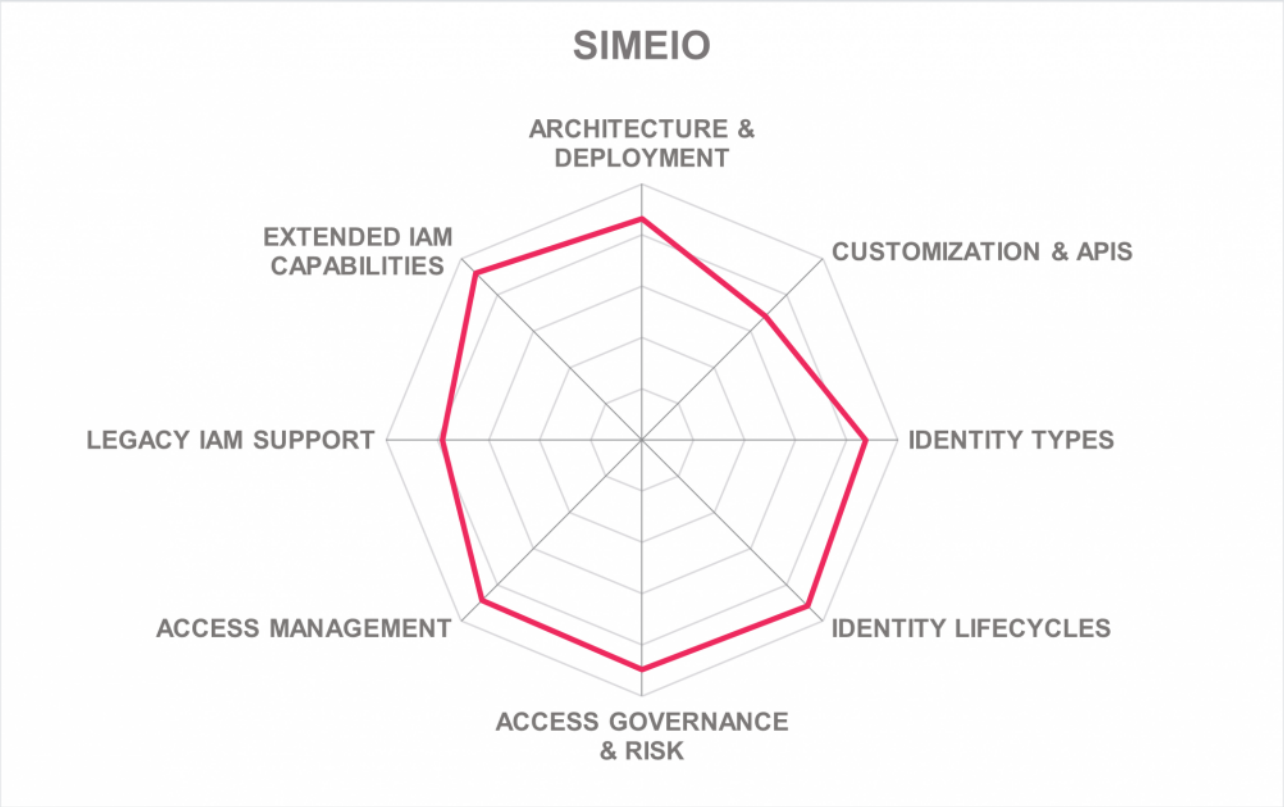
- Well-thought-out approach on orchestrating existing IAM products
- Broad partner ecosystem, involving many of the established vendors
- Simeio provides MSP and IDaaS services, operated from their own operations centers
- Consistent set of REST APIs for an Identity API layer
- Supports gradual migration of existing IAM solutions
- Provides a single sign-on experience across all IAM services
- Simeio acts as a product vendor with an independent roadmap, while also operating as MSP and IDaaS

Challenges

- Despite having a broad partner ecosystem, few major IAM products are not supported out-of-the-box
- Deployment might require a varying level of customization, depending on the type of and state of solutions to be integrated; simplified deployment is a roadmap item
- Though they are active in most regions and expanding into EMEA, the main market of Simeio is still North America

Leader in





5.13 WSO2

WSO2 is another established vendor in the IAM market, with a long history in delivering IAM solutions. Their overall portfolio also comprises an Enterprise Integration Platform and API Management and Security. For IAM, the product is WSO2 Identity Server, which is primarily targeted at Access Management. Together with the other offerings of WSO2, the company delivers a strong foundation for delivering digital services, including the Identity Management backend required for these.

WSO2 Identity Server delivers a range of capabilities. It provides support for Single Sign-On to a range of target applications, including federated applications. All major standards such as OpenID Connect, SAML, and WS-Federation are supported. Features also include Adaptive Authentication and MFA (Multi-Factor Authentication), plus password-less authentication based on the FIDO2 standard. Generally speaking, WSO2 provides strong support for open standards.

Other capabilities of the platform include Privacy and Consent Management and API Security. WSO2 has a focus on customer-centric use cases, which fits well to their overall strategy of delivering platforms for building digital services, powered by the identity services. On the other hand, WSO2 Identity Server has limited capabilities in User Lifecycle Management and widely lacks Access Governance capabilities. Additionally, connectivity to legacy applications and legacy IAM systems is limited.

Positively, WSO2 has built a solution following a modern architecture model from the very beginning, thus providing a flexible solution with modular architecture and a strong set of APIs, which suits the requirements

of Identity Fabrics well.

In sum, WSO2 Identity Server is an interesting foundation for building an Identity Fabric, but will need other vendors' solution to complement it, specifically around IGA and PAM. While WSO2 has a significant number of customers, we still see some room for improvement regarding their global partner ecosystem.

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

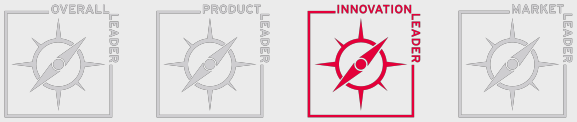
Strengths

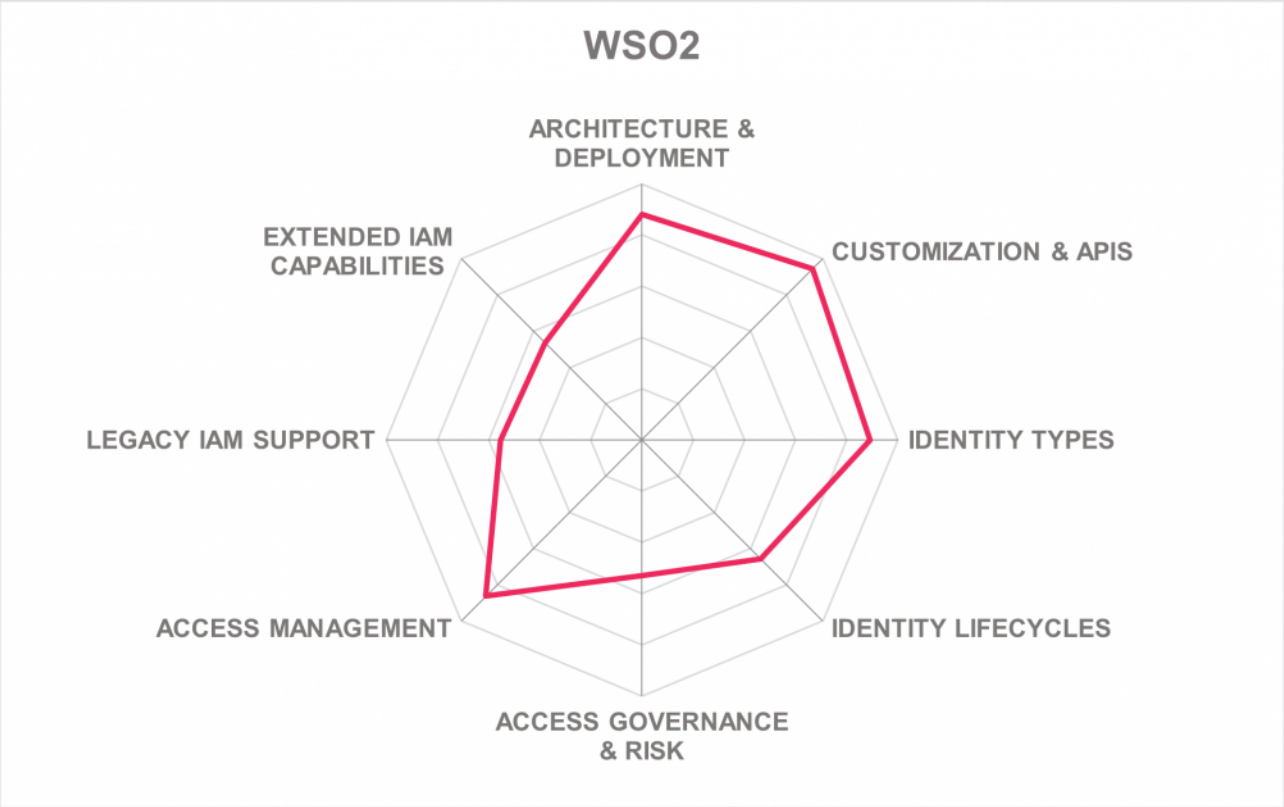
- Modern architecture
- Strong set of APIs, including API Security capabilities
- Proven scalability, focused on consumer-centric use cases and delivering to digital services
- Strong support for standards in Access Management
- Solid capabilities for Access Management and Identity Federation
- Strong support for Adaptive Authentication and MFA

Challenges

- Limited capabilities for User Lifecycle Management
- No specific support for Access Governance requirements
- No support for additional IAM capabilities such as PAM

Leader in




WSO2
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
EXTENDED IAM CAPABILITIES

6 Vendors and Market Segments to watch

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

6.1 Atos/Evidian

Atos and its IAM solution provider Evidian are delivering a range of IAM solutions. The most interesting of these is their Cloud Identity and Access Management solution, which provides a newly architected solution as a service, leveraging existing capabilities of the Evidian and Atos IAM products.

Why to watch: Atos is building on proven technology and has the ability to deliver IDaaS services from a European cloud.

6.2 Auth0

Auth0 offers a platform for providing authentication services, including Adaptive Authentication and MFA, that is targeted at developers and is API-centric. It is a good foundation for the Access Management part of Identity Fabrics but lacks advanced capabilities in IGA and for other IAM capabilities.

Why to watch: Strong set of Identity APIs and leading-edge Access Management capabilities.

6.3 Axiomatics

Axiomatics is one of the established vendors in the IAM sub-segment of Dynamic Authorization Management. These capabilities will become increasingly important when applications are built against a central Identity API Layer, which also should include authorization management.

Why to watch: Might deliver additional, leading-edge authorization capabilities to an Identity Fabric.

6.4 CyberArk

CyberArk, with the acquisition of Idaptive, has moved from a PAM specialist to a provider of a comprehensive set of IAM capabilities. These now also include Access Management, including Adaptive Authentication and MFA, Endpoint and Mobile Security, and a good baseline support for Identity Provisioning and User Lifecycle Management. With the further integration and extension of their portfolio, they have the potential of becoming a strong contender in the Identity Fabrics market segment.

Why to watch: Good portfolio for overall IAM, with Access Management and IGA delivered as IDaaS.

6.5 Fischer International

Fischer International is a US-based vendor that started early in delivering IDaaS solutions. Their products are also available on-premises and cover both Access Management and IGA. With their overall capabilities and experience in delivering IDaaS, they are specifically attractive to mid-market organizations in North America.

Why to watch: Proven IDaaS solution covering Access Management and IGA.

6.6 iC Consult/ServiceLayers

German system integrator iC Consult with their ServiceLayers division is delivering an integrated solution for Access Management and IGA that builds on the products of Ping Identity, ForgeRock, and One Identity, and extends these towards an integrated solution with consistent user experience and APIs. They have specific expertise in supporting manufacturing companies in global roll-out and operations.

Why to watch: Delivery of an integrated solution that builds on mature products and adds a consistent API layer plus flexible, container-based deployment.

6.7 Identity Automation

Identity Automation is an US-based provider of an integrated IAM solution covering both Access Management and IGA requirements. Their main focus is on higher education, but they also serve other market segments.

Why to watch: Provider of a solution for IAM that is well-suited for higher education and mid-market

companies, following a platform approach.

6.8 Micro Focus

Micro Focus, with the heritage of the former Novell and NetIQ products, has a broad range of solutions for IAM that are also provided in as-a-service deployment models. The solutions are undergoing gradual modernization and provide a very mature and extensive set of IAM capabilities.

Why to watch: Strong and mature IAM capabilities that are modernized and shifting towards a modern Identity Fabric approach.

6.9 Microsoft

Microsoft with its Azure Active Directory is, from our perspective, one of the most interesting players in the emerging market for Identity Fabrics. They already provide leading-edge Access Management capabilities and also have baseline IGA and PAM features included in that platform. They are increasingly extending their reach towards legacy applications. Based on their modern architecture, however being IDaaS-only in deployment, they are an interesting option either as foundation or as an element in Identity Fabrics.

Why to watch: Azure Active Directory is widely used, and provides an increasingly broad set of capabilities including support for legacy applications. When Azure Active Directory is in use, its role in a modern Identity Fabric must be evaluated anyway.

6.10 N8 Identity

Canadian software vendor N8 Identity delivers a solution for IGA, specifically Access Governance, that runs in the cloud. It leverages the capabilities of Microsoft Azure Active Directory for Access Management and complements this solution with its own capabilities. In that combination, the two offerings build an interesting foundation for an Identity Fabric, specifically for mid-market organizations.

Why to watch: Extends Microsoft Azure Active Directory with Access Governance capabilities towards a comprehensive Identity Fabric foundation for mid-market organizations.

6.11 One Identity

One Identity is well-known as one of the leading vendors in the IGA market and also for delivering a strong PAM solution. However, after the discontinuation of the Cloud Access Manager, they don't have their own offering for Access Management anymore. This is a gap for delivering a comprehensive foundation for Identity Fabrics, which One Identity addresses via partnerships with Access Management specialists such as Ping Identity.

Why to watch: One Identity, specifically with their recent addition of SaaS support, count amongst the leading vendors in both IGA and PAM, and thus can be combined with other solutions for full Identity Fabrics.

6.12 OpenIAM

OpenIAM is a provider of an open source IAM solution that covers both IGA and Access Management. They have built their solution following a modern architecture approach from the beginning, thus offering a solution with a good set of capabilities and flexible deployment models, making it an interesting option for constructing the own Identity Fabric, specifically for organizations that focus on open source.

Why to watch: One of the leading open-source offerings in the IAM market with a modern architecture.

6.13 Optimal IdM

Optimal IdM delivers a range of IAM solutions, covering both Access Management and IGA, and being available as a service, but also for on-premises deployments. With their overall solution, they are an interesting vendor for providing the foundation for an Identity Fabric, specifically when looking for IDaaS offerings.

Why to watch: Flexible deployments and good set of capabilities for both Access Management and IGA.

6.14 Oracle

Oracle has a mature on-premises IAM portfolio, but also developed its Oracle Identity Cloud over the past years, delivering IAM as a service. The focus is on delivering security and identity to the other Oracle offerings such as databases and business applications. Thus, the solution is of specific interest to

customers building strategically on Oracle as a vendor. However, it can serve other vendor's applications as well and isn't limited to the Oracle ecosystem.

Why to watch: Interesting alternative for customers that have a strategic relationship with Oracle.

6.15 PlainID

PlainID is a specialist vendor for Dynamic Authorization Management and policy-based authorizations. While not delivering a complete IAM portfolio, they are an interesting complement to other solutions, adding the authorization capabilities required for delivering an advanced level of identity services for building new digital services.

Why to watch: Might deliver additional, leading-edge authorization capabilities to an Identity Fabric.

6.16 Ping Identity

Ping Identity counts amongst the leaders in the Access Management market, adding further capabilities such as Dynamic Authorization Management and support for decentralized identities. While not providing IGA or PAM capabilities, Ping Identity is an interesting vendor for delivering the Access Management piece of an Identity Fabric based on their leading-edge technologies.

Why to watch: Ping Identity can deliver the Access Management services for creating comprehensive Identity Fabrics together with other vendor's products.

6.17 RSA

RSA provides various IAM solutions, both for IGA and Access Management. In the latter area, their main focus is on Adaptive Authentication and MFA. The solutions are integrated into the RSA SecurID Suite. Currently, the deployment is by standard an on-premises deployment.

Why to watch: Mature solution with a good set of capabilities, specifically around Adaptive Authentication, MFA, and Access Governance.

6.18 SailPoint

While being leading-edge in IGA, with both on-premises and cloud-based versions as well as IDaaS service and AI-based Access Risk Analytics, SailPoint does not deliver Access Management or PAM. SailPoint could be paired with other relevant IAM products and services to create a more complete identity fabric.

Why to watch: Leading-edge specialist vendor for IGA capabilities, that could become an Identity Fabric if used with other vendor's Access Management solutions.

6.19 Saviynt

Saviynt is one of the cloud born IGA vendors, providing a broad set of IGA capabilities. They also have partnerships with various other vendors in the market such as Okta, and provide integrations for their solutions. Furthermore, they deliver extensive control to business applications such as SAP. This makes them an interesting vendor to complement cloud-based Access Management solutions for providing a comprehensive Identity Fabric.

Why to watch: One of the leading-edge offerings for IGA as a service plus existing partnerships with Access Management specialists.

6.20 Strata.io

Strata is a start-up that delivers a cloud-based IAM platform that is focused on supporting hybrid and multi-cloud environments, by orchestrating identities from different platforms and enabling organizations to re-use identities on different platforms seamlessly. Together with their modern architecture, this can make them an interesting element in Identity Fabrics.

Why to watch: Startup that provides an innovative solution for orchestrating identities from different platforms, delivering seamless access to applications.

7 Related Research

Leadership Compass: CIAM Platforms – 80040
Leadership Compass: Access Governance & Intelligence – 80098
Leadership Compass: Access Control Tools for SAP Environments – 80104
Leadership Compass: Privileged Access Management – 80088
Leadership Compass: Identity Governance & Administration (IGA) – 80063
Leadership Compass: API Management and Security – 70311
Leadership Compass: Identity as a Service (IDaaS) IGA – 80051
Leadership Compass: IDaaS Access Management – 79016
Market Compass: Dynamic Authorization Management – 71144
Buyer's Compass: Access Management – 80201
Buyer's Compass: Privileged Access Management – 80200
Buyer's Compass: API Management and Security – 80215
Buyer's Compass: Consumer Identity and Access Management Solutions – 80018
Buyer's Compass: Identity-as-a-Service (IDaaS) – 71526
Executive View: ForgeRock Access Management – 80319
Executive View: Hitachi ID Privileged Access Manager – 80142
Executive View: Hitachi ID IAM Suite – 80399
Executive View: IBM Cloud Identity – 79065
Executive View: Ilantus Compact Identity – 80177
Executive View: SAP Cloud Identity Access Governance - 80418
Executive View: Simeio Identity Orchestrator – 80151
Executive View: Symantec Identity Governance and Administration - 80324
Executive View: Symantec Privileged Access Manager - 80331
Executive View: WSO2 Identity Server – 80060
Leadership Brief: 10 Top Trends in IAM – 80335
Leadership Brief: Leveraging Identity Fabrics on your way towards Cloud Based IAM – 80501
Leadership Brief: Identity Fabrics – Connecting Anyone to Every Service – 80204

Methodology

About KuppingerCole's Leadership Compass

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

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

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

Types of Leadership

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

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

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

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

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

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

understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

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

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

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

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

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

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.

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

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

Vendor rating

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

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

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

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

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

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

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

Rating scale for products and vendors

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

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

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

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

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

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

Inclusion and exclusion of vendors

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

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

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

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

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

Content of Figures

Copyright

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

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

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