KuppingerCole Report

LEADERSHIP COMPASS

By Martin Kuppinger

May 19, 2022

Identity Fabrics

This report provides an overview of the market for Identity Fabrics, which are comprehensive IAM solutions built on a modern, modular architecture. It 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 / Executive Summary

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.

The term “Identity Fabrics” stands for a paradigm and concept of a comprehensive and integrated set of Identity Services, delivering the capabilities required for providing seamless and controlled access for everyone to every service. Identity Fabrics 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 necessarily based on a technology, tool, or cloud service, but a paradigm for architecting IAM within enterprises. Commonly, the services are provided by a combination of several tools and services, with up to three solutions forming the core of the Identity Fabric. 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.

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
- delivering 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 (with some solutions being cloud-only)
- 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 Key Findings

- The market for Identity Fabrics is evolving quickly. The number of vendors in the rating has grown significantly, as well as the maturity of solutions. However, the market is still not at the level of maturity as, e.g., IGA or Access Management. Positively, we observe significant innovation happening in this market segment.
- Few vendors are supporting all three major areas of IAM, i.e., IGA, Access Management, and PAM, with own capabilities. Thus, Identity Fabrics virtually always will consist of offerings provided by several vendors.
- This also leaves space for the leading-edge specialist solutions in the areas of Access Management such as Ping Identity, and in IGA, such as SailPoint or Saviynt. Such solutions can well complement other vendors offerings for forming a comprehensive Identity Fabric.
- We observe a growing number of specialist vendors that add sophisticated capabilities, e.g., for policy-based access or integrating existing identity siloes. Looking at these specialists can help in closing gaps that the core platforms of an organization's Identity Fabric leaves.
- The support for exposing capabilities via modern APIs is growing fast. However, many vendors still don't expose all capabilities via an integrated and complete set of REST APIs.
- Many of the vendors, including some of the IAM veterans, are still on their modernization journey for their platforms. While all vendors in the rating have a defined roadmap and showing execution on this roadmap, the current state of transition must be carefully analyzed.
- The deployment approaches supported by vendors vary significantly, and range from multi-tenant, public cloud deployments only to implementations that are single-tenant and run as MSP or private cloud implementations. We advise customers to carefully analyze flexibility in deployment, but also the flexibility for customizations and the approach for updating and patches in this context.
- Overall Leaders are (in alphabetical order) Broadcom, EmpowerID, ForgeRock, IBM, Microsoft, Okta, One Identity, Oracle, SecurID (RSA), and Simeio.
- Product Leaders are (in alphabetical order) Broadcom, EmpowerID, ForgeRock, IBM, Microsoft, Okta, One Identity, and Simeio.
- Innovation Leaders are (in alphabetical order) Accenture, Avatier, Broadcom, Cloudentity, EmpowerID, ForgeRock, IBM, Microsoft, Okta, One Identity, Oracle, SecurID (RSA), and Simeio.

1.2 Market Segment & Trends

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, and mobile systems. 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.

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 (BYOI).
- 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.

Traditional IAM systems meet, if at all, only a fraction of current requirements. They are often monolithic in design and implementation, making it difficult to break them down into individual components. For seamless access for all users from everywhere to every service, organizations must shift 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 in a public cloud, they can be deployed in private clouds or even on-premises, and they even can encapsulate legacy applications during a transition phase. 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. They must meet the requirements for scalability, performance and resilience.

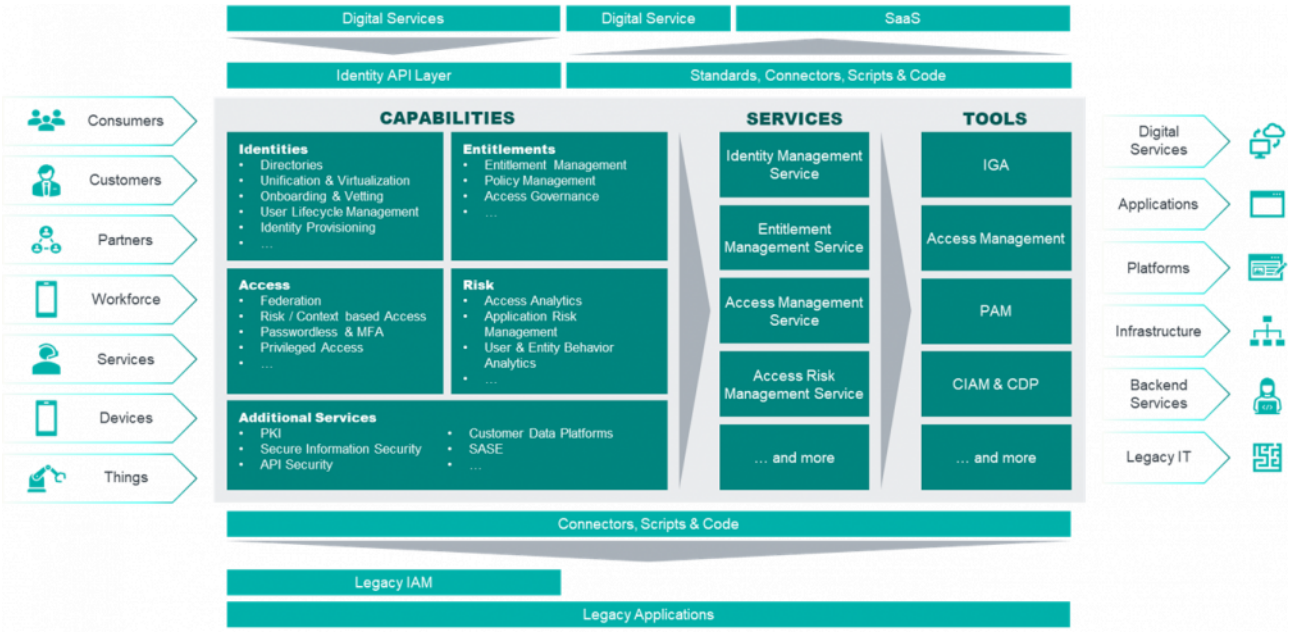


Figure 1: A sample high-level, conceptual architecture for an Identity Fabric. The set of capabilities and services provided depends on the specific requirements of the organization.

Identity Fabrics combine current and proven IAM concepts with modern concepts like 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.

KuppingerCole recommends the following strategic approach for moving towards an Identity Fabric, 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.

Over the past two years, we have observed a significant uptake in the adoption of the Identity Fabrics paradigm, by both vendors and end user organizations. Several organizations have defined an IAM architecture following the Identity Fabrics model and are on their journey of modernizing their legacy IAM. Also, several vendors are actively promoting this model and positioning their solutions as Identity Fabrics.

We expect to see further momentum, with the continuing and further increasing need for modernizing and extending IAM as well as for better serving digital services. Also, with the ongoing transformation of legacy IAM solutions into modern architectures with strong API support and flexible deployment models, more offerings become available and integration of multi-vendor solutions into a unified Identity Fabric becomes simplified. This all will contribute to further adoption of the Identity Fabrics model by both vendors and end user organizations.

1.3 Delivery Models

Identity Fabrics are 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, pure-play IDaaS also is a valid approach. Options, e.g., include

- 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.

Overall, we prefer solutions that can be deployed and orchestrated flexibly, supporting different deployment models, or pure-play IDaaS solutions. Flexible deployment options give customers the choice for a gradual migration to the cloud, but also enable support for more complex scenarios such as geographically dispersed deployments and hybrid scenarios.

This Leadership Compass expects the availability of as-a-service deployments but is open to all forms from managed services to public cloud delivered IDaaS.

1.4 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.

Furthermore, we expect to see a certain degree of Privileged Access Management capabilities, specifically for managing entitlements, access, and privileges across multi-cloud, multi-hybrid environments. This, sometimes referred to as CIEM (Cloud Infrastructure Entitlement Management), is a capability that should be part of Identity Fabrics.

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 either 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 provide as-a-service deployments will not be considered for this Leadership Compass.
- 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.

2 Leadership

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

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.

2.1 Overall Leadership

Figure 2: The Overall Leadership rating for the LC Identity Fabrics.

The Overall Leadership chart indicates a significant increase in market maturity and relevance, compared to the first edition of this Leadership Compass. The number of vendors in the rating has grown significantly, as the number of vendors that achieved an Overall Leader rating has grown.

In the evaluation, we see Microsoft with their Azure Active Directory ecosystem of solutions slightly ahead of a group of three vendors being positioned head-to-head, which are (in alphabetical order), ForgeRock, IBM, and Okta. These vendors all provide feature-rich solutions in modern architectures, while being different from each other in the architecture and preferred delivery models. These differences indicate that selecting platforms as a foundation for an organization's Identity Fabric requires further thorough evaluation. This KuppingerCole Leadership Compass provides a significant amount of detail in further sections.

Further vendors placed in the Overall Leader segment include, again in alphabetical order, Broadcom, EmpowerID, One Identity, Oracle, SecurID (RSA), and Simeio. All provide comprehensive solutions for serving the needs of organizations implementing an Identity Fabric, with most of the vendors being in mature stages of their journey on modernizing their traditional IAM offerings.

The Challenger section is populated by several other vendors. These vendors have quite diverse backgrounds. Avatier and Hitachi ID are established providers of IAM offerings, providing a good level in breadth and depth of capabilities, but with lesser market presence than most of the leaders. Cloudentity is a specialized solution focusing more on the authorization aspects, and thus also well-positioned as an add-on to other vendor's solutions. Accenture delivers a modern platform with strong IoT support. Ilantus has its strengths in serving mid-market and medium-sized organizations with a good set of IAM capabilities.

The other four vendors (in alphabetical order) in this rating are N8 Identity, OptimalIDM, Radiant Logic, and Strata Identity. N8 Identity is a smaller player, but providing a good set of capabilities focused exclusively on Identity Governance, while leveraging existing vendor tools for Access Management. OptimalIDM provides its OptimalCloud with focus on the SMB market. Radiant Logic has its strength in integrating identity data from various sources and federating access, while Strata Identity positions as an Identity Orchestrator. Both, Radiant Logic and Strata Identity, have unique and innovative offerings that are well-suited to complement other vendors' offerings.

Overall Leaders are (in alphabetical order):

- Broadcom
- EmpowerID
- ForgeRock
- IBM
- Microsoft
- Okta
- One Identity
- Oracle
- SecurID (RSA)
- Simeio

2.2 Product Leadership

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

Figure 3: The Product Leadership rating for the LC Identity Fabrics.

In the Leaders segment, we again see Microsoft on top, with leading-edge capabilities in Access Management, but also a growing set of capabilities in IGA, PAM, and CIEM capabilities. Closely following, we see ForgeRock and IBM, with mature and feature-rich products that are serving both IGA and Access Management requirements well, with IBM being stronger on the IGA and ForgeRock in Access Management.

Okta, with its strengths in Access Management and increasingly expanding into the IGA, PAM, and CIEM segments, also takes a strong position, closely followed by a group of four more vendors, including (in alphabetical order) Broadcom, EmpowerID, One Identity, and Simeio. Broadcom has, backed by its long-standing experience under the CA Technologies brand, evolved its offerings into a modern platform. EmpowerID provides a comprehensive and innovative set of capabilities, with a strength on the IGA side. One Identity also has innovated and extended its offerings significantly, and has added strong Access Management capabilities with the acquisition of OneLogin. Simeio's strength stem from its integration capabilities for other IAM solutions, supporting a gradual IAM modernization.

In the Challengers section, we find Oracle on top, being close to achieving a Leader's rating, with their evolving IDaaS offerings and their continued modernization of their overall IAM portfolio. A group of vendors, all with good sets of capabilities, is following them closely, with (in alphabetical order) Accenture, Avatier, Cloudentity, and Ilantus.

Hitachi ID is next, being strong in IGA and PAM but lacking elaborated Access Management capabilities. However, together with an Access Management specialist, they are well-suited to form the IDaaS core. N8 Identity and OptimalIDM, both being focused more on SMB to mid-market customers, are further vendors in this section.

We also find two Followers in the rating, with Strata Identity and Radiant Logic. Both don't deliver comprehensive Identity Fabrics offerings, but are delivering targeted capabilities that can well complement other vendor's offerings for authentication and identity orchestration (Strata Identity) and identity data integration (Radiant Logic).

Product Leaders (in alphabetical order):

- Broadcom
- EmpowerID
- ForgeRock
- IBM
- Microsoft
- Okta
- One Identity
- Simeio

2.3 Innovation Leadership

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

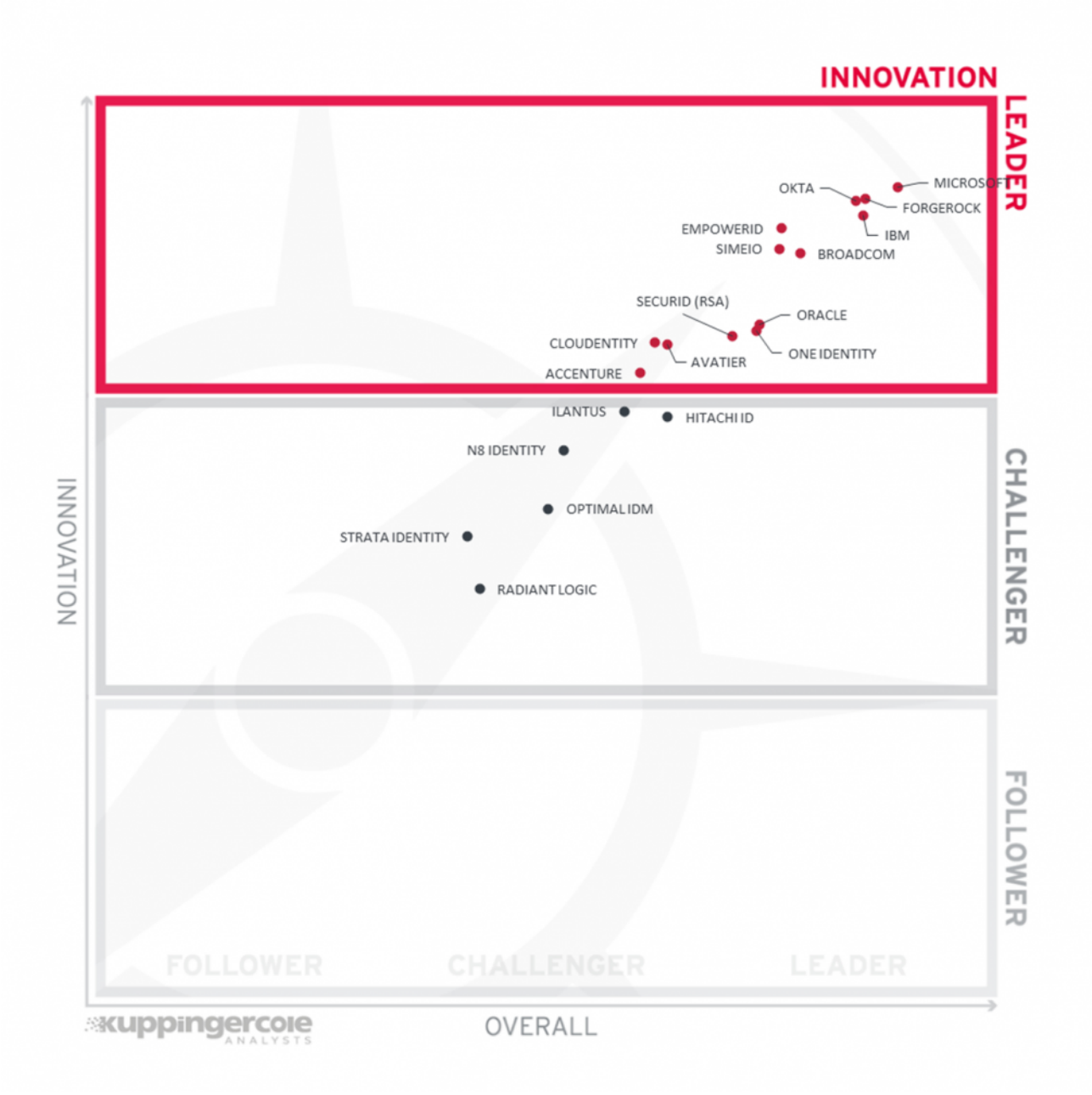


Figure 4: The Innovation Leadership rating for the LC Identity Fabrics.

The Leader's segment is crowded, indicating the significant level of innovation we observe in this market, both regarding capabilities and architectures & deployment models. A group of four vendors is in lead, consisting of (in alphabetical order) ForgeRock, IBM, Microsoft, and Okta. All vendors are investing massively in innovation and are following a strategy towards providing a comprehensive Identity Fabric since a couple of years.

Closely following them, there is another group of three vendors, consisting of (again in alphabetical order) Broadcom, EmpowerID, and Simeio. While these three vendors follow different approaches for their product offerings, all three provide are highly innovative as well.

We also see a strong level of innovation delivered by the other three vendors in this segment, which are (in alphabetical order) Accenture, Avatier, Cloudentity, One Identity, Oracle, and SecurID (RSA).

In the Challenger section, we find Hitachi ID and Ilantus, followed by N8 Identity and OptimalIDM. Most of these vendors are focusing on SMB and mid-market offerings, thus targeting their investments and innovations on the concrete needs for these market segments.

Finally, Strata Identity and Radiant Logic are highly innovative in their respective domains but focused on specific capabilities, thus not scoring across the full range of innovative capabilities. Again, both can provide very valuable contributions to an Identity Fabric, adding to other solutions.

There are no vendors in the Follower segment, proving the strong level of innovation we observe in the Identity Fabrics market segment.

Innovation Leaders (in alphabetical order):

- Accenture
- Avatier
- Broadcom
- Cloudentity
- EmpowerID
- ForgeRock
- IBM
- Microsoft
- Okta
- One Identity
- Oracle
- SecurID (RSA)
- Simeio

2.4 Market Leadership

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

view, requires global reach.

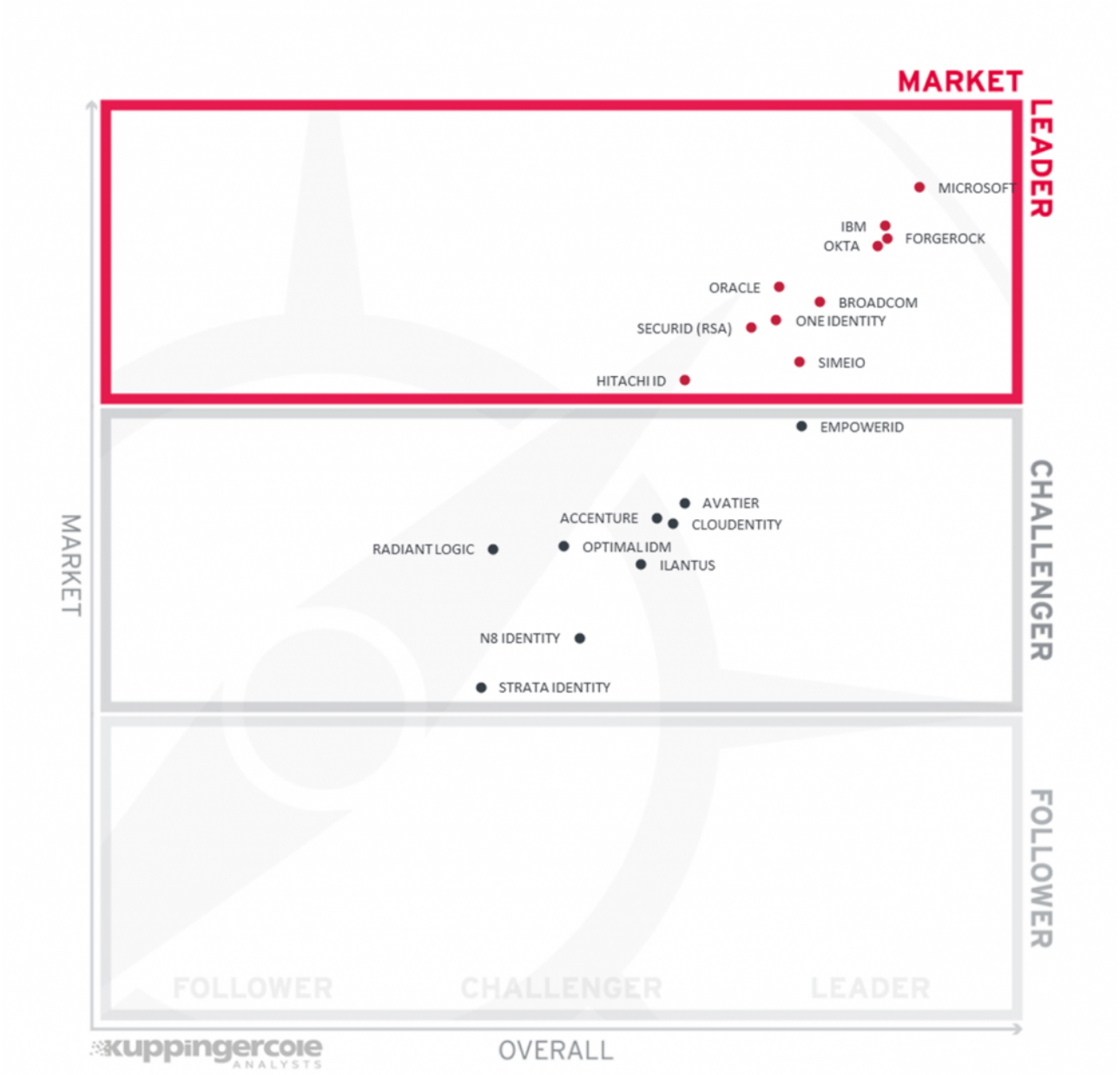


Figure 5: The Market Leadership rating for the LC Identity Fabrics.

Market Leadership, as indicated, focuses on global reach and partner ecosystems as well as the number of customers and other factors. Thus, it is no surprise seeing several of the well-known, established, and large players in the IAM and overall IT markets in the Leader segment. Microsoft again takes the lead, followed by (in alphabetical order) ForgeRock, IBM, and Okta.

With (again in alphabetical order) Broadcom, One Identity, Oracle, and SecurID (RSA), we find another group closely following. All are established IAM vendors with a significant customer base and global reach and ecosystems.

Simeio, which have grown their customer base massively over the past couple of years, and Hitachi ID, being part of Hitachi group and benefiting from the global presence, are further vendors in the Leader segment.

All other vendors are positioned in the Challenger section. EmpowerID is still a relatively small player, but with large customers in both North America and Europe. The next group with (in alphabetical order) Accenture, Avatier, Cloudentity, Ilantus, Optimal IDM, and Radiant Logic all are weak in the one or other aspect of Market Leadership, be it the global reach, the number of active customers, or the global partner ecosystem. N8 Identity with its focus on the mid-market also is still relatively small, as is Strata Identity, being a highly innovative vendor but still in the early stages of its go-to-market.

Market Leaders (in alphabetical order):

- Broadcom
- ForgeRock
- Hitachi ID
- IBM
- Microsoft
- Okta
- One Identity
- Oracle
- SecurID (RSA)
- Simeio

3 Correlated View

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

3.1 The Market/Product Matrix

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

Figure 6: The Market/Product Matrix.

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

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership. All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

The correlation between Market Leadership and Product Leadership is overall good, but significantly lower than it is the case in mature market segments. This indicates that the Identity Fabrics market, despite the increase in maturity over the past two years, still is an emerging market segment.

In the upper right segment, we find a group of vendors that score well in both the Product Leadership and the Market Leadership. These all are also placed amongst the Overall Leaders. More interestingly, to the middle-top, we find Oracle, SecurID (RSA), and Hitachi ID, which have a strong market position, but are not yet Product Leaders. While Hitachi ID suffers from the gap in advanced Access Management capabilities, Oracle and SecurID (RSA) are still on their modernization journey and expected to further increase their position near-term.

In the middle-right quadrant, we only find EmpowerID, with a strong product offering, but not yet being rated as a Market Leader. In the center, we find various other vendors that provide Identity Fabrics solutions, but not yet being perceived as Leaders. To the middle-left, there finally are the two highly specialized solution providers, Radiant Logic and Strata Identity, which are adding to Identity Fabrics without providing a comprehensive solution by their own. Radiant Logic can build on a significant installed base, while focusing on further innovation within their specialized focus.

3.2 The Product/Innovation Matrix

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

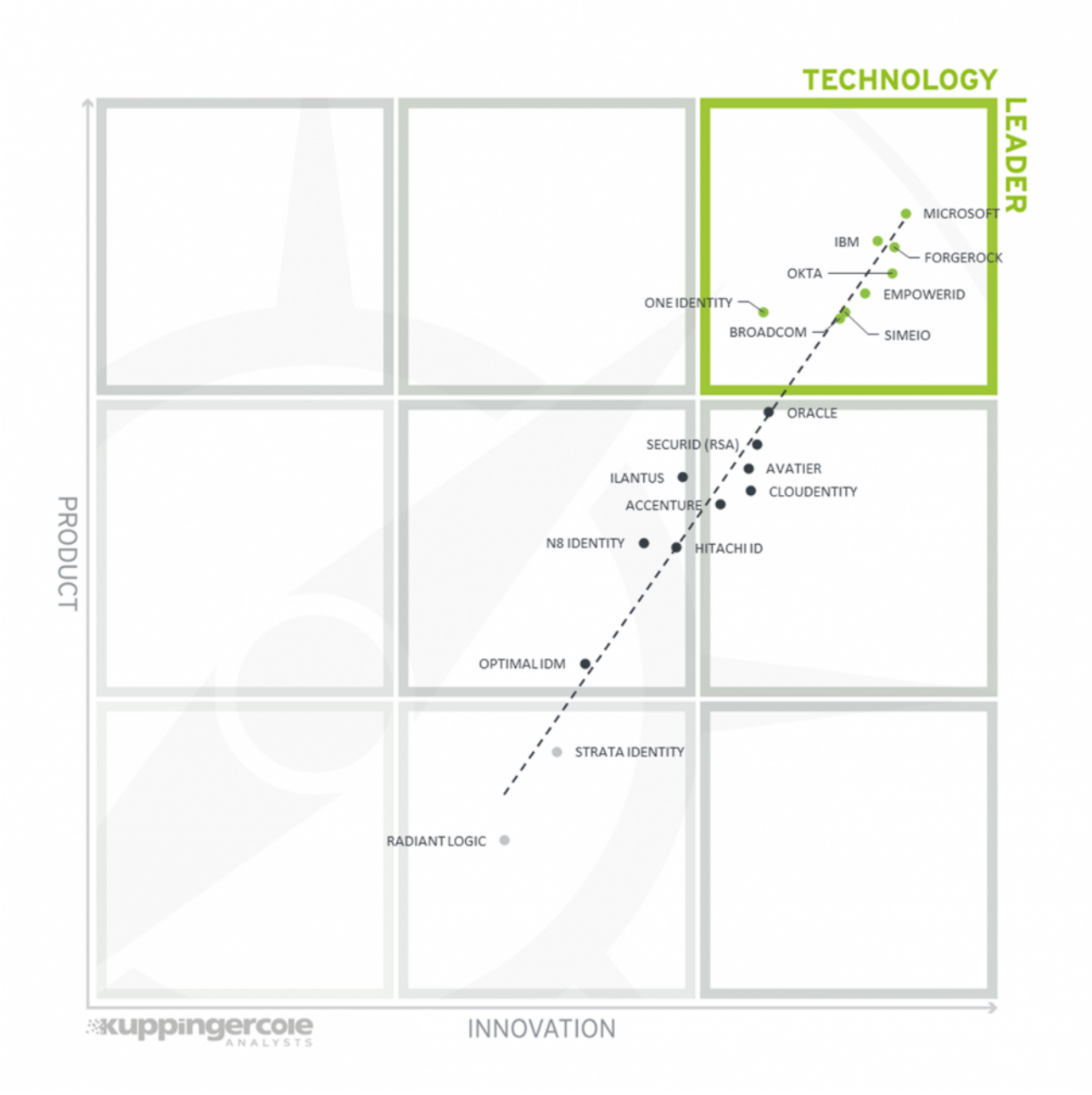


Figure 7: The Product/Innovation Matrix.

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

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

In this diagram, correlation between the Innovation rating and the Product Leadership rating is much closer. Vendors that are providing a high degree of innovation tend to score better in Product Leadership, and vice versa. Notably, the line is more to the right than in most Leadership Compass documents, indicating that

there vendors provide a lot of innovative features, while it is still an emerging market with product capabilities aren't yet at a stable and fully mature level.

Again, Strata Identity and Radiant Logic deserve a specific mention. Both are highly innovative, but focused. While being leading-edge in their respective domains, they don't provide innovation or product capabilities across the full range of Identity Fabrics capabilities we are considering in our analysis.

3.3 The Innovation/Market Matrix

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

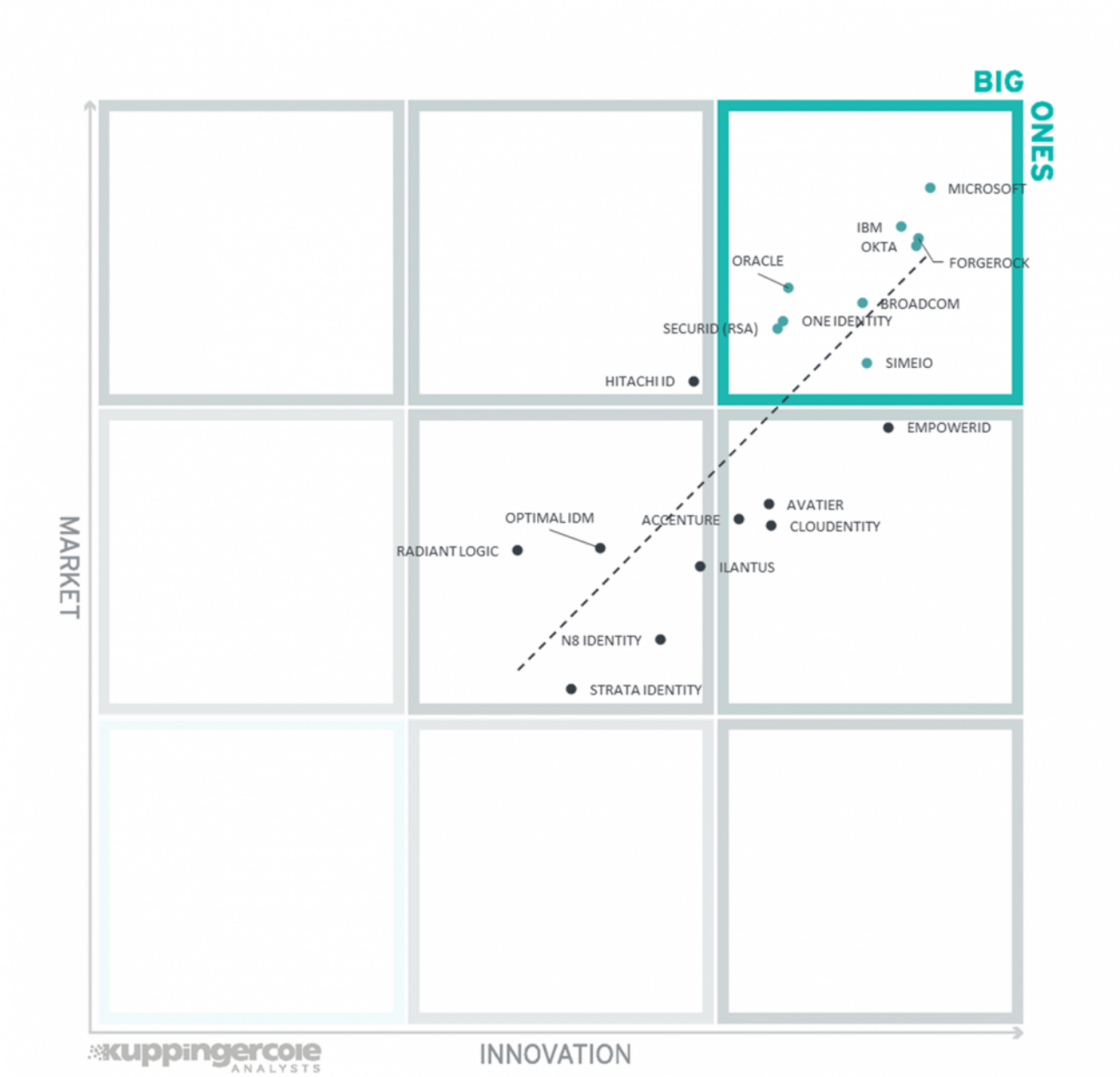


Figure 8: The Innovation/Market Matrix.

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

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

For this analysis, correlation again is relatively low, compared to other Leadership Compass reports, indicating that the Identity Fabrics market segment is still emerging. Special attention goes to the vendors in

the middle-right segment, i.e., in alphabetical order, Acccenture, Avatier, Cloudentity, and EmpowerID, which all provide a strong level of innovation, which is not fully reflected in their market presence. These vendors show a strong potential for further growth.

4 Products and Vendors at a Glance

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

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

Product	Security	Functionality	Deployment	Interoperability	Usability
Accenture Security Memority	strong positive	positive	strong positive	positive	strong positive
Avatier Identity AnyWhere	positive	positive	strong positive	positive	strong positive
Cloudentity Identity & Authorization Control Plane	strong positive	positive	strong positive	positive	strong positive
EmpowerID	strong positive	strong positive	strong positive	strong positive	strong positive
ForgeRock Identity Platform	strong positive	strong positive	strong positive	strong positive	strong positive
Hitachi ID Bravura Security Fabric	positive	positive	positive	positive	positive
IBM Security Verify	strong positive	strong positive	strong positive	strong positive	strong positive
Ilantus Compact Identity	positive	positive	positive	positive	strong positive
Microsoft Azure Active Directory	strong positive	strong positive	strong positive	strong positive	strong positive
N8 Identity TheAccessHub Enterprise	strong positive	positive	strong positive	positive	strong positive
Okta Identity Cloud	strong positive	strong positive	strong positive	strong positive	strong positive
One Identity Unified Identity Security Platform	strong positive	strong positive	positive	positive	positive
Optimal IdM OptimalCloud	positive	positive	positive	positive	positive
Oracle Cloud Infrastructure	strong positive	positive	positive	strong positive	positive
Radiant Logic RadiantOne Suite	positive	neutral	positive	positive	positive
SecurID	strong positive	positive	positive	positive	positive
Simeio Identity Orchestrator	strong positive	positive	strong positive	strong positive	positive
Strata Identity Maverics	positive	neutral	strong positive	positive	positive
Symantec Identity Security (Broadcom)	strong positive	strong positive	strong positive	strong positive	strong positive
Legend		critical	weak	neutral	positive	strong positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Accenture Security	strong positive	neutral	positive	neutral
Avatier	strong positive	neutral	positive	positive
Broadcom Inc.	strong positive	positive	strong positive	strong positive
Cloudentity	strong positive	neutral	neutral	positive
EmpowerID	strong positive	positive	positive	positive
ForgeRock	strong positive	strong positive	strong positive	strong positive
Hitachi ID Systems	positive	positive	strong positive	positive
IBM	strong positive	strong positive	strong positive	strong positive
Ilantus Technologies	positive	neutral	critical	positive
Microsoft	strong positive	strong positive	strong positive	strong positive
N8 Identity	positive	weak	neutral	neutral
Okta	strong positive	strong positive	strong positive	strong positive
One Identity	positive	positive	positive	positive
Optimal IdM	positive	neutral	neutral	neutral
Oracle	positive	positive	strong positive	strong positive
Radiant Logic	positive	neutral	neutral	positive
SecurID	positive	positive	positive	positive
Simeio Solutions	strong positive	positive	positive	positive
Strata Identity	positive	weak	neutral	neutral
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

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

Spider graphs

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

- PAM & CIEM/DREAM
  This dimension focuses on support for Privileged Access Management and the new disciplines of CIEM (Cloud Infrastructure Entitlement Management) and DREAM (Dynamic Ressource Entitlement & Access Management), the latter taking a broader perspective than CIEM to all multi-cloud multi-hybrid workloads in agile IT & DevOps environments. Integrated support for such capabilities becomes increasingly relevant with the convergence of these capabilities, and for supporting identity types such as services.

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, and increasingly is adding the depth of capabilities also found in other vendor's solutions. A weak spot remains Access Governance, where Memority still only provides 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.

Memority has a modern, modular architecture and provides a comprehensive set of APIs, exposing all capabilities that are available via the graphical user interface also as APIs. It also comes with a highly flexible data model, allowing to easily adjust to specific use cases. 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	●●●●○
Deployment	●●●●●
Interoperability	●●●●○
Usability	●●●●●

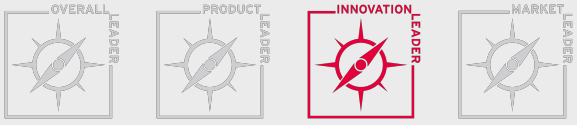
Strengths

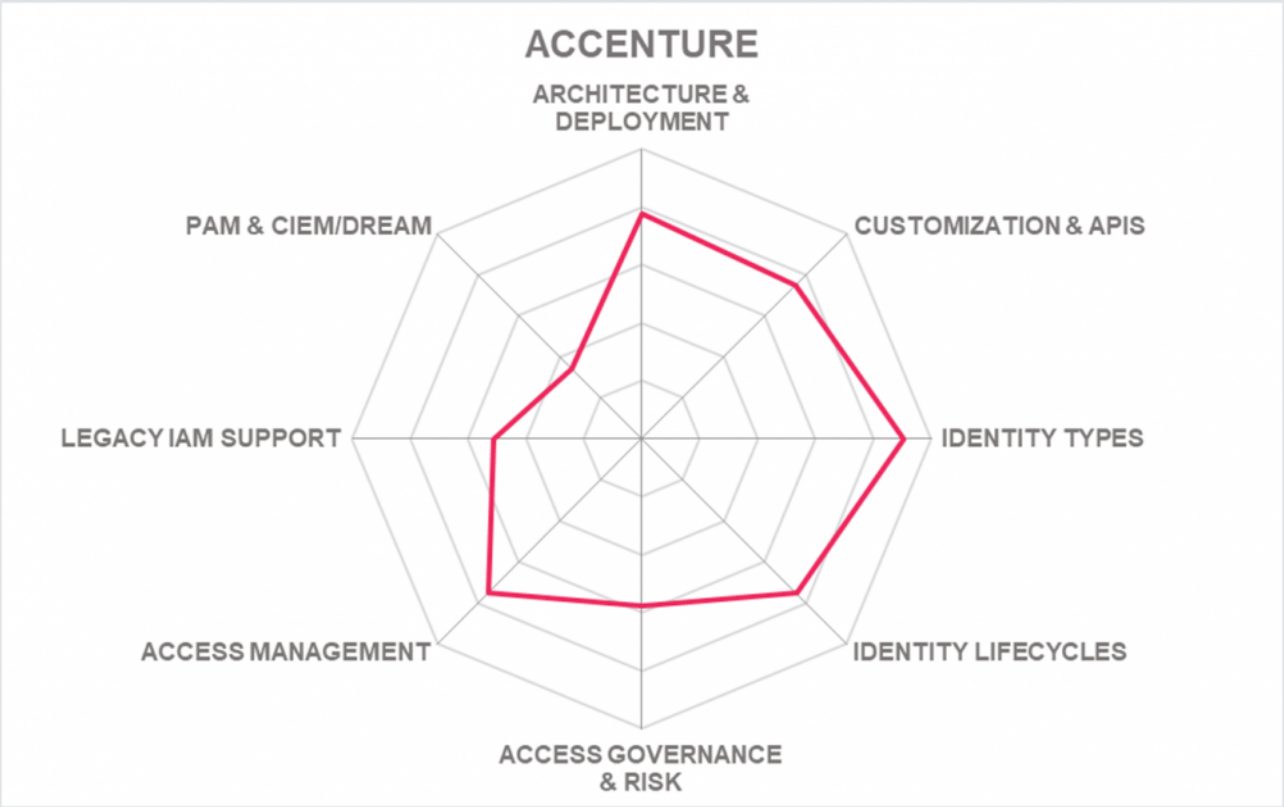
- Integrates IGA and Access Management capabilities into a unified offering
- Comprehensive set of APIs
- Modern, modular architecture
- Excellent support for a broad range of identity types, including connected things
- Ability to deliver industry-specific implementations based on Accenture practices
- Commitment to supporting modern standards
- Supports IoT device integration and management.
- Significantly improved reporting capabilities and Identity Analytics
- Flexible data model

Challenges

- Only baseline Access Governance capabilities
- No partner ecosystem outside of Accenture
- Still relatively low number of customers and presence focused on central Europe

Leader in




ACCENTURE
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

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 a 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, but with a growing number of partners and customers in EMEA. Avatier provides well-thought-out approaches for managing patches and updates for their partners, depending on the deployment model chosen.

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 and Slack integration, and strong mobile support, which provides easy access to the capabilities. Avatier also has improved the workflow capabilities by adding an integrated, patented workflow builder for auto-generating workflows. This is a simple, but relatively inflexible approach in comparison to leading-edge solutions.

Avatier is an interesting alternative to the established vendors, specifically for mid-market companies in North America, but increasingly also in EMEA. If Avatier manages to further 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	●●●●○
Deployment	●●●●●
Interoperability	●●●●○
Usability	●●●●●

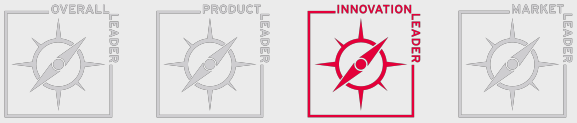
Strengths

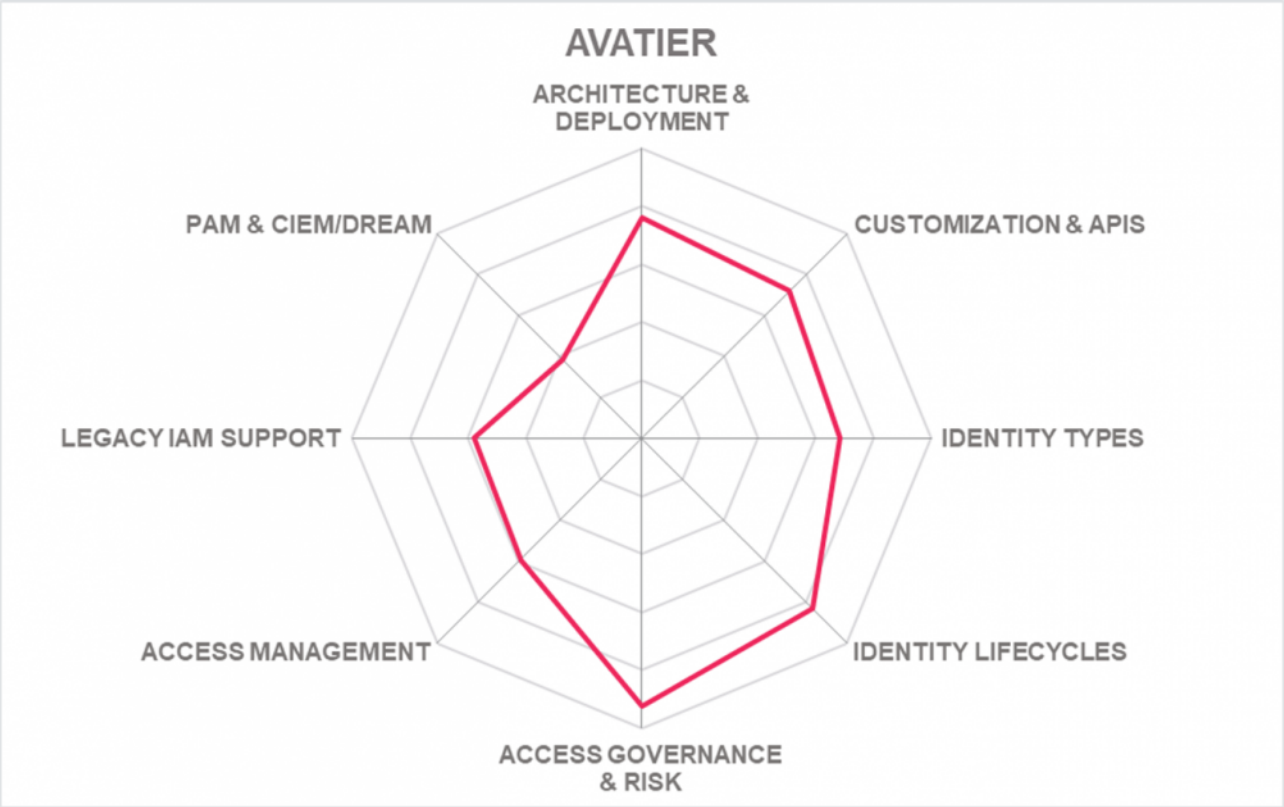
- Good set of capabilities for IGA and Access Management
- Established vendor with a long-standing presence in the market
- Modern, innovative user experience and strong mobile support, also integrating a chatbot
- Out-of-the-box integration into ServiceNow, Teams, Slack, and other platforms
- Integrated catalog of pre-configured workflows
- Out-of-the-box integration into hundreds of applications for Access Management
- Container-based deployment with flexibility in deployment

Challenges

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

Leader in




AVATIER
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.3 Broadcom Inc.

Broadcom Software and the Symantec Identity Security solutions have emerged following the mergers of Broadcom, CA Technologies, and Symantec. Symantec Identity Security 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, Symantec Identity Security 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 in capabilities, while having undergone significant modernization and improvements over the past years. Thus, today's Symantec Identity Security comes as a modern, microservices-based solution.

Symantec Identity Security supports a range of deployment options as well as good support for standards and comprehensive APIs. It also is proven to scale well in large installations. Broadcom is targeting such large customer installations. For these customers, the portfolio is commonly adapted to specific use cases and requirements.

The overall functionality across IGA, Access Management, and PAM is strong. As mentioned above, Symantec benefits from the long experience in these fields, but also increasingly from the continuous modernization and integration of the portfolio. Additionally, it integrates well with the legacy portfolio of former CA Technologies, which is of specific relevance when supporting and modernizing the infrastructures of organizations with a large amount of legacy applications in place.

Broadcom Software positions itself as a provider of enterprise solutions for large businesses. In that context, Symantec Identity Security is an interesting option as a foundation for an Identity Fabric, specifically with the ongoing modernization of that service and the integration of IGA, Access Management, and PAM into one solution, which only very few vendors deliver. Backed by a global ecosystem, the company can deploy such solutions at scale. Furthermore, there are strong integrations, both technical and in licensing, to the security portfolio of Broadcom Software, which might be of interest to enterprise customers.

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

Symantec

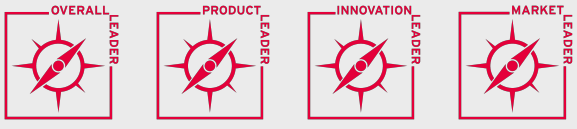
Strengths

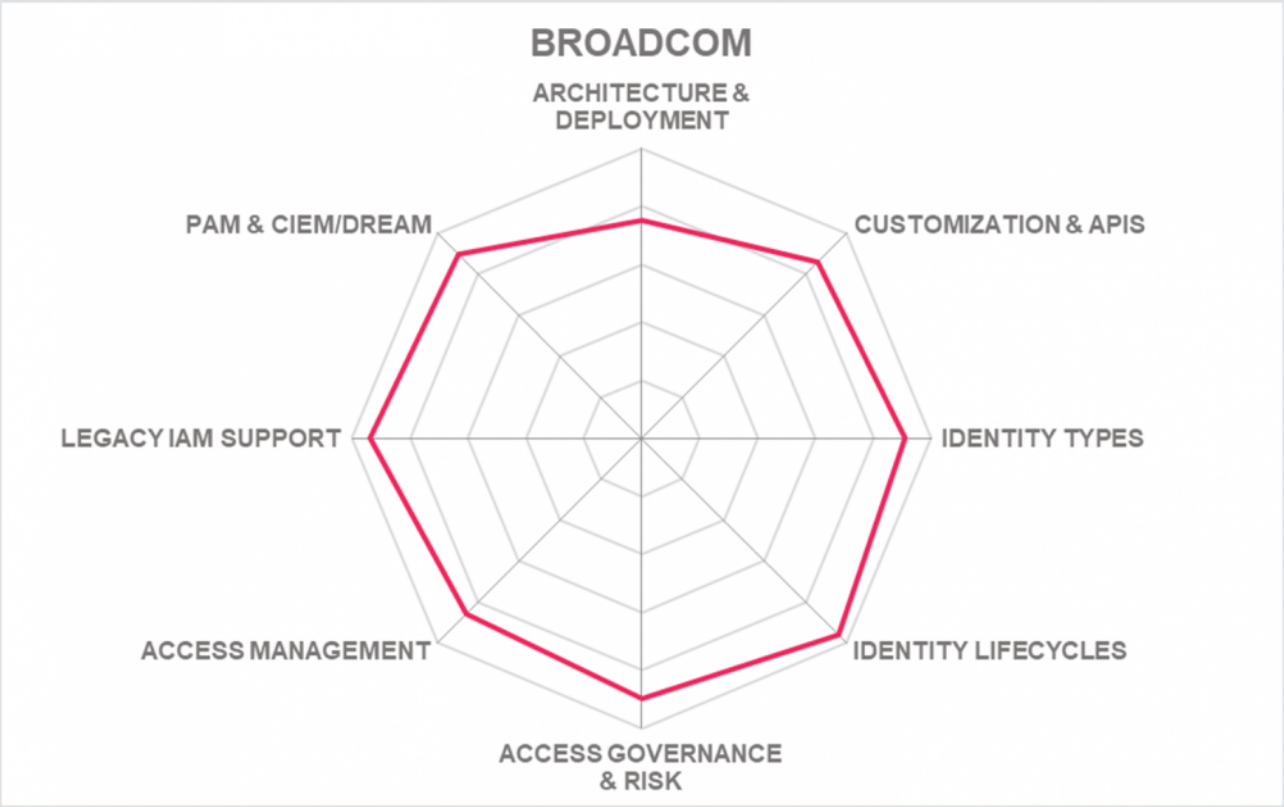
- Proven set of solutions bundled and integrated into a common service
- Solution set following an API-first approach, being multi-tenant and architected as microservices
- Broad range of managed service offerings
- Comprehensive set of capabilities comprising IGA, Access Management, and PAM
- Global ecosystem and ability to scale for large enterprise deployments
- Integration with the security portfolio of Broadcom
- Integrates well with legacy Symantec/CA IAM portfolio

Challenges

- While focusing on a modern, API-first approach, some extended features in legacy support might require integration to Symantec/CA legacy applications
- Focused on large organizations
- Requires professional services in deployment and customization

Leader in




BROADCOM
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.4 Cloudentity

Cloudentity is a relatively young vendor in the broader IAM market that delivers solutions for managing user and machine identities whilst controlling authorization at the API/service 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 APIs and their authorization and consent. Their strength in an Identity Fabric approach is in complementing other solutions with advanced authorization and identity integration capabilities.

Cloudentity's unique approach builds on an Identity Fabric that bridges clouds, existing IdPs, applications, and existing APIs by decoupling identity context and authorization from IdPs. This abstraction of data from IdPs, existing entitlement and data stores, and fraud engines allows for real-time evaluation of identity context at the edge of the service. Key features include automated discovery of applications, services and workloads, automated onboarding of applications and automated protection through baseline policies covering NIST-853 and/or industry specific policy packs. The Cloudentity platform is built as a set of highly scalable, distributed microservices that can be delivered in a public SaaS, managed customer virtual private cloud,or in a customer data center providing flexible deployment options for cloud and edge protection.

The Cloudentity Authorization Control Plane focuses on context-aware authorization per transaction at the API edge. It provides capabilities such as dynamic API Discovery to generate an API/service Catalog, Consent Management, Authorization Policy Governance, Data Lineage, and Open Banking/FAPI support. This component provides strong capabilities for exposing a rich set of authorization and consent APIs and plugs into Kubernetes, service mesh, FaaS, and API Gateway infrastructures, creating identities for APIs and services that then become part of an Identity Fabric. Cloudentity also provides a specialized Policy Decision Point and API Security solution named MicroPerimeter. It also supports OPA (Open Policy Agent) as an emerging standard approach in authorization management.

The second part of the product we analyzed is Cloudentity Identity Plane. This solution focuses on aggregation of identity data from a broad range of sources such as IdPs, IGA solutions, risk engines, entitlement stores, and others, to build out the user profile. It provides capabilities such as lightweight user registration, MFA, SSO and BYOD support, and delegated administration. While the main focus of the solution is on data aggregation and adding authorization to control data flows in B2C and B2B use cases, it also can support more traditional CIAM and workforce IAM initiatives. Furthermore, in combination with the other components, there is strong support for other identity types such as APIs, services, and machines. A specific strength of this solution is the data lineage support, which provides visualization of the flow of identity data between, e.g., the IdP and applications.

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 newer vendor to the market, has a still relatively small but growing global partner ecosystem, including strong regional partners in all major geographies. On the other hand, Cloudentity is very innovative and provides a modern solution that scales well and fits to the architecture requirements of a modern Identity Fabric and thus can serve as a functional extension to other vendor's solutions.

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

CLOUDENTITY

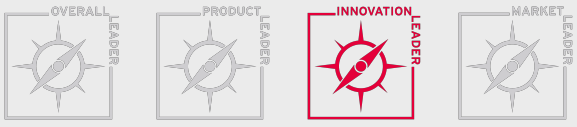
Strengths

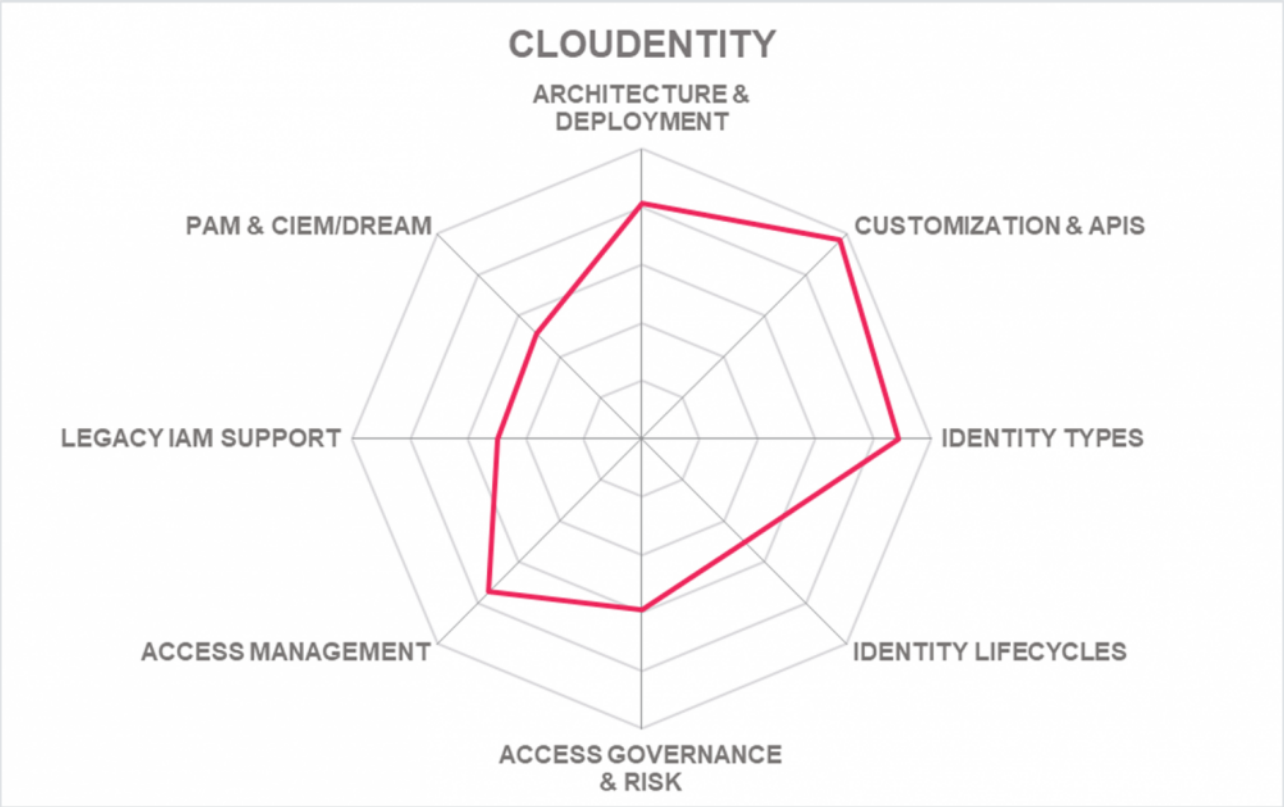
- Strong API Management and API Security capabilities
- Excellent foundation for exposing, managing, and securing a consistent Identity API Layer
- Central management of authorizations at the API level, including API Governance
- Might complement existing legacy IAM and other vendor's IAM solutions in an IAM Fabric with additional services
- Strong Access Management capabilities, specifically for B2C and B2B use cases
- Modern architecture
- Adds governance for APIs and for data exchanged with partners, customers & business units
- Adds data lineage for identity data
- Integrates with consent management solutions

Challenges

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

Leader in




CLOUDENTITY
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

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	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

empowerID

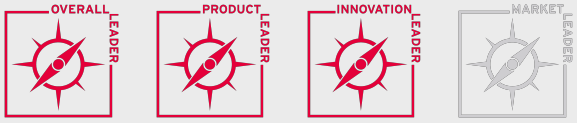
Strengths

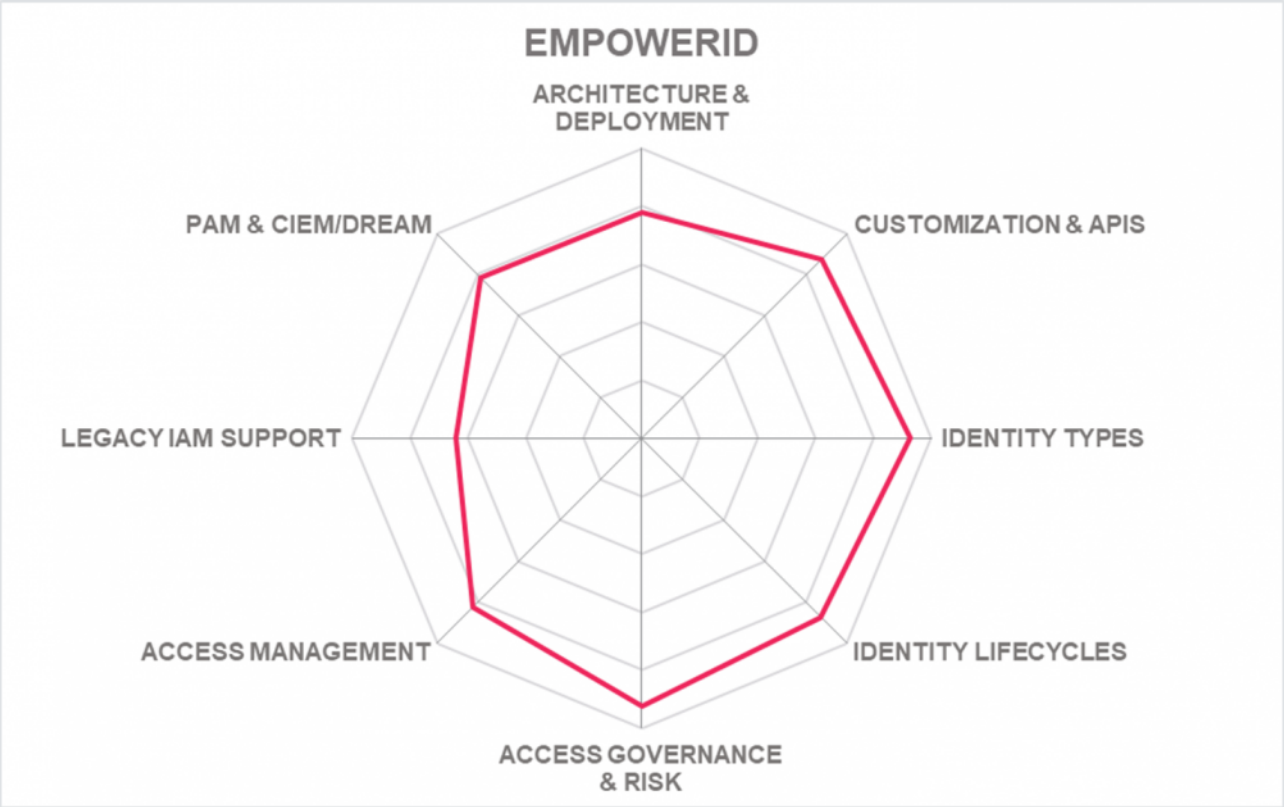
- Integrated suite, covering all major areas of IAM including PAM
- Good breadth and depth of features, specifically for IGA and Access Management
- Integrates neatly with Microsoft Azure Active Directory for Access Management
- Various innovative features, such as for connecting to SaaS services
- Broad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

Challenges

- Still a relatively small vendor, but with some very large customers in both the U.S. and Europe
- Global partner ecosystem is growing, including some global consultancies
- Some few components still need modernization

Leader in




EMPOWERID
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

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, but also new solutions such as ForgeRock Autonomous Access for continuous access risk analysis. The core solutions are well-established and complemented by new, innovative solutions. All components 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. Additionally, the new ForgeRock Autonomous Access adds further intelligence for identity fraud detection. 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	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

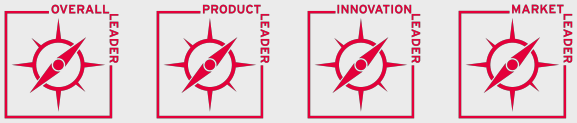
Strengths

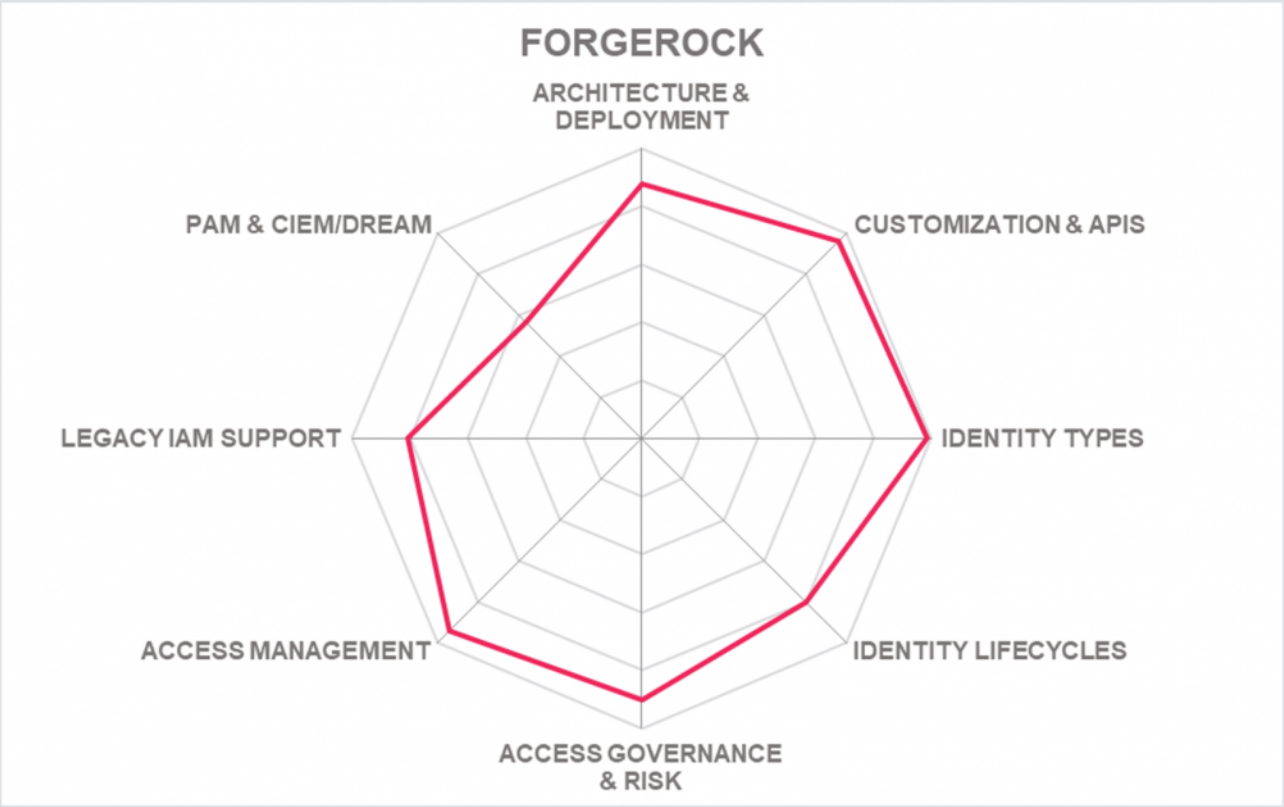
- Leading-edge Access Management capabilities, including strong features for Adaptive Authentication
- Strong features for User Lifecycle Management and Identity Provisioning
- Innovative AI-based capabilities for augmenting users in managing access requests
- Innovative capabilities for access fraud analytics and anomaly detection
- Modern architecture with a comprehensive set of APIs
- Excellent developer support
- Significant improvements in out-of-the-box user interfaces
- 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
- Supports single-tenant as-a-service deployments with automated delivery, update, and patching, but no multi-tenant public cloud support

Leader in




FORGEROCK
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

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. Aside of improving the existing components, Hitachi ID also works on feature extensions by integrating with partners, such as for Application Risk Management, i.e., access controls and governance for Line of Business applications.

Bravura Pass has evolved from a password and authentication solution towards a more comprehensive Access Management offering, supporting SAML-based logins to other systems. It now also supports the Apple MacOS. 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.

Hitachi ID supports a wide range of deployment models. The architecture of the various components is undergoing modernization. While the number of REST APIs exposed is growing, these are still not yet complete. However, there is a feature-complete set of SOAP APIs. Additionally, other capabilities for integration have been added or modernized, such as the SCIM 2.0 connector.

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 continuing their journey on modernizing and extending the solutions.

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

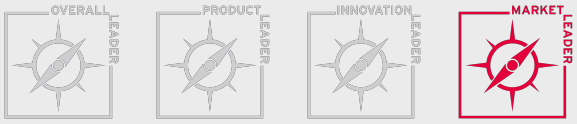
Strengths

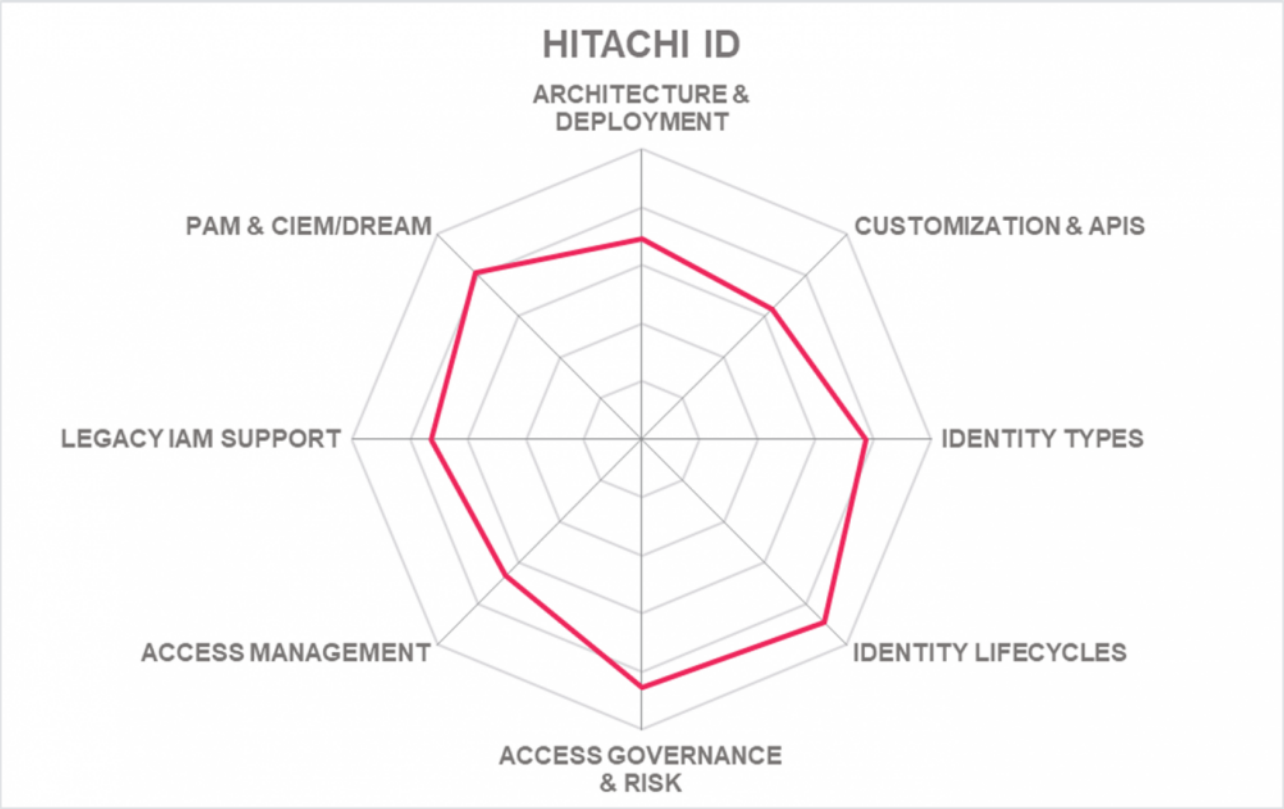
- Strong IGA capabilities, both in breadth and depth of features
- Strong PAM capabilities
- Conceptually following a “Fabric” approach in integrating a comprehensive solution
- Excellent capabilities for managing authentication
- Good support for various deployment models and own system integrator services
- Consequently extending capabilities, including endpoint protection support and integration with 3rd party Application Risk Management solutions
- Strong support for password management, including Apple MacOS
- Backed by large parent company, strong ability to scale and execute

Challenges

- Relatively weak in Access Management capabilities, specifically Identity Federation and Web Access Management
- Solution is undergoing modernization and modularization, but not yet all features exposed via modern APIs
- Still relatively small but growing partner ecosystem

Leader in




HITACHI ID
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

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	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

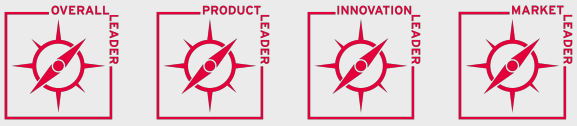
Strengths

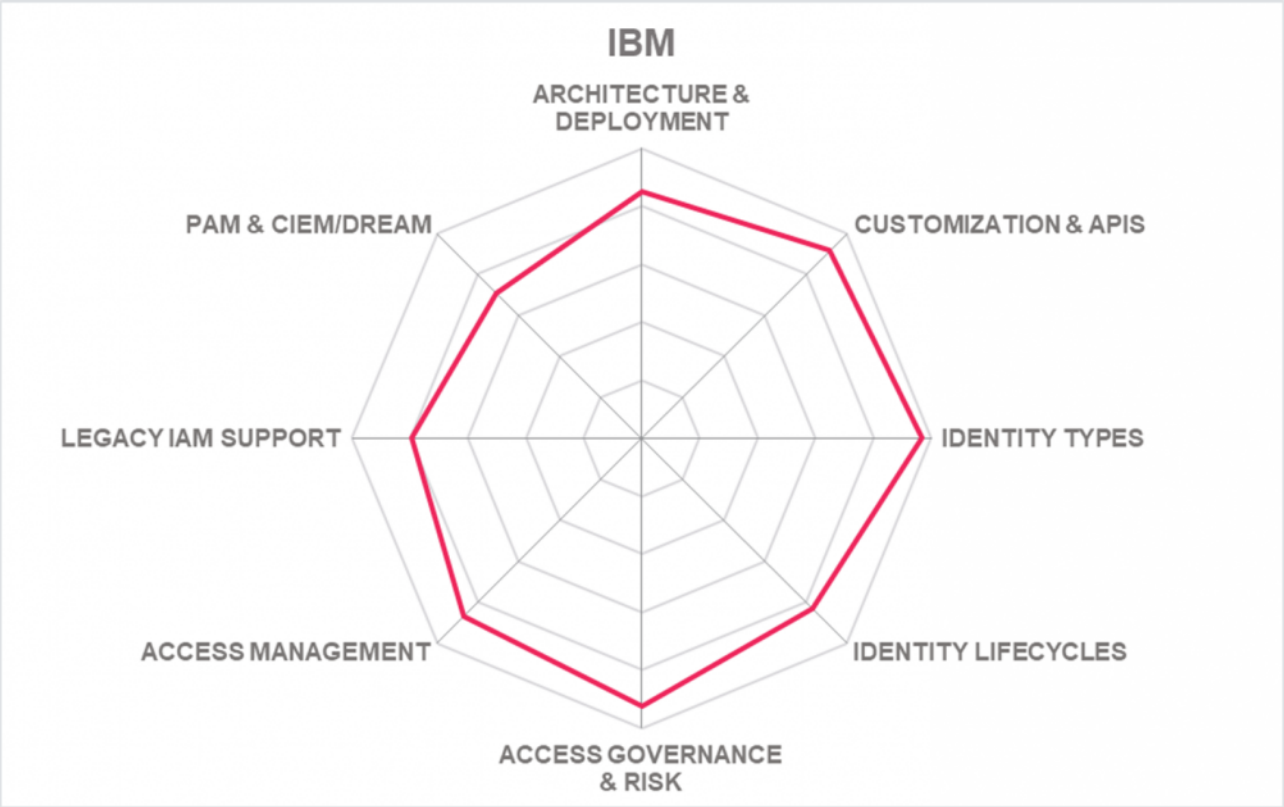
- Very broad set of capabilities across Access Management, IGA, and PAM
- Modern architecture, developed as cloud-native solution
- Own cloud services and professional services
- Strong legacy support, both directly and via integration to Verify Governance (previously ISIGI) and Verify Access (previously 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




IBM
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.9 Ilantus Technologies

Ilantus , which started as a system integrator, has moved fast to provide offerings targeted at different types of customers. They recently split between Ilantus as a system integrator, and Ilantus Products as their product unit. 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 some level of PAM capabilities, 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, baseline 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 mid-market 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. They also have a baseline API gateway integrated. A challenge of Ilantus is that they still don't expose all capabilities via modern REST APIs, which is a limitation for customization.

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.

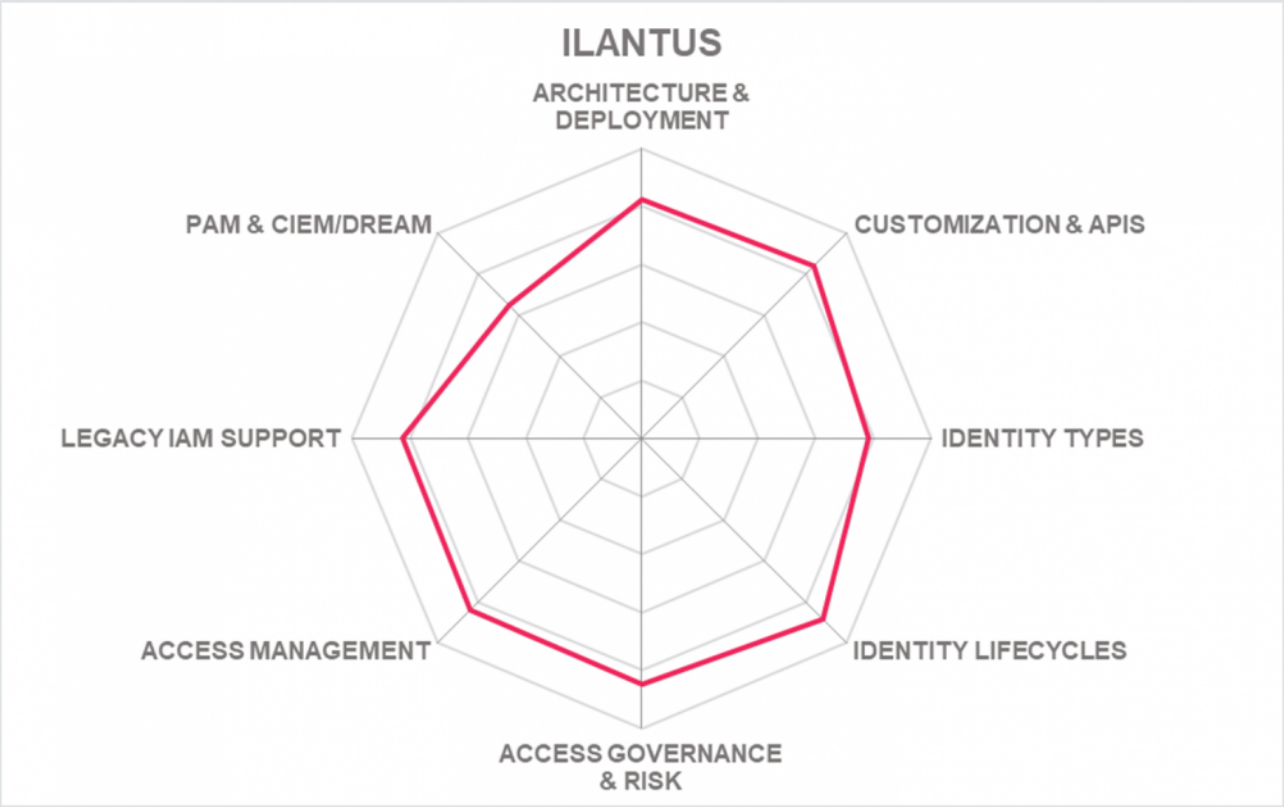
Security	●●●●○
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●●

Strengths

- Service bundle tailored to meet the mid-market 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
- Designed to deliver quick application on-boarding and support lean IAM operations
- Innovative list of capabilities on roadmap
- Baseline PAM capabilities such as password vault
- Baseline API gateway integrated
- Supports a pay-per-use licensing model

Challenges

- Customer presence is still primarily focused on US and a few Asian countries, still low but growing in EMEA
- Focused on mid-market organizations
- Access Governance capabilities are good but not exceptional
- Capabilities still only partially exposed via APIs


ILANTUS
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.10 Microsoft

Microsoft Azure Active Directory (Azure AD) has evolved over the past years from a Cloud Directory and Access Management solution for the Microsoft environment towards a comprehensive IAM solution providing a broad set of capabilities, including IGA (Identity Governance & Administration), PAM (Privileged Access Management), and support for CIEM (Cloud Infrastructure Entitlement Management), the latter through their acquisition of CloudKnox Security. This makes Microsoft a leading provider of a platform to build a modern Identity Fabric on.

Microsoft Azure Active Directory has, also due to its mandatory use for Microsoft Azure and Microsoft 365, achieved wide-spread deployment across organizations of all size. Many organizations have decided for using Azure AD as a strategic platform, at minimum for Access Management requirements, and thus put the platform at the center of their Identity Fabric.

In Access Management, Azure AD counts amongst the leading-edge solutions. It provides excellent support for modern, cloud-based and standards-based (OAuth, OIDC, and others) applications, but also has added a good level of support for downstream applications which don't support modern standards.
In IGA, Azure AD comes with a good set of capabilities, also supporting features such as RBAC (Role Based Access Control) and access certification. While these capabilities are not yet at the level of the leading-edge solutions in the IGA market, they are well above just baseline. However, provisioning capabilities to legacy applications are still only baseline. For PAM, the capabilities are more at a baseline level, but well-integrated with the security analytics capabilities of Azure AD and the broader Microsoft 365 platform.

With their recent addition of CIEM features, Microsoft is becoming a vendor offering a leading-edge breadth in capabilities for an Identity Fabric, even while not delivering the depth of specialist vendor's solutions in all feature areas yet.

In sum, Microsoft has evolved to a leading player in the IAM space with the evolution of Azure AD, making the platform an interesting choice for the foundation of an Identity Fabric. The support for multi-cloud, multi-hybrid environments is strong, while deployment always is as a public, multi-tenant cloud service. The latter might be perceived as a limitation by certain customers.

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

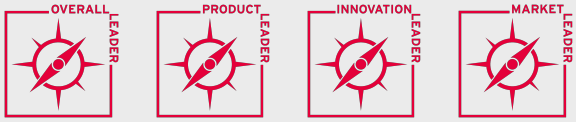
Strengths

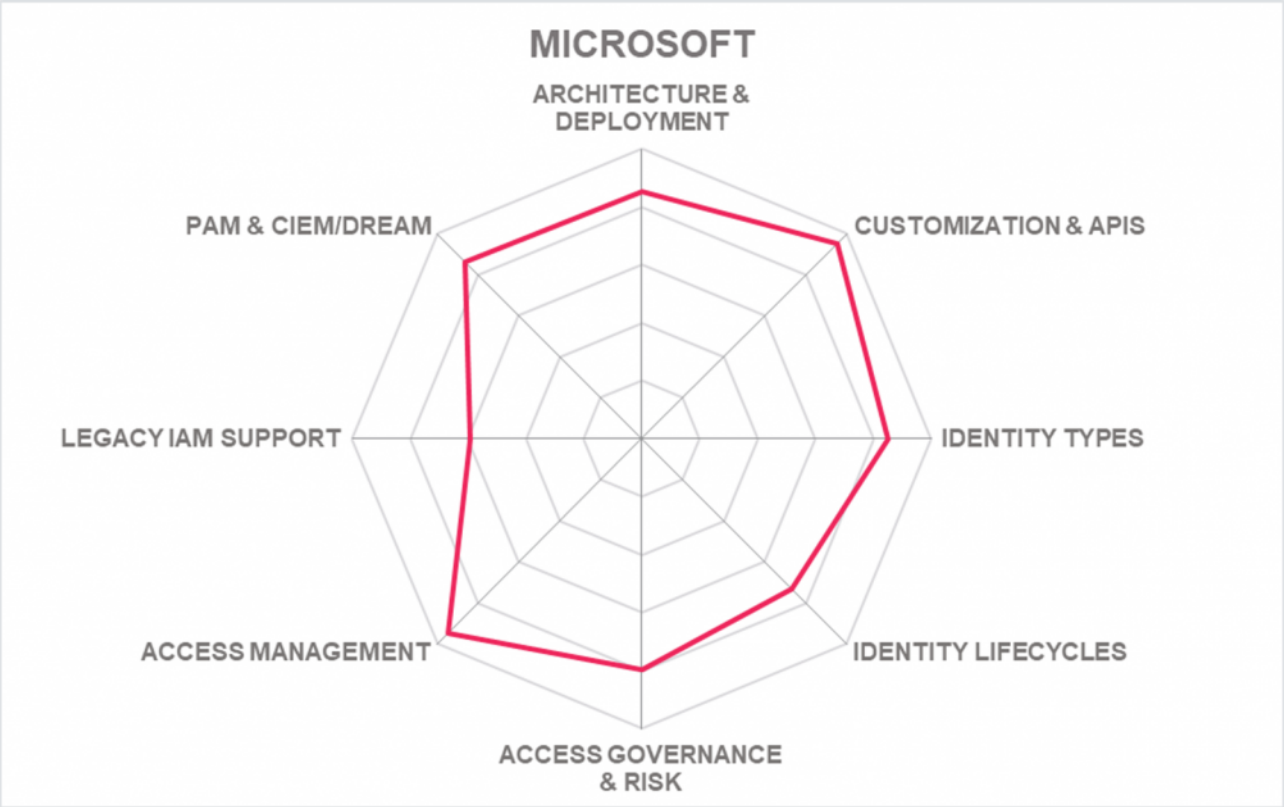
- Very large number of customers, including many large-scale deployments
- Coverage of all major areas of IAM in an integrated solution
- One of the few vendors supporting CIEM capabilities
- Excellent Access Management capabilities
- Strong standards support in all areas
- Gateways for integrating back to on-premises environments
- Strong, global partner ecosystem
- Integrates with security and risk analytics of the Azure Active Directory and Microsoft 365 ecosystem

Challenges

- Only available as multi-tenant, public cloud service
- Good, but not exceptional support for legacy applications, specifically in IGA
- Only baseline PAM support

Leader in




MICROSOFT
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.11 N8 Identity

N8 Identity is one of the specialist vendor's we have evaluated in this Leadership Compass. Their main focus is on the IGA part and herein specifically Access Governance. However, due to a close integration with Microsoft Azure Active Directory and Microsoft 365 as well as support for other Access Management solutions, they can deliver a comprehensive solution for their focus customers in the mid-market.

N8 Identity provides an IDaaS solution, named TheAccessHub Enterprise. That solution covers the IGA capabilities across access request management & approval, identity provisioning, identity analytics & reporting, and access certification & governance. Access Management functions including authentication are provided via the integration to Microsoft Azure Active Directory. N8 Identity delivers good support for targets that run as SaaS services such as Microsoft 365, ServiceNow, Salesforce, Google Apps, and others. The solution also provides a strong set of connectors for on-premises applications via a gateway approach. The user interface of TheAccessHub is based on dashboards as the entry point, showing the current risk score. From there, users can drill down into the specific capabilities such as peer analysis-based recommendations for access entitlements, role mining, and other features.

N8 Identity delivers several innovative features. In their "Identity Learning Fabric", they are using ML (Machine Learning) to learn about appropriate access entitlements and supporting users by automating and augmenting standard access governance tasks. N8 Identity further is working on increasing their capabilities for JIT (just-in-time) provisioning of access to SaaS services, which then is valid only for a limited time. N8 Identity has also been working with multiple government agencies to evolve the identity proofing and lifecycle management for decentralized identity.

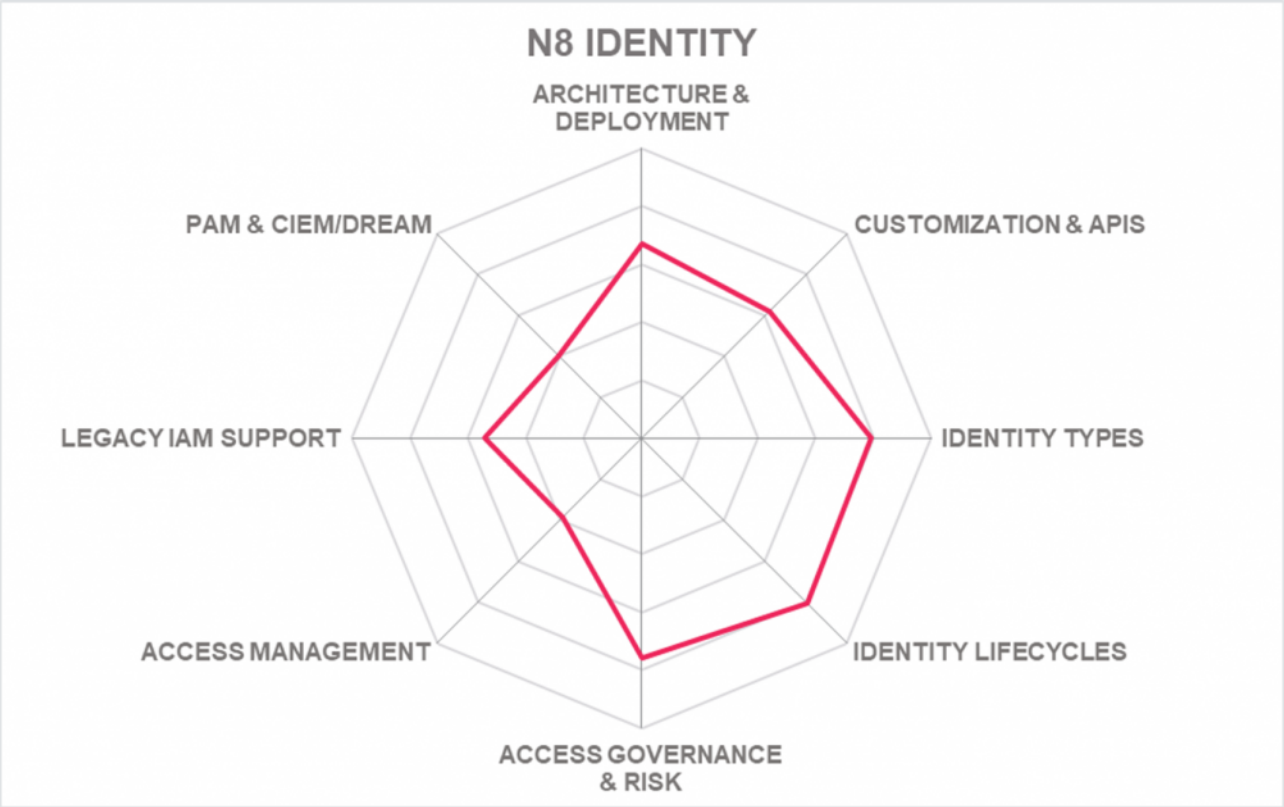
As mentioned above, the N8 Identity TheAccessHub is not a comprehensive offering for an Identity Fabric, but can well complement other vendor's solutions, specifically the ones having gaps in the area of Access Governance. It also seamlessly integrates with Microsoft Azure Active Directory and thus can deliver an interesting proposition for the mid-market target customers of N8 Identity.

Strengths

- Good capabilities in IGA for both lifecycle management and access governance
- Provided as IDaaS, also available for deployment in private clouds
- Clear focus on supporting IGA for SaaS services
- Lean approach and good user interface, good fit for mid-market organizations
- Neat integration to Microsoft Azure Active Directory for Access Management
- Supports other Access Management solutions such as Okta, based on OpenID Connect
- Utilizes Machine Learning for automating and augmentation of users
- Good support for on-premises applications via a gateway

Challenges

- No own support for Access Management and PAM
- Limited but growing global reach and partner ecosystem


N8 IDENTITY
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.12 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 still lacks the breadth and depth of capabilities found in other IGA solutions, specifically around Access Governance and support for legacy applications. However, Okta continues adding capabilities in this field such as self-service access requests, access certification, and governance-focused reporting. Okta also delivers some baseline PAM capabilities as part of their Okta Advanced Server Access solution.

Due to the strong Access Management features, the modern approach to workflows, and with strong 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-heavy environments and other services, or for customers that have limited 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	● ● ● ● ●
Deployment	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

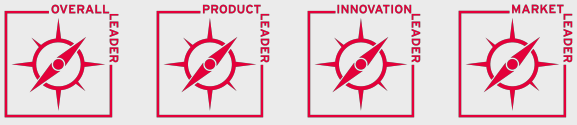
Strengths

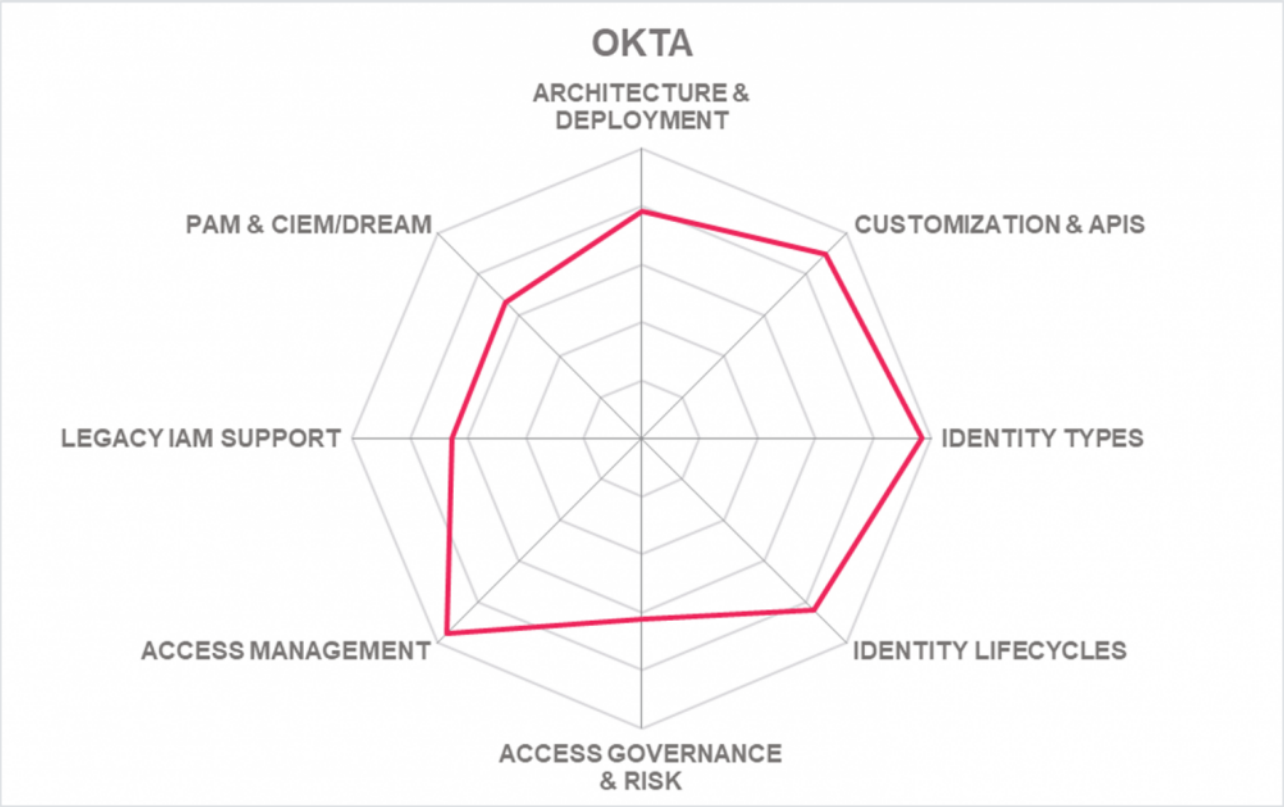
- Leading-edge Access Management capabilities and large number of out-of-the-box integration
- Strong support for Adaptive Authentication and MFA
- Built-in capabilities for anomaly detection in access
- Access Gateway to connect legacy applications
- Innovative, feature-rich workflow capabilities
- Integrates API Security
- Excellent support for connecting to SaaS applications
- Strong support for customer-centric use cases
- Global partner ecosystem
- Lean deployment as SaaS service

Challenges

- Not yet leading-edge in Access Governance, but providing strong User Lifecycle Management and Identity Provisioning to SaaS applications as well as access request and certification support
- Baseline PAM capabilities
- Deployment limited to SaaS only

Leader in




OKTA
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.13 One Identity

One Identity, a Quest company, counts amongst the established IAM vendors. While their main focus had been on IGA and PAM in the past, they have emerged to a full-suite IAM vendor with the recent acquisition of OneLogin. One Identity is one of the few vendors in the market that is covering all major areas (IGA, Access Management, PAM) of IAM with own solutions. Additionally, One Identity is investing heavily in modernizing and integrating the IGA and PAM portfolio and providing these solutions as modern IDaaS services, such as the already releases Starling PAM solution.

In the field of IGA, One Identity Manager is an established solution with a large customer base. Over the past years, One Identity has invested in modernizing the solution architecture and providing it as an IDaaS solution (One Identity Manager on Demand), while preserving the richness in features and the strong integration capabilities, e.g., to SAP environments. Additionally, One Identity has developed an integration platform to SaaS services, Starling Connect, which allows for simplified integration into SaaS services. Starling Connect comes with a broad set of connectors and is evolving in the depth of supported integrations. A specific strength in the field of IGA is the Data Governance add-on.

For Access Management, One Identity has become one of the leaders in the market segment with the acquisition of OneLogin. The company now owns a comprehensive IDaaS platform for Access Management, supporting both workforce and consumer use cases. It also has started integration to the IGA platform such as lightweight governance for access request and approvals.
In the field of PAM, One Identity always had been a strong contender. Recently, they have addressed their previous limitations regarding the hardware-bound deployment of some modules and are now offering the PAM solution also as IDaaS, with SafeGuard on Demand. The solution is feature-rich and covers a variety of PAM use cases, including Endpoint Privilege Management.

As it is common for a portfolio that is both migrated from traditional on-premises deployments to IDaaS, and for integrations with acquired solutions, this is still a journey, where both modernization and integration are not yet fully completed, but on their way and showing strong potential. With that, the One Identity Unified Security Platform is moving closer to unification and is – taking the overall feature set – amongst the most feature-rich solutions in the market.

With the ongoing modernization of the One Identity product portfolio and the integration between the various components, One Identity is an interesting alternative in the Identity Fabrics market. For existing customers, there is a clearly defined pathway towards a modern, comprehensive Identity Fabric, but the solution also shows a strong potential for new customers as an option for the strategic platform to build the future Identity Fabric on.

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

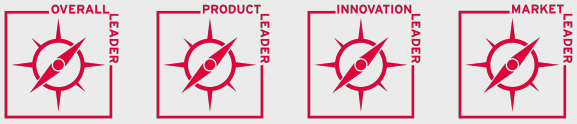
Strengths

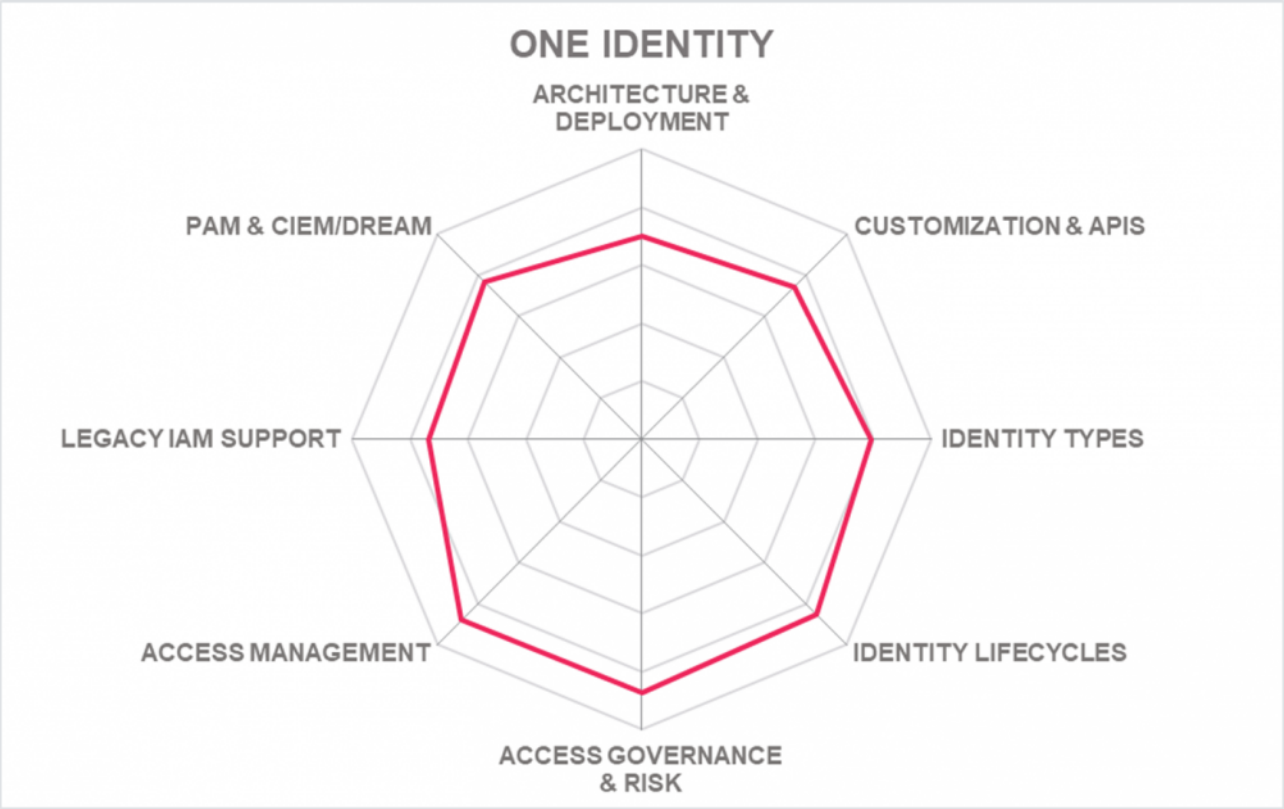
- One of the few vendors with broad and in-depth coverage of IGA, Access Management, and PAM use cases
- Leading-edge IGA capabilities, based on long experience
- Strong support for managing access in SAP environments
- Leading-edge Access Management capabilities through OneLogin acquisition
- Support for Access Management for both workforce and customer use cases
- Strong PAM capabilities with an initial IDaaS release available
- Defined roadmap for further evolution and integration of the platform with IDaaS focus
- Broad support for non-human identities, including RPA

Challenges

- No full integration of the various components yet, but making significant progress in this area
- Starling Connect providing good set of connectors, but needs to further increase depth of integrations
- Not all capabilities available as IDaaS, but delivering on roadmap for modernization and integration

Leader in




ONE IDENTITY
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.14 Optimal IdM

Established in 2005, Optimal IdM is headquartered in the U.S, with U.S. and Australia. Optimal IDM offers the OptimalCloud as its primary IDaaS service providing Single Sign-On, MFA, and Federation functions. The OptimalCloud is a multiple and single-tenant SaaS delivery offering delivering a fully managed service that provides the hosting as well as all of the configurations and customizations for the customer. It is one of the specialist solutions covered in this Leadership Compass, focusing primarily on the Access Management capabilities.

OptimalCloud is built on top of the Optimal IdM virtual directory, which is a virtual identity store. The virtual directory allows an organization to access the user information in their existing data store such as Active Directory, database, or LDAP directory, rather than having to consolidate all of the user information into one single repository.

OptimalCloud supports the most common federation protocols including SAML 2.0, OpenID Connect, OAuth 2.0, WS-Federation, WS-Trust, Shibboleth, and JWT. They also support other standards such as FIDO2. Bulk provisioning is supported out-of-the-box via SCIM from LDAP and to/from cloud services. OptimalCloud provides federated Single Sign-On capabilities. They maintain a catalog with a long list of pre-integrated federated applications for Single Sign-On that can be connected using a “one-click” feature. The list contains many popular SaaS services and applications, as well as some legacy on-premises application options.

OptimalCloud provides dynamic authorization giving fine-grained access control enabling Attribute Based Access Control (ABAC) policy enforcement including step-up and MFA. User group entitlement management is also given. On the other hand, workflow capabilities are very limited, and thus also IGA support.

The solution can be deployed as public cloud solution or as private dedicated cloud tenant. It can be run on top of various IaaS platforms. The OptimalCloud has SOC Type 2 certification. While being an interesting option for Access Management for mid-market organizations, in the overall Identity Fabrics perspective, it is more an add-on to other solutions with a stronger IGA and PAM focus.

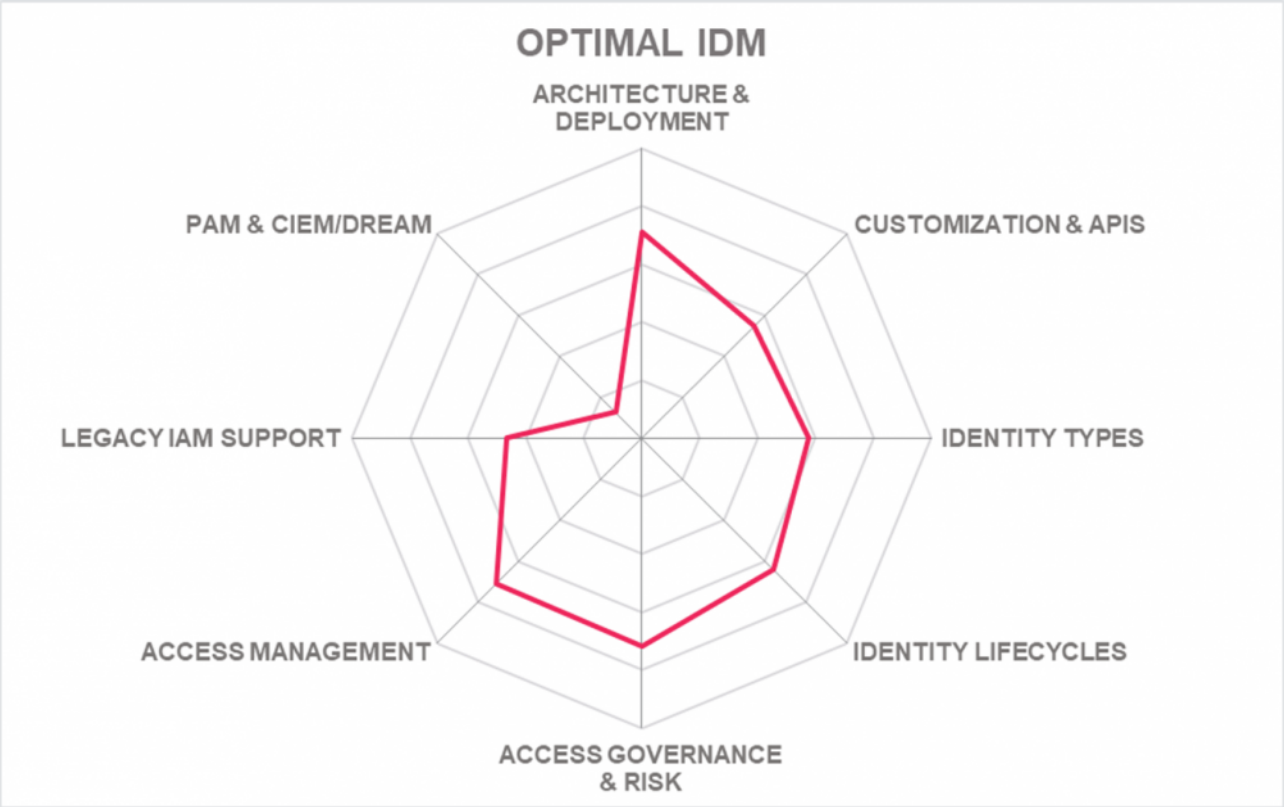
Security	●●●●○
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●○

Strengths

- Strong federation support both inbound and outbound
- Advanced support for delegated administration
- Well thought-out features for MFA
- Flexible directory integration capabilities
- Does not require synchronizing on premises identities to the cloud
- Flat-fee pricing model

Challenges

- Small but well-selected partner ecosystem
- No support for IGA and PAM capabilities
- Not a full Identity Fabrics solution, but can serve as Access Management component, specifically for mid-market organizations


OPTIMAL IDM
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.15 Oracle

Oracle has been in the IAM market for decades. With their OCI IAM (Oracle Cloud Infrastructure Identity Access Management) offering, Oracle now delivers a modern IDaaS solution to the market. As first element of their IDaaS solution portfolio, Oracle has released an Access Management offering, with the cloud-native Access Governance Cloud Service following soon and then providing a comprehensive, integrated IDaaS platform covering both Access Management and IGA.

The Oracle Identity Cloud Service is providing the IAM backbone for OCI (Oracle Cloud Infrastructure) and the Oracle Cloud Applications, but also can serve heterogeneous cloud and application environments. The prior focus on the Oracle ecosystem has been changed towards delivering a comprehensive platform for the entire IT ecosystem of the customers.

For Access Management, the Oracle Identity Cloud Service provides a strong set of capabilities for storing identities, baseline management of their lifecycles, and Access Management. The core focus is on strong and adaptive authentication, including managing the access within multi-cloud environments.

For IGA, the solution still builds on the Oracle enterprise IAM suite and OIG (Oracle Identity Governance), which are soon to be replaced by the cloud-native Access Governance Cloud Service, then delivering a comprehensive and integrated platform for building an Identity Fabric. Oracle will continue to further support their own legacy on-premises IAM applications, allowing existing customers to migrate and extend their environments at their own pace, and for providing advanced integration capabilities for legacy-heavy environments.

Oracle is fully back in the IAM market as a contender with the Oracle Identity Cloud Service and upcoming further IDaaS capabilities. For existing Oracle customers, this provides a pathway towards modernizing their IAM into an Identity Fabric approach. For others, Oracle provides an interesting solution of cloud services, business applications, and infrastructure services such as IAM, with the ability to serve also large scale environments, and strong legacy support wherever required.

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

ORACLE

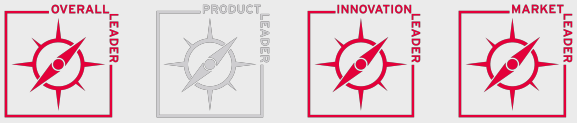
Strengths

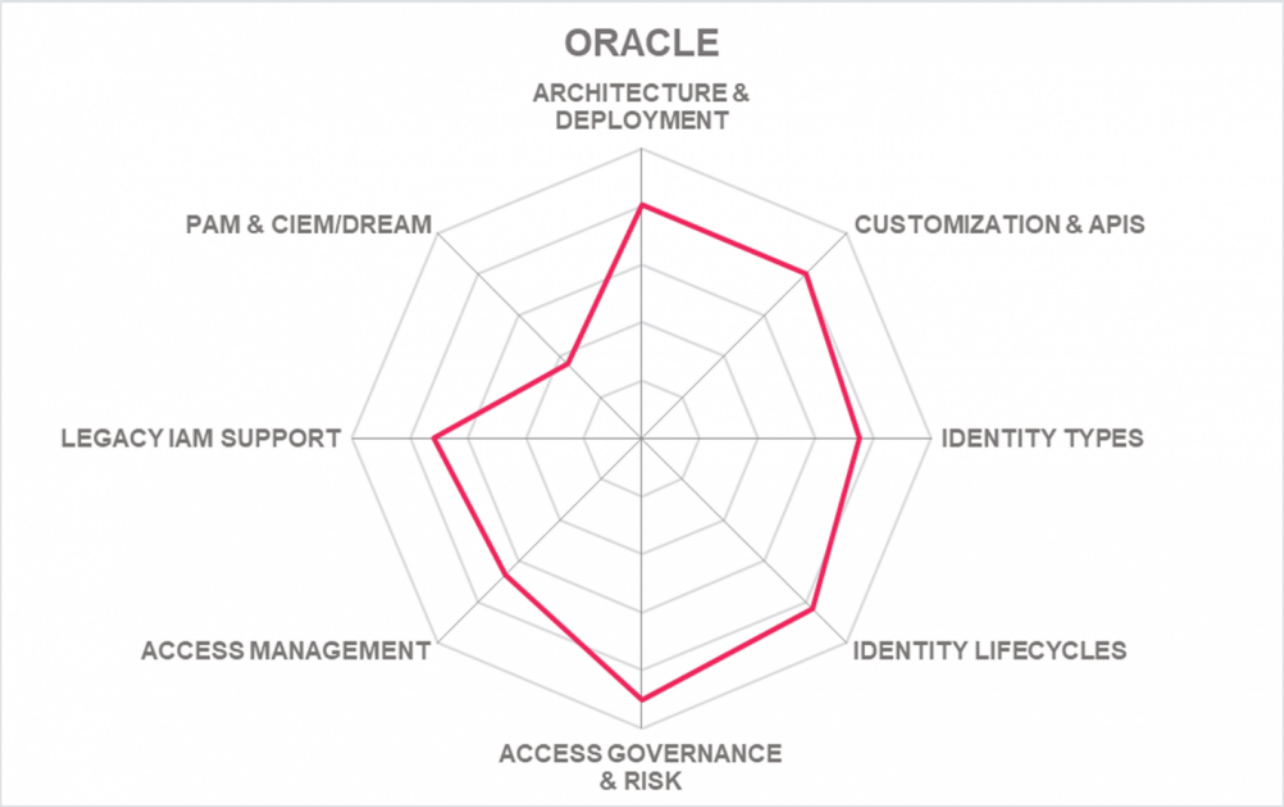
- Modern IDaaS solution for Access Management use cases
- Good IGA capabilities, but Access Governance capabilities still based on on-premises solution
- Clearly defined strategy and roadmap, consequent execution on roadmap
- Strong support for OCI and Oracle Cloud applications, but also for 3rd party environments
- Experienced vendor in the field of IAM
- Defined strategy for modernization of existing customer IAM environments
- Strong legacy support
- Existing IAM solutions are neatly integrated with new IDaaS services

Challenges

- IGA including Access Governance as IDaaS will be released soon
- No support for Privileged Access Management use cases
- Strong but still evolving feature set

Leader in




ORACLE
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.16 Radiant Logic

Radiant Logic is a provider of solutions that help turn identity into such key business enabler, and address the fragmentation of identity data as well as the lack of reliable data, i.e., the lack of good-enough Identity Information Quality. The RadiantOne platform is a solution that fits in between the various sources of identities, and the central identity services that form a comprehensive Identity Fabric. RadiantOne delivers Identity Unification capabilities required for the Identity Fabric. With their specialization, they are well-positioned as an add-on vendor for Identity Fabrics.

RadiantOne is a platform delivering a set of capabilities that helps in integrating identity data across a wide range of sources, from on-premises directory services to legacy application and cloud platforms. It creates a unified view on the identities that can serve as the authoritative source of truth for the depending services, be it the services within an Identity Fabric or the services consuming identities from the Identity Fabric via the Identity API layer. RadiantOne offers a variety of interfaces— LDAP, SQL, web services— for flexibility in accessing the unified data layer.
The identity integration layer of RadiantOne is based on delivering an integrated view across all identity information. RadiantOne on one hand provides access via traditional standards such as LDAP, but also allows to access information via modern federation standards.

The modules included in RadiantOne are the Federated Identity Engine for providing identity federation capabilities, the Universal Directory, Global Synchronization for integrating and unifying identity data, Directory Migration, and SSO. RadiantOne comes with good reporting capabilities.

While RadiantOne for itself does not provide everything needed for a comprehensive Identity Fabric, it adds capabilities that are commonly lacking in other vendor's solutions. With their ability to integrate and standardize information from many sources and to flexibly federate with a variety of such systems, RadiantOne is a valuable addition specifically for large and complex environments that struggle with insufficient identity information quality.

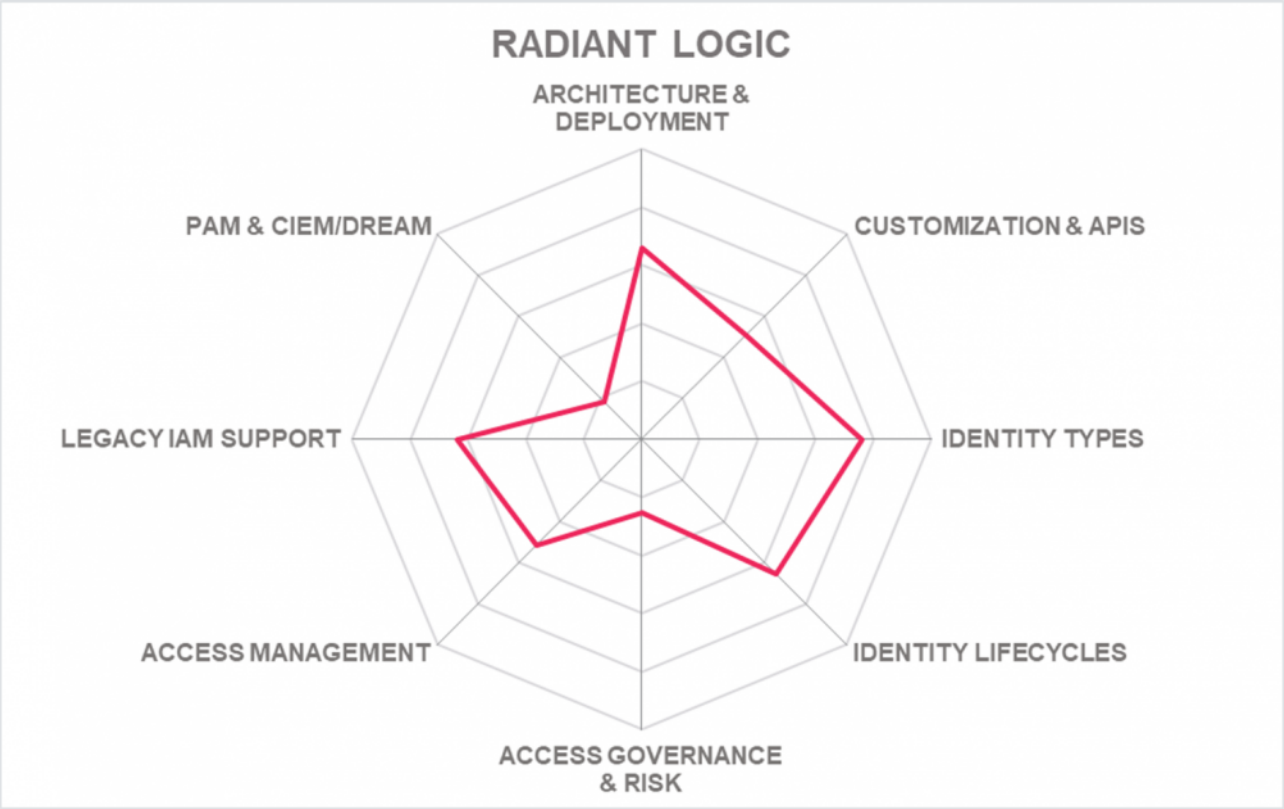
Security	●●●●○
Functionality	●●●○○
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●○

Strengths

- One of the very few providers for directory virtualization
- Can integrate and improve information from a variety of sources
- Supports federation and SSO across this range of sources
- Good set of APIs
- Various interfaces to source systems for identity data, including LDAP, SQL, and web services
- Proven capabilities in identity data integration at scale
- Well-suited for complementing other solutions for complex use cases
- Making good progress on modernizing the underlying platform and adding capabilities

Challenges

- Not a comprehensive Identity Fabrics offering, but specialized on the identity integration and quality improvement use cases
- Integrates with IGA and PAM solutions, but no integrated IGA and PAM capabilities
- Platform is undergoing modernization and extension in capabilities
- Limited, but well-selected partner ecosystem


RADIANT LOGIC
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.17 SecurID

With the de-merger of RSA from Dell, SecurID has become the brand for all IAM solutions provided by RSA. RSA SecurID covers a good set of IAM capabilities already, supporting on-premises and IDaaS deployments, with support for authentication and Access Management, Access Governance, and identity lifecycles. While providing a good set of features, the solution is still in its transition from the well-established on-premises solutions into a modern, feature-rich and fully integrated platform for serving the needs of modern Identity Fabric architectures.

The strongest part of the current SecurID offering is their support for modern authentication. They support access management and single sign-on for a broad variety of solutions, both on-premises and in the cloud. The solution supports risk-based authentication and comes with excellent support for a wide variety of authenticators, including RSA SecurID's own strong authentication technologies. With the ongoing integration to the RSA SecurID Risk Engine, more and more capabilities for anomaly detection and risk-based access controls are added.

RSA SecurID is continuing to support both on-premises and cloud deployments, giving customers the choice of deployment, depending on the types of applications that need to be supported, and the state of the infrastructure. Customers can add on-premises capabilities if required for better serving legacy-heavy infrastructures or add IDaaS to existing on-premises environments for a gradual migration.

RSA SecurID has significantly improved its user interfaces, adding capabilities such as broader self-service support and modern mobile apps. Workflow support is improving, but not yet leading-edge. The solution comes with an integrated portal, including dashboarding and analytical capabilities. On the other hand, the support of RSA SecurID for supporting on-premises applications counts amongst the strong ones in the market.

Overall, RSA SecurID is still in a transition phase of SecurID from a traditional IAM solution towards a comprehensive IDaaS offering covering IGA and Access Management for modern Identity Fabric architectures. We see the solution quickly catching up with the market in both architecture and deployment, and in the breadth and depth of capabilities, while continuing to deliver a very broad set of integrations.

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

RSA SecurID®

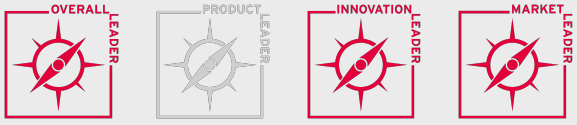
Strengths

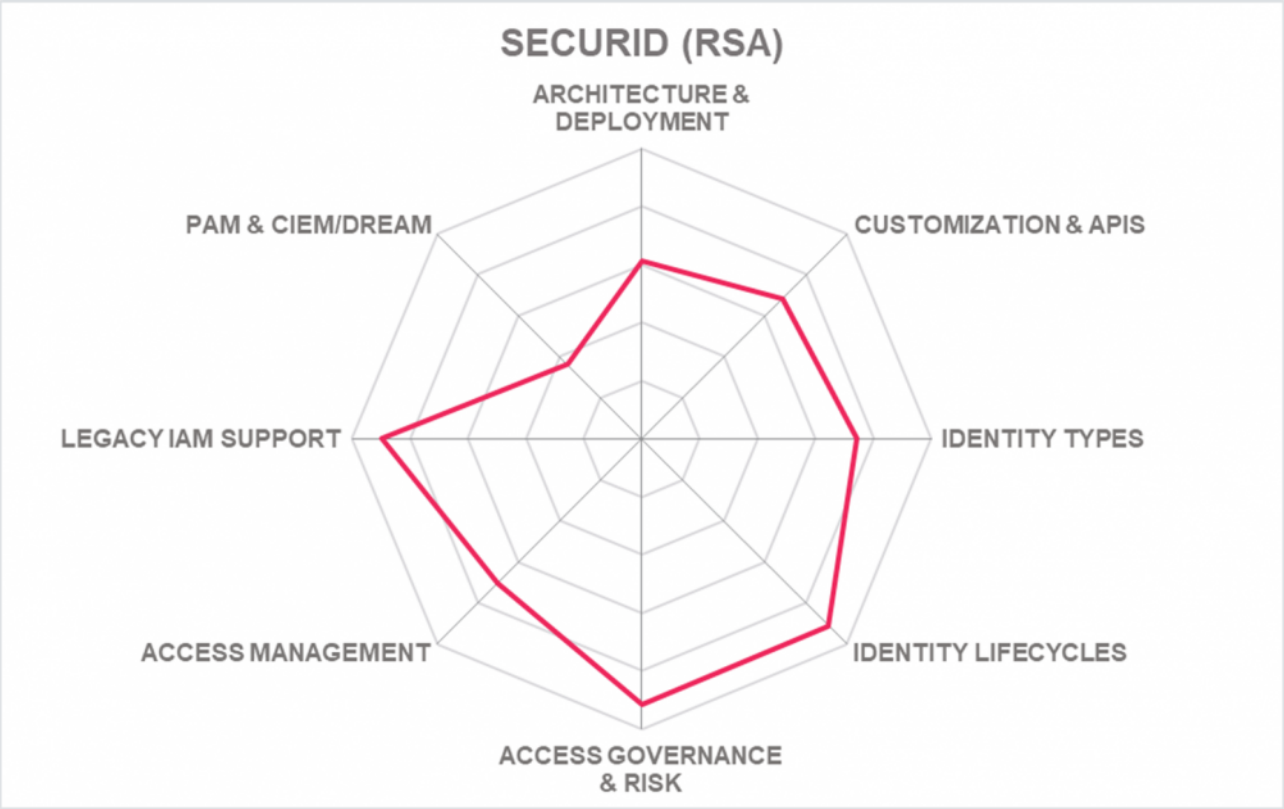
- Leading-edge access management capabilities
- Strong support for a broad variety of authenticators
- Own strong authentication capabilities as part of RSA SecurID
- Large number of certified out-of-the-box integrations for access management
- Good, but not outstanding IGA support
- Flexible support for running on-premises or as IDaaS
- Well-defined roadmap
- Large partner ecosystem at global scale

Challenges

- Still in the modernization from traditional IAM platforms to full IDaaS
- No support for PAM use cases
- Still some gaps in support for modern standards, but on roadmap
- Deployment can be challenging, but improved packaging and deployment on roadmap

Leader in




SECURID (RSA)
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.18 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, specifically for customers that own various IAM tools and are on their modernization journey, building on what they already have in place.

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

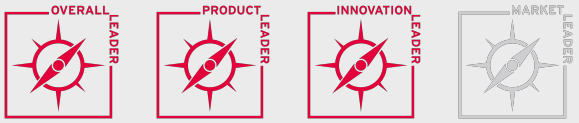
Strengths

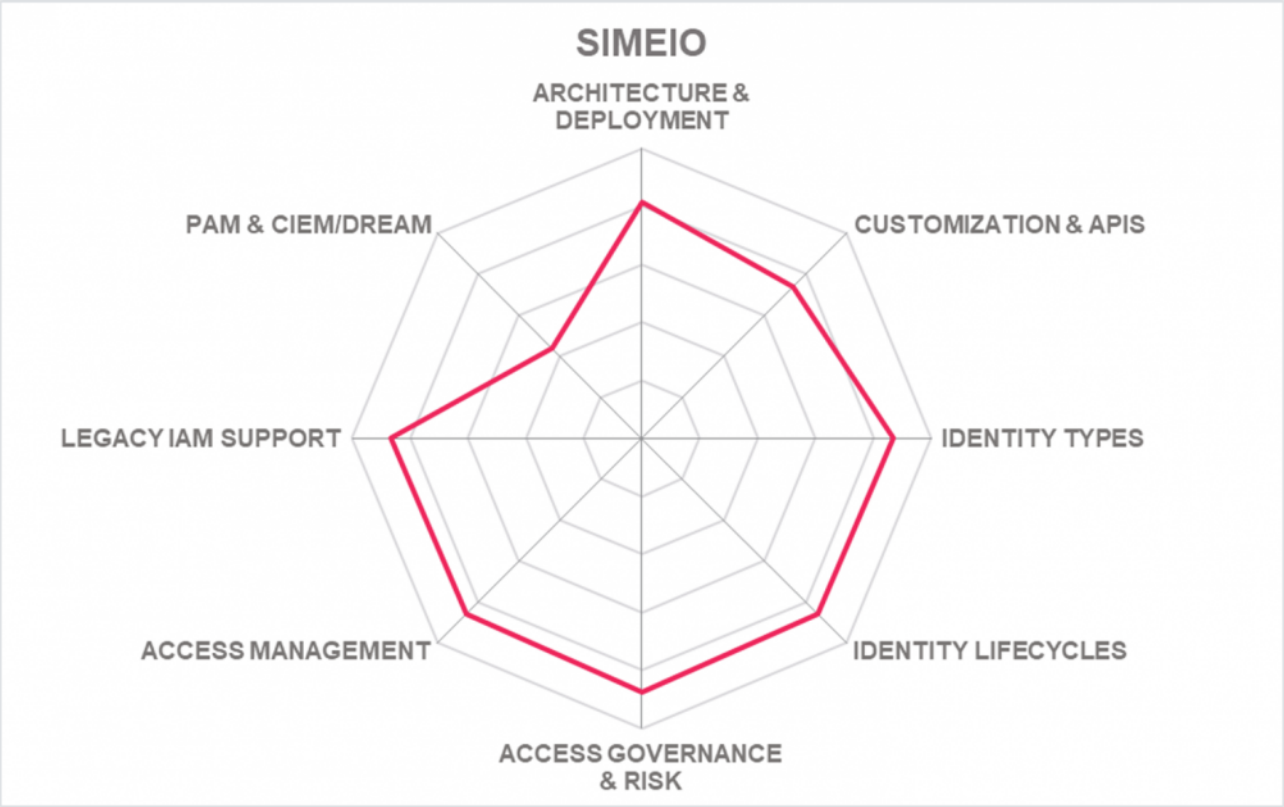
- Well-thought-out approach on orchestrating existing IAM products
- Broad partner ecosystem, involving many of the established vendors
- Simeio provides MSP and IDaaS services, operated from their own operations centers
- Consistent set of REST APIs for an Identity API layer
- Supports gradual migration 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
- Integration platform, not covering all IAM capabilities by their own

Leader in




SIMEIO
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

5.19 Strata Identity

Strata Identity is one of the specialist vendors in this Leadership Compass. In contrast to others, they don't provide a comprehensive Identity Fabric, but an interesting addition that complements other solutions by helping in integration existing Access Management solutions and identity siloes. The company is still small in size, but has an interesting position in the market due to its unique approach.

Strata Identity Maverics is a solution that is focused on managing identity siloes in today's quickly evolving IT infrastructures. Such infrastructures commonly contain a lot of identity siloes such as Microsoft Active Directory and others, but also new solutions that keep identities such as Microsoft Azure Active Directory, Google Cloud Platform, or AWS. Managing identities and access in such environments quickly becomes challenging.

Maverics is constructed as an abstraction layer on top of these various services, a fabric that integrates everything while avoiding creating large amounts of custom codes. It comes with an API that provides a consistent interface to the variety of identity and access management solutions and then delivers runtime orchestration and access to the existing applications. This helps customers that, e.g., run both Okta and Microsoft Azure Active Directory, or a range of legacy Access Management products.
Maverics is not limited to human identities but also servers service and other technical accounts. It comes with a modern user interface and a comprehensive set of APIs. A specific strength is the support of IDQL (Identity Query Language), a standard developed and proposed by Strata Identity.

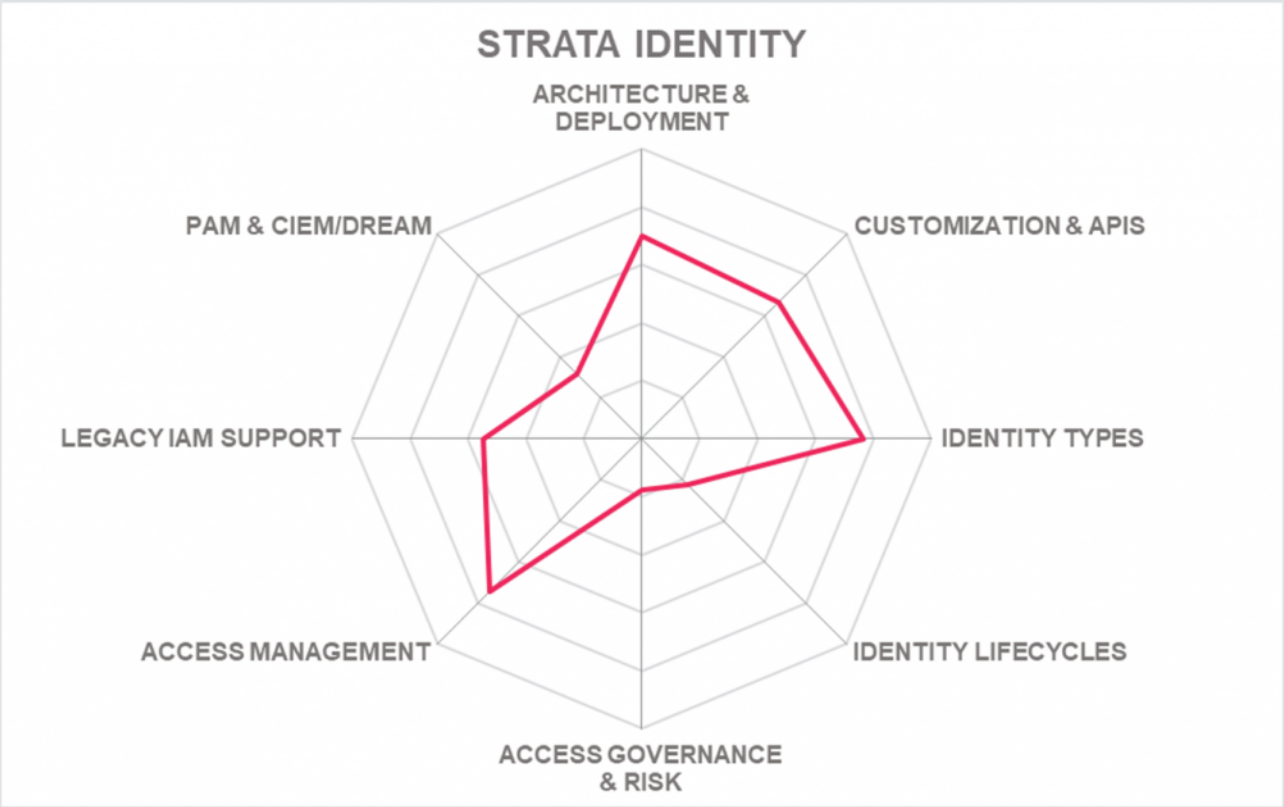
Strata Identity provides a range of interesting features that are not found in other products in the market. With many organizations struggling with a variety of identity siloes, even in modern cloud and SaaS environments, there is a need for integration, which is addressed by Strata Identity. This makes Strata Identity an interesting addition to other vendor's solution in building a comprehensive Identity Fabric.

Strengths

- Unique capabilities for integrating identity siloes at runtime
- Good support for a variety of cloud and on-premises Access Management solutions
- Modern user interface and policy-based controls
- Strong API support
- Delivering its own query language, IDQL
- Innovative vendor with a strong understanding of real-world IAM challenges

Challenges

- Still a small but growing number of customers, including some large deployments
- Small partner ecosystem, not yet at global scale
- Focused on a particular use case, not supporting the full breadth of Identity Fabrics capabilities


STRATA IDENTITY
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
PAM & CIEM/DREAM

6 Vendors to Watch

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

- **Atos** – is one of the largest IT consultancies, and has with the DirX portfolio and the Evidian products to own product offerings. DirX, under the Atos brand, provides a comprehensive set of IAM capabilities targeted at complex, large-scale environments.
  Why worth watching – Atos DirX solutions are proven in their support for complex, large-scale environments and cover both IGA and Access Management capabilities.
- **Authlete** – is a vendor specializing in offloading authentication and protocol specifics for the OAuth and OIDC protocol. This is a unique offering, which is of specific interest for organizations creating their own digital services.
  Why worth watching – complements other solutions by its specialized support for complex authentication use cases and thus adds to an Identity API layer.
- **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 worth watching – delivers additional, leading-edge authorization capabilities to an Identity Fabric.
- **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 worth watching – Good portfolio for overall IAM, with Access Management and IGA delivered as IDaaS.
- **Evidian** – is 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 as IDaaS solution.

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

- **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 worth watching – Proven IDaaS solution covering Access Management and IGA.
- **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 worth watching – Delivery of an integrated solution that builds on mature products and adds a consistent API layer plus flexible, container-based deployment.
- **Identity Automation** – Identity Automation is an US-based provider of an integrated IAM solution covering both Access Management and IGA requirements. Their focus is on higher education, but they also serve other market segments.
  Why worth watching – Provider of a solution for IAM that is well-suited for higher education and mid-market companies, following a platform approach.
- **Imprivata** – is a provider focusing on the Healthcare industry but providing solutions that also can well serve customers in other industries. Aside of their traditional strength in Enterprise Single Sign-On, Imprivata has created a comprehensive IAM portfolio through acquisitions.
  Why worth watching – specifically for Healthcare organizations, Imprivata provides a leading-edge solution with specific support for specialized industry applications.
- **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 increasingly modernized and provide a very mature and extensive set of IAM capabilities.
  Why worth watching – Strong and mature IAM capabilities that are modernized and shifting towards a modern Identity Fabric approach.
- **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 worth watching – One of the leading open-source offerings in the IAM market with a modern

architecture.

- **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, as well as strong workflow and orchestration capabilities. 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, specifically with IAM shifting away from standing privileges and towards just-in-time access.
  Why worth watching – Ping Identity can deliver the Access Management services for creating comprehensive Identity Fabrics together with other vendor's products.
- **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 worth watching – Delivers additional, leading-edge authorization capabilities to an Identity Fabric.
- **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 worth watching – Leading-edge specialist vendor for IGA capabilities, that could become an Identity Fabric if used with other vendor's Access Management solutions.
- **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 a range of solutions, including SAP Cloud Identity Access Governance, SAP Cloud Identity Authentication, SAP Cloud Identity Provisioning, SAP Identity Management, and SAP Single Sign-on.
  Why worth watching – broad set of capabilities, many of these provided as IDaaS solutions, and excellent support for the SAP ecosystem.
- **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 worth watching – it xxx One of the leading-edge offerings for IGA as a service plus existing partnerships with Access Management specialists.
- **Soffid** – is a provider of an open source IAM platform that covers IGA, Access Management, and PAM.

The solution provides a good baseline support for IAM functionalities, with strengths in the Single Sign-On use case. The solution can be provided in private clouds by the customer
Why worth watching – one of the few open source offerings in the Identity Fabrics market, with good baseline support across IAM capabilities.

- **Systancia** – is providing support for both Access Management and IGA use cases, but also for ZTNA (Zero Trust Network Access) and other capabilities. Their solution comes with strong support in certain areas such as workplace integration.
  Why worth watching – interesting alternative to the established vendors, specifically due to their integration into workplace access and ZTNA.
- **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.
  Why worth watching – strong platform for building digital services with good support for IAM; targeting primarily developers.

7 Related Research

Leadership Compass Access Control Solutions for SAP and other Business Applications
Leadership Compass Identity as a Service (IDaaS) IGA
Leadership Compass Privileged Access Management
Leadership Compass Identity Governance & Administration
Leadership Compass Access Management
Market Compass IGA Solutions for ServiceNow Infrastructures
Executive View Hitachi ID Bravura Privilege
Executive View Hitachi ID Bravura Security Fabric
Executive View Simeio Identity Orchestrator
Executive View One Identity Manager On Demand
Executive View Accenture Memority
Executive View IBM Security Verify for CIAM
Executive View Cloudentity Authorization Control Plane

Methodology

About KuppingerCole's Market Compass

KuppingerCole Market Compass is a tool which provides an overview of a particular IT market segment and identifies the strengths of products within that market segment. It assists you in identifying the vendors and products/services in that market which you should consider when making product decisions.

While the information provided by this report can help to make decisions it is important to note that it is not sufficient to make choices 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.

Product Rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Deployment
- Interoperability
- Usability
- Market Standing

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

the way the vendor deals with them.

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

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

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

Market Standing is a measure of financial strength and market position. This is based on publicly available information, and takes the amount of funding received, the profitability, and the private or public status of the vendor into consideration.

We focus on security, deployment, interoperability, usability, and market standing for the following key reasons:

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

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

Rating scale for products

For vendors and product feature areas, we use a separate rating with five different levels. These levels are:

- **Strong positive**

Outstanding support for the subject area, e.g. product functionality, or security etc.)

- **Positive**
  Strong support for a feature area but with some minor gaps or shortcomings. Using Security as an example, this could indicate some gaps in fine-grained access controls of administrative entitlements.

- **Neutral**
  Acceptable support for feature areas but with several of our requirements for these areas not being met. Using functionality as an example, this could indicate that some of the major feature areas we are looking for aren't met, while others are well served.

- **Weak**
  Below-average capabilities in the area considered.

- **Critical**
  Major weaknesses in various areas.

Content of Figures

Copyright

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

KuppingerCole, founded in 2004, is a global, 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.