KUPPINGERCOLE ANALYSTS

Identity Fabrics

Martin Kuppinger

February 20, 2024

LEADERSHIP COMPASS 2024

This report provides an overview of the market of providers of technology for building Identity Fabrics, which are comprehensive IAM solutions built on a modern, modular architecture. It provides a compass to help organizations find the solution that best meets their needs. We examine the market segments, product functionality, the market position of vendors, and the innovative approaches to providing solutions that serve customers best in building their Identity Fabrics.

Contents

Figures

Introduction

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. To better understand the fundamental principles this report is based on, please refer to KuppingerCole's Research Methodology.

> Here is how we explained it in our foundational document on Identity Fabrics: 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 differing 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 or commonly based on a single technology, tool, or cloud service, but a paradigm for architecting IAM within enterprises. Commonly, the services are provided as a combination of several tools and services, with up to three solutions forming the core of the Identity Fabric, covering the core capability areas of identity and access management (IAM) such as identity governance and administration (IGA), access management, and Privileged Access Management (PAM). These core solutions are complemented by specialized solutions for advanced capabilities or filling functional gaps. Most organizations that use this paradigm to evolve their IAM capabilities tend to build on a core platform for major features and complement it with point solutions, as needed.

Recently, we have observed a trend toward deploying orchestration solutions as a core component of Identity Fabrics. Orchestration solutions extend IAM solutions to deliver integrated identity services, but they also help to provide integration with legacy IAM technology. Some vendors include orchestration as part of a comprehensive IAM suite / Identity Fabrics offering, while others provide orchestration as a standalone product.

Given the state of the market, this Leadership Compass analyzes which of the IAM offerings are best suited to form the foundation for an Identity Fabric that delivers:

- a broad range of IAM capabilities, including a foundational level of both IGA and access management (including identity federation, multi-factor authentication)—or alternatively providing an orchestration platform for IAM
- a comprehensive set of APIs for consuming identity services, beyond the admin and end user interface and user experience (UI/UX)
- a modern architecture, following patterns for microservices architectures and container-based deployments
- support for different deployment models, enabling customers to deploy in their preferred operating models (with some solutions being cloud-only)
- support for all types of identities, including workforce, business partners, customers, devices, and services

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

Highlights

Identity Fabrics is the foundational paradigm for IAM, enabling organizations to define a holistic and integrated technical architecture for IAM. Since we first introduced the concept in 2019, an increasing number of organizations have successfully established their own Identity Fabrics that deliver modern, integrated IAM services to their organizations.

- The market for Identity Fabrics is evolving quickly and the maturity of solutions has improved significantly. However, the market is still not at the same level of maturity as other established IAM disciplines, such as IGA or access management. Nevertheless, the Identity Fabrics market remains a center of significant innovation.
- Few vendors provide all three major components of IAM, (IGA, Access Management, and PAM) natively. As a result, Identity Fabrics almost always require a multivendor strategy.
- Major IAM vendors also leave space for leading-edge solutions in specialized segments. For example, Okta (which provides both IGA and PAM capabilities) integrates with pure-play IGA solutions from vendors such as SailPoint and Saviynt. Such solutions can well complement other vendors solutions to weave a comprehensive Identity Fabric.
- A growing number of specialist vendors have emerged that add sophisticated features for authorization and orchestration across existing identity solutions and silos. These specialists can help organizations close gaps in core IAM platforms. These vendors include, but are not limited to, Cloudentity and Strata Identity.
- The support for exposing capabilities via modern APIs is growing rapidly. Most vendors expose all relevant capabilities via an integrated and complete set of REST and other modern APIs.
- Several vendors, including most of the “IAM veterans” such as Oracle, RSA, IBM, or Broadcom (which includes former CA Technologies), are still on their modernization journey for their platforms. Most of them are demonstrating considerable progress in executing on their roadmaps. The current state of transition must be carefully analyzed, nonetheless.
- The deployment approaches supported by vendors range from supporting only multi-tenant, public cloud deployments to implementations that are single-tenant and run as managed service provider (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.
- The Overall Leaders are Microsoft, Ping Identity, IBM, Broadcom, One Identity, Oracle, OpenText, CyberArk, RSA Security, EmpowerID, and Exostar.
- The Product Leaders are Ping Identity, Microsoft, IBM, EmpowerID, Broadcom, OpenText, One Identity, Exostar, Oracle, and CyberArk.

- The Innovation Leaders are Ping Identity, Microsoft, EmpowerID, One Identity, IBM, Broadcom, Exostar, OpenText, Simeio, Oracle, CyberArk, RSA Security, Cloudentity, and Strata Identity.
- The Market Leaders are Microsoft, IBM, Oracle, CyberArk, Broadcom, Ping Identity, OpenText, RSA Security, and One Identity.

The Identity Fabrics Market Segment in 2023

Digital business has evolved from the simple e-commerce websites of the nineties. Modern digital business models are complex, distributed, and multidimensional and involve many parties in a variety of roles. This trend directly impacts 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, things, and processes use and provide services. Access occurs from any conceivable location to services that may reside in on-premises data centers, the cloud, or mobile systems. The formerly classic corporate network with clearly defined "inside" and "outside" has given way to a massively hybrid, new IT reality. IAM has emerged as the essential security infrastructure from which enterprises can facilitate new services, models, and forms of cooperation.

To make this possible, IAM must be converted into a consolidated portfolio of isolated but corresponding services that enable connectivity to anyone and anything via a comprehensive architecture. IAM platforms also must make services available to users everywhere in a secure, scalable fashion without organizations losing control of critical data and systems.

“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 context 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 (especially consumer identities) must be integrated quickly and securely in user-friendly flows.
- B2B onboarding and IAM in the challenging context of Supply Chain Security.
- User control over their identities by bringing their own identities with them (BYOI).
- Employees (on-site and remote) using their preferred devices they.
- Securing access to working environments regardless of where users and systems are located.
- Zero Trust features, such as continuously verifying access must be part of the capabilities.

- Linking identities to reflect relationships within teams, companies, families, or partner organizations.
- Maintenance of identities in trusted organizations, which can be directly and reliably integrated and authorized in each organization's IAM.
- Using identities, conduct business and execute payments.
- Observation of all relevant laws and regulations.
- Optimization of know your customer (KYC) processes.
- Providing data about identities, entitlements, and their usage in analytics and artificial intelligence (AI) applications.
- Support for all types of identities, so that devices, services, and networks are integrated into next-generation IAM infrastructure.

Traditional IAM systems meet only a fraction of today's requirements. They are often monolithic in design and implementation, making it difficult to consume them as discrete components. To achieve seamless access for all users from everywhere to every service, organizations must shift away from isolated, bespoke 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.

Supported services can be in public or private clouds, on-premises (private datacenter), or (in the case of legacy applications) in a hybrid deployment during a transitional phase. It might even be valid to integrate redundant services for different usage scenarios. What these services 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. As such, they must meet the requirements for scalability, performance, and resilience. Figure 1 illustrates how Identity Fabrics must support a wide variety of services and topologies.

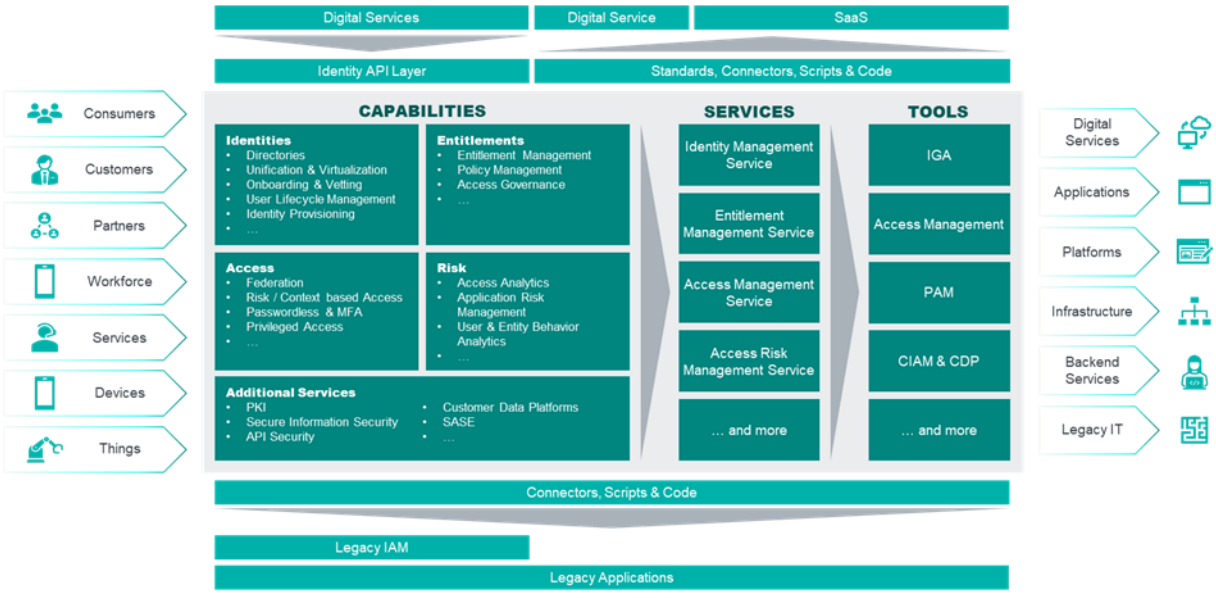


Figure 1: A sample high-level, conceptual architecture for an Identity Fabric. The set of capabilities and services provided depends on the specific requirements of the organization.

Identity Fabrics combine current and proven IAM concepts with modern concepts such as security by design and APIs, service-oriented IT (often implemented as microservices), and modern delivery channels for cloud, hybrid infrastructures, containers, and their orchestration or serverless infrastructures.

KuppingerCole Analysts 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 that 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 or augment outdated or functionally incomplete components along the way, but, ideally, 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 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.

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. The implementation of an Identity Fabric commonly builds on one or two main technical components for IGA and Access Management and is complemented by additional components that provide further services and capabilities. There might even be some level of redundancy, either in migration or for technical or organizational reasons. However, the concept of Identity Fabrics applies to designing and implementing a modern IAM that is modular, flexible, and provides the capabilities required this includes deploying a consistent identity API layer that allows digital services to consume the identity services.

In recent years, we have witnessed 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. Several vendors are actively promoting this model and positioning their solutions as Identity Fabrics.

We expect to see further gains in momentum, with the continuing increased need for modernizing and extending IAM as well as for improved support for digital services. With the continued transformation of legacy IAM solutions into modern architectures with strong API support and flexible deployment models, more solutions will become available and integration of multi-vendor solutions into a unified Identity Fabric becomes simpler. This all contributes to the further adoption of the Identity Fabrics model by both vendors and enterprise organizations.

Delivery Models

Identity Fabrics are agnostic to the deployment model. Ideally, components can be deployed in several types of topologies, for example, components running in different locations such as a public cloud and on the edge of the on-premises infrastructure. This allows for an integrated solution approach, while keeping certain services closer to the premises, running them as a full Identity as a Service (IDaaS) service, or in a shielded environment, for instance due to regulatory compliance requirements. However, pure-play IDaaS also is a valid approach. Options include:

- Multi-tenant public cloud services
- Single-tenant public cloud services, particularly where updates, patches, and fixes need to be 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, which can operate in various deployment models, such as in private or public clouds or even on-premises, provided they can be operate in a full “as-a-service" model, including updates, patches, etc. being provided or even deployed by the service provider across all tenants with full automation. Again, this requires adequate, modern software architectures (segregation of customizations and data from application code)

Furthermore, delivery must meet the enterprise’s expectations regarding licensing models (pay-per-use), elasticity, and scalability. Beyond that, as mentioned above, we expect modern software architectures, which provide 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; they also enable support for more complex scenarios such as geographically dispersed deployments and hybrid scenarios.

For this Leadership Compass, we prefer the availability of “as-a-service" deployment architecture but is open to all forms from managed services to publicly delivered IDaaS.

Required Capabilities

Identity Fabrics must support a baseline level of both IGA and access management; from there, they could further provide capabilities such as integrated directory services, PAM, and other IAM capabilities that are commonly required by customers.

IGA solutions cover two areas of capabilities:

- Identity lifecycle management/identity provisioning
- Access Governance, including access reviews and access intelligence

The focus is on solutions that cover both aspects of IGA, i.e., not being solely limited to either identity provisioning or access governance.

Main capabilities of IGA solutions are:

- Automated user provisioning
- Connectors both to cloud services and on premises applications
- Toolkits for customizing connectors
- Integration and/or synchronization to directory services
- Self-service for credentials and user profile administration
- Access request & approval workflows
- Entitlement management, including role management
- Segregation of Duty (SoD) controls management and enforcement
- Access certification and recertification
- Identity and access analytics
- Auditing, reporting and dashboarding

Access Management consists of various capability areas such as:

- Identity federation and, for legacy environments, Web Access Management (WAM)
- MFA and adaptive authentication (risk-/context-based)

Again, we expect solutions to support both areas. The primary capabilities in access management for Identity Fabrics include, but are not limited to:

- Support for inbound and outbound federation
- Support for all major identity federation standards, including SAML and OAuth
- WAM capabilities for integrating applications without built-in federation support
- User onboarding and registration workflows
- Self-service interfaces for managing credentials and user profiles
- Integration and/or synchronization to directory services
- Support for federated provisioning
- Auditing, reporting and dashboarding
- Support for a broad range of authenticators, including decentralized identities
- Toolkits for adding additional authenticators

- Support for 2FA/MFA and FIDO2 standards
- Step-up authentication
- Risk- and context-based authentication
- Passwordless authentication

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

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

And finally, scalability and support for multiple types of identities and the required scale paramount to the success of any solution.

Included in this Leadership Compass are solutions that serve both IGA and access management requirements, 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.

We also cover specialized orchestration vendors that can serve as a core element in integrating existing identity services and building an Identity Fabric, even when these are limited in their IGA and Access Management capabilities.

Excluded from this Leadership Compass are:

- Vendors that only cover IGA or access management (except specialized orchestration offerings for Identity Fabrics). We expect at least core foundational capabilities in both areas and prefer to see additional IAM capabilities, where traditional IGA capabilities also can be replaced by adequate other features such as strong policy-based access management.
- Vendors that have multiple products with incongruent architectures and little or no integration regarding deployment, operations, architecture, UI/UX, or APIs.
- Vendors that do not meet the definition of IDaaS. This includes pure MSP deployments as well as solutions without a pay-per-use licensing model.
- Vendors without active deployments at customers (such as start-ups in stealth mode).
- Solutions with a traditional architecture, not supporting modern deployment models such as container-based deployments.
- Solutions that lack a comprehensive set of APIs.
- Solutions that are targeted at either only employees/business partners or at customers/consumers.

Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

Figure 2: Overall Leadership for Identity Fabrics (graphic has no vertical axis).

The **Overall Leadership** chart indicates that a sizable number of vendors have achieved a high level of maturity, with more than half of the vendors being placed in the Leaders segment. Microsoft is slightly ahead of Ping Identity, due to their strong market position. Ping Identity, after the merger with ForgeRock, is now part of the rating and takes a strong position with the combined portfolio, despite some integration work still to do. Following them is a group of established IAM vendors, including IBM, Broadcom, One Identity, OpenText (with the NetIQ portfolio), and Oracle. CyberArk is also close to this group, with their extended portfolio. Furthermore, EmpowerID and Exostar are in this group of vendors.

In the Challenger segment, Simeio is well-positioned with its powerful integration platform. Behind them, at some distance, are several smaller and highly specialized vendors. Cloudentity and Strata Identity are innovative orchestration platforms. Soffid and OpenIAM are open source IAM platforms. XAYone and Trustbuilder are focusing on access management and customer IAM (CIAM) use cases. Bravura Security, formerly Hitachi-ID, is

in the conversion towards IDaaS and Optimal IdM is focusing on the mid and low-end of the IAM market.

Overall Leaders are (in alphabetical order):

- Broadcom
- CyberArk
- EmpowerID
- Exostar
- IBM
- Microsoft
- One Identity
- OpenText
- Oracle
- Ping Identity
- RSA Security

Product Leadership

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

Figure 3: Product Leadership for Identity Fabrics.

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services. Again, we find several vendors in the Leaders segment. These include Ping Identity with the combined Ping / ForgeRock product Portfolio, Microsoft, and then several vendors that are head-to-head, including Broadcom, EmpowerID, IBM, One Identity, and OpenText. Exostar is also close to this group and both CyberArk and Oracle have also made it into the Leaders segment.

The other vendors are placed in the Challenger segment, with Simeio and RSA Security being close to becoming Leaders. These other vendors are all positioned more towards the center of the Challenger segment.

Product Leaders are (in alphabetical order):

- Broadcom
- CyberArk
- EmpowerID
- Exostar
- IBM
- Microsoft
- One Identity
- OpenText
- Oracle
- Ping Identity

Innovation Leadership

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

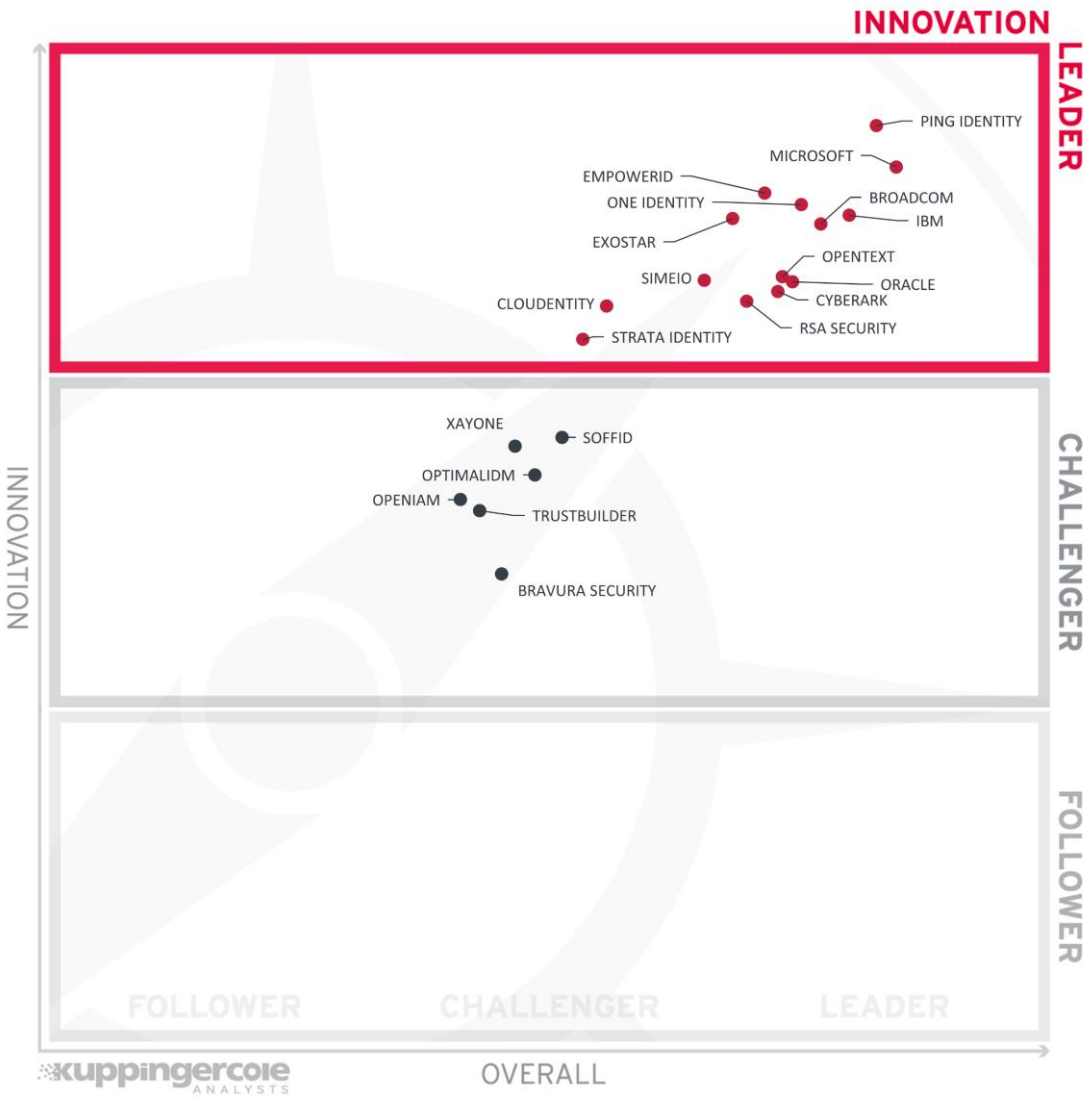


Figure 4: Innovation Leaders for Identity Fabrics.

While the solutions for Identity Fabrics have matured over the recent years, the market continues to innovate, both by established and specialist vendors. Accordingly, many vendors are positioned in the Leaders segment. Innovation is driven by new capabilities such as orchestration, identity analytics, and the addition of capabilities powered by AI/ML; this category also includes vendors rethinking traditional approaches, such as in the field of IGA.

In the Leaders segment, Ping Identity comes in ahead of Microsoft, closely followed by a group of five vendors, consisting of Broadcom, EmpowerID, Exostar (with its very modern and well-architected platform), IBM, and One Identity. Other vendors in this segment include CyberArk, OpenText, Oracle, and RSA Security, as well as the three orchestration-focused vendors Simeio, Cloudentity, and Strata Identity.

In the Challenger section, we find Soffid and XAYone on top, closely followed by Optimal IdM, OpenIAM, and Trustbuilder. Bravura Security, being in the IDaaS transformation, is slightly distanced, but has an ambitious roadmap for innovation.

Innovation Leaders (in alphabetical order):

- Broadcom
- Cloudentity
- CyberArk
- EmpowerID
- Exostar
- IBM
- Microsoft
- One Identity
- OpenText
- Oracle
- Ping Identity
- RSA Security
- Simeio
- Strata Identity

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, also requires global reach.

Figure 5: Market Leaders for Identity Fabrics

Microsoft is leading the market, being a dominant player in the IAM space. Following them are large IT vendors with a considerable footprint in the IAM market; these are IBM, Oracle, CyberArk, and Broadcom. Ping Identity, OpenText, RSA Security, and One Identity are also positioned in the Leader segment.

Other vendors, including EmpowerID, Simeio, and Exostar, are rated as Challengers. Additional vendors who made it into this segment include Bravura Security, Strata Identity, Optimal IdM, and Cloudentity.

In the Follower section, we find Soffid, TrustBuilder, XAYone, and OpenIAM, all of which are smaller vendors with mostly small partner ecosystems and limited market presence at global scale.

Market Leaders (in alphabetical order):

- Broadcom
- CyberArk
- IBM
- Microsoft
- One Identity
- OpenText
- Oracle
- Ping Identity
- RSA Security

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.

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

The Market/Product Matrix

Figure 6: The Market/Product Matrix shows the correlation between 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 could be considered “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 Market Champions include most of the large, established players in the IAM market, including Microsoft, IBM, Oracle, CyberArk, Broadcom, Ping Identity, OpenText, and One Identity. RSA Security, demonstrating good progress after focusing on IAM only again, is close to entering this segment.

In the other segments, the one to the center right, is of specific interest. Both EmpowerID and Exostar have strong product offerings but a comparably low market presence. These vendors show, based on their technology, a strong potential for growth.

The Product/Innovation Matrix

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

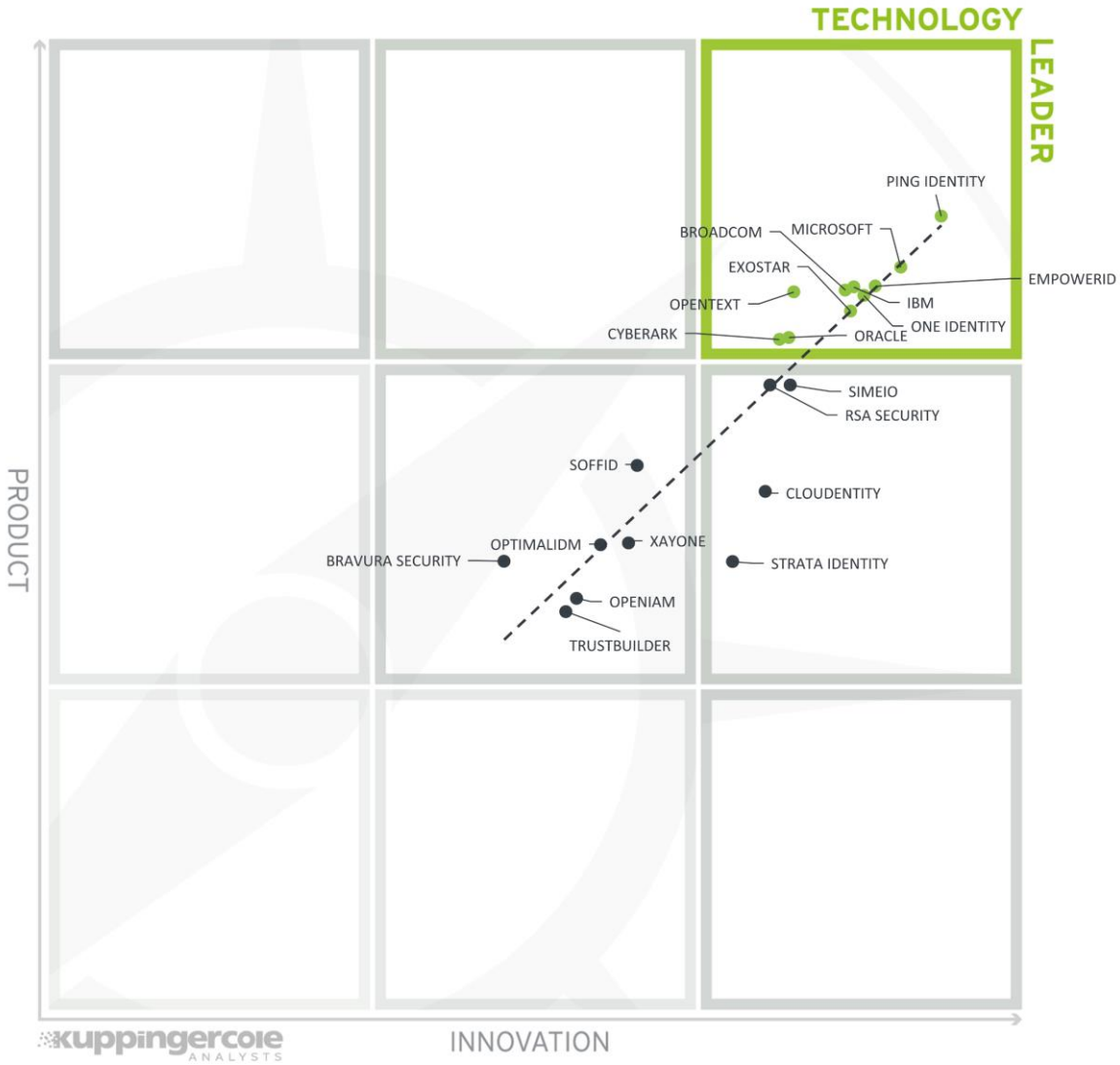


Figure 7: The Innovation/Product Matrix shows the correlation between Innovation Leadership and Product Leadership.

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative. For this Leadership Compass, we see a good correlation of product capabilities and innovative features.

Technology Leaders include Ping Identity, Microsoft, EmpowerID, IBM, One Identity, Broadcom, Exostar, OpenText, CyberArk, and Oracle. All these vendors have strong product offerings but are also very innovative.

Simeio and RSA Security are close to entering the top right segment of Technology Leaders with their offerings.

In the center right segment, we also find Cloudentity and Strata Identity, which are taking a different approach with their solutions, focusing on orchestration of identity solutions.

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. 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.

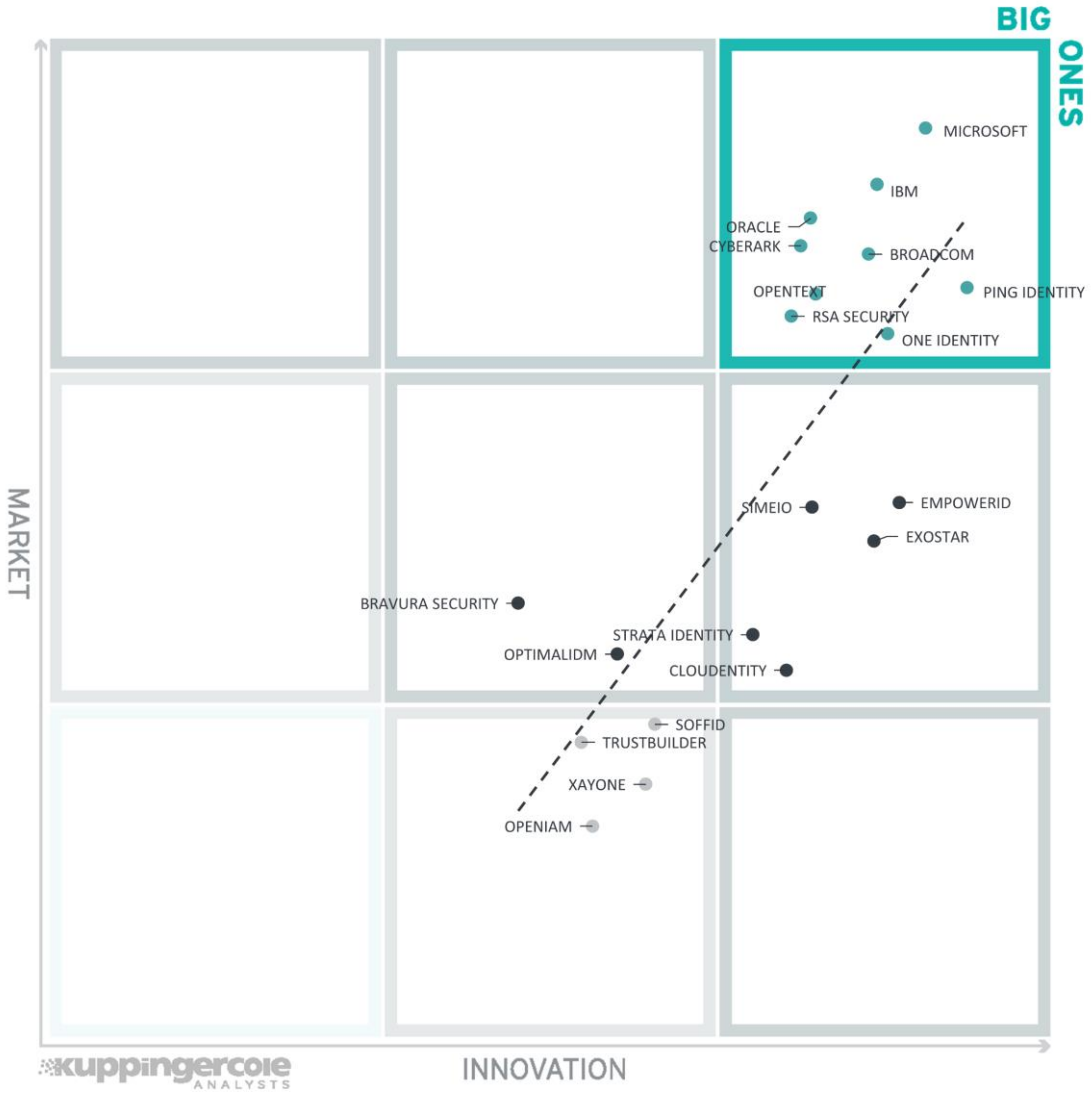


Figure 8: The Innovation/Market Matrix shows the correlation between Innovation Leadership and Market Leadership.

Vendors above the line are performing well in the market and show Innovation Leadership. Vendors below the line show an ability to innovate, and although they have less of the market share, they have the biggest potential for improving their market position.

Not surprisingly, the segment of the “Big Ones” is populated by the established IAM vendors, including Microsoft, IBM, Oracle, CyberArk, Broadcom, Ping Identity, OpenText, RSA Security, and One Identity.

To the center right, we find the vendors that are highly innovative but not yet that big, including EmpowerID, Exostar, Simeio, Strata Identity, and Cloudentity.

Identity Fabrics: 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. Since some vendors may have multiple products, these are listed according to the vendor's name.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
BRAVURA SECURITY	positive	positive	neutral	positive	positive
BROADCOM	strong positive	strong positive	strong positive	strong positive	strong positive
CLOUDENTITY	strong positive	neutral	strong positive	positive	strong positive
CYBERARK	strong positive	positive	positive	strong positive	strong positive
EMPOWERID	strong positive	strong positive	strong positive	strong positive	strong positive
EXOSTAR	strong positive	positive	strong positive	strong positive	strong positive
IBM	strong positive	strong positive	positive	strong positive	strong positive
MICROSOFT	strong positive	strong positive	strong positive	strong positive	strong positive
ONE IDENTITY	strong positive	strong positive	positive	strong positive	strong positive
OPENIAM	positive	positive	neutral	positive	positive
OPENTEXT	strong positive	strong positive	positive	strong positive	strong positive
OPTIMAL IDM	positive	neutral	positive	positive	positive
ORACLE	strong positive	strong positive	strong positive	strong positive	strong positive
PING IDENTITY	strong positive	strong positive	positive	strong positive	strong positive
RSA SECURITY	strong positive	positive	positive	strong positive	strong positive
SIMEIO	strong positive	neutral	positive	strong positive	strong positive
SOFFID	positive	positive	positive	positive	strong positive
STRATA IDENTITY	positive	neutral	strong positive	positive	neutral
TRUSTBUILDER	positive	neutral	positive	positive	positive
XAYONE	positive	neutral	positive	positive	positive

Table 1: Comparative overview of the ratings for the Identity Fabrics 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
BRAVURA SECURITY	neutral	neutral	positive	positive
BROADCOM	strong positive	strong positive	strong positive	strong positive
CLOUDENTITY	positive	neutral	positive	positive
CYBERARK	positive	strong positive	strong positive	strong positive
EMPOWERID	strong positive	neutral	positive	positive
EXOSTAR	strong positive	neutral	positive	positive
IBM	strong positive	strong positive	strong positive	strong positive
MICROSOFT	strong positive	strong positive	strong positive	strong positive
ONE IDENTITY	strong positive	positive	strong positive	positive
OPENIAM	neutral	weak	neutral	neutral
OPENTEXT	positive	positive	strong positive	strong positive
OPTIMAL IDM	positive	neutral	positive	neutral
ORACLE	positive	strong positive	strong positive	strong positive
PING IDENTITY	strong positive	positive	positive	strong positive
RSA SECURITY	positive	positive	positive	strong positive
SIMEIO	positive	neutral	positive	positive
SOFFID	positive	weak	neutral	neutral
STRATA IDENTITY	positive	weak	neutral	positive
TRUSTBUILDER	positive	weak	neutral	neutral
XAYONE	positive	weak	neutral	neutral

Table 2: Comparative overview of the ratings for Identity Fabrics vendors.

Product/Vendor evaluation

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

Spider graphs

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

- **Additional IAM Capabilities**: This dimension focuses on support for Privileged Access Management and the new disciplines of cloud **i**nfrastructure entitlement management (CIEM) and other advanced capabilities. Integrated support for such capabilities becomes increasingly relevant with the convergence of these capabilities, and for supporting identity types such as services.

Bravura Security – Bravura Identity

Bravura Security is a company with roots dating back to M-Tech, a Canadian software vendor that was acquired by Hitachi and renamed to Hitachi-ID, with the product portfolio being renamed to Bravura. After a recent spin-off, the company name changed to Bravura Security, with the identity products being Bravura Identity and the recently launched, cloud-based solutions Bravura Cloud.

Bravura is in a conversion phase from the established products Bravura Pass for password management, Bravura Identity for IGA, and Bravura Privilege for PAM into IDaaS based, integrated set of solutions. The suite of products is known as Bravura Security Fabric. Bravura Cloud now adds, in a first phase of evolution, an additional layer that will support Identity Information Quality (cleanse), identity inventories, and risk-based Identity Governance capabilities. In subsequent phases, additional capabilities such as policy-based access control and behavioral monitoring will be added.

Bravura Cloud is based on a modern architecture, backed by a modern data architecture supporting graph-based access, and following an API-first approach. It can run in different models, ranging from hosted and managed by Bravura Security to deployments on the customer's on-premises or VPC (Virtual Private Cloud) infrastructure. The first release, with above-mentioned capabilities, is named Security Data Engine, building the foundation for future additional capabilities. Data from Bravura Security can be discovered and imported into Bravura Cloud.

Bravura Cloud comes with a modern UI (user interface) which is, due to the somewhat limited functionality, still a bit empty. It provides dashboard, risk-based analytics, and other capabilities. The first step to developing the existing solution is to enable more coverage in the modern cloud services by modernizing for container-based deployments, and then adding API's.

For existing current customers, this strategy provides an interesting modernization approach. New customers can rely on the proven, solid capabilities of the Bravura Security Fabric, but will have to undergo stepwise migration towards the new Bravura Cloud.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Positive
Usability	Positive

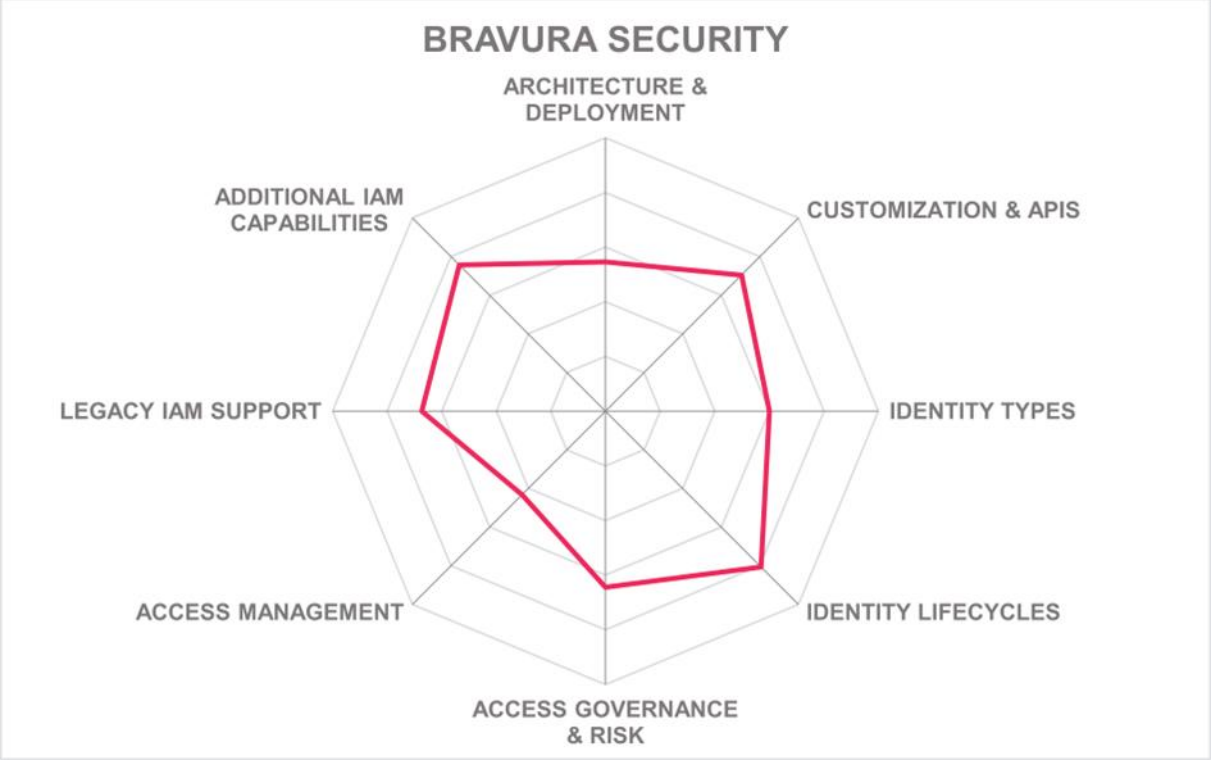
Table 3: Bravura Security's rating

Strengths

- Modern cloud platform for integration
- Cloud platform uses GraphQL and webhooks and follows an API-first approach
- Flexible deployments of Bravura Cloud
- Adding dashboards and modern UI in Bravura Cloud
- Integration of Bravura Cloud to legacy Bravura Security solutions
- Solid IGA functionality in Bravura Identity
- Proven password management features in Bravura Pass
- Solid PAM capabilities in Bravura Privilege

Challenges

- Core capabilities still relying on legacy Bravura Security products
- Lack of innovative capabilities in current release, but is on the roadmap for Bravura Cloud
- Weak capabilities for Access Management
- Bravura Cloud, while adding new capabilities. Requires gradual migration of Bravura Security solutions
- Current capabilities of Bravura Cloud still limited



Broadcom – Symantec Identity Security

Broadcom Software and the Symantec Identity Security solutions have emerged following Broadcom's acquisitions of CA Technologies and Symantec. Symantec Identity Security comprises multiple solutions for access management, authentication, IGA, and PAM. These are based on several flagship products including 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. Broadcom consequently builds on a "fabric" model in integrating and orchestrating components and delivering a solution with a proven high scalability.

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 and have also undergone significant modernization and improvements in recent years. As a result, 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's target customers are global enterprises with large user bases. For these customers, the Symantec portfolio is particularly adapted to their use cases and requirements.

The overall functionality across IGA, Access Management, and PAM is strong. As mentioned above, Symantec benefits from its 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 many 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 a very few vendors can deliver. Backed by a global ecosystem, the company can deploy such solutions at scale and fast. Furthermore, there are strong integrations, both technical and in licensing, into the security portfolio of Broadcom Software, which might be of interest to enterprise customers.

Security	Strong Positive
Functionality	Strong Positive
Deployment	strong positive
Interoperability	Strong Positive
Usability	strong positive

Table 4: Broadcom's rating

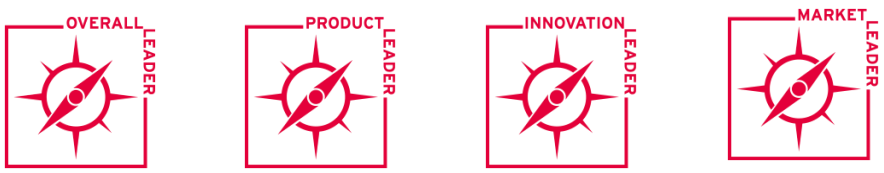
Strengths

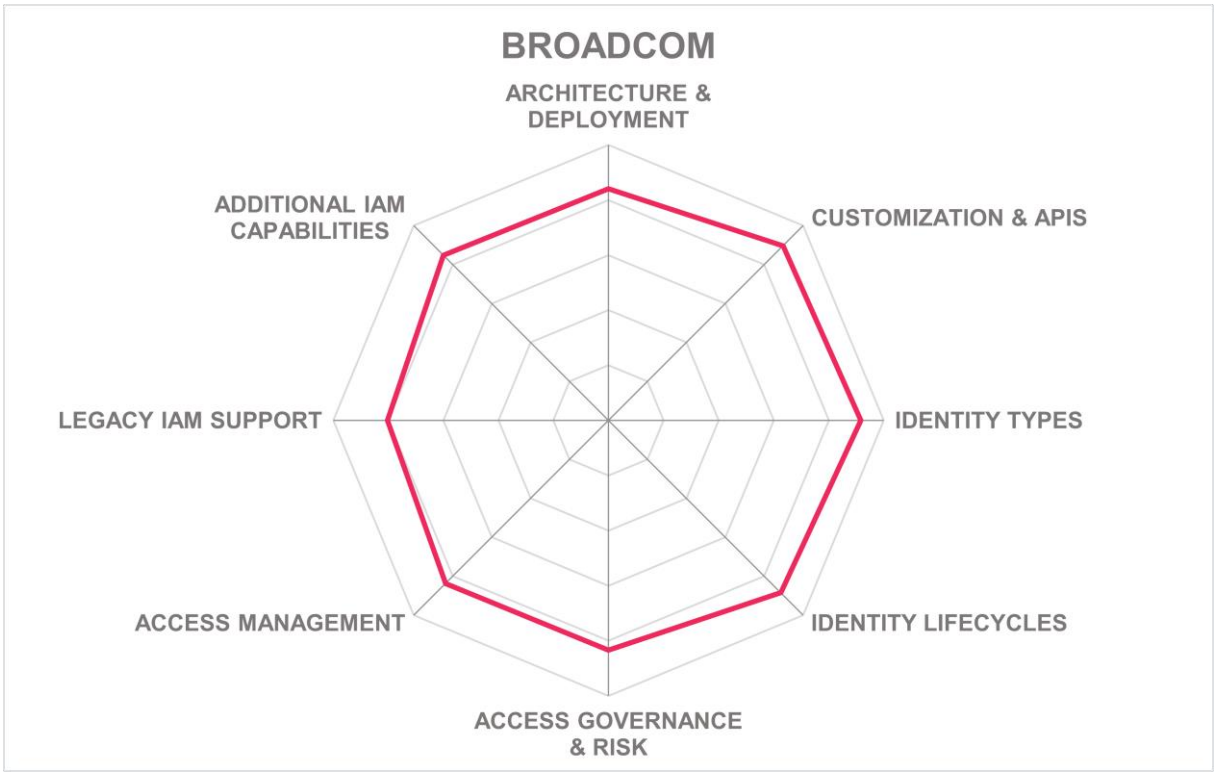
- Proven set of solutions bundled and integrated into a common service
- Solution set following an API-first approach, being multi-tenant and architected as microservices
- Broad range of managed service offerings
- Comprehensive set of capabilities comprising IGA, Access Management, and PAM
- Strong and proven capabilities across all major areas of IAM
- Global ecosystem and ability to scale for large enterprise deployments
- Support for delivering to complex, custom use cases
- 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
- Backed by a range of heterogeneous products with different origin

Leader in




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

Cloudentity – Cloudentity

Cloudentity became acquired by SecureAuth just ahead of the publication of this Leadership Compass. The combined capabilities are not yet reflected in the rating. They are one of the vendors in the market that focuses on orchestration and interoperability for delivering CIAM (Consumer IAM) services. The company's focus is on managing user and machine identities, while controlling authorization at the API/service level. This makes them an interesting vendor for future Identity Fabrics, specifically when integrating either existing IAM products or custom IAM-related services. Cloudentity delivers strong access management capabilities, provides a modern architecture, and provides full control about APIs and their authorization, including user consent. Their main priority is B2C and B2B use cases and the areas of data sharing between different parties. 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 (Function as a Service), 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 (PDP) and API Security solution named MicroPerimeter. It also supports Open Policy Agent (OPA) as an emerging standard approach in authorization management.

The second part of the product we analyzed is Cloudentity Identity Plane. This solution centers on aggregation of identity data from a broad range of sources (such as IdPs, IGA solutions, risk engines, and entitlement stores) to build out the user profile. It provides capabilities such as lightweight user registration, MFA, SSO and Bring Your Own Device (BYOD) support, and delegated administration. While the 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.

Cloudentity scores well in some areas in our Identity Fabrics evaluation. While there are gaps when it comes to supporting legacy IAM and IGA, Cloudentity's goal 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 still has a relatively small but growing global partner ecosystem, including strong regional partners in all major geographies. Cloudentity is innovative and provides a modern solution that scales well and fits to the architecture requirements of a modern Identity Fabric and can serve as a functional extension to other vendor's solutions.

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

Table 5: Cloudentity's rating

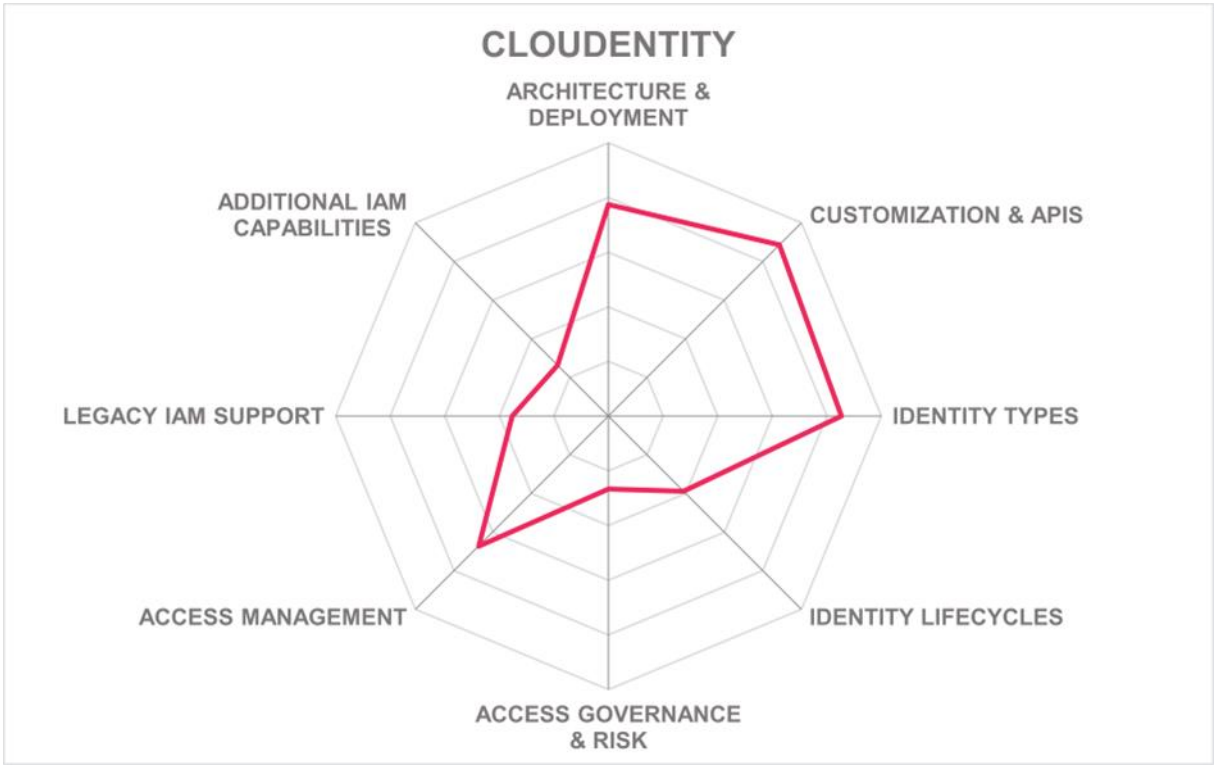
Strengths

- 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, and business units
- Supports authorizing data access in data sharing between different parties
- Adds data lineage for identity data
- Integrates with consent management solutions

Challenges

- Limited capabilities in IGA, specifically Access Governance
- No comprehensive coverage of B2E related IAM use cases
- 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



CyberArk – Identity Security Platform

CyberArk is primarily known as a leading PAM vendor, and in recent years have but recently broadened their product portfolio. With the acquisition of Idaptive in 2020, CyberArk added solutions for access management and Identity Lifecycle Management as well as automation and orchestration capabilities. These complement the strong PAM features, including Endpoint Privilege Security.

CyberArk has modernized its architecture as part of their journey towards the cloud. The Identity Security Platform can be deployed in a range of models from self-hosted deployments to SaaS / IDaaS deployments. It builds on a set of shared services such as the unified administrator portal, a common workflow engine, a unified authentication and authorization layer, unified logging, auditing, and analytics.

CyberArk's focus is on access management, access authorization, and privileged access for workforce and customers. IGA capabilities are currently limited. While there are options for adding users and assigning roles, the focus is on providing users with seamless access, not on managing role models, access requests & approval workflows, or access certification.

The platform consists of six modules. Workforce Access and Customer Access provides access management capabilities, including support for MFA. Endpoint Privilege Security adds PAM support for endpoints. Privileged Access Management is the PAM module, backed by the extensive set of PAM features CyberArk provides. Secrets Management is backed by the Conjur product for managing secrets and supporting in securing the DevOps tools chain. Cloud Security adds additional capabilities for securing cloud environments and managing cloud entitlements, thus fulfilling CIEM requirements. Finally, Identity Management adds features such as identity flows for no-code workflows and baseline identity lifecycle management.

For the areas of PAM and Access Management, the CyberArk Identity Security Platform provides leading-edge capabilities. These are backed by the shared services, including Identity Security Intelligence for spotting anomalies, and audit capabilities.

Overall, the CyberArk Identity Security Platform is a strong solution if the focus is on Zero Trust and securing access of all types of users, including privileged access. For IGA capabilities, specifically when it comes to supporting legacy and on-premises applications, customers may need to complement the platform with third party solutions.

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

Table 6: CyberArk's rating

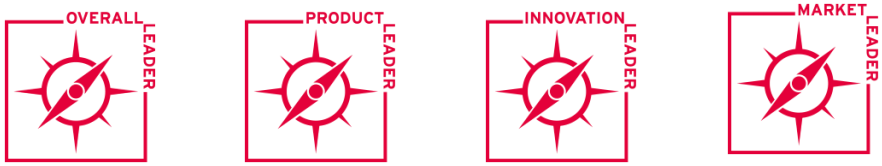
Strengths

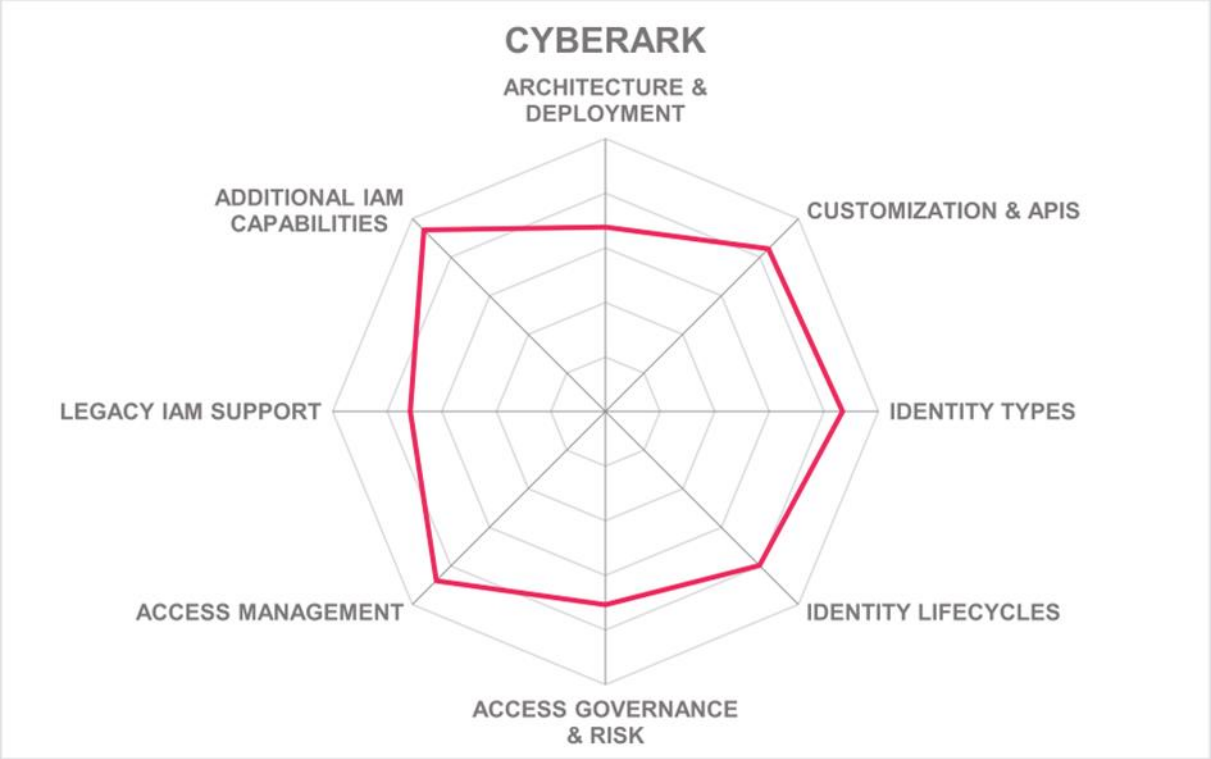
- Integrated platform, cloud-ready and offers flexible deployment options
- Shared service approach for analytics, auditing, and administration
- Good support for both workforce and consumer use cases
- Leading-edge PAM capabilities
- Adds Endpoint Privilege Management and CIEM as options
- Various options for secure remote access
- Good Access Management capabilities
- MFA support
- Advanced password management capabilities

Challenges

- Limited IGA capabilities for workforce
- No comprehensive support for role management and recertification
- Integrated, but relying on several products with different origin; administrative UI has become unified

Leader in




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

EmpowerID – EmpowerID

EmpowerID, by delivering an integrated platform for IAM that consists of a set of modules that can be flexibly licensed, is one of the few vendors in the market that provides a comprehensive, integrated solution for all areas of IAM. While the company focuses on IGA, their solution also covers access management and PAM. It also integrates well with Microsoft Entra ID, utilizing the Access Management capabilities and extending the IGA and other services.

EmpowerID provides leading-edge IGA features, including strong workflow capabilities and well-thought-out integration capabilities for modern SaaS services based on a unified Simple Cloud Identity Management (SCIM) connector that is easy to adapt for different SaaS services. While there are connectors to a wide range of platforms, customization of the connectors for target systems with customizations can require coding.

From an architecture perspective, EmpowerID benefits from its approach for providing an integrated solution. All modules within the solution except the low-code workflow engine have been modernized over the past few years and meet the requirements for a modern, microservices-based architecture. The workflow engine is still based on Microsoft .NET 4.x, with a new, fully modernized release anticipated to be released in 2024. Additionally, EmpowerID comes with a consistent set of APIs that allow for efficient and proven customization and orchestration. The solution also provides a feature-rich integration with ServiceNow.

EmpowerID also increasingly leverages bots and AI capabilities for augmenting users. Other areas of innovation include the use of managed OPA for replacing legacy authorization systems.

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 several regions.

EmpowerID, despite still being a relatively small vendor, has demonstrated its ability to serve customers in different geographies and at a variety of scales. 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	Strong Positive
Functionality	Strong Positive
Deployment	strong positive
Interoperability	strong positive
Usability	Strong Positive

Table 7: EmpowerID's rating

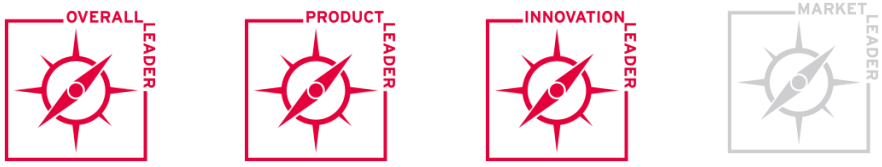
Strengths

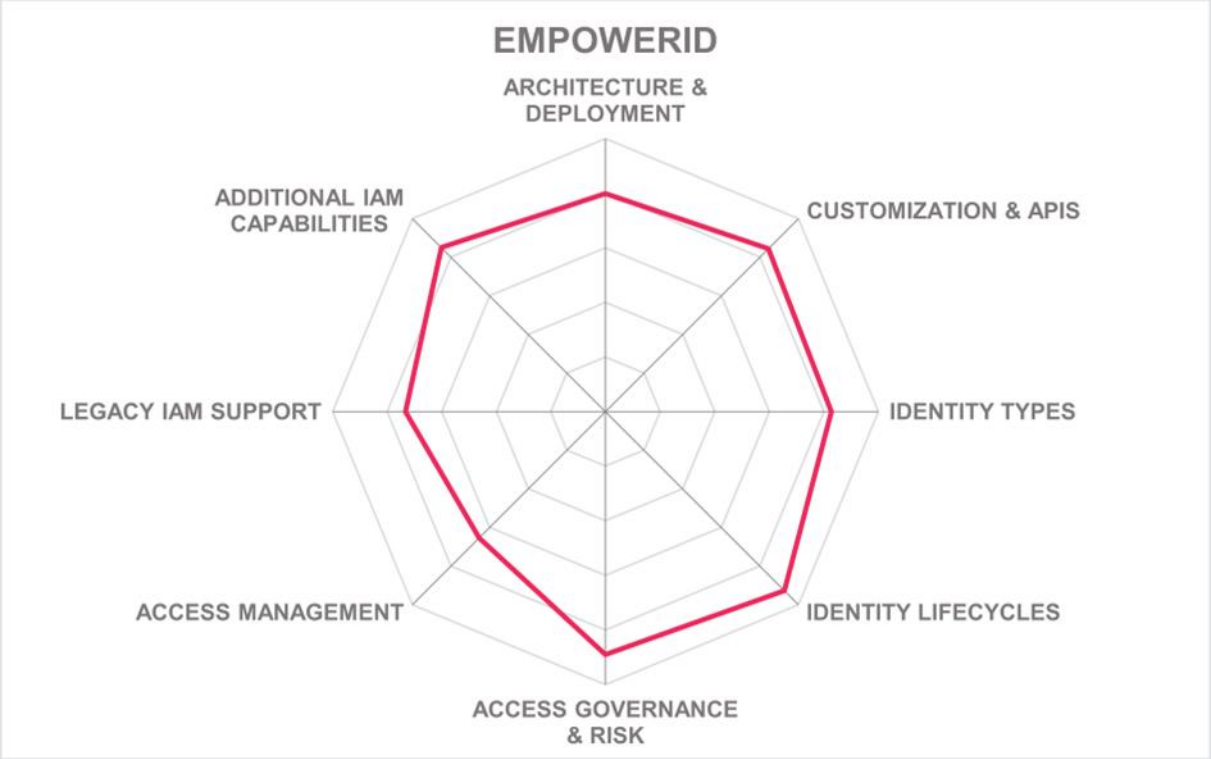
- Integrated suite, covering all major areas of IAM, including baseline PAM
- Good breadth and depth of features, specifically for IGA and access management
- Integrates neatly with Microsoft Entra ID for access management
- Various innovative features, such as for connecting to SaaS services
- Supporting bots and utilizing AI for augmenting users
- Broad set of APIs for flexible customization and orchestration with other services
- Built-in integration with ServiceNow
- Modern architecture (except workflow module, which is a roadmap item)
- 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 small but growing, including some global consultancies
- Workflow module still awaiting modernization
- Customization of connectors sometimes requires coding

Leader in




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

Exostar – Exostar Platform

Exostar was founded in 2000. Its headquarters are in Herndon, Virginia, USA with additional development centers in the UK and Bengaluru, India. Exostar significantly expanded its portfolio through the acquisition of Pirean in 2018. Exostar is a leader in secure, compliant cloud-based solutions that improve collaboration, information sharing, and supply chain management for hundreds of thousands of organizations in 175 countries. Exostar focuses on supporting trusted collaboration across communities in highly regulated industries such as defense, aerospace, life sciences, healthcare, energy, telecommunications, and financial services. It focuses on providing specialized solutions tailored to specific industries rather than attempting to cater to a broad variety of customers. Coverage includes North America, Europe, Latin America, and the APAC region.

Within the Exostar Platform, the Access: One product offers an IAM platform that can be delivered as a service or deployed on-premises. It prioritizes security, time to value, and flexibility, providing a range of packaged services for both consumer and enterprise access management. Additionally, it allows easy creation and publication of custom IAM services and user journeys using a no-code workflow builder and secure plugin integration service. Access: One stands out by targeting highly regulated markets and adhering to the latest security standards, including OpenID Connect, OAuth, Financial Grade API, Consumer Data Rights, NIST-800-63-B, FIDO 2, and WebAuthn.

Key features include user journey orchestration through a graphical workflow builder, seamless integration with third party interfaces via the plugin architecture, pre-built services for various enterprise and consumer use cases, versatile API access management capabilities, and the ability to create custom IAM APIs using Access: One's workflow and plugin interfaces.

Exostar can onboard organizations and individuals very rapidly, delivering a connect-once, single sign-on, passwordless authentication experience for application owners and internal/external app users. However, the company's focus is on consumers and partners, with somewhat limited capabilities when it comes to workforce IGA features.

Exostar provides innovative identity proofing capabilities and validation services for high-assurance environments, supports PKI and two-factor authentication services such as one-time passwords (OTP), mobile-based push authentication, smartcards, and other forms of enterprise identity. Moreover, Exostar is a Certification Authority and has been named a full-service credential service provider by the Kantara Initiative. Exostar also supports JWT, Kerberos, OAuth2, OIDC, and SAML tokens/protocols. The platform provides full FIDO2 support, including support for passkeys and Windows Hello. In addition, the Access: One Mobile Identity provides secure and convenient access to digital resources and applications using mobile devices. Users can authenticate themselves, conduct transaction signing, perform self-service password resets, and more.

Exostar is different from other vendors by being focused on highly regulated industries. Exostar and its identity proofing, passwordless, and credentialing capabilities provide a good

alternative for customers in complex and highly regulated industries. Exostar appears in the Product, Innovation, and Overall leadership categories.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	strong positive
Usability	Strong Positive

Table 8: Exostar's rating

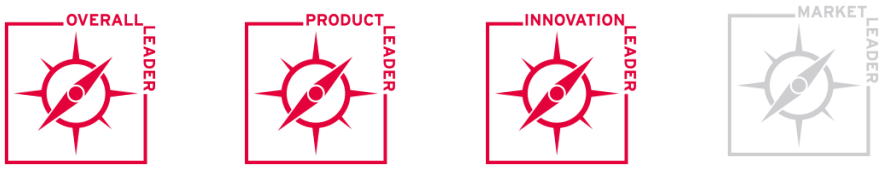
Strengths

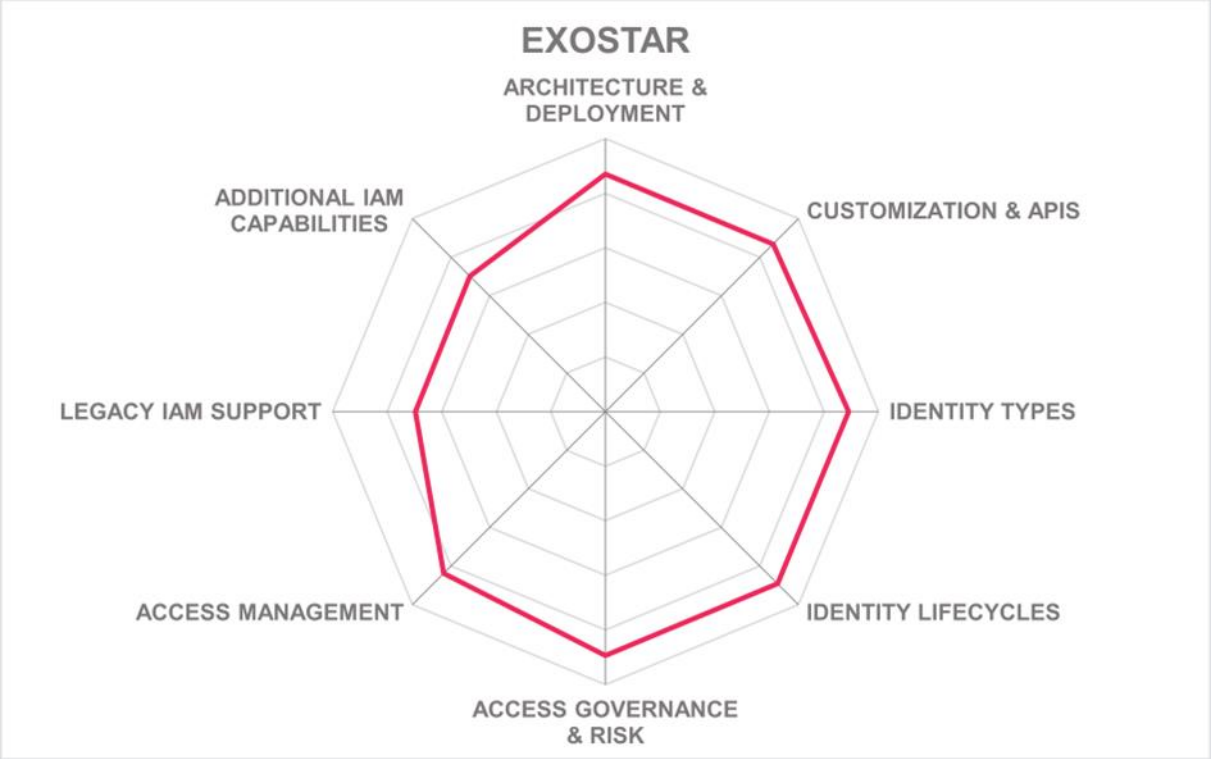
- FIDO 2 support
- Strong partner ecosystem and global presence
- Certified compliance with multiple standards
- Breadth of authentication options
- Flexible deployment models
- Strong identity proofing capabilities
- Good federation, SSO, and session management
- Extensive experience and well-established vendor in highly sensitive industries
- Strong API support and modern architecture

Challenges

- Limited support for IGA, such as role management and recertification
- Remote access is currently not supported
- Lack of analytics and access intelligence capabilities
- Limited visibility in the market

Leader in




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

IBM – Security Verify

In recent years, IBM has developed a modern IAM solution that is provided as a service and while continuing to be available in other deployment models. As well as being a cloud provider IBM is also a leading system integrator, so they can support a variety of options for their customers. IBM Security Verify is the solution formerly named IBM Security Cloud Identity and integrate with the on-premises IAM products provided by IBM.

From a feature perspective, IBM Security Verify is one of the most comprehensive solutions on the market. The breadth of the company's solution makes it a leading candidate as the foundation of an Identity Fabric. IBM Security Verify supports Access Management, IGA, and—via their OEM relationship with Thycotic—also PAM capabilities. IBM has vast experience in connecting legacy applications. Together with the strong SaaS support of IBM Security Verify, this provides excellent support for complex, hybrid IT environments.

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). This allows existing customers to migrate stepwise. The set of components which 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 with other IBM services such as IBM QRadar. Identity Threat Detection Response (ITDR) is a roadmap item as native capability. As well as having a strong global partner ecosystem, IBM can also deploy and operate the solution based on its own services, meaning that the company does not need to rely on other IaaS providers for a SaaS-style deployment of the solution.

With the noteworthy progress 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. IBM is also working on adding an orchestration platform for connecting various identity services, beyond the already available IBM Application Gateway. Their typical customers are organizations with a broad range of hybrid IT solutions in place and / or requiring support for custom use cases that can be implemented by IBM and its partners.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	strong positive

Table 9: IBM's rating

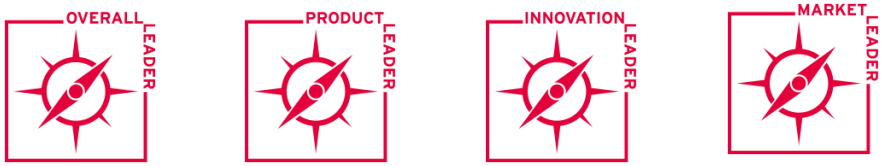
Strengths

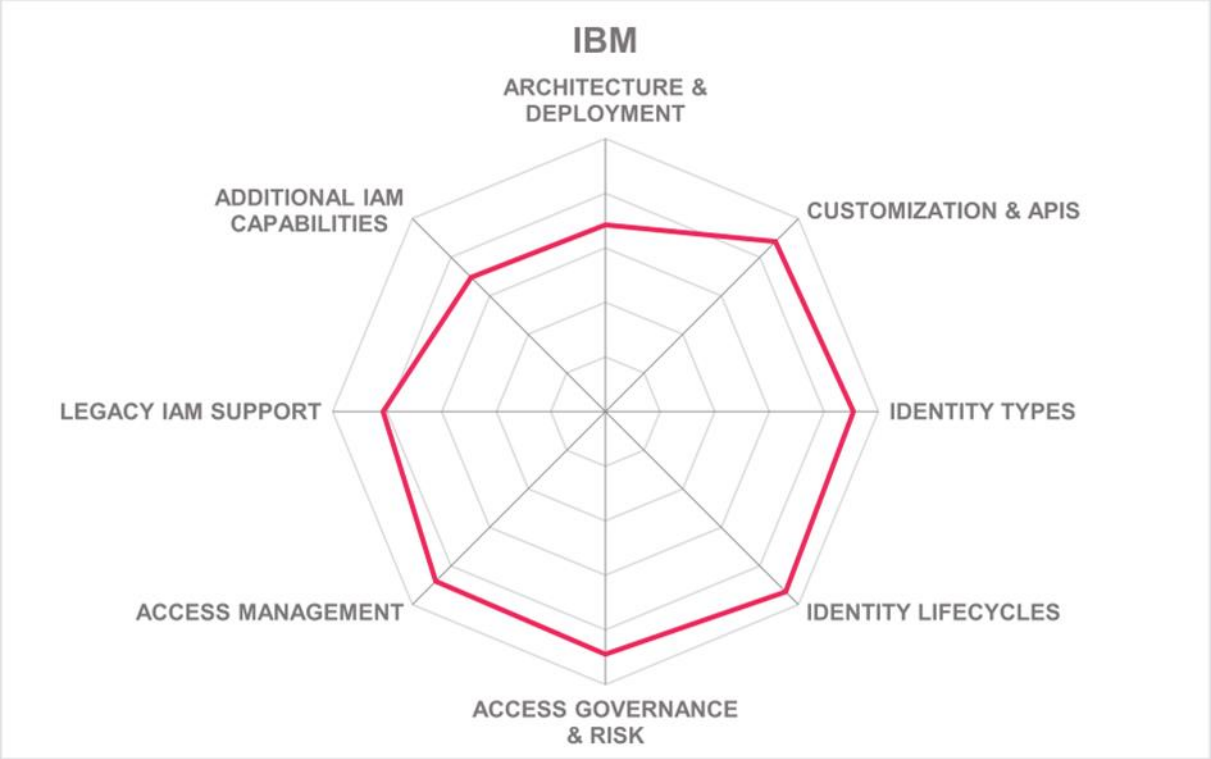
- Very broad set of capabilities across access management, IGA, and PAM
- Modern architecture, developed as cloud-native solution
- Own cloud services and professional services
- Strong legacy support, both directly and via integration to Verify Governance (previously ISIGI) and Verify Access (previously ISAM)
- IBM Application Gateway for connecting to non-IBM IdPs
- Integrates with a range of other IBM offerings such as IBM QRadar
- Strong global partner ecosystem
- Proven scalability
- Well thought-out roadmap

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
ADDITIONAL IAM CAPABILITIES

Microsoft – Entra ID

Microsoft Entra ID, formerly known as Azure Active Directory (Azure AD), has evolved over the years from a cloud directory and access management solution for the Microsoft environment to a comprehensive IAM solution, providing a broad set of capabilities, including IGA, PAM, and CIEM—the latter through their acquisition of CloudKnox Security. This makes Microsoft a leading provider of a platform on which to build a modern Identity Fabric.

Microsoft Entra ID, due to its mandatory use in Microsoft Azure and Microsoft 365, has achieved wide-spread deployment across organizations of all sizes. Many organizations have decided to use Entra ID 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, Entra ID counts amongst the leading-edge solutions. It provides excellent support for modern, cloud-based, and standards-based (including OAuth and OIDC) applications, but also has added a proficient level of support for downstream applications which do not support modern standards.

In IGA, Entra ID comes with a good set of capabilities and also supports features such as Role Based Access Control (RBAC) 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 baseline and benefit from innovative features such as recommendations for access recertification. However, provisioning capabilities to legacy applications are still only at baseline, particularly regarding breadth and depth of specialized connectors. For PAM, the capabilities are at a baseline level, but well-integrated with the security analytics capabilities of Entra ID 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.

Microsoft Entra ID comes with excellent API support for a wide range of capabilities. Automation via PowerShell can be integrated with CI/CD tools such as Chef for controlled lifecycles of scripts. The UI is modern and mostly integrated, except for Microsoft Entra Permissions Management. Microsoft has a series of additional solutions in security, data governance, and privacy management which complement Entra ID. They also provide support for decentralized identities.

Microsoft has evolved to a leading player in the IAM space with the evolution of Entra ID, 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	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 10: Microsoft's rating

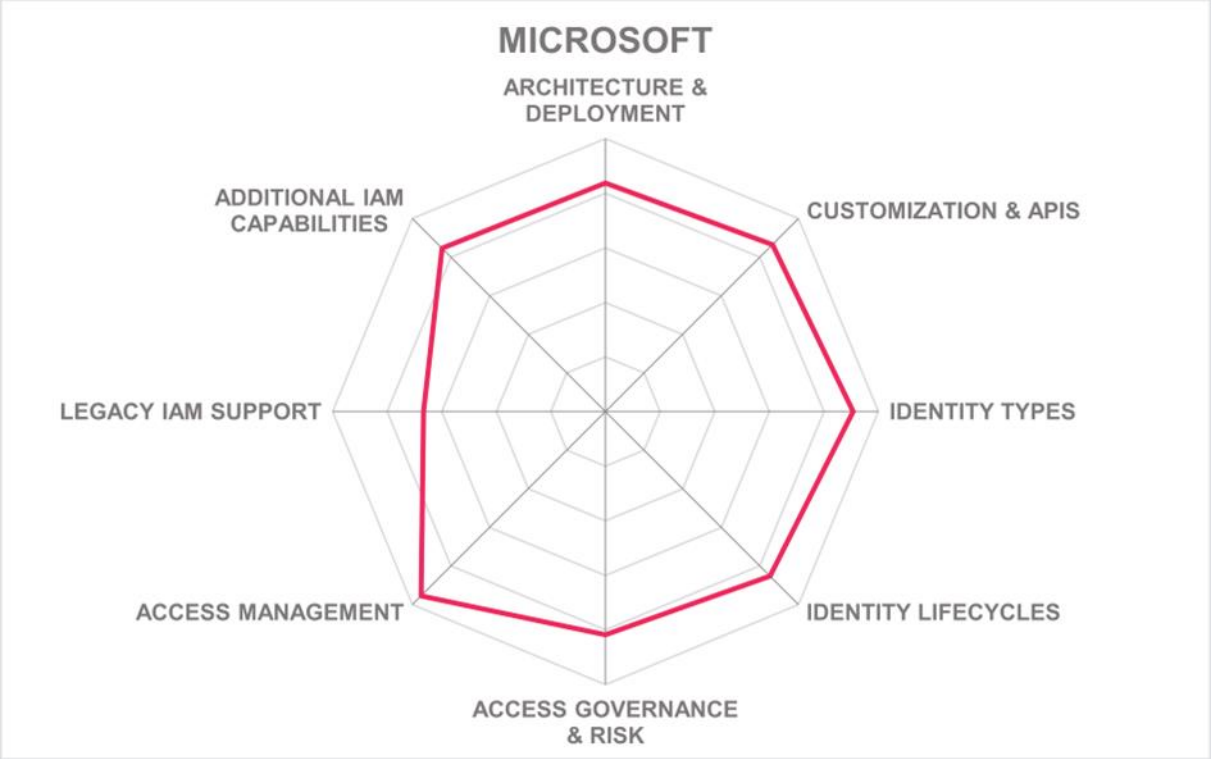
Strengths

- 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 that supports 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 Microsoft Entra ID and Microsoft 365 ecosystem
- Integrated support for decentralized identities
- Good support for IGA use cases

Challenges

- Only available as multi-tenant, public cloud service
- Permissions Management (CIEM) not yet fully integrated into the administrative UI (user interface)
- Only baseline PAM support

Leader in


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

One Identity – One Identity Manager, OneLogin, Safeguard

One Identity, a Quest company, is an established IAM vendor. While their focus had been on IGA, PAM, and Active Directory Management in the past, they have emerged as a full-suite IAM vendor with the acquisition of OneLogin in October 2021. One Identity is one of the few vendors in the market that covers all major areas (IGA, Access Management, PAM) of IAM with their own solutions. Additionally, One Identity is investing heavily in modernizing and integrating the IGA and PAM portfolio, providing these solutions as SaaS offerings, such as the already available One Identity Manager on Demand and One Identity Safeguard On Demand, as well as providing IGA and PAM capabilities as optional modules within OneLogin.

In the field of IGA, One Identity Manager is an established solution with a large customer base. Over recent years, One Identity has invested in modernizing their solution architecture and providing it as a SaaS 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 has also 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 SaaS, with Safeguard on Demand. The solution is feature-rich and covers a variety of PAM use cases, including Endpoint Privilege Management.

As 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 completed, but are on their way and showing strong potential. However, the One Identity Unified Security Platform is moving closer to unification and is—taking the overall feature set—among 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 on which to build the future Identity Fabric.

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

Table 11: One Identity's rating

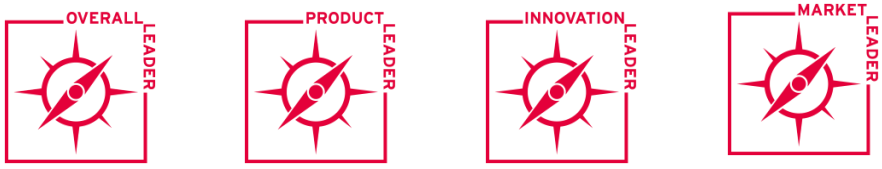
Strengths

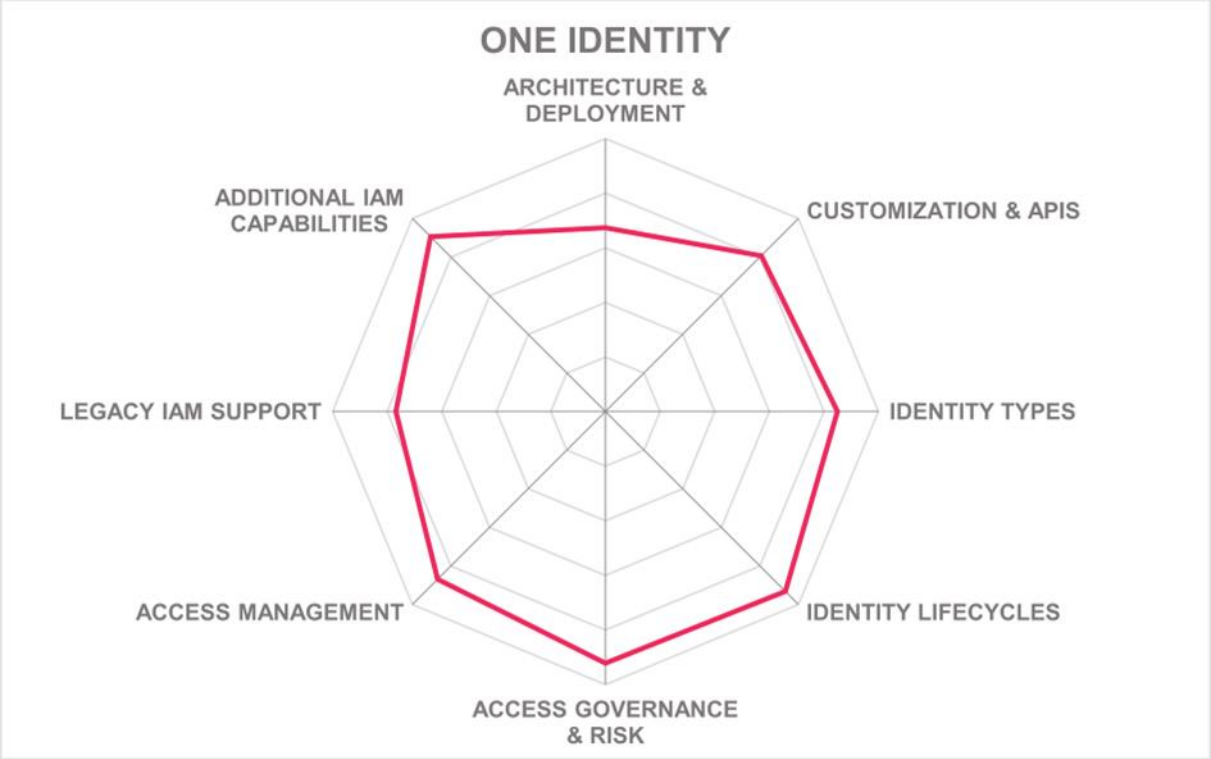
- One of the few vendors with broad and in-depth coverage of IGA, Access Management, and PAM use cases
- Leading-edge IGA capabilities, based on long experience
- Strong support for managing access in SAP environments
- Leading-edge access management capabilities through OneLogin acquisition
- Support for Access Management for both workforce and customer use cases
- Strong PAM capabilities also available as IDaaS
- Defined roadmap for further evolution and integration of the platform with IDaaS focus
- Broad support for non-human identities, including RPA
- Syslog-ng adds logging and analytics capabilities across heterogeneous systems
- Strong global partner ecosystem

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
- Most capabilities available as IDaaS, some still on roadmap for modernization and integration
- Mix of different licensing models

Leader in




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

OpenIAM – OpenIAM

OpenIAM is one of several open source IAM solutions available. The company is headquartered in the U.S. and has been active since 2008. Today's OpenIAM platform has been constructed from the ground up, building on a modern microservices architecture, supporting container-based deployments. It supports both IGA and Access Management capabilities, which are complemented by baseline PAM features.

User lifecycle management, using one or more authoritative sources for automated, role-and-rule-based provisioning and deprovisioning, as well as supporting reconciliation and management of orphaned accounts, is one of the key capabilities. As a PAM-related feature, service accounts and administrative accounts can also be put under management.

OpenIAM also supports approval workflows including support for enforcing Service Level Agreements (SLAs) and triggering escalations. Requests can be requested using a shopping cart approach, building on a service catalog, and can be fully tracked as well. Access certification and SoD controls are also supported. Another important feature is the built-in contractor management.

Access management capabilities of OpenIAM are reasonably featured, providing integrated features—including MFA and FIDO2 —and the ability to integrate with IdP solutions such as Microsoft Entra ID and Okta.

OpenIAM has started to add support for eID approaches, currently supporting first eIDs from Europe, with support for other approaches including support for the EUDI wallet (EU Digital Identity) on the roadmap.

The set of connectors provided by OpenIAM is good, and also covers several line-of-business (LoB) applications including SAP and Oracle. OpenIAM also provides SCIM support and pre-defined integrations to a range of SaaS services.

OpenIAM provides strong API support, following an API-first approach and supporting integration into DevOps processes. The user interface has been modernized, based on the comprehensive APIs exposed by the OpenIAM platform.

Overall, OpenIAM has matured significantly and benefits from the integrated and modernized approach, providing an interesting alternative in the IAM market, specifically for organizations looking for an open-source solution in IAM or the ones focusing on platforms following an API-first approach.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Positive
Usability	Positive

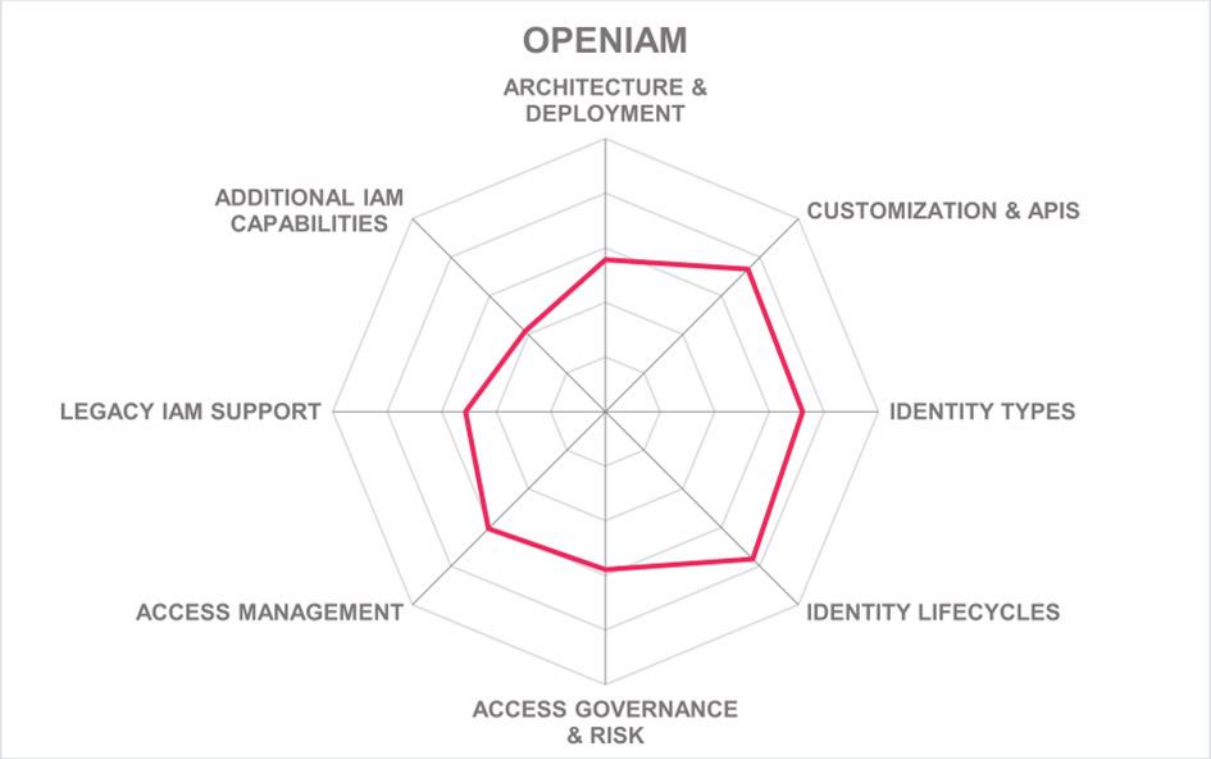
Table 12: OpenIAM's rating

Strengths

- Open source based IAM solution
- Coverage of Access Management, IGA, and baseline PAM support in an integrated platform
- IGA includes the ability to identify and resolve orphaned accounts
- SLAs and escalations supported for approval flows
- Access request management backed by service catalog and shopping cart approach
- FIDO2 support in Access Management
- Integration to Microsoft Entra ID and Okta support included
- Good set of connectors, SCIM support

Challenges

- Relatively small vendor with limited visibility in the market
- Acceptable partner network, but potential to grow
- PAM capabilities only being baseline, focused on managing privileged identities
- No full IDaaS offering available, but flexible deployment models


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

OpenText – Various Products

OpenText, with their acquisitions of major parts of Micro Focus, specifically the former NetIQ assets, has expanded its cybersecurity significantly, specifically with respect to IAM. NetIQ by OpenText is the brand used within the OpenText Cybersecurity group. Like other established IAM vendors, OpenText is in the process of merging their NetIQ IAM portfolio, building on, and modernizing proven capabilities, as well as providing additional IDaaS capabilities.

Based on the NetIQ portfolio, the functional coverage of the solution is very broad, spanning all core areas of IAM including IGA, Access Management, and PAM, and also providing other capabilities such as Data Access Governance and Privacy/Consent Management. With these capabilities, both workforce (including B2B/partner access) and consumer use cases are supported. The solutions build on a set of foundational, shared services for managing identities (directory services) and resources, for auditing, logging, and analytics, for self-service capabilities, and for risk management across all components. Also, the Cloud Bridge features that support hybrid deployments are part of the common, foundational layer.

The solution comes with its own Secure API Manager that helps in exposing the APIs of the various solution components in a well-managed and well-secured manager. The solution covers functions such as topology hiding, API authentication and API authorization, on top of auditing and analytics. It supports modern REST, traditional SOAP, and legacy APIs.

OpenText supports a range of deployment options, including OpenText single-tenant managed services, OpenText multi-tenant SaaS Services, and deployments on-premises and in VPCs (Virtual Private Clouds). Components running in different deployment models can be connected using Cloud Bridge. This allows for efficient delivery of IAM in complex hybrid environments consisting of legacy applications as well as modern SaaS services.

The platform itself comes with a wide range of capabilities from access management and adaptive authentication, including Privacy & Consent Management, to IGA, Directory Services, and PAM features. While building on proven capabilities, OpenText has evolved significantly regarding the underlying architecture, while not having everything modernized regarding architecture and user interfaces.

Beyond the continuous improvement of the platform components, OpenText has added a range of new features. These include telemetry for deployment on public clouds, continuous governance and improved SoD management, deployment based on Docker containers and Terragrunt scripts, and integration of identity assurance and identity verification services with integration to national digital ID infrastructures.

On the SaaS side, beyond the managed service delivery, the components are increasingly added to the OpenText cloud environments, adding to the flexibility in deployment. With the recent developments in the past year, OpenText NetIQ is demonstrating that they continue their modernization journey while utilizing their powerful capabilities built over the past decades.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	strong positive

Table 13: OpenText's rating

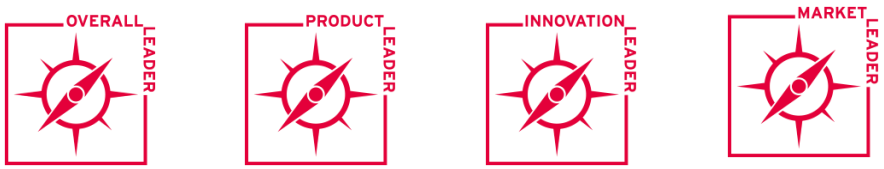
Strengths

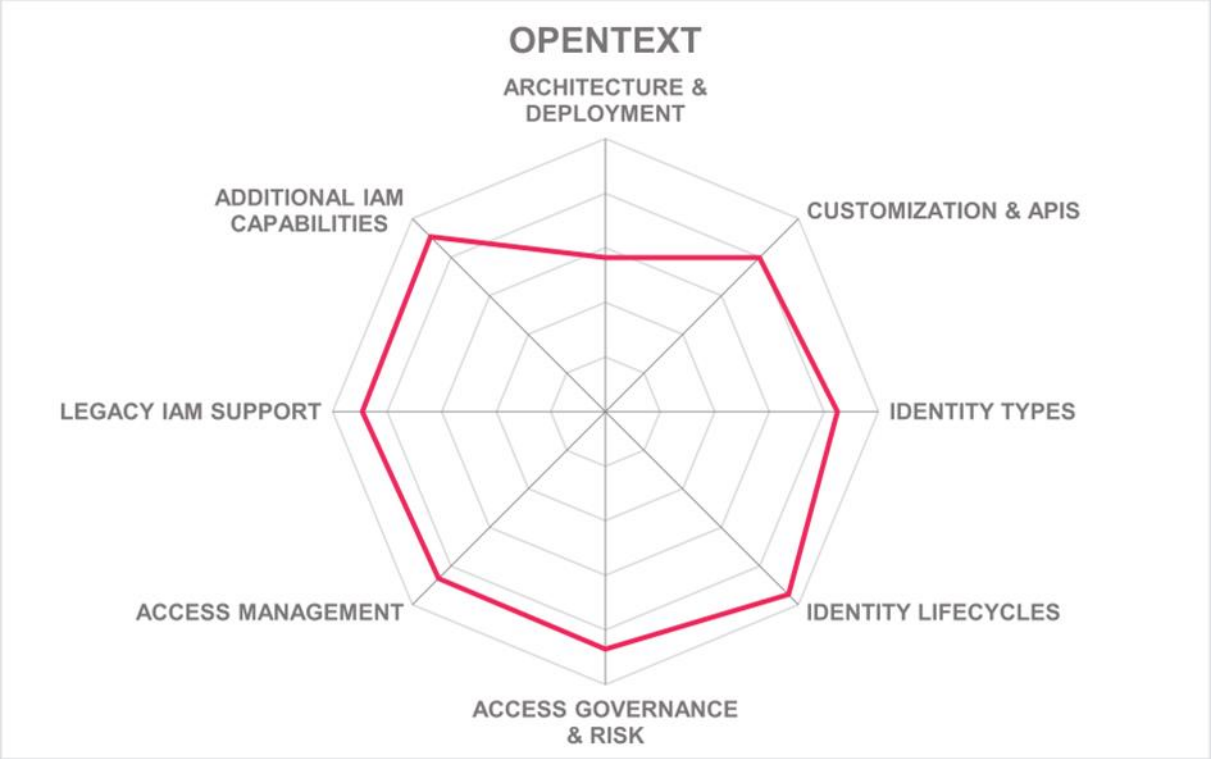
- Proven solutions covering the major areas of IAM
- Excellent connectivity to a wide range of target systems
- Strong API management and security capabilities
- Flexible deployment options, increasingly offering services as part of the OpenText cloud
- Support for automated deployment and updates based on containers and scripts
- Improved Access Governance and SoD management capabilities
- Integrates with identity verification services of national digital ID infrastructures
- Common, foundational services
- Strong global partner ecosystem
- Data Governance module provided

Challenges

- Various components required for building a comprehensive Identity Fabric
- Several of the modules are not yet fully modernized
- Deployment and operations require careful planning due to mix of solutions and some legacy modules

Leader in




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

Optimal IdM – The OptimalCloud

Established in 2005, Optimal IdM is headquartered in the U.S, with offices in the U.S. and Australia. Optimal IdM offers the OptimalCloud as its primary IDaaS service providing SSO, MFA, and federation functions. The OptimalCloud is a multiple and single-tenant SaaS delivery offering a fully managed service that provides the hosting as well as all 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 with some IGA support including SCIM support for connecting to target systems and access certification.

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 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 via SCIM from LDAP and to/from cloud services. OptimalCloud provides federated SSO capabilities. The product maintains a catalog with an extensive list of pre-integrated federated applications for SSO 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. The UI follows industry standards and is easy to use.

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. There is support for managing license for Microsoft Entra ID and Microsoft 365. Workflow capabilities are very limited, as is 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, from the overall Identity Fabrics perspective, it is more an add-on to other solutions with a stronger IGA and PAM focus.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Positive
Usability	Positive

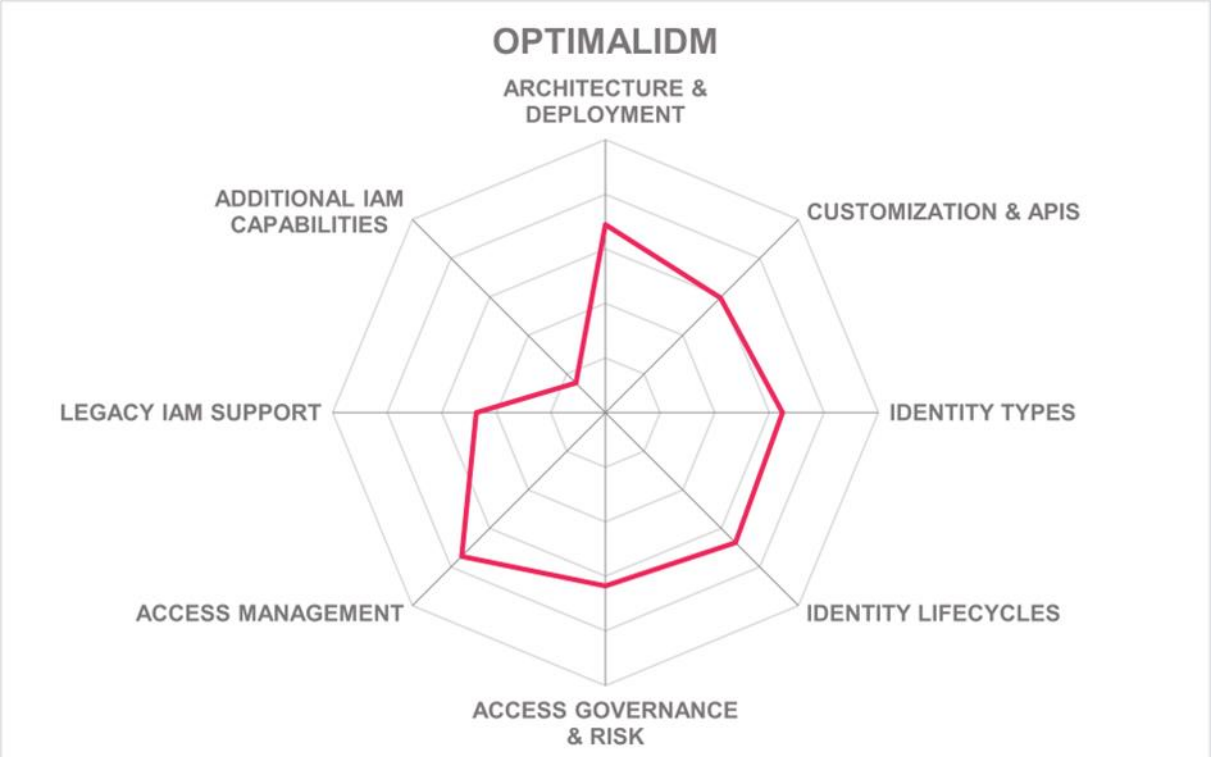
Table 14: Optimal IDM's rating

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
- License management for Microsoft Entra ID and Microsoft 365

Challenges

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



Oracle – OCI IAM

Oracle has been in the IAM market for decades. With Oracle Cloud Infrastructure Identity Access Management (OCI IAM), Oracle delivers a modern IDaaS solution to the market. The Oracle Cloud Identity Fabric is a cloud-native, integrated platform that can be integrated with Oracle's on-premises IAM portfolio. As the first element of their IDaaS solution portfolio, Oracle had released an Access Management solution, followed by the cloud-native Access Governance Cloud Service. They now provide a comprehensive, integrated IDaaS platform covering both Access Management and IGA.

OCI IAM provides the IAM backbone for OCI (Oracle Cloud Infrastructure) and the Oracle Cloud Applications, it can also serve heterogeneous cloud and application environments. The prior focus on the Oracle ecosystem has been changed towards delivering a comprehensive platform for an entire IT ecosystem.

Regarding Access Management, OCI IAM 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 access in multi-cloud environments.

For IGA, the solution now can utilize either the new cloud-native Access Governance service or continue to build on the Oracle enterprise IAM suite and Oracle Identity Governance (OIG). Oracle will continue to support their own 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. Also, Oracle continues to innovate these solutions, including offering them as cloud-hosted solutions.

Oracle is back in the IAM market as a contender with OGI IAM and Access Governance 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 large-scale environments, and strong legacy support wherever required. While the main focus of Oracle is on their enterprise customer base, the solutions are also of interest to customers that need to deliver IAM for heterogeneous and hybrid environments.

Security	Strong Positive
Functionality	Strong Positive
Deployment	strong positive
Interoperability	Strong Positive
Usability	strong positive

Table 15: Oracle's rating

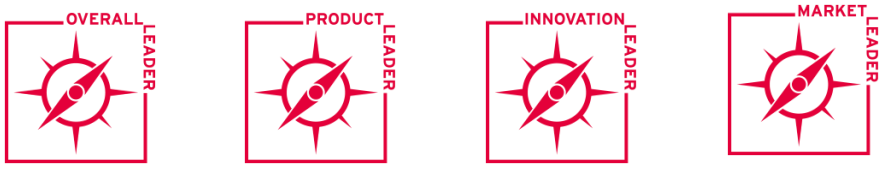
Strengths

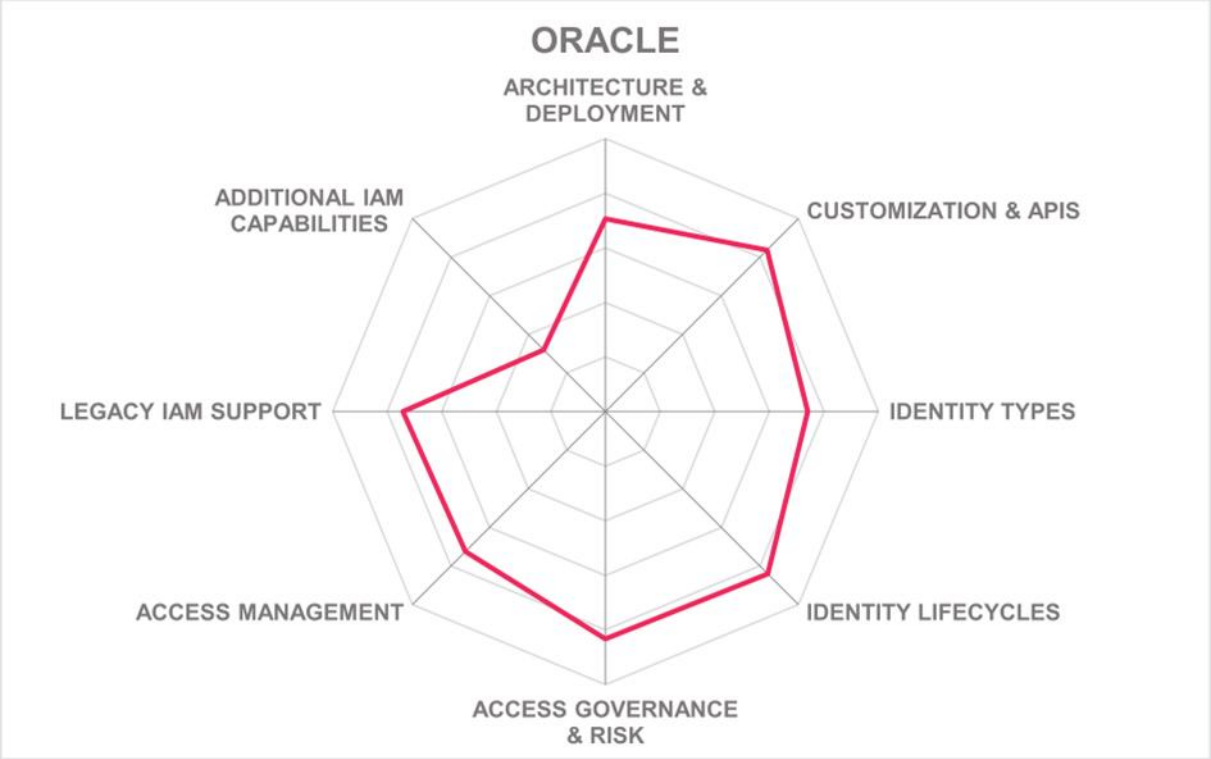
- Modern IDaaS solution for access management use cases
- Good IGA capabilities, also available as native cloud service
- Clearly defined strategy and roadmap, consequent execution on roadmap
- Strong support for OCI and Oracle Cloud applications, but also for third party environments
- Experienced vendor 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

- Depending on required features and integrations, other Oracle IAM solutions (on-premises or cloud-hosted) might be required
- No support for PAM use cases
- Strong but still evolving feature set
- Primarily focused on Oracle enterprise customers

Leader in




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

Ping Identity – PingOne Cloud Platform and ForgeRock

With the acquisition of Ping Identity and ForgeRock by Thoma Bravo and the recent merger of the two companies, two strong, established vendors in the IAM field are joining forces. Ping Identity has unveiled the first integrations and a roadmap for the further, quick evolution of a combined and integrated product portfolio.

The combination adds IGA capabilities to Ping Identity's leading-edge portfolio in access management. ForgeRock also has a strong access management portfolio. Additionally, Ping Identity over the years has acquired solutions for identity orchestration and supporting decentralized identity. Both portfolios contain directory services as well as API management and security features.

As with every combined portfolio and despite integration already having started, it will take time until a fully merged portfolio becomes available. However, the integrated Ping Identity has already made immediate progress in converging capabilities in the short term. The unified company will continue providing multi-tenant SaaS (PingOne) and dedicated SaaS (PingOne Advanced) and software solutions, providing customers with flexible deployment options. This involves some overlap in capabilities between dedicated SaaS offerings, but also offering customers a choice between the benefits of modular configuration (PingOne Advanced Services) or a customizable platform (PingOne Advanced Identity Cloud, formerly known as ForgeRock Identity Cloud).

For IGA, Ping Identity now provides strong identity lifecycle management for all types of identities, including machine identities, business partners, and consumers. Access Governance capabilities are good. However, ForgeRock brings strong Identity Analytics features based on AI/ML.

In regards Access Management and CIAM, both vendors already have strong offerings in place, supporting all common use cases in that area, including flexible authentication flows that can be configured graphically and excellent standards support. The support for legacy applications is excellent.

While offering several innovative capabilities such as API management and security, others such as PAM and CIEM are not provided by Ping Identity and require third party solutions.

Ping Identity is in a strong position in the market for Identity Fabrics with robust support for hybrid environments and being very feature rich. As integration is a process, customers must carefully analyze the state of integration for the capabilities they require. The Ping identity orchestration capabilities simplify deployments, including hybrid deployments.

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

Table 16: Ping Identity's rating

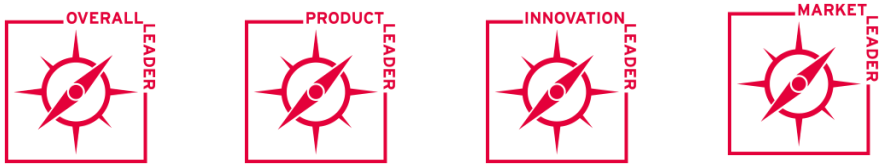
Strengths

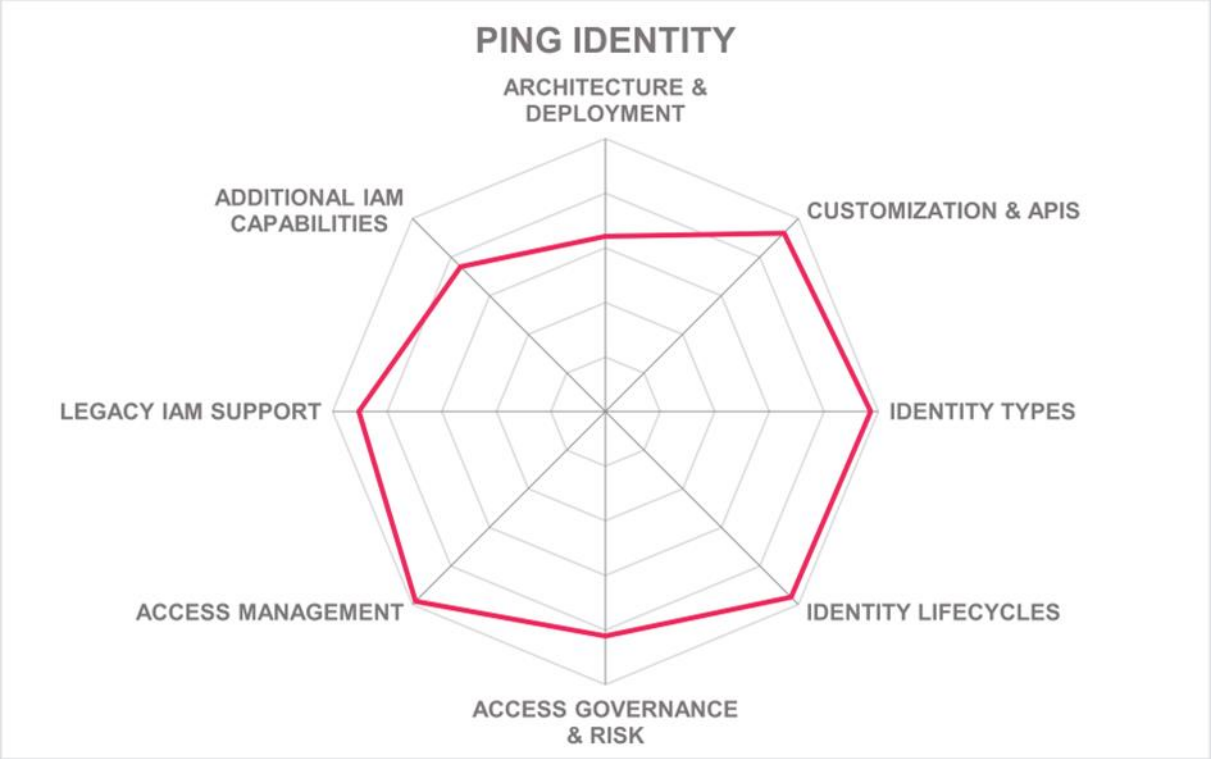
- Strong portfolio of solutions becomes combined
- Strong support for identity lifecycles across all identity types
- Excellent API support
- Good IGA capabilities
- Leading-edge capabilities in Access Management
- Strong identity orchestration platform
- Strong legacy support
- Support for decentralized identities
- Strong global partner network

Challenges

- Integration in progress, but not yet fully done
- Wide range of solution components requiring careful evaluation and planning

Leader in




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

RSA Security – Unified Identity Platform

In the last year, RSA Security has focused on bringing three product suites together – ID Plus, SecurID, and Governance & Lifecycle – via what they call the RSA Unified Identity Platform (UIP). The RSA UIP seeks to provide organizations with the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. A closer look at the three product suites reveals that RSA ID Plus provides identity and access management (IAM) capabilities across cloud, hybrid, and on-premises environments; RSA SecurID protects on-premises resources with secure access, authentication, and identity management capabilities; and RSA Governance & Lifecycle includes identity governance and administration (IGA) capabilities delivered via cloud, hybrid, and on-premises deployments.

With these changes, RSA now is focusing on enhancing its capabilities in the IDaaS space. While providing a good set of features, the solution is still in its transition from the well-established, on-premises solutions to a modern, feature-rich, and fully integrated platform for serving the needs of modern Identity Fabric architectures. While some expansions such as Risk AI for risk intelligence have been added, supporting ITDR, there are still several important features on the roadmap, including more support for identity proofing, a lightweight IGA approach, and additional dashboards.

The strongest part of the current solution 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 evolution of their Risk Engine, increased capabilities for anomaly detection and risk-based access controls are added.

RSA continues to support both on-premises and cloud deployments, giving customers options for deployment, depending on the types of applications that need to be supported, and the state of their 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 has significantly improved its user interfaces, adding capabilities such as broader self-service support and modern mobile apps. Workflow support in ID Plus has improved and now includes support for new secure enrollment workflows, such as support for third party ID verification. Additionally, the workflow engine within Governance & Lifecycle has been upgraded in the latest release. The solution comes with an integrated portal, including dashboarding and analytical capabilities. The support provided by RSA for on-premises applications is amongst the strongest available in the market.

Overall, RSA is still in the transition phase of converting their portfolio 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 an extremely broad set of integrations.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	strong positive
Usability	strong positive

Table 17: RSA Security's rating

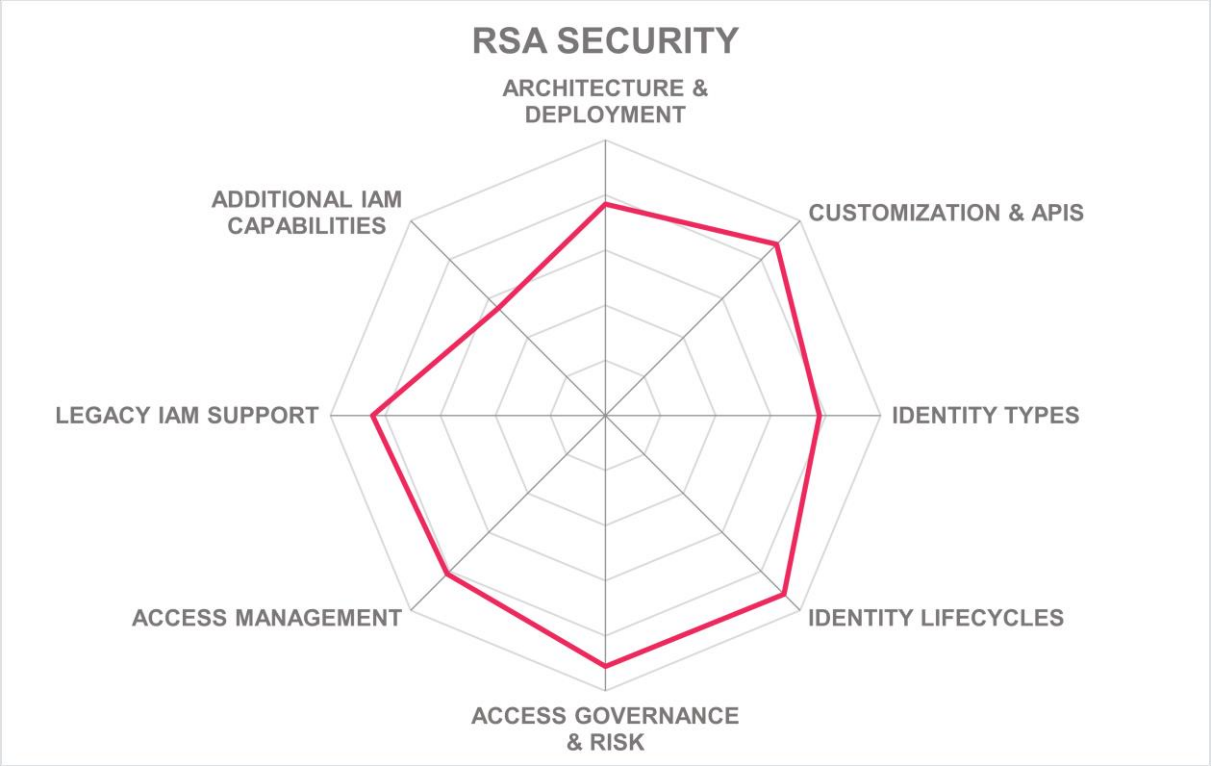
Strengths

- Leading-edge access management capabilities
- Strong support for a broad variety of authenticators
- Own strong authentication capabilities as part of RSA SecurID and RSA ID Plus
- Large number of certified out-of-the-box integrations for access management
- Good IGA support
- Flexible support for running on-premises or as IDaaS
- Well-defined roadmap and corporate focus on IAM again
- Large partner ecosystem at global scale

Challenges

- Still in the modernization from traditional IAM platforms to full IDaaS
- No native PAM support, but out-of-the-box integrations
- Deployment in hybrid mode and across products can involve some complexity

Leader in


RSA SECURITY
ARCHITECTURE & DEPLOYMENT
CUSTOMIZATION & APIS
IDENTITY TYPES
IDENTITY LIFECYCLES
ACCESS GOVERNANCE & RISK
ACCESS MANAGEMENT
LEGACY IAM SUPPORT
ADDITIONAL IAM CAPABILITIES

Simeio – Identity Orchestrator

Simeio is a US-based vendor in the IAM market. They deliver their Simeio Identity Orchestrator as a solution that supports customers in orchestrating the IAM solutions they have in place or that they deploy in addition to their current solutions. Thus, while Simeio Identity Orchestrator (IO) delivers some IAM capabilities on its own, it primarily—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 the breadth and number of IAM solutions supported. Simeio IO comes with integration capabilities for about a dozen IAM vendors, covering all major areas including IGA, access management, and PAM.

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

Simeio not only provides the technology but 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. 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, primarily around UI and dashboards, in a modern microservices architecture. This makes Simeio IO an interesting option for building an Identity Fabric, specifically for customers that own various IAM tools and are on a modernization journey, by building on what they already have in place.

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

Table 18: Simeio's rating

Strengths

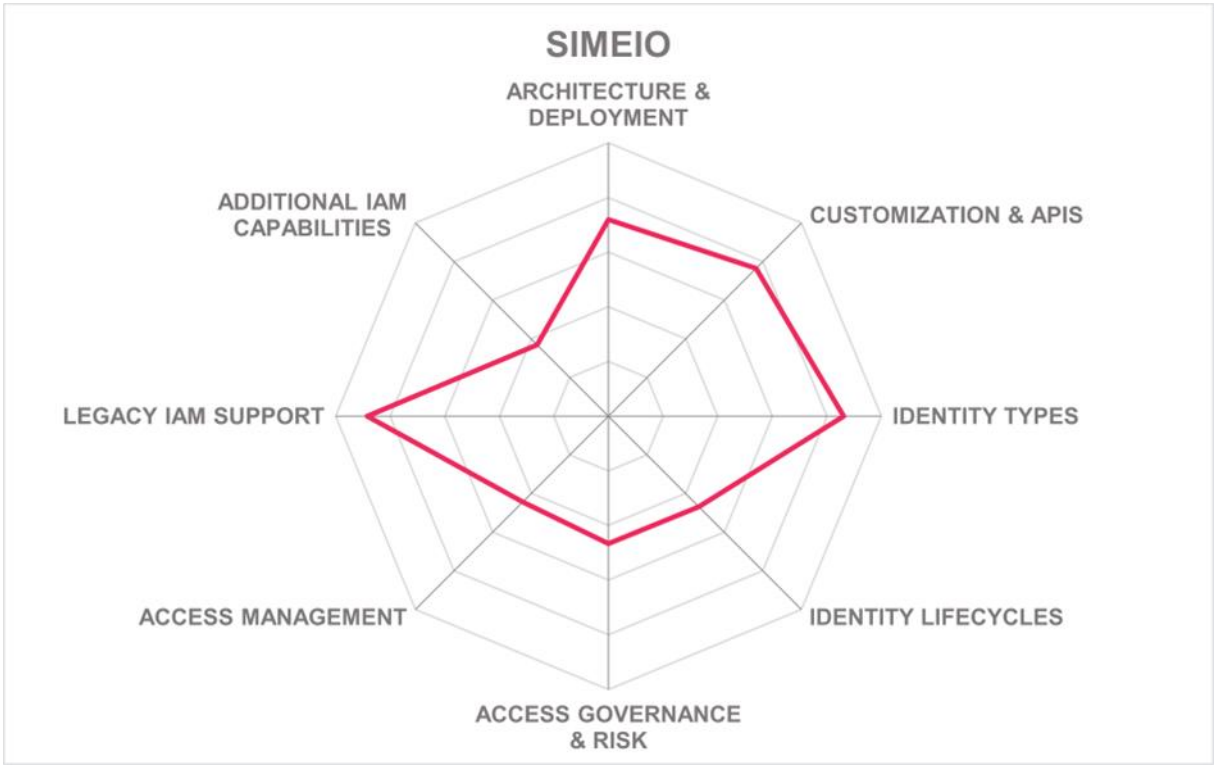
- Well-thought-out approach on orchestrating existing IAM products

- Broad technology 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, some more specialized IAM solutions are not supported natively
- Deployment has been simplified and vastly automated, but still might require some level of customization for existing IAM solutions to be integrated
- Integration commonly provided by Simeio, not by independent system integrators
- Integration platform, limited coverage of IAM capabilities by their own

Leader in



Soffid IAM – Identity Converged Platform

Soffid is a provider of a converged IAM platform supporting IGA, access management, and PAM capabilities. The company is headquartered in Spain and is one of the few open source IAM vendors in the market.

Over the years, Soffid has evolved from a specialized IGA solution to what they call a converged platform, covering a range of capabilities. Customers can choose the modules needed if they do not want to deploy the entire platform. Soffid supports both on-premises deployments and single-tenant IDaaS deployments. For cloud deployments, GCP in combination with OVHcloud is used, providing an active standby across to cloud providers.

For access management, the expected functionality is supported, including strong/multi-factor authentication, SSO, password management, support for biometric and passwordless authentication, as well as adaptive authentication features. Several capabilities for legacy support such as RADIUS support have been added, but also passwordless authentication supporting iOS and Android devices. The platform can also consume signals via the emerging standards CAEP and RISC.

The IGA capabilities, in the nomenclature of Soffid, are split into two areas. IGA focuses on Identity Lifecycle Management and Provisioning, while Identity Risk & Compliance (IRC) comprises the product's access governance capabilities. Identity sources can be connected using a wizard that supports source and target system connectivity, best practices for workflows, and other features. However, the number of provided connectors is fairly limited. For access governance, the support of so-called Issue Management allows dealing with integration and identity data quality issues in a standardized way.

As one of the few products on the market supporting IGA, Access Management, and PAM, Soffid comes with a good baseline support for PAM, including an Identity Vault for managing administrative and shared passwords and with session recording including OCR analysis. Soffid has also improved its network detection engine for identifying systems that should be put under their management.

The user interface of Soffid is modern, with icons helping in easily spotting capabilities. The wizards, while being valuable, requires some more integrated automation features, since in their current state, they act more as guides to the administrators.

The Soffid solution has matured significantly over the years and is a leading solution in the open source based IAM products. While they are not yet as feature rich as some other solutions available and lack depth and breadth of connectors, Soffid provides an interesting alternative to the established vendors in the market.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

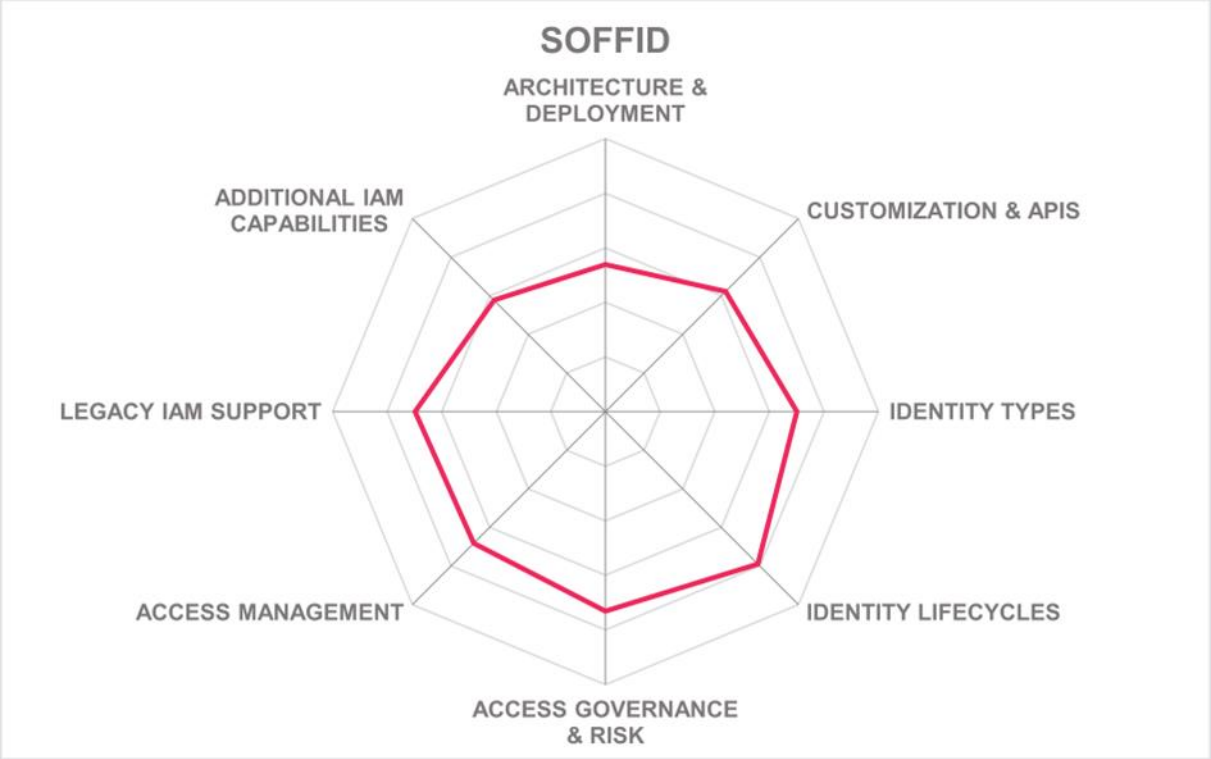
Table 19: Soffid's rating

Strengths

- Coverage of IGA, Access Management, and PAM capabilities
- Integrated platform
- Modern UI
- Supports SaaS-type deployments, but single-tenant
- Open-source approach
- Can automatically identify systems and identities and put them under management
- Overall good set of features across IAM domains

Challenges

- Small vendor with a still limited partner ecosystem
- While providing a good set of features, there remains room for improvement
- No graphical workflow editor
- Limited set of built-in connectors


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

Strata Identity – Maverics Identity Orchestration Platform

Strata Identity is one of the specialist vendors in this Leadership Compass. In contrast to others, they do not provide a comprehensive Identity Fabric, but an interesting addition that complements other solutions by helping integration of existing access management solutions and identity silos. The company is small but has an interesting position in the market due to its unique approach.

Strata Identity Maverics Identity Orchestration Platform is a solution that is focused on managing identity siloes in today's ever evolving IT infrastructures. Such infrastructures commonly contain a lot of identity silos such as Microsoft AD and others, but also fresh solutions that keep identities such as Microsoft Entra ID, 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 Entra ID, 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 Identity Query Language (IDQL), a standard developed and proposed by Strata Identity.

Strata Identity provides a range of interesting features that are not found in other products on 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.

Security	Positive
Functionality	Neutral
Deployment	Strong Positive
Interoperability	Positive
Usability	Neutral

Table 20: Strata Identity's rating

Strengths

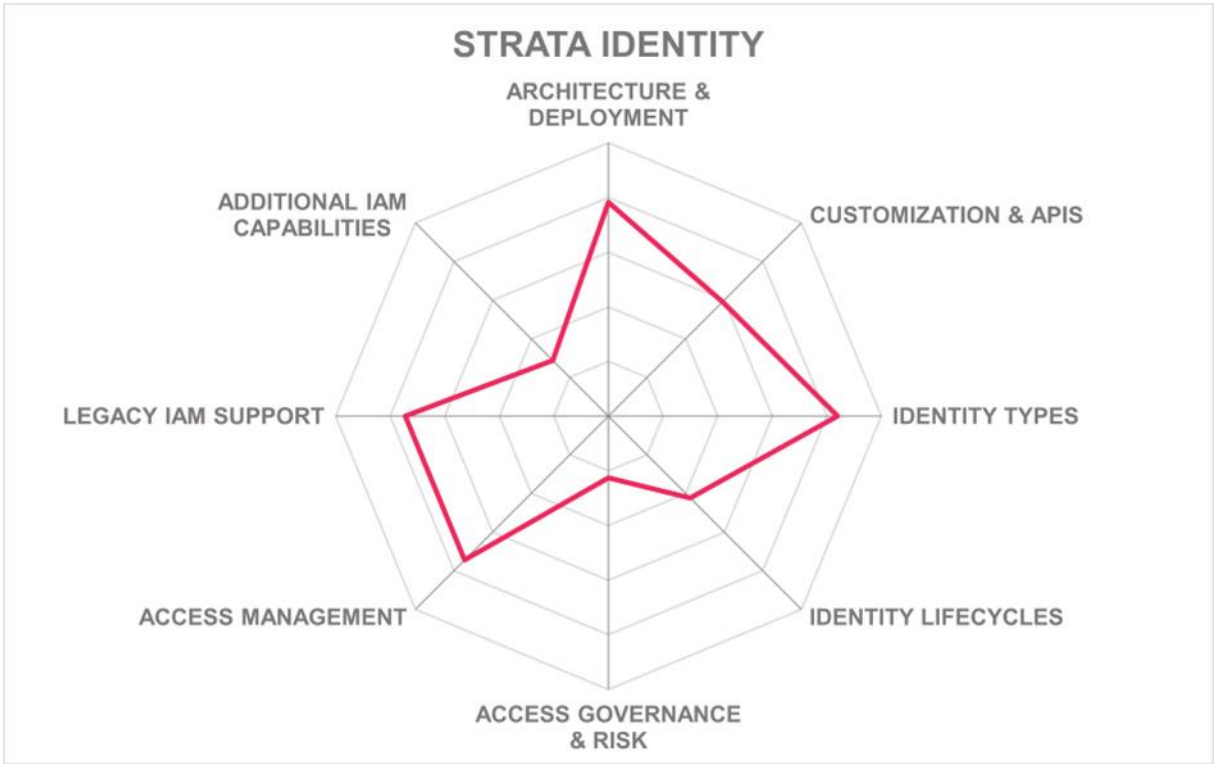
- Unique capabilities for integrating identity siloes at runtime

- 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
- Unique position in the market for access orchestration
- Various technology partnerships in place

Challenges

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

Leader in



TrustBuilder – TrustBuilder.io

TrustBuilder is a company that is headquartered in Belgium, with a large French subsidiary with offices in Italy, Spain, and the U.S., these are the result of the merger of the former TrustBuilder and French inWebo. The company focuses on delivering a strong solution for providing consumer and workforce access. The TrustBuilder.io. suite of products supports baseline lifecycle management, primarily targeted at customer and consumer use cases. It also supports policy-based authorization and API security use cases.

TrustBuilder.io. consists of different modules. TrustBuilder Access Manager is the component that provides Access Management and federation capabilities. TrustBuilder.io Multi-Factor Authentication adds capabilities for MFA and passwordless authentication, with TrustBuilder.io Notification Service as an addition providing OTP authentication based on SMS. TrustBuilder.io Identity Management supports identity lifecycles for secure customer onboarding. Self-service capabilities are added by the TrustBuilder.io Self-Service module. API security comes via TrustBuilder.io API. Finally, there is TrustBuilder.io Insights for reporting and analytics.

TrustBuilder provides one of the few solutions in the market that enhances common CIAM capabilities with KYC and identity verification based on ID documents for customer and consumer onboarding. They also deliver consent management features.

For enterprise use cases, the focus is also on access management, making TrustBuilder a component of Identity Fabrics, but with significant limitations for IGA. While identity lifecycles are supported and can be adjusted for simple workforce use cases, access governance is limited to analytics and reporting. It also provides self-service capabilities for access and for management of the user's identity data. User flows can be configured flexibly. A shortcoming of the current release is their lack of support for FIDO2 based authentication, which is a near-term roadmap item.

The solution comes with a strong feature set for authentication and policy-based access control to backend systems as well as federation support and many other features such as delegated administration, MFA support for Windows login, and mobile apps.

A particular strength is the support for policy-based and contextual authorization of access. TrustBuilder includes an authorization engine, allowing policies to control the concrete access entitlements. API security is a notable capability, with TrustBuilder also working on adding API-level Machine-to-Machine (M2M) security.

TrustBuilder, after the merger with inWebo, is showing progress on the integration and parallel modernization of the two product stacks, focusing on a modern, microservice-based architecture.

Due to the limited feature set around Identity Lifecycle management and IGA, TrustBuilder is to be considered more complementary within an Identity Fabric, serving certain capabilities including Access Management at a high level.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Positive
Usability	Positive

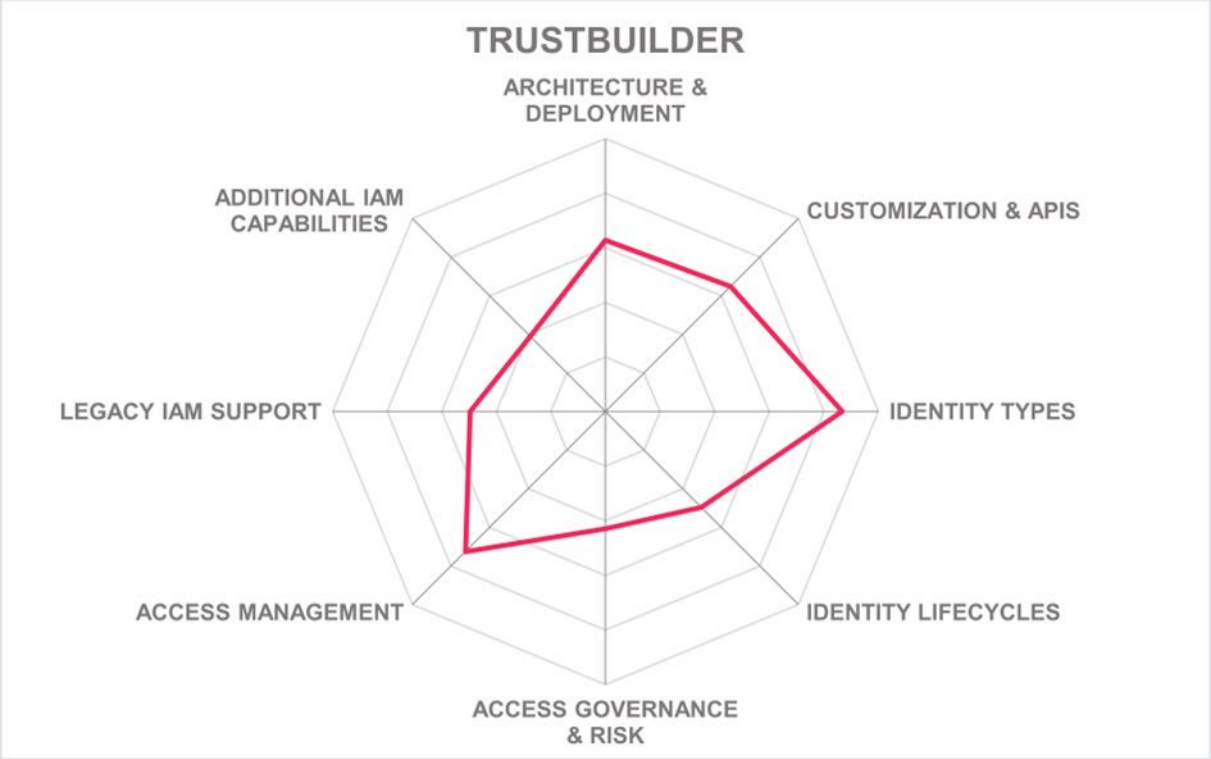
Table 21: TrustBuilder's rating

Strengths

- Strong access management and MFA capabilities
- Support for API security use cases
- Built-in support for passwordless authentication
- Supports KYC use cases in regulated industries
- Scales for CIAM use cases
- Supports policy-based and contextual authorization
- Authenticator apps available
- Modernizing components towards microservices architecture

Challenges

- FIDO2 support still lacking, but on roadmap
- Very limited feature set for Workforce identity lifecycle management
- Very limited IGA capabilities
- No global partner ecosystem yet, focus on Europe
- No PAM capabilities
- Modules not yet fully integrated


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

XAYone – XAYone Platform

XAYone, headquartered in Luxembourg with offices in Casablanca and Dubai, is a provider of an integrated IAM platform. While the focus is on CIAM use cases and additional trust services, the technology also can serve broader IAM use cases with its broad set of capabilities.

The XAYone platform consists of two major components. One is XAYone Advanced Identity Management, focusing on Identity Lifecycle Management and Access Management. The other is XAYone Trust Services, adding identity verification based on document identification, electronic signature management, and other capabilities that are specifically relevant for customer and citizen use cases and in areas where a high level of regulatory compliance, for instance around KYC processes, is needed.

For IGA capabilities, the focus of the solution is on Identity Lifecycle Management. This is supported by flexible workflows that can be configured using a graphical editor as well as in BPNM notation. The access governance capabilities are limited and will not cover the needs in regulated industries requiring sophisticated role management and certification capabilities but are strong for customer-focused use cases and provide a range of good baseline features. Also, the number of connectors is limited. While the solution supports Microsoft AD, Entra ID, and other common platforms, it lacks support for LoB applications such as SAP, Salesforce, and others. For SaaS services, the SCIM connector can be used. On the onboarding side, the focus is also more on consumers and citizens, including support for registration via social network accounts, while advanced HR integration is lacking.

For Access Management, the XAYone platform comes with extensive support for a range of requirements, specifically for federation and authentication to SaaS services. This includes support for common standards such as OpenID Connect and SAML, but also a graphical configurator for authentication flows. A specialty of XAYone is their extensive support for identity verification, also supporting a wide range of globally used ID documents. XAYone also provides an app for registration and authentication, as well as an SDK. It also has consent management features built in.

XAYone comes with a modern UI and provides powerful dashboards. They provide insight into the status of the system as well as into the state of managed identities. Dashboards support both the Identity Management and Access Management capabilities of the solution. The administrative capabilities are well-structured and flexible. The XAYone platform is built on segregated engines (microservices) exposing REST APIs. The UI uses these APIs. The architecture is modern and extensible and allows for flexible customization of the solution.

XAYone still lacks a strong partner ecosystem and still has a small customer base, but this includes a range of flagship customers such as airports and financial services, specifically in Africa. With its specific capabilities, it is an interesting solution particularly for governmental and financial services use cases and other highly regulated industries, when focus is on customer and citizen use cases.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Positive
Usability	Positive

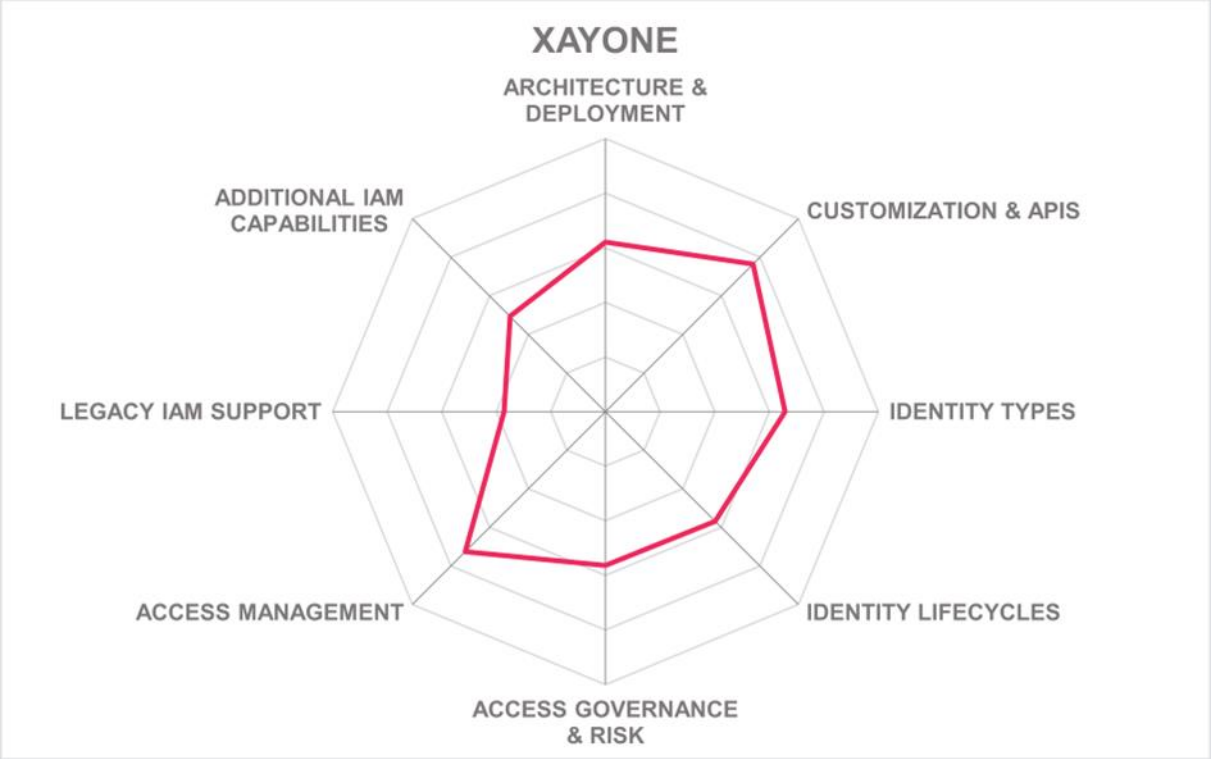
Table 22: XAYone's rating

Strengths

- Modern UI
- Well thought-out product architecture, based on microservices and API-first strategy
- Strong support for identity verification, including support for many national ID cards
- Strong Access Management capabilities
- Good standards support
- Strong CIAM support
- Some large-scale flagship customers
- Good presence in Africa

Challenges

- Very limited support for IGA use cases
- No PAM support
- Limited set of connectors for LoB applications
- Still a small vendor with limited visibility in the market
- Small partner ecosystem, not yet on a global scale


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

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.

Authlete

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.

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.

Why worth watching – feature-rich approach with modern user experience for building the foundation of an Identity Fabric.

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.

Cross Identity

Cross Identity is a spin-off of Ilantus, a large system integrator. Their solution 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. Cross Identity also integrates a PAM solution, and with an integrated Web Access Management capability covers all aspects on the IAM stack.

Why worth watching – feature-rich solution targeting medium-sized and mid-market organizations, good speed in innovation.

Eviden

Eviden is part of Atos and its IAM solution provider. Eviden is 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 Eviden and Atos DirX 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/Service Layers

German system integrator iC Consult with their Service Layers 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

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.

Memority

Memority is a spin-off from Accenture and delivers an integrated solution that supports most areas of IAM, specifically IGA and Access Management. Memority is based in France, as most of the current customers using Memority are. They have some very large installations of Memority deployed.

Why worth watching – modern architecture, proven scalability and support for complex use cases including supporting machine identities in the IoT (Internet of Things) field.

N8 Identity

N8 Identity is one of the specialist vendor's we have evaluated in this Leadership Compass. Their 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.

Why worth watching – interesting to complement Microsoft Entra ID with good IGA solutions, specifically for mid-market customers.

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.

Why worth watching – while having its strengths in Access Management and CIAM (Consumer IAM), Okta also supports a wide range of capabilities in other areas.

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.

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 positions itself as Identity Data Fabric and thus has a unique position in the market.

Why worth watching – powerful add-on for dealing with identity-related data and complementing other solutions in addressing the Identity Information Quality challenges.

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 several 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.

Systancia

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.

Transmit Security

Transmit Security has evolved from an identity verification and authentication platform towards a powerful CIAM solution, also covering identity flows for users. This makes them increasingly an interesting option within an Identity Fabric.

Why worth watching – modern solution with strong authentication and identity verification capabilities and a growing set of features that are relevant to Identity Fabrics.

WALLIX

Having started as a PAM vendor, WALLIX has added Access Management and IGA capabilities through acquisitions. These have been integrated into the WALLIX One platform. With the growing and integrated portfolio, WALLIX is moving into the role of a provider of a wide set of essential capabilities for Identity Fabrics.

Why worth watching – broadening portfolio of IAM capabilities with PAM features standing out.

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.

Related Research

Leadership Compass Access Management

Leadership Compass Access Governance

Leadership Compass Privileged Access Management

Leadership Compass Identity Governance and Administration

Leadership Compass Passwordless Authentication

Leadership Compass CIAM Platforms

Executive View Hitachi ID Bravura Security Fabric

Executive View Hitachi ID Bravura Privilege

Executive View Cloudentity Authorization Control Plane

Executive View CyberArk Privilege Cloud

Executive View IBM Security Verify for CIAM

Executive View Microsoft Entra Permissions Management

Executive View One Identity Manager on Demand

Executive View PingOne Authorize

Executive View Simeio Identity Orchestrator

Executive View Atos DirX Access

Executive View Atos Evidian IDaaS

Executive View Eviden DirX Identity

Executive View Authlete API Authorization

Executive View PlainID Policy Manager

Executive View SailPoint Non-Employee Risk Management

Executive View SailPoint Identity Security Cloud

Executive View Saviynt Cloud PAM

Executive View Saviynt Enterprise Identity Cloud

Copyright

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

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making 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.