

Identity Fabrics

Martin Kuppinger

May 6, 2025



LEADERSHIP
COMPASS
2025

This report provides an overview of the Identity Fabrics market as the core market for IAM and a compass to help you find a solution that best meets your needs. It examines solutions that provide an integrated set of IAM capabilities and strong identity orchestration features to help organizations in building a comprehensive Identity Fabric. It provides an assessment of the capabilities of these solutions to meet the needs of all organizations to understand which solution best suits their specific needs.

Contents

Executive Summary	5
Key Findings.....	6
Market Analysis	7
Market Size and Segmentation.....	8
Delivery Models.....	9
Required Capabilities	10
Trends and Evolution.....	12
Leadership	14
Overall Leadership	14
Product Leadership	16
Innovation Leadership	18
Market Leadership.....	20
Products and Vendors at a Glance.....	22
Product/Vendor evaluation.....	25
Spider graphs.....	25
Bravura Security – Bravura Security Fabric	27
Broadcom – Symantec Identity Security	29
Cross Identity – Cross Identity.....	31
CyberArk – Identity Security Platform	33
Delinea – Delinea Platform.....	35
EmpowerID – EmpowerID	37
Exostar – Access: One	40
IBM – Security Verify	43
Microsoft – Entra ID.....	45
Monokee – Monokee	47
Okta – Customer Identity Cloud & Workforce Identity Cloud.....	49
One Identity – One Identity Manager, OneLogin, Safeguard.....	51

Optimal IdM – OptimalCloud.....	53
Oracle – OCI IAM	55
Ping Identity – Platform	58
RSA Security – Unified Identity Platform.....	60
SailPoint – Identity Security Platform.....	63
SAP – Cloud Identity Services.....	66
Saviynt – Identity Cloud.....	68
SecureAuth – SecureAuth CIAM & SecureAuth Workforce.....	70
Simeio – Identity Orchestrator	72
Soffid – IAM.....	74
Strata Identity – Mavericks Identity Orchestration Platform.....	76
TrustBuilder – TrustBuilder.io	78
XAYone – XAYone Platform	80
Vendors to Watch	82
Authlete.....	82
Avatier.....	82
Axiomatics.....	82
Baar-ID.....	82
cidaas.....	83
Eviden	83
Fischer International.....	83
Identity Automation.....	83
Ilex	84
Imprivata	84
Memory	84
N8 Identity.....	84
Netwrix	84
Pathlock	85
PlainID.....	85
Omada	85
OpenText	85
Radiant Logic	86
Systancia.....	86

Teleport.....	86
Thales	86
Transmit Security	87
WALLIX.....	87
WSO2.....	87

Executive Summary

Identity Management and Identity Security are indispensable in the digital age. The concept of "Identity Fabrics" offers a comprehensive suite of Identity Services that enable seamless yet regulated access to services across the entire spectrum of users and devices. It represents a paradigm, not confined to a single technology, tool, or service, for structuring Identity and Access Management (IAM) within modern enterprises.

Identity Fabrics merge the traditional IAM components with modern orchestration and integration capabilities, allowing enterprises to roll out seamless services across complex IT environments. These fabrics are essential in scenarios where legacy systems coexist with newer, cloud-based services, providing a cohesive approach to manage this blend. They are envisioned to support diverse identity types: ranging from employees and business partners to consumers, devices, and connected things; thereby delivering secure, well-managed, and contextually accessible services.

At its core, an Identity Fabric is constructed around robust orchestration capacities, essential for integrating modern IAM solutions with older, legacy systems. These orchestration capabilities allow for adaptive integration of multiple identity services from various providers, progressing beyond a singular greenfield approach to a more unified solution. Organizations usually have two main pathways to establish an Identity Fabric: by building on a solid core platform supplemented with specialized solutions or utilizing an orchestration platform to integrate diverse IAM tools and services.

This Leadership Compass delves into various IAM solutions within the market, identifying those most capable of forming a foundational base for Identity Fabrics. It emphasizes solutions that provide:

- A broad range of IAM capabilities imperative for cohesive and accessible identity services.
- An extensive set of APIs enabling the consumption of identity services, far beyond traditional UI/UX interfaces.
- Modern architecture that builds on microservices, container-based deployments, and flexible operational models.
- Comprehensive deployment options, supporting business diversity in operating models.
- Support for all identity types, including employees, partners, consumers, devices, and more.

The flexibility in deployment models—from cloud to on-premises to hybrid scenarios—alongside strong interoperability with an organization's necessary operational frameworks, is central to the concept of Identity Fabrics. The modern identity services landscape necessitates not only the typical provisioning of user identities but also advanced management of entitlements, risk-based access controls, and adaptive authentication methodologies.

Identity Fabrics demand solutions that integrate various IAM elements, including Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM), and more. The convergence of these diverse capabilities ensures robust management of identities, also supporting emerging business needs such as Zero Trust, decentralized identities, and policy-based access models.

In today's environment, the swift adoption of Identity Fabrics is not only essential for enhancing security and operational efficiency but also fundamental in driving digital transformation initiatives. They provide the foundation upon which organizations can build scalable, secure, and adaptive identity services that match the dynamic demands of digital interaction. As organizations pursue the rollout of their own Identity Fabrics, selecting the right blend of capabilities, architecture, and orchestration methods will be critical in successfully navigating the complexities of current and future identity landscapes.

For information about the Leadership Compass process, see our [KuppingerCole Leadership Compass Methodology](#).

Key Findings

Identity Fabrics are now 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.

- Identity Fabrics represent a paradigm shift in IAM, emphasizing a comprehensive set of identity services for secure, seamless access to all services.
- This framework is not a one-size-fits-all; it integrates multiple tools across IAM capabilities, tailored to organizational needs.
- Core Identity Fabrics can be built on strong platforms for key functions, supplemented by specialized solutions for orchestration and integration.
- Solutions are evaluated on architecture, deployment flexibility, APIs, and support for all identity types, from employees to devices.
- Integration and orchestration are key as Identity Fabrics must bridge modern and legacy IAM systems in a cohesive manner.
- Identity services expose capabilities not only through UI/UX but also via comprehensive APIs for digital and cloud service consumption.
- Modern architectural paradigms—microservices, container-based deployments—are crucial for robust Identity Fabric infrastructure.
- This Leadership Compass evaluates IAM solutions' preparedness to serve as a foundation for Identity Fabrics, noting a trend towards increased maturity in these solutions.
- Overall Leaders (in alphabetical order) include CyberArk, EmpowerID, Microsoft, Okta, One Identity, Ping Identity, Sailpoint, and Saviynt.
- Product Leaders (in alphabetical order) include CyberArk, EmpowerID, Exostar, Microsoft, Okta, One Identity, Ping Identity, Sailpoint, and Saviynt.

- Innovation Leaders (in alphabetical order) include CyberArk, EmpowerID, Microsoft, Okta, One Identity, Ping Identity, RSA Security, SailPoint, and Saviynt.
- Market Leaders (in alphabetical order) include CyberArk, IBM, Microsoft, Okta, One Identity, Ping Identity, RSA Security, SAP, SailPoint, and Saviynt.

Market Analysis

The Identity Fabrics paradigm elevates enterprise identity and access management to the next, future-proof level by introducing a comprehensive and integrated framework. It deviates from conventional singular solutions by deploying a multifaceted approach, aiming to provide seamless, yet controlled, access for any identity type to diverse services. The model is not restricted to a specific technology but rather embraces a collection of mutable services to accomplish enterprise identity and access goals.

Identity Fabrics allow organizations to choose between constructing a centralized IAM core or adopting an orchestration-centric Identity as a Service (IDaaS) model, both of which ensure modernization and integration of identity services.

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.
- 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 to conduct business and execute payments.
- Compliance with 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.

This leads, also in the broader context of Identity Security, to the demand for integrated yet flexible solutions that serve a wide range of requirements organizations are facing today.

Market Size and Segmentation

Identity Fabrics must provide flexibility and adaptability in integrating various identity services to support modern enterprise requirements:

- **Comprehensive Identity Fabrics Solutions:** Leverage a converged IAM platform supporting a broad range of IAM capabilities including Identity Governance and Administration (IGA), Access Management (AM), and Privileged Access Management (PAM). These core systems often serve as the backbone of Identity Fabrics.
- **Orchestration-Focused Solutions:** Utilize an orchestration layer to facilitate the integration of assorted tools and services, enhancing the interoperability between legacy IAM frameworks and cutting-edge systems. This approach fosters a seamless operational environment where legacy systems can synergize with contemporary IAM applications.
- **Specialized Vendors:** Fill critical gaps in IAM frameworks, focusing on specific areas such as advanced authorization technologies and sophisticated orchestration systems. These vendors complement core IAM solutions by addressing specialized security needs.

Supported services can be in public or private clouds, on-premises (private data center), 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.

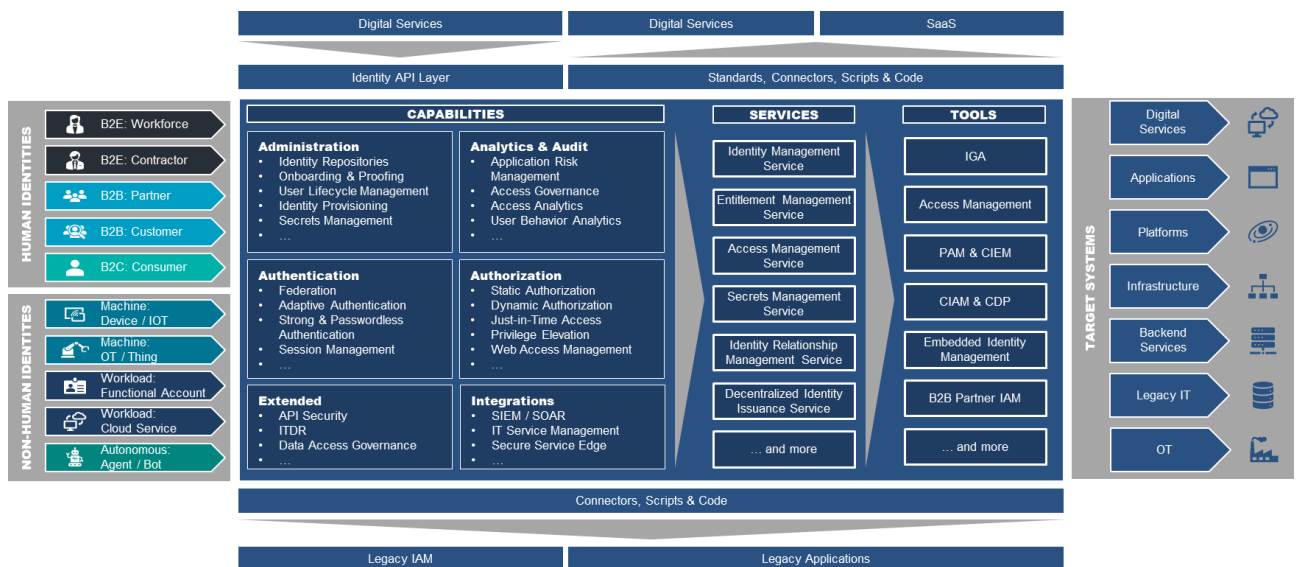


Figure 1: The KuppingerCole Identity Fabric.

KuppingerCole Analysts recommends taking a 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 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.

Delivery Models

The delivery models for Identity Fabrics emphasize versatility and adaptation to enterprise-specific needs. Multi-tenant public cloud services, favored for their scalability and ease of administration, cater to organizations seeking straightforward IDaaS solutions. Single-tenant models, accessible within both public and private cloud environments, provide adaptability

for organizations prioritizing compliance and bespoke operational controls. This multifaceted delivery approach accommodates enterprises with distinct data residency requirements and regulatory obligations. Moreover, the inherent elasticity and scalability of these delivery models ensure robust performance across diverse deployment scenarios, whether cloud-based or on-premises.

- 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.

Required Capabilities

Identity Fabrics must support a baseline level of both IGA and Access Management. From there, they could provide further capabilities such as integrated directory services, PAM, and other IAM capabilities that are commonly required by customers. Some solutions in the market are focused on Access Management or IGA only, but either provide additional capabilities such as PAM, or focus on orchestration that is essential when building an Identity Fabric.

Common Capabilities

- Comprehensive API support for modern identity services.
- Advanced identity lifecycle management features.
- Integrated access management functionalities.
- Dynamic real-time monitoring and analytics.
- SCIM and custom connectors for seamless integration.
- Multifactor authentication (MFA) support for enhanced security.
- Risk-based access control with adaptive authentication options.
- Modular architecture supporting microservices and containerized deployments.

- Robust identity federation and Single Sign-On (SSO) capabilities.
- Strong governance with access reviews and audit capabilities.

IAM Core Solutions Subsegment

- Full coverage of IGA, including provisioning and governance.
- Integrated directory management for identity data synchronization.
- Sophisticated role and entitlement management.
- Policy-based access control models, including ABAC.
- Identity analytics for compliance and risk management.
- Workflow management with self-service options for users.

Orchestration Solutions Subsegment

- Vendor-agnostic orchestration layer allowing seamless service integration.
- Low-Code/No-Code interface for workflow and process automation.
- Cross-identity provider (IDP) failover capabilities.
- In-place migration support for legacy applications.
- Supports diverse identity types including employees, partners, and IoT devices.

Specialized Vendors Subsegment

- Tailored solutions targeting advanced authorization and security gaps.
- Enhanced orchestration capabilities for legacy system integration.
- Extendable features for continuous service improvement.
- API-first architecture supporting diverse digital services and applications.

Excluded from this Leadership Compass are:

- Vendors that only cover IGA or access management (except specialized orchestration solutions 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 usage-based licensing model.
- Vendors without active deployments at customers (such as start-ups in stealth mode).
- Solutions with traditional architecture, not supporting modern deployment models such as container-based deployments.
- Solutions that lack a complete set of APIs.
- Solutions that are targeted at either only employees/business partners or at customers/consumers.

Trends and Evolution

The evolution of Identity Fabrics can largely be attributed to the increasing complexity of digital business landscapes, where a broad array of identities—including employees, customers, partners, devices, and services—demand secure access to a multitude of applications and services. Organizations are increasingly leveraging Identity Fabrics as a unifying architecture that supports heterogeneous environments and integrates disparate identity services into a coherent framework.

A significant trend within Identity Fabrics is the movement towards highly modular, microservices-based architectures. This trend facilitates flexible deployment options that accommodate hybrid environments, spanning on-premises and cloud infrastructures. With the rise of microservices, organizations can create agile IAM ecosystems that are capable of rapidly adapting to changing business requirements and technological advancements. This modularity is vital not only for reducing integration overheads but also for enhancing scalability and resilience in the face of evolving security threats.

Orchestration plays a central role in the ongoing evolution of Identity Fabrics. As organizations seek to bridge modern and legacy IAM systems, orchestration capabilities become indispensable. They allow integration and interoperability across varied identity management tools and services, ensuring that organizations can orchestrate identity operations effectively and maintain a cohesive security posture. Furthermore, orchestration complements API-centric architectures, providing a platform through which many different digital services can consume identity capabilities reliably and securely.

Another prominent trend is the expanding scope of identity types supported by Identity Fabrics. Beyond traditional workforce and customer identities, Identity Fabrics are increasingly focused on managing machine identities and IoT devices, which are becoming integral to modern enterprise infrastructures. This expansion necessitates advanced IAM capabilities, such as automated identity lifecycle management and dynamic policy-based access controls, to handle the scale and diversity of identity interactions across complex, distributed networks.

Equally important is the market's shift towards incorporating Zero Trust principles within Identity Fabrics. As cyber threats become more sophisticated, Zero Trust architectures, which emphasize continuous verification, least privilege access, and strict authentication measures, are being integrated into IAM strategies. Identity Fabrics are evolving to support these principles, enhancing security through adaptive and context-aware authentication mechanisms and identity governance frameworks.

The trend towards leveraging Identity Fabrics for improved compliance is also noteworthy. Organizations are increasingly using these fabrics to centralize identity data management, ensuring that they can meet stringent regulatory requirements related to privacy, data protection, and security. By streamlining governance processes and enhancing visibility into identity-related activities, Identity Fabrics aid enterprises in maintaining regulatory compliance and mitigating risks associated with identity mismanagement.

As the market for Identity Fabrics continues to mature, vendor solutions are increasingly sophisticated, reflecting a convergence of comprehensive IAM capabilities. Vendors are expanding their portfolios to include integrated suites or focusing on orchestration and API management solutions that complement existing IAM infrastructures. This evolution not only fosters innovation but also enables enterprises to adopt a multivendor approach, selecting best-of-breed components to construct their ideal Identity Fabric.

In summary, the trends and evolution within the Identity Fabrics market segment highlight the paradigm's growing importance in modern IAM and Identity Security strategies. As businesses navigate the complexities of digital transformation, Identity Fabrics provide a flexible framework for managing identities and access in an interconnected world, driving innovation, and supporting secure digital ecosystems across industries.

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 various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

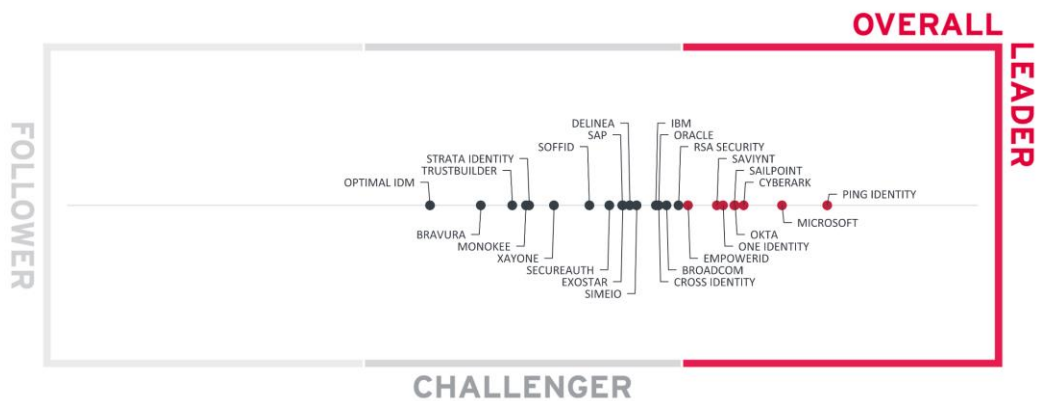


Figure 2: Overall Leadership in the Identity Fabrics market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

Among the Overall Leaders we see Ping Identity leading ahead of Microsoft. Both vendors deliver a full set of IAM capabilities. Ping Identity excels in the support for both modern and legacy environments, their orchestration capabilities, and support for new areas such as decentralized identity. Microsoft also provides strong coverage across IAM areas and also integration into their broader identity and security portfolio. Following them we find CyberArk,

which has evolved from being a PAM vendor into a provider of a broad range of capabilities we are looking for in the Identity Fabric, close together with Okta and SailPoint. While Okta has a strong foundation in Access Management and CIAM, as well as support for other capabilities, SailPoint has extended from IGA into areas such as CIEM and modern PAM. Close to them we find One Identity and Saviynt, followed by EmpowerID, all providing a strong foundation for building an Identity Fabric.

Among the Challengers, we find a group of established IAM vendors to the right. Broadcom, IBM, Oracle, and RSA Security all have broad solution portfolios, but are still in the process of modernization. Cross Identity with their converged platform is positioned close to them. With, Delinea, SAP, Exostar, and Simeio, we find an assortment of vendors, all with specific strengths, but also gaps in either depth or breadth in their portfolios. Simeio stands out as an orchestration platform that primarily focuses on integrating other vendors' solutions.

SecureAuth, after the acquisition of Cloudentity, is next, followed by Soffid, who are providing an open source IAM solution. Other vendors in the Challenger section include XAYone, TrustBuilder, Monokee, Strata Identity, Bravura, and OptimalIDM. Strata Identity and Monokee are focusing on orchestration.

There are no Followers in this overall leadership rating.

Overall Leaders are (in alphabetical order):

- CyberArk
- EmpowerID
- Microsoft
- Okta
- One Identity
- Ping Identity
- SailPoint
- Saviynt

Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.



Figure 3: Product Leadership in the Identity Fabrics market

Ping Identity is taking the lead in this perspective of our analysis, delivering an extensive portfolio including strong orchestration capabilities, which also support integrating the former ForgeRock solutions. Microsoft also provides a strong portfolio, also supporting PAM and other capabilities, but lacking depth in capabilities in some areas such as PAM and IGA.

Following them we find a group of vendors with CyberArk, Okta, and One Identity, all delivering a wide range of IAM capabilities. Okta is lacking depth and breadth of capabilities in areas such as PAM and IGA, while CyberArk will need to fully integrate the recently acquired Zilla Security, and One Identity still not being fully done with modernization and integration of the portfolio. We then also find EmpowerID, Saviynt, SailPoint, and Exostar in this group. While SailPoint and Saviynt are lacking their own, powerful Access Management capabilities, they excel across various other areas of IAM. Exostar and EmpowerID provide a wide range of capabilities, also being positioned well as a foundational element for an Identity Fabric.

The Challenger section is crowded. Again, we find the established vendors such as Broadcom, IBM, Oracle, and RSA Security at the top, close to the Leader segment. Simeio, Soffid, and Cross Identity also all are placed in that upper region. Following them, we find Delinea providing a robust authorization platform, but with limited Access Management capabilities; XAYone, providing an increasingly feature-rich solution; SAP, where the IGA solution SAP Identity Management isn't considered anymore in the rating due to the announced end-of-life; and SecureAuth after the acquisition of Cloudentity. Further vendors in this segment include TrustBuilder, Monokee, Bravura Security, Optimal IDM, and Strata identity.

Product Leaders (in alphabetical order):

- CyberArk
- EmpowerID
- Exostar
- Microsoft
- Okta
- One Identity
- Ping Identity
- SailPoint
- Saviynt

Innovation Leadership

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

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

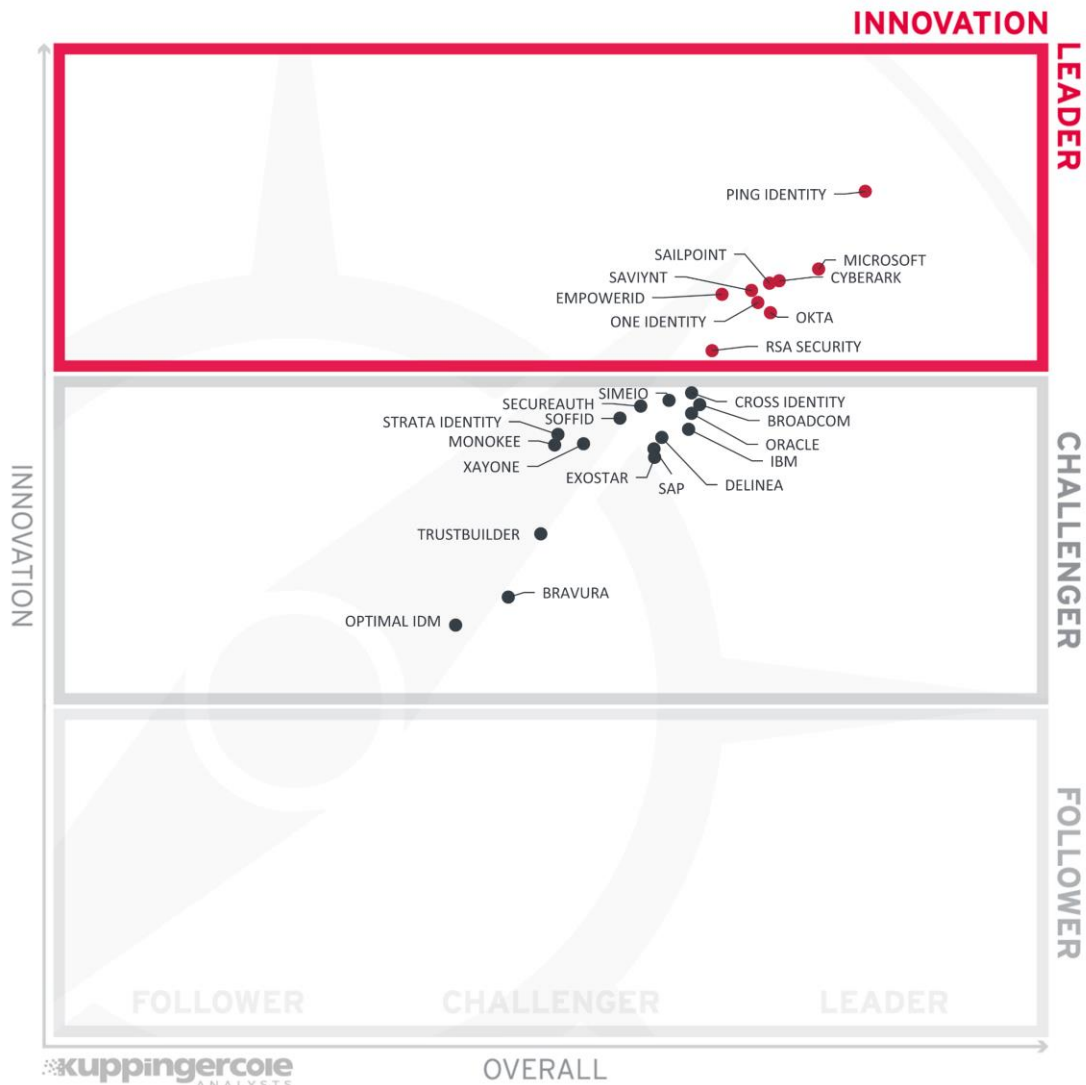


Figure 4: Innovation Leadership in the Identity Fabrics market

Innovation Leaders are those vendors that deliver cutting-edge products, not only in response to customers' requests but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

Again, Ping Identity is leading, based on their strong engagement in developing standards and due to forward-looking acquisitions in fields such as policy-based access controls, decentralized identity, and identity orchestration. Microsoft again takes a strong position, based on their broad portfolio and also their commitment to developing standards. CyberArk, SailPoint, Saviynt, EmpowerID, One Identity, and Okta are following closely, all demonstrating a range of relevant innovations in their product portfolios and most of them including Okta are engaged in leading the industry in developing standards. RSA Security also has entered the leader segment.

In the Challenger section, we find a large group of vendors at the top, including (in alphabetical order) Broadcom, Cross Identity, Delinea, Exostar, IBM, Monokee, Oracle, SAP, SecureAuth, Simeio, Soffid, and XAYone. All demonstrate a good level of innovation. That also holds true for Strata Identity, but their focus is limited on access orchestration. Further vendors in the section are TrustBuilder, Bravura Security, and OptimalIDM.

Innovation Leaders (in alphabetical order):

- CyberArk
- EmpowerID
- Microsoft
- Okta
- One Identity
- Ping Identity
- RSA Security
- SailPoint
- Saviynt

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, the geographic distribution of customers, revenue, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.



Figure 5: Market Leaders in the Identity Fabrics Market

Here, we see Microsoft at the top, with their broad global customer base and partner ecosystem. Ping Identity is following, serving customers across the entire range of Identity Fabrics components. Okta is next, closely followed by SailPoint and CyberArk. CyberArk is expected to further strengthen its position by the recent acquisition of Zilla Security. Other market leaders include One Identity, IBM, SAP, RSA Security, and Saviynt.

In the Challenger section, we see a group of large software vendors on top, including Broadcom, Delinea, and Oracle. Following them, we find emerging vendors, including Cross Identity, EmpowerID, Simeio, SecureAuth, Exostar, Bravura, and TrustBuilder. Other vendors in this segment include OptimalIDM, Strata Identity, Soffid, and XAYone.

Market Leaders (in alphabetical order):

- CyberArk
- IBM
- Microsoft
- Okta
- One Identity
- Ping Identity
- RSA Security
- SAP
- SailPoint
- Saviynt

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this Leadership Compass. 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	positive	positive	neutral	neutral	positive
BROADCOM	strong positive	positive	positive	positive	positive
CROSS IDENTITY	strong positive	positive	strong positive	positive	positive
CYBERARK	strong positive	strong positive	positive	strong positive	positive
DELINEA	strong positive	positive	positive	positive	positive
EMPOWERID	strong positive	positive	strong positive	strong positive	strong positive
EXOSTAR	strong positive	positive	positive	positive	positive
IBM	strong positive	positive	positive	positive	positive
MICROSOFT	strong positive	strong positive	strong positive	positive	strong positive
MONOKEE	strong positive	positive	positive	positive	positive
OKTA	strong positive	strong positive	strong positive	positive	strong positive
ONE IDENTITY	strong positive	strong positive	positive	strong positive	positive
OPTIMAL IDM	positive	neutral	positive	neutral	positive
ORACLE	strong positive	positive	positive	positive	positive
PING IDENTITY	strong positive	strong positive	strong positive	strong positive	strong positive
RSA SECURITY	strong positive	positive	positive	strong positive	positive
SAILPOINT	strong positive	positive	positive	positive	strong positive
SAP	positive	positive	positive	neutral	positive
SAVIYNT	strong positive	positive	strong positive	strong positive	strong positive
SECUREAUTH	strong positive	positive	positive	positive	positive

SIMEIO	strong positive	positive	positive	positive	positive
SOFFID	strong positive	positive	positive	positive	positive
STRATA IDENTITY	positive	neutral	positive	positive	positive
TRUSTBUILDER	positive	positive	neutral	neutral	positive
XAYONE	strong positive	positive	positive	positive	positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
BRAVURA	neutral	neutral	positive	positive
BROADCOM	positive	positive	strong positive	positive
CROSS IDENTITY	positive	positive	neutral	positive
CYBERARK	strong positive	strong positive	strong positive	strong positive
DELINEA	positive	positive	strong positive	strong positive
EMPOWERID	strong positive	neutral	positive	positive
EXOSTAR	positive	neutral	strong positive	neutral
IBM	positive	positive	strong positive	positive
MICROSOFT	strong positive	strong positive	strong positive	strong positive
MONOKEE	positive	neutral	neutral	neutral
OKTA	strong positive	strong positive	strong positive	strong positive
ONE IDENTITY	positive	positive	strong positive	positive
OPTIMAL IDM	neutral	neutral	positive	neutral
ORACLE	positive	positive	strong positive	neutral
PING IDENTITY	strong positive	strong positive	positive	strong positive
RSA SECURITY	positive	positive	positive	positive
SAILPOINT	positive	neutral	strong positive	strong positive
SAP	positive	positive	strong positive	positive
SAVIYNT	strong positive	positive	positive	positive
SECUREAUTH	positive	positive	positive	neutral
SIMEIO	positive	neutral	positive	positive
SOFFID	positive	neutral	neutral	positive
STRATA IDENTITY	positive	neutral	neutral	positive
TRUSTBUILDER	neutral	positive	positive	neutral
XAYONE	positive	weak	neutral	neutral

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

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

Spider graphs

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

Architecture & deployment: This category represents the combination of architecture and 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.

Orchestration: In this new category, which is related to connectivity and integrations, we look at the orchestration capabilities to deliver processes and workflows spanning various IAM modules but also integrating with external services such as ITSM (IT Service Management). We expect graphical orchestration support and strong API support.

Connectivity & Integrations: This category is related to architecture but focuses more on the comprehensiveness of APIs, the simplicity of customization, and the breadth and depth of integrations to target systems, including legacy systems and legacy IAM solutions. Our expectation of 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.

IGA capabilities: 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. As the second part of IGA, access governance and access risk management, including access analytics, are represented by this axis of the spider charts.

AM capabilities: 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.

Other IAM capabilities: This dimension focuses on support for Privileged Access Management and the new disciplines such as cloud infrastructure entitlement management (CIEM) and other advanced capabilities including Non-Human Identity Management (NHI)

support. Integrated support for such capabilities becomes increasingly relevant with the convergence of these capabilities, and for supporting identity types such as services.

Authorization management: Managing identity security across the entire Identity Fabric requires support for modern approaches. This is why we decided to add authorization management as a separate category in the spider chat, including PBAC (Policy Based Access Controls) that span multiple areas of the Identity Fabric modules.

Identity type support: 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.

Bravura Security – Bravura Security Fabric

Bravura Security, originally established as M-Tech Information Technology in Canada in 1992, has evolved significantly over the years. Initially known for password management solutions, the company underwent several acquisitions and rebranding, eventually emerging as Bravura Security under Volaris. Headquartered in Calgary, Alberta, Bravura Security focuses on providing a comprehensive Security Fabric that converges Identity Management, Privileged Access, Password, and Passwordless Governance, but also analytical capabilities. Their solutions aim to reduce overall risk and optimize total cost of ownership by delivering both on-premises and SaaS solutions through the Bravura Security Fabric.

The Bravura Security Fabric encompasses a wide array of capabilities, including identity and privilege automation, anomaly detection, and self-service identity management. Key features include secure password storage, dynamic risk profiling, and traditional federation (SAML) and MFA support across cloud and on-premises services. Bravura Security's focus on automation and comprehensive identity governance supports complex environments, ensuring efficient lifecycle management and policy enforcement. Additionally, their platform integrates well with SIEM and SOAR systems, providing extensive reporting and analytics tools for identity security data visibility.

A unique aspect of Bravura Security's solution is the integration of decentralized credential management and an extensive library of compliance and access policies, accessible via GraphQL and REST APIs. This provides organizations with structured, actionable insights and enhances identity security across various sources. Despite having many features, Bravura Security's reliance on legacy components and outdated user interfaces requires modernization efforts, particularly in user experience areas. While current identity governance capabilities are solid, the potential for innovation remains somewhat limited, pending further development of their security analytics solutions.

Bravura Security's solutions are particularly attractive to enterprises seeking extensive identity and access management capabilities with flexibility in deployment options. The company's strengths lie in catering to finance, insurance, manufacturing and higher education sectors, among others. Bravura Security's presence in North America and Europe means it is well-suited for organizations in these regions requiring strong identity governance and protection. Those looking to unify identity and security data and reduce operational risks will find value in evaluating Bravura Security's solutions.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Neutral
Usability	Positive



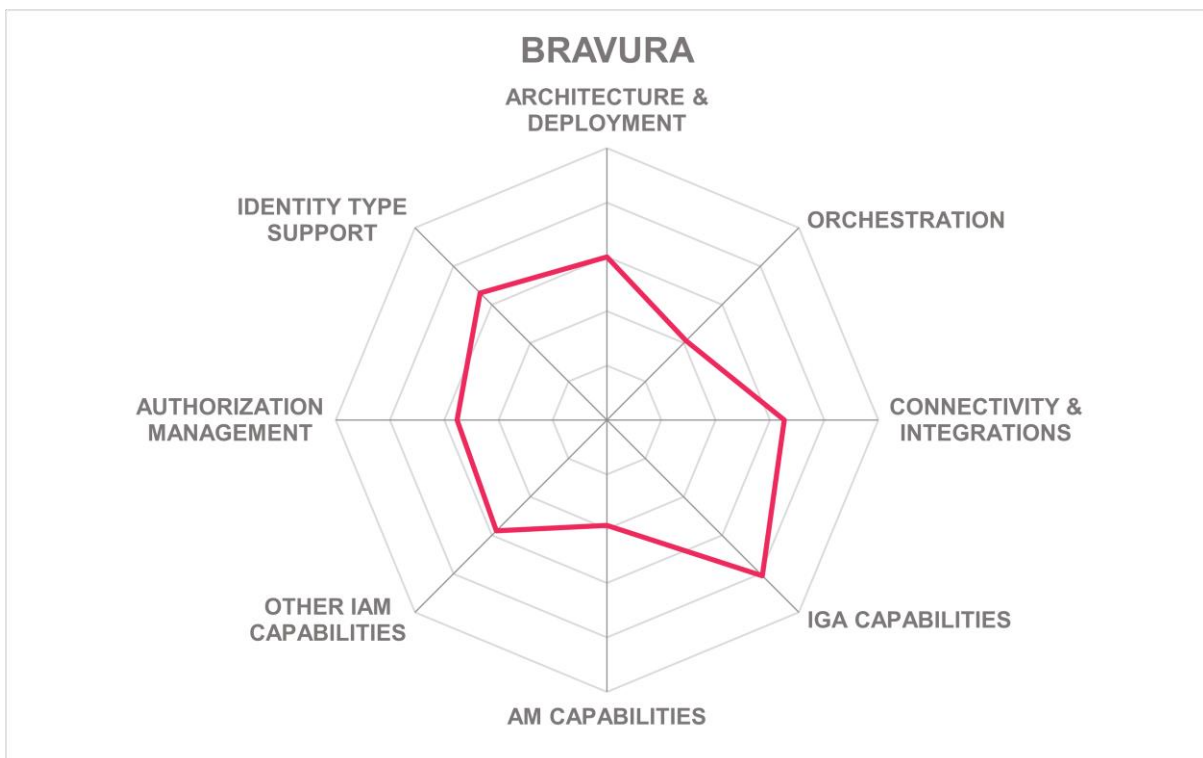
Table 3: Bravura Security's rating

Strengths

- Security Fabric approach beyond IAM, including various solutions for identity management.
- Strong self-service identity and password management features.
- Advanced reporting and analytics capabilities.
- Flexible deployment options, including SaaS and on-premises, but a mix of modern and legacy components.
- Robust compliance and access policy library.
- Integrated anomaly detection.

Challenges

- Legacy components limit UI modernization.
- Limited innovation in current capabilities.
- Requires gradual migration of legacy solutions.
- Initial setup complexity for new users.
- Lack of broader access management support beyond MFA.
- Deficiencies in modern federation standards support such as FIDO2



Broadcom – Symantec Identity Security

Broadcom, headquartered in San Jose, CA, was founded in 1991. In the IAM market, they built a suite of IAM solutions acquired through CA Technologies and Symantec. The company’s Symantec Identity Security suite interlinks access management, authentication, IGA and PAM to support a secure, modern IT environment. Through its commitment to API-driven architectures and microservices, Broadcom remains an influential player for organizations looking to innovate their identity infrastructures, primarily former CA Technologies IAM infrastructures, without sacrificing existing investments. Broadcom, with the addition of VMware to their portfolio, also owns a platform that can support large-scale operations of identity infrastructures at customers and MSPs (Managed Service Providers).

Broadcom's Identity Fabric strategy integrates all components of its IAM suite, offering key features including MFA, passwordless access, and session-based risk management. The Security Services Platform (SSP) enables real-time risk services sourced externally, backed by integrations within the broader Symantec and Layer7 API Management products. Broadcom also prioritizes advanced federation through support for standards such as SAML, OpenID Connect, and SCIM. They also support CAEP (Continuous Access Evaluation Protocol). They support a range of deployment options across cloud, on-premises, and hybrid deployments.

Distinctively, Broadcom excels in merging scalability with granular policy enforcement. These solutions are tailored for enterprises with complex, hybrid deployments, particularly where ownership of identity infrastructure and integration flexibility are paramount. The extensive heritage of Symantec and CA Technologies adds complexity to Broadcom's modernization journey. It is why the development of a new platform to enable modern applications combined with the integration with existing products has been the focus. Nevertheless, the diversity of the solutions' origins necessitates professional services for optimal integration, which could be enhanced by streamlining product interoperability further across legacy and new platforms.

The comprehensive suite appeals primarily to large global enterprises that require strong integrations with existing IAM infrastructures and legacy applications, which is the main focus of Broadcom navigates. Organizations in sectors with substantial regulatory demands, such as finance and telecommunications, find the Symantec Identity Security suite particularly attractive. For those needing advanced scalability and policy-driven access for wide-reaching operations, Broadcom’s solutions are well-suited.

Security	Strong Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

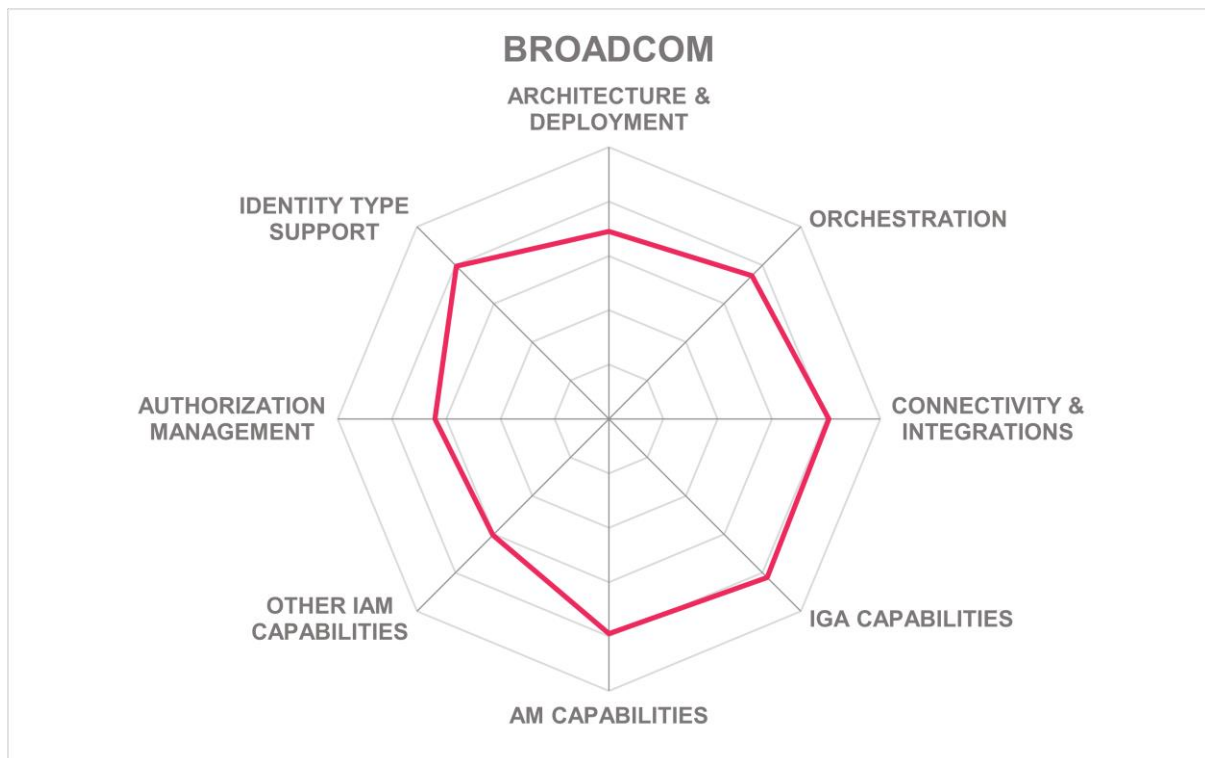
Table 4: Broadcom's rating

Strengths

- Strong foundation based on former Symantec and CA portfolios.
- Ability to deliver leading-edge managed services and large-scale on-premises deployments based on VMware capabilities.
- API-first, multi-tenant architecture for the modernized components.
- Rich service offering for global enterprises.
- Strong IAM capabilities across major areas.
- Proven infrastructure for complex use cases.
- High scalability for large deployments.
- Strong support for industry standards.
- Support a way forward for traditional CA Technologies customers via integration of legacy IAM solutions with SSP.

Challenges

- Professional services required for deployment.
- Focus on large organizations, solution not well-suited for mid-market and smaller organizations.
- Not yet all capabilities provided by SSP, some extended features require legacy support.
- Further user interface modernization needed.



Cross Identity – Cross Identity

Cross Identity, established in 2000 and headquartered in India, positions itself as a full-service provider in the Identity Fabrics segment. Supported by venture capital, the firm delivers a suite of identity and access management solutions including Cross Identity and Access Sphere. Their solutions focus on providing feature-rich, converged identity services supporting a broad range of deployment scenarios, spanning on-premises, cloud, and hybrid environments.

Cross Identity offers a comprehensive identity and access management platform that integrates Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM), and Cloud Infrastructure Entitlement Management (CIEM). The solution is architected on a microservices framework and supports various deployment models, including container-based platforms Kubernetes and Docker. Its functionality includes role mining, access certification, integrating with prominent IGA tools such as SailPoint and Micro Focus, and offering a broad set of authentication methods including FIDO 2.0.

Cross Identity focuses on a strong convergence strategy, unifying a comprehensive IAM suite under a single source code. Its support for a wide range of integrations, as demonstrated by connectors for systems such as SAP, Microsoft EntraID, and AWS, promising rapid deployment. However, the platform could further enhance its user interface, which appears somewhat dated compared to market expectations. On the other hand, the user interface is integrated across all product capabilities. Cross Identity builds on a common set of AI services that are already used for various capabilities such as delivering baseline ITDR (Identity Threat Detection and Response) services. However, expanding AI-based capabilities could position Cross Identity even more competitively against leaders leveraging advanced analytics across more use cases.

The platform serves a global clientele with a considerable presence in North America, APAC, and EMEA regions. Industries such as finance, retail, and healthcare feature prominently among their clients. Given its capability to cater to mid-market and enterprise segments with a need for adaptable, identity-centric solutions, Cross Identity appeals to organizations seeking a feature-rich yet flexible and lean approach to managing access controls across hybrid ecosystems.

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

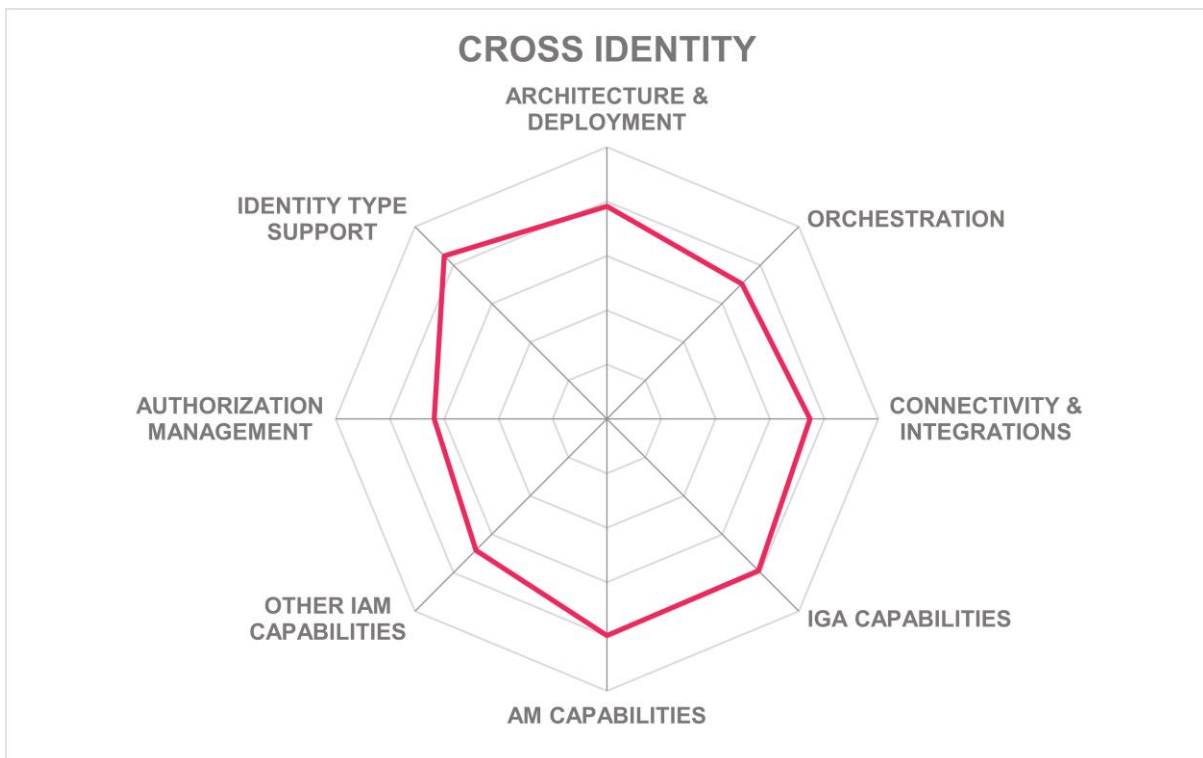
Table 5: Cross Identity's rating

Strengths

- Comprehensive IAM suite on one platform.
- Strong integration capabilities with leading IGA and PAM solutions.
- Supports multitenant cloud as well as on-premises deployments.
- Contextual adaptive authentication methods available.
- Supports key standards including FIDO, SAML 2.0, and OAuth2.
- API-first design permits extensive customization and configuration.
- Broad range of automation capabilities and support for low-code orchestration workflows.

Challenges

- Integrated user interface across all components, but may benefit from further modernization in design.
- Common AI capabilities used in some areas, but advanced analytics could be further developed.
- Limited out-of-the-box support for emerging standards including Verifiable Credentials, but flexible integration and extension capabilities.
- Manual intervention required for some security orchestration tasks.



CyberArk – Identity Security Platform

CyberArk, established in 1999 and headquartered in Newton, Massachusetts, stands as a major player in the domain of identity security. Recognized amongst the leaders in the Identity Fabrics market segment, CyberArk focuses on convergence in managing identity and access across diverse environments by delivering a unified Identity Security platform. Its solutions are categorized into standard and enterprise editions, tailored to meet the specific needs of workforce users, IT administrators, developers, and machine identities. CyberArk is a global leader, with thousands of customers across various regions, including a significant presence in the Americas and EMEA.

The CyberArk Identity Security Platform is engineered to address critical identity security challenges. The platform provides extensive capabilities such as Privileged Access Management (PAM) and identity lifecycle management, supporting both human and machine identities, the latter backed by the acquisition of Venafi. Their seamless integration capabilities are enhanced by collaboration with over 265 technology partners as well as thousands of connectors available for diverse applications. Compliance highlights include support for standards including FIPS 140-2, ISO/IEC 27001, and SOC 2, ensuring strong data protection. Their solution builds on a modular architecture that allows easy integration of additional capabilities.

CyberArk's platform distinguishes itself with a wide set of capabilities in access control, device security, and privilege management, making it an industry leader in zero-trust environments. The platform has been enhanced for supporting automation and orchestration through No-Code integration. However, while it has made significant progress in expanding its IGA capabilities, further refinement is required to fully capitalize on their acquisition of Zilla Security. Another area for improvement is the user interface unification, which is underway to enhance the overall administrative experience.

The CyberArk Identity Security Platform is particularly relevant for organizations seeking protection of both human and machine identities. Industries with a strong focus on regulatory compliance and those operating in hybrid environments can benefit significantly from their solutions. The platform's extensibility and robust partner ecosystem make it well-suited for large enterprises. Companies already leveraging CyberArk's PAM features may find significant advantages in expanding their capabilities with CyberArk's integrated solutions.

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

Table 6: CyberArk's rating

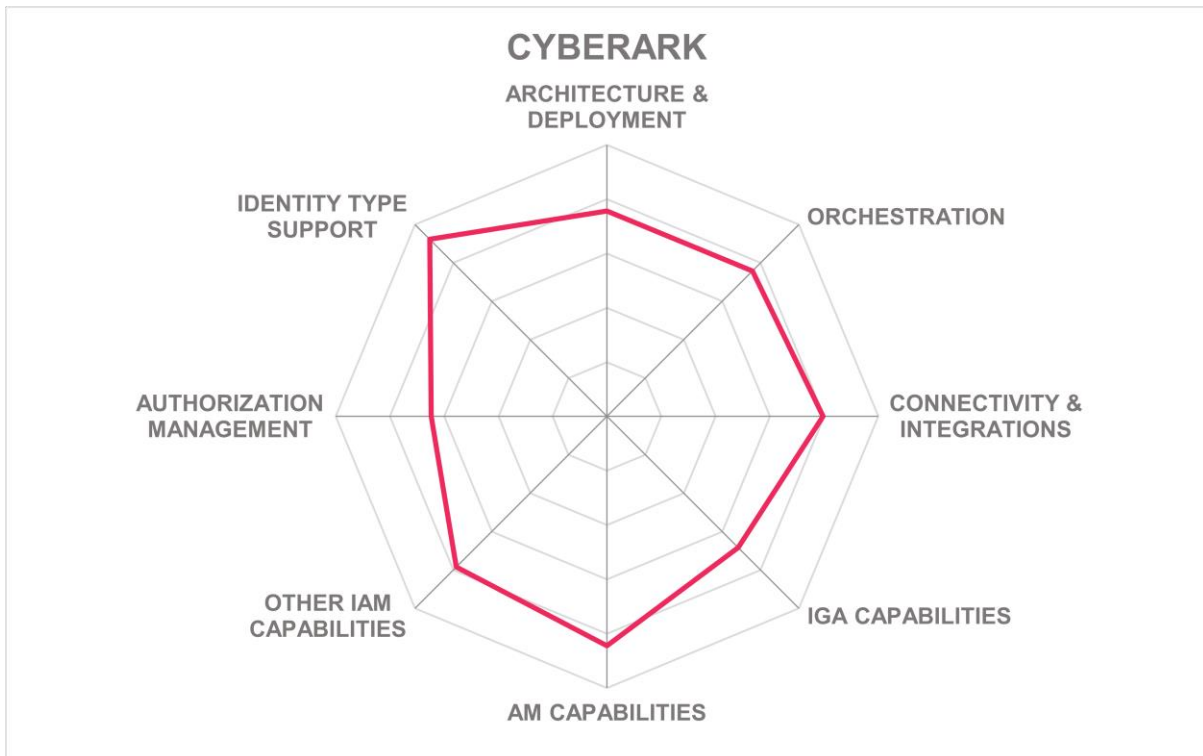
Strengths

- Comprehensive access management platform.
- Extensive third-party interoperability.
- Advanced privilege control capabilities for human and machine identities.
- Large, global partner ecosystem.
- Flexible deployment scenarios, moving to IDaaS.
- End-to-end identity management across all identities and major IAM areas.
- Unified access policies and workflows across the platform.
- Enterprise-grade security compliance.

Challenges

- Need for UI consistency and integration for recent acquisitions.
- Limited standalone IGA market presence yet.
- Dependencies on multiple product integrations.
- Must demonstrate its ability to expand PAM customers into Identity Fabric customers.

Leader in



Delinea – Delinea Platform

Delinea, with its predecessors established in 2004 and headquartered in the United States, positions itself as an entrant into the Identity Fabrics landscape through its combination of PAM and IGA solutions. With the integration of Thycotic and Centrify under TPG Capital ownership, Delinea provides secure and managed privileged access, focusing on heterogeneous IT environments. The Fastpath acquisition added IGA to that. Serving medium to large enterprises globally, Delinea's platform aims to provide full identity and access management, based on a product suite that includes functionalities from the Vaulting from Secret Server to Privileged Remote Access and IGA.

Delinea's product suite has its roots in the PAM market, delivering capabilities such as credential management, strong user authentication (MFA) and authorization of privileged access, password vaulting, and session monitoring. The platform supports integration with AWS, Microsoft Azure, and Google Cloud Platform, ensuring secure access across a wide range of infrastructures. The unified suite also includes CIEM for entitlement management, PAM for controlled privilege elevation, and DevOps Secrets Vault, enhancing both security and operational efficiency. Delinea offers identity threat protection with continuous discovery, capable of identifying anomalies, assessing risks, and providing real-time insights.

The Delinea Platform comes with a modern UI. The solution also provides real-time control over privileges. The product's centralized policy management across hybrid environments helps in simplifying the complexity of multi-vendor integrations, although the integration of IGA into a comprehensive suite is not yet fully completed. The need for unifying its administrative interface presents an area for further improvement. However, the platform's intelligence-driven, rule-based policy automation remains a standout feature.

Delinea's targets are medium-sized to large enterprises across all industries, with strong presence in North America and substantial presence across EMEA and APAC regions. The product is well-suited for organizations still lacking a centralized PAM strategy, serving as a trusted go-to for secure privileged access across hybrid multi-cloud environments. Its robust integration capabilities with popular systems and support for frameworks such as PCI-DSS and ISO 27001 make it particularly relevant for industries with stringent compliance requirements.

Security	Strong Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

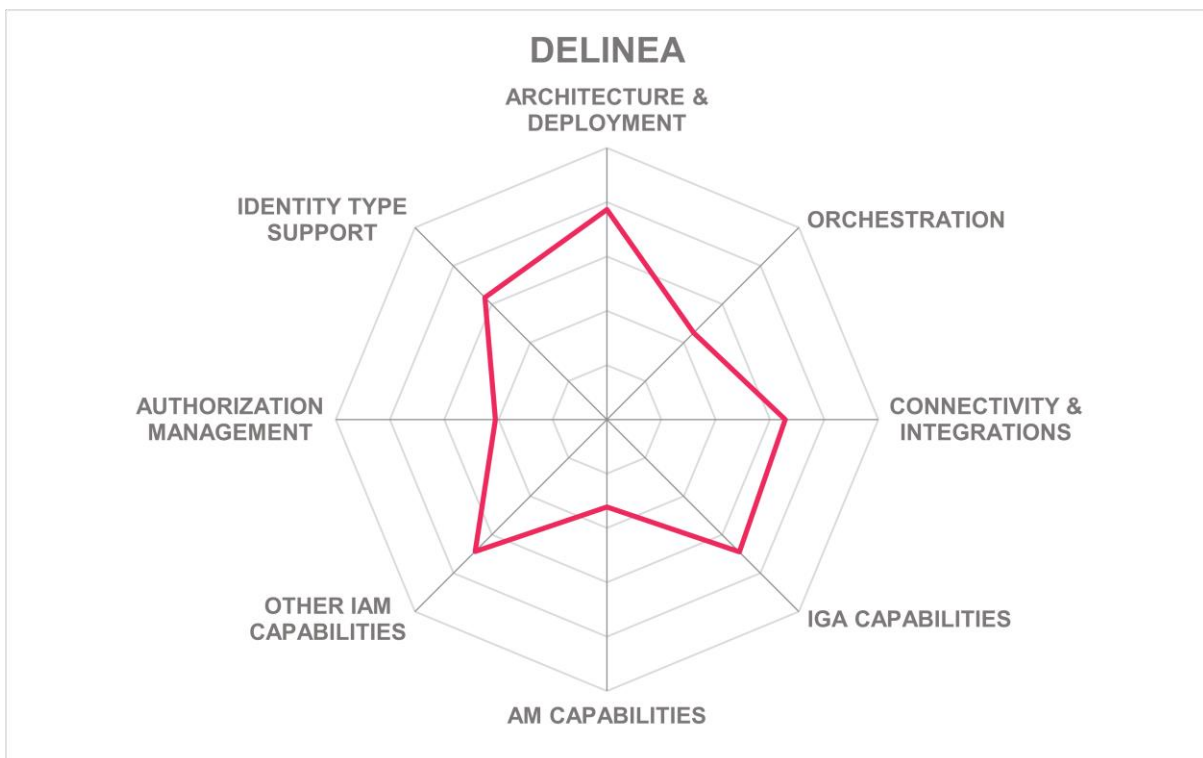
Table 7: Delinea's rating

Strengths

- Full-featured privilege management and monitoring.
- Seamless integration with cloud platforms.
- Dynamic policy management and centralized control.
- Advanced DevOps secret management.
- Flexible identity threat protection.
- IGA providing a good set of identity lifecycle and access governance capabilities.
- Continuous cloud entitlement discovery.
- Global coverage and customer base.

Challenges

- Need for further UI integration across the platform.
- Good, but not leading-edge IGA capabilities yet.
- Integration of recent acquisitions remains ongoing.
- No support for Access Management.



EmpowerID – EmpowerID

EmpowerID is an established player in the Identity and Access Management (IAM) domain, founded in 2005 and headquartered in Dublin, Ohio. The company has grown from a traditional provider of IGA and PAM solutions into a provider of a comprehensive Identity Fabric platform. The platform is powered by a leading-edge integration platform that allows integration of EmpowerID services and other vendor's IAM solutions. It also delivers CIEM capabilities as well as some Access Management capabilities with good standards support including OAuth2, OIDC, FIDO2, and others. While the core platform still ships with its own IdP, most deployments plug EmpowerID into other IdPs such as Microsoft Entra ID or Okta. EmpowerID is known for its distinctive use of AI-driven technologies and strives to revolutionize IAM solutions by reducing complexity and operational costs, making it a complement to other vendor's solutions and highly scalable.

EmpowerID stands out with its microservices-based architecture that leverages AI for intelligent orchestration of identity services. This platform is particularly focused on automating complex identity operations, including user onboarding, lifecycle management, and adaptive access controls. Key capabilities include its Zero Trust security model which employs dynamic access policy enforcement and its pioneering Low-Code/No-Code orchestration for streamlined identity workflows. Additionally, EmpowerID's integration supports standards such as SCIM, SAML, and OAuth, facilitating interoperability with systems such as Microsoft Entra ID and ServiceNow.

EmpowerID recently released additional innovative AI and authorization capabilities including their Data Collector & CRUD service that significantly reduces the effort for target system integrations. This allows relying on a common integration platform and AI-support for analyzing the APIs and data model of the target systems. A challenge is that certain advanced scenarios still benefit from developer level tuning. The remaining legacy .NET workflow engine and UI is gradually being retired in favor of the new identity fabric graph workflow engine.

EmpowerID is particularly attractive to mid-sized and large enterprises seeking a flexible Identity Fabric with strong automation capabilities and the ability to neatly integrate the EmpowerID services with other vendor's IAM solutions that are already in place into a comprehensive Identity fabric. Its suite of tools and AI-centric approach suits organizations requiring integration with both legacy and modern systems, ensuring compliance with GDPR and CCPA. Companies with a substantial Microsoft ecosystem and those needing enhanced automated workflows might find EmpowerID especially beneficial.

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



Table 8: EmpowerID's rating

Strengths

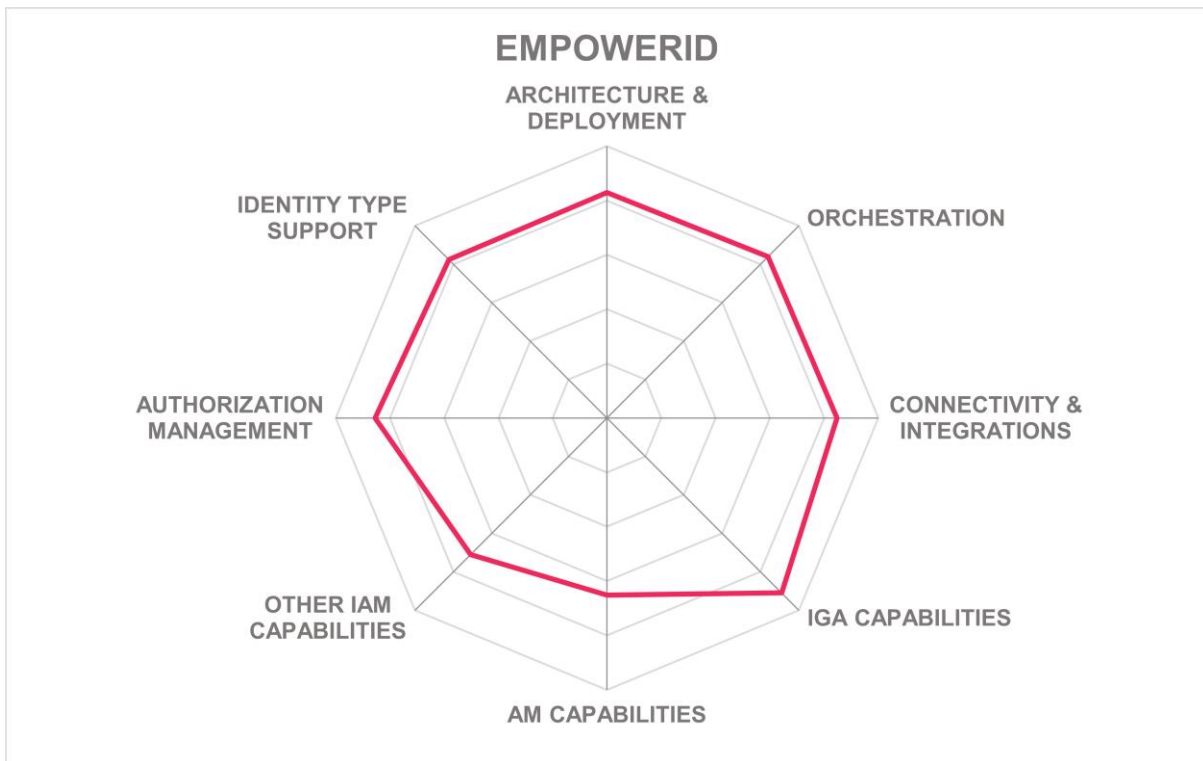
- Feature-rich IAM platform with advanced AI capabilities.
- Integrates with multiple enterprise systems, utilizing an AI-powered integration approach.
- Flexible Low-Code/No-Code workflow support.
- Strong Zero Trust security with dynamic policy enforcement.
- Target system integration also can be used by other vendor's IAM solutions.
- Supports multiple identity types and relationships.
- Extensive API and standards support for integration.
- Real-time analytics and risk management features.
- Innovative AI-driven automation for identity operations.

Challenges

- Complexity in customization might require developer skills.
- Small vendor size could affect perception in global markets.
- Limited marketing and pricing clarity for components.
- Initial setup requires deep IAM understanding.

Leader in





Exostar – Access: One

Exostar, a provider of secure, compliant cloud-based solutions that enable industry collaboration, was founded in the year 2000 with its headquarters situated in Herndon, Virginia, USA. The company, with additional offices and development centers in the UK, India, and Australia, is positioned in a niche by focusing on the combination of enhancing collaboration, information sharing, and supply chain management across highly regulated industries. Through the acquisition of Pirean in 2018 and Robot Morning and ComplyUp in 2024, Exostar has significantly elevated its portfolio, underscoring its commitment to secure, compliant collaborations in industries like defense, aerospace, life sciences, healthcare, and financial services, reaching markets across North America, Europe, Latin America, and the APAC region.

Exostar's Access: One product, part of the Exostar Platform's Secure Access Module suite of Identity and Access Management (IAM) solutions, is their solution for IGA, CIAM, and Access Management. The product offers capabilities for both consumer and enterprise access management services, enabling organizations to rapidly deploy customized IAM services using its No-Code workflow builder. Access: One has strengths in API access management and supports standards such as OpenID Connect, OAuth, Financial Grade API, and more, thereby ensuring a high level of security compliance. Notable capabilities include passwordless authentication, thorough identity proofing, and validation services. Exostar also is demonstrating good progress in their workforce IGA capabilities, adding features such as policy-based authorization support, role management, and flexible access recertification.

What sets Exostar apart is its strategic focus on highly regulated sectors including FedRAMP Moderate equivalence. Its strong suite of authentication options, certified compliance with various standards including ISO 27001 and ITAR, and partner ecosystem are significant positives. However, the platform still exhibits room for improvement, particularly in the areas of workforce IGA features advanced capabilities in analytics and access intelligence. It also can benefit from broader and deeper adoption of AI-backed capabilities. While Exostar provides a solid IAM foundation, its plan to increase R&D spending could augment its competitive edge in the evolving market.

Exostar predominantly targets organizations within defense, life sciences, and aerospace, offering them a tailored solution in those rigorously regulated industries that need high assurance identity services. The geographical coverage spans North America and Europe predominantly, with growing traction in Latin America and the APAC region. For businesses seeking a streamlined, secure IAM experience within these sectors, Exostar is worth considering, especially for those also building on the Exostar supply chain management and collaboration solutions.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive



Table 9: Exostar's rating

Strengths

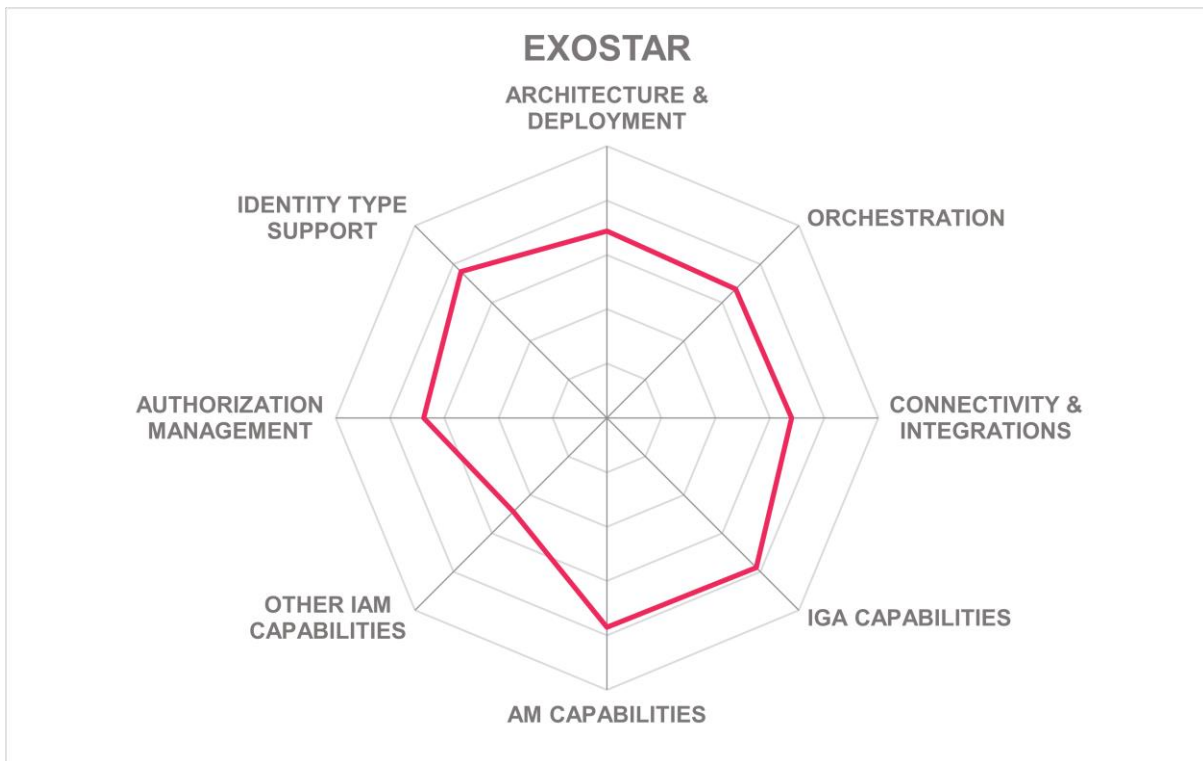
- Certified compliance with multiple security standards such as ISO 27001.
- Multiple authentication options offered, including FIDO 2 support. Integrates high assurance identity proofing.
- Good federation and session management.
- Solid workforce IGA capabilities.
- Well-established in highly sensitive industries.
- Well thought-out roadmap for adding further capabilities in orchestration and NHI Management.

Challenges

- Analytics and intelligence capabilities need enhancement.
- Improvement needed in market visibility.
- Still limited use of AI, but roadmap plans for enhanced usage.
- No PAM or CIEM features.

Leader in





IBM – Security Verify

IBM, headquartered in Armonk, New York, was established back in 1911. IBM Security Verify offers a comprehensive set of Identity Fabric capabilities. This solution, encompassing Access Management, Identity Governance, and PAM, is designed to meet the needs of enterprise environments. Through their Verify SaaS platform and on-premises options, IBM provides a broad portfolio of IAM capabilities, including good support for non-human identity management requirements through their recent acquisition of HashiCorp.

IBM Security Verify is based on a proven portfolio of solutions, some of these stemming from legacy IAM, that addresses key areas of identity management, from Access Management with risk-based authentication to Identity Governance and analytics. The platform comes with integration capabilities to various cybersecurity solutions such as IBM QRadar. This also enables IBM to deliver a good set of capabilities for ITDR (Identity Threat Detection and Response) and ISPM (Identity Security Posture Management). It also provides support for a wide range of standards such as OpenID Connect and SAML. IBM Security Verify has many integrations with third-party solutions, such as with Microsoft Entra ID, SAP, and Google Apps.

IBM has a partnership with Thycotic for PAM. The introduction of Low-Code/No-Code orchestration capabilities aim to streamline identity services. Nonetheless, a dependence on OEM components and added complexity in hybrid deployments are areas requiring attention. Moreover, the need to use separate interfaces for some legacy applications hinders the user experience. Challenges such as these require further development and simplification across the portfolio.

IBM mainly draws interest from large or highly regulated enterprises with complex identity requirements. The solution’s global coverage coupled with its ability to support complex environments involving many legacy systems makes it suitable for organizations with diverse IT landscapes. Sectors such as finance, government, and healthcare, where compliance and security are priority and legacy integration a common challenge, will find IBM Security Verify particularly appealing. These capabilities, backed by IBM's extensive partner ecosystem, make it a solution worthy of consideration as foundation of an Identity Fabric.

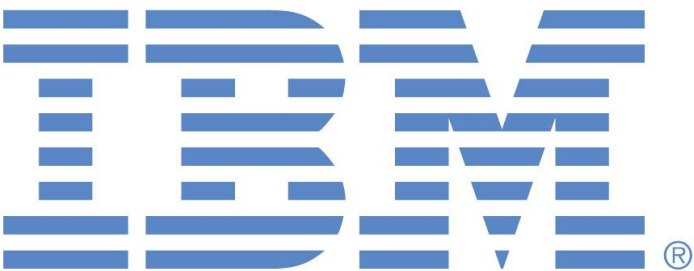
Security	Strong Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

Table 10: IBM's rating

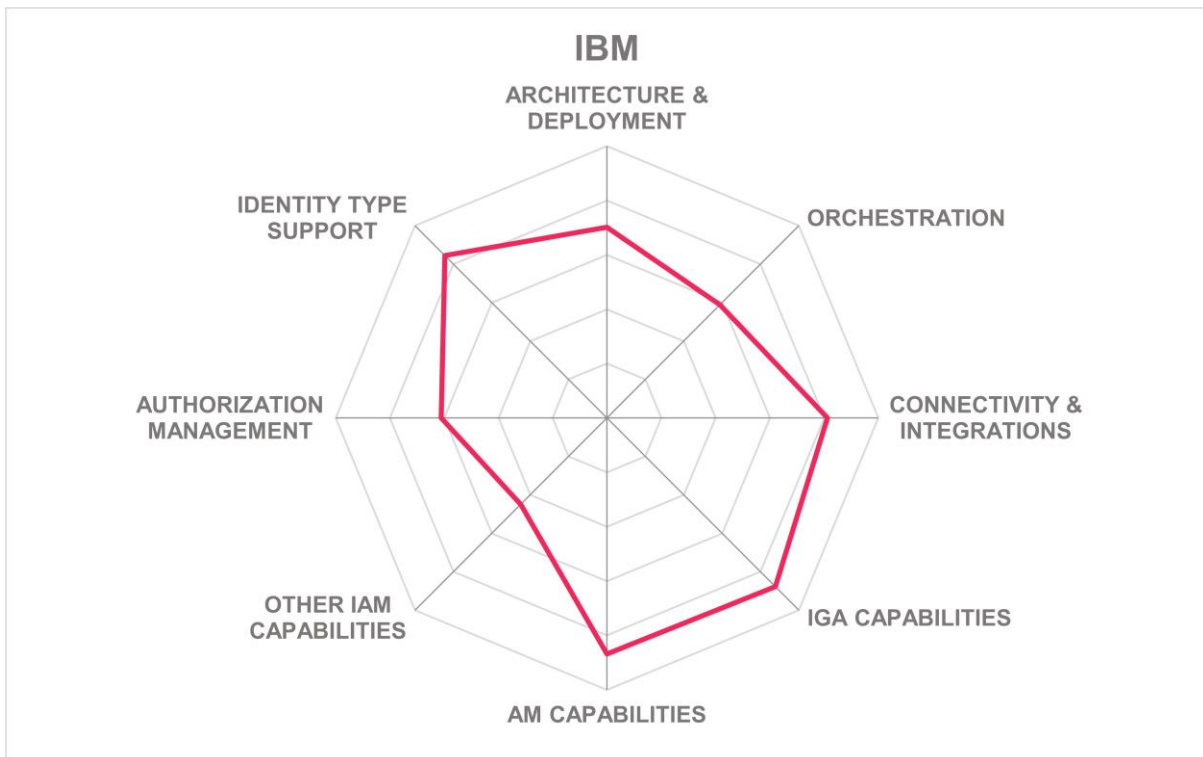
Strengths

- Broad capabilities in access management, IGA, and PAM.
- Cloud-native architecture for the modern components of the solution.
- Strong legacy support via integrations to a wide range of legacy target systems.
- Integration with IBM security solutions including QRadar.
- Proven scalability and reliability.
- Global partner ecosystem.
- Strong NHI management support via HashiCorp.

Challenges

- PAM component provided by OEM Thycotic.
- Complexity due to hybrid deployment options.
- Advanced features incur extra costs.
- Full set of capabilities might require IBM on-premises IAM components.

Leader in



Microsoft – Entra ID

Founded in 1975 and headquartered in Redmond, Washington, Microsoft stands as a pivotal entity in the technology landscape. The Microsoft Entra product suite, part of Microsoft's vast portfolio, provides the components for their Identity Fabrics solution. Entra's capabilities extend across securing digital identities and access management. Microsoft's commitment to providing robust, standards-based solutions has moved it to the forefront of the identity and cybersecurity sectors.

Microsoft Entra offers a broad suite of capabilities encapsulating identity management, governance, and protection. It supports zero trust principles through its conditional access features, based on the Continuous Access Evaluation Protocol (CAEP). The suite supports API-driven administration using Microsoft Graph API and supports the following: , OAuth, OIDC, and SAML. Entra ID and ID Governance can connect with many third-party systems and include features such as privileged identity management.

Microsoft Entra is distinguished by its innovation in AI-driven security management, leveraging tools such as Microsoft Security Copilot for AI-driven insights. It boasts extensive capabilities in managing both human and non-human identities, securing complex and varied application ecosystems in the cloud and on-premises. However, despite its broad feature set, certain administrative interfaces, such as Permissions Management, are not fully integrated. Additionally, while it excels in access management, the depth of its provisioning capabilities for legacy applications could be improved.

Microsoft Entra is well-suited for enterprises seeking powerful identity management solutions, particularly those already engaged with the following Microsoft services, Azure and Microsoft 365. Its effective zero trust and risk-based conditional access features cater to security-conscious organizations. Large enterprises will find value in their ability to unify identity management across cloud and on-premises environments, promoting efficient IT operations. As organizations navigate complex security needs, Entra can safeguard digital interactions and secure identities across many different platforms, making it a key contender in Identity Fabrics.

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

Table 11: Microsoft's rating

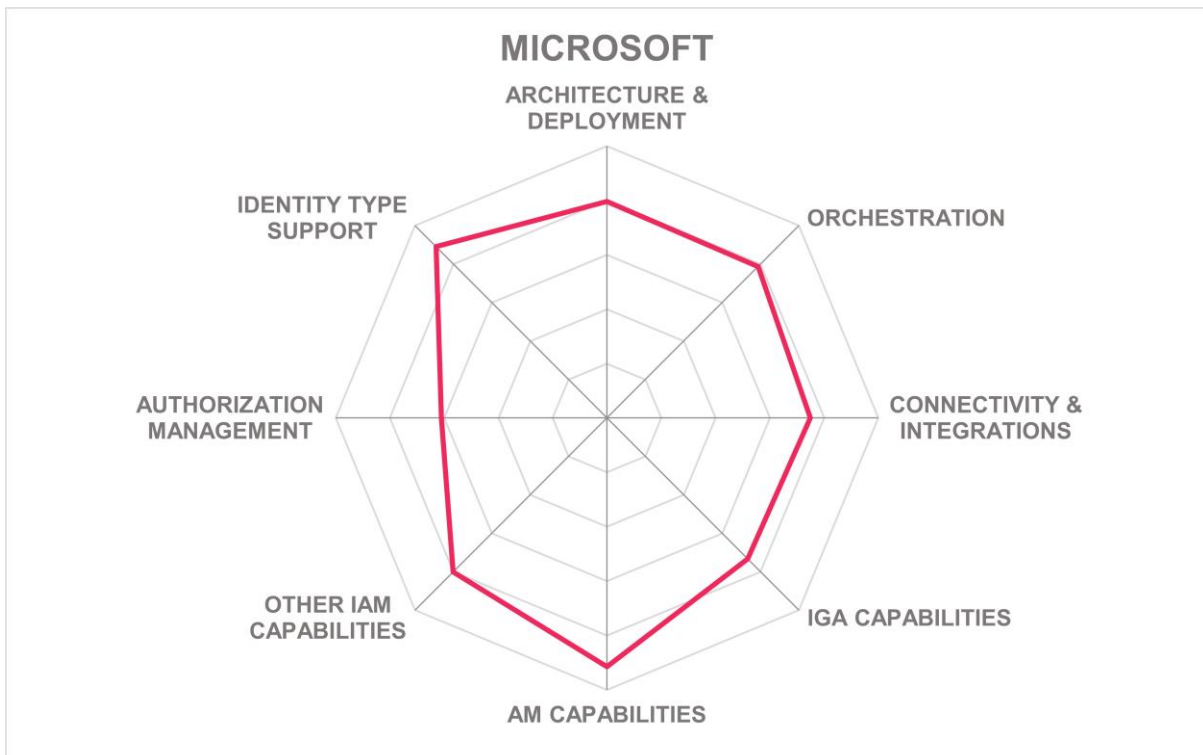
Strengths

- Broad standards support and compliance.
- Leading-edge access management capabilities.
- Good level of identity governance features.
- Vast user base and global reach.
- Advanced conditional access solutions.
- Strong partnership and integration ecosystem.
- Extensive use of AI for threat detection and supporting administrators.

Challenges

- Full integration of administrative interfaces needed.
- Limited depth in legacy system provisioning.
- Public cloud-only deployment may limit certain users.
- Good, but not leading-edge IGA capabilities that would deserve further innovation.

Leader in



Monokee – Monokee

Monokee, established in 2017 and headquartered in Italy, is emerging as an innovative player in the identity and access management sector. Their focus is on the orchestration and integration of identity solutions, and the company positions itself as both a service provider and enabler, enhancing ecosystem interoperability rather than delivering a traditional turn-key solution. Their operations extend beyond Italy, notably establishing a presence in the US, reflecting ambitions to play a global role on the IAM and identity fabrics market.

Monokee's platform is characterized by its modularity, with a focus on Access Management (AM) and IGA use cases. It boasts adaptive access and contextual authorization, complying with the standards SAML and OAuth 2.0. The Visual Identity Orchestrator (V.I.O.) stands out as a tool by simplifying user journey designs and improving operational efficiency. Security capabilities include SSL termination and OAuth 2.0 authenticated API-based communications. The solution supports several authentication methods, including FIDO2, OAuth 2, OIDC and various others, and can be deployed in Docker, Podman, and Kubernetes environments.

Monokee differentiates itself with strong orchestration capabilities and a foundational emphasis on being an API-first, cloud-native, and containerized orchestration platform instead of a full-featured IAM solution. However, it is more of a base to be developed upon, rather than a ready-to-use IAM solution, while this is a benefit for customization, it is a barrier for standardized use-case delivery. While the user interface is modern, its development-heavy nature may limit immediate attractiveness for end users. Furthermore, documentation and full IGA capabilities remain development targets.

Monokee's platform appeals particularly to enterprises and government entities requiring integration solutions for existing IAM and for delivering new capabilities in integration with digital services. Its flexibility may make it a suitable choice for organizations in need of a scalable, integration-driven platform for extensive identity workflows. The solution is particularly relevant for industries in Europe and North America, with emphasis on manufacturing and public sector clientele. Its ability to model complex user journeys and deliver authentication options will be of interest to organizations seeking adaptable identity frameworks.

Security	Strong positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

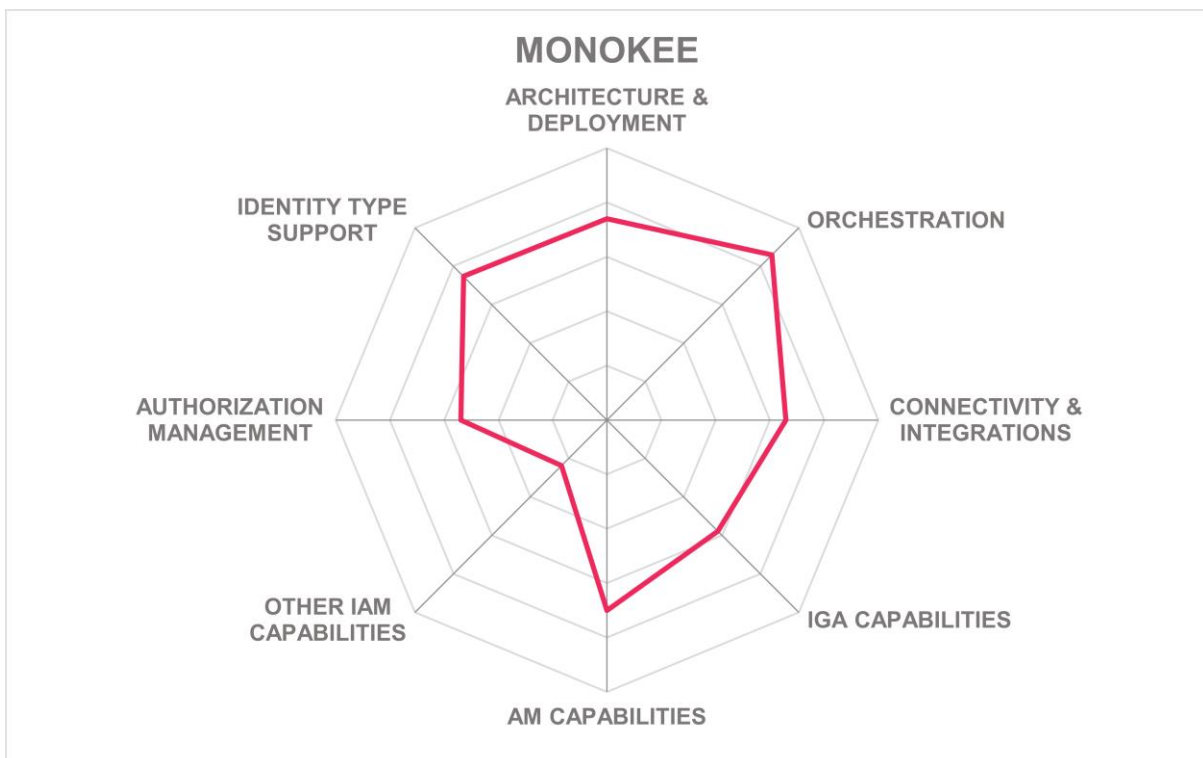
Table 12: Monokee's rating

Strengths

- Strong integration capabilities across IAM, FRIP, CIAM, and other solutions.
- Supports a wide range of authentication methods.
- Modular and scalable microservices architecture.
- Flexible deployment options including on-premises and cloud.
- Visual tool for designing user journeys.
- Adaptive access controls with contextual authorization.
- Focused on API-first integrations, delivering an orchestration platform for building Identity Fabrics.

Challenges

- User interface design focused on administrators and developers.
- Not yet a full IGA solution.
- Lacking PAM capabilities.
- Absence of comprehensive documentation.
- More development-heavy than out-of-the-box solutions.
- Limited immediate appeal to end-users, being developer-focused.



Okta – Customer Identity Cloud & Workforce Identity Cloud

Founded in 2009, Okta is a prominent player in the identity and access management space, based in San Francisco, USA. The company positions itself as an identity security firm. Okta's Secure Identity Platform delivers identity orchestration for both modern and traditional systems, supporting a breadth of applications and APIs. Their solution supports a broad range of identities including human and non-human entities.

Key features of Okta's solutions include real-time threat detection and dynamic access policies powered by machine learning. Okta Workflows provides No-Code orchestration to streamline identity-centric processes. Okta's ability to consume and act on various risk signals enhances its security posture, allowing for immediate session terminations or access modifications. For instance, Okta can evaluate policy violations and enforce universal logouts or other access controls. While Okta excels in Access Management, the IGA and PAM capabilities are not leading-edge, but can provide a modern, lean solution for these areas.

Okta stands out with its many integrations: offering upwards of 8,000 pre-built connections within its Okta Integration Network, covering ITSM tools such as ServiceNow, and extending into SIEM systems such as Splunk and Microsoft Sentinel and integrations to many other types of solutions such as Unified Endpoint Management (UEM). However, integration is primarily API based, imposing limitations for legacy systems such as mainframes. Despite these strengths, further alignment between Okta and Auth0 platforms could enhance user interface coherence. Their extensive yet separate customer identity solutions might benefit from a more unified approach. Nevertheless, Okta's strong AI capabilities in threat prediction and prevention remain compelling.

Targeting large enterprises, Okta serves those looking to secure identity structures across all industry sectors. The platform is particularly interesting for organizations seeking a lean identity fabrics approach that integrates securely across modern systems and infrastructure. Okta's support and active involvement in the core working groups for standards including OpenID and the emerging IPSIE standard, but also many others, and integrations with platforms including AWS Secrets Manager make it an interesting choice in the market.

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



Table 13: Okta's rating

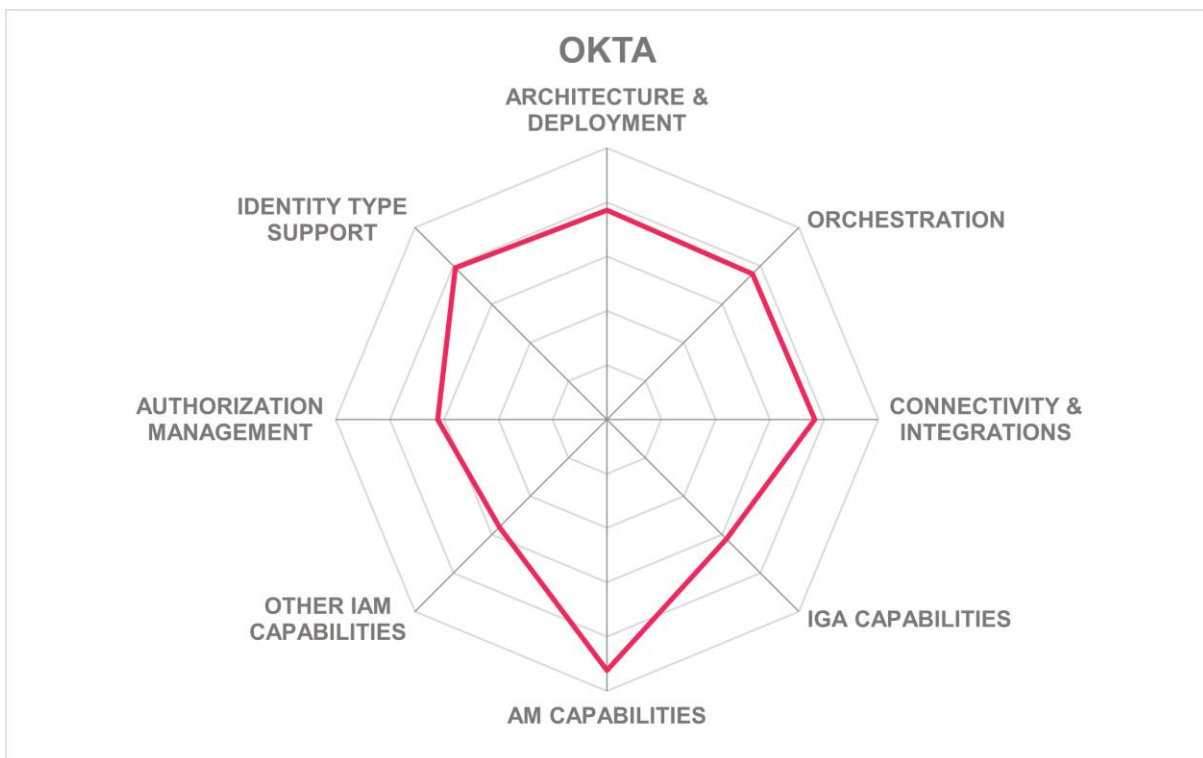
Strengths

- Strong No-Code orchestration with Okta Workflows.
- Extensive integration network across enterprise systems, including areas such as ITSM or UEM.
- Built-in AI capabilities for threat detection.
- Real-time session control and risk adaptation.
- Support for different identity types, including some NHI support.
- Competitive CIAM solutions with customizable solutions (Auth0).
- Powerful no-code to pro-code orchestration capabilities and extensibility.

Challenges

- Need for tighter integration between Okta and Auth0.
- User interface differences across platforms.
- IGA and PAM capabilities are not yet leading-edge.
- Many connectors, but some limitations in connecting to legacy systems.

Leader in



One Identity – One Identity Manager, OneLogin, Safeguard

One Identity, established in 2016 and headquartered in Aliso Viejo, California, is a renowned player in the IAM market. The vendor offers a broad suite of solutions that addresses the comprehensive needs of Identity Fabrics, covering IGA Access Management, and PAM. As a significant IAM provider, One Identity has enhanced its portfolio over time, including the acquisition of OneLogin to expand its capabilities across workforce and consumer use cases.

One Identity delivers a broad set of functionalities, including behavior-driven governance through the integration of One Identity Manager and OneLogin. It enables just-in-time (JIT) privileges with its Safeguard and Active Roles, dynamically managing privileged access. The solution supports a wide spectrum of standards and integrations, offering interoperability with systems such as SAP Access Control, Microsoft 365, and Microsoft Entra ID. The company empowers organizations to manage identities efficiently while ensuring compliance with GDPR and SOX regulations.

One Identity's product differentiation lies in its comprehensive coverage across IAM domains. Their strategic acquisitions and subsequent, yet ongoing integration work have strengthened their standing, particularly with the capabilities of OneLogin for access management including identity federation and passwordless MFA. However, the full integration of components and modernization towards a full IDaaS solution within their suite remains a work in progress, as they address the ongoing challenge of unifying diverse systems and enhancing integration depth through solutions such as PAM Essentials.

One Identity primarily targets mid-market to large enterprises seeking a strategic platform in the Identity Fabrics domain. Its solutions are particularly beneficial for organizations operating in environments that are looking for a wide range of features across the various IAM domains. Companies with significant investments in SAP or Microsoft looking for powerful identity lifecycle management will find One Identity's solution valuable. With continuous advancements toward an integrated cloud-based Identity Fabric, the vendor presents a compelling choice for organizations aiming to embark on or enhance their identity management journey.

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

Table 14: One Identity's rating

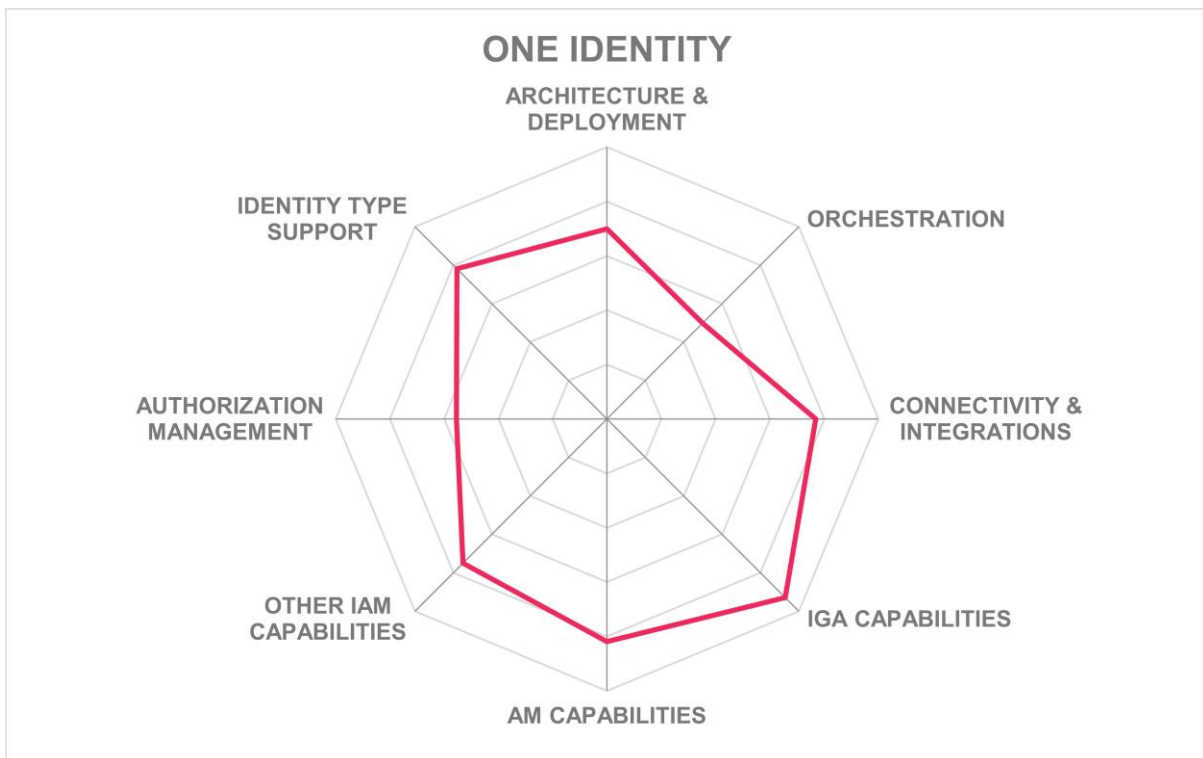
Strengths

- IAM suite with a wide range of features spanning IGA, Access Management, PAM, and Directory Security.
- Enhanced access management via OneLogin, including passwordless MFA.
- Behavior-driven governance capabilities.
- Good SAP environment management.
- Just-in-time privileges via Active Roles integration.
- Extensive global partner ecosystem.

Challenges

- Full component integration still in progress.
- Further integration depth needed for Starling Connect.
- Balancing varied licensing models.
- Modernization towards a comprehensive IDaaS architecture still in progress.

Leader in



Optimal IdM – OptimalCloud

Optimal IdM, established in 2005 and headquartered in the United States, is focused on Identity and Access Management solutions with its primary product being the OptimalCloud. This platform provides scalable and customizable IAM services delivered via dedicated or multi-tenant clouds, ensuring secure access to various applications through SSO technology. Beyond the US, Optimal IdM has a presence with offices in Australia. The company's approach caters to businesses looking for a good set of IAM capabilities without having to consolidate user information into a single repository, leveraging its unique virtual directory services. Their virtual directory is also used specifically for identity integration by larger organizations, complementing the customer's Identity Fabric.

Optimal IdM's OptimalCloud offers integration capabilities with prominent identity systems such as Azure Active Directory, Google Cloud, and AWS. It excels in federation support, employing common federation protocols such as SAML 2.0, OpenID Connect, OAuth2, and WS-Federation. It supports API-based management and orchestration functions, with extensive capabilities via SCIM and REST APIs for identity lifecycle management. It also supports a wide range of authenticators. Additionally, it offers dynamic and fine-grained access controls incorporating ABAC (Attribute-Based Access Control) principles, alongside custom alerting mechanisms and extensive reporting capabilities.

Distinct features of OptimalCloud include its robust virtual directory services, which avoids the need for synchronizing on-premises identities to the cloud. Moreover, its flexible directory integration and strong federation capabilities position it as an access management component for organizations. Nonetheless, UI enhancements are necessary to resolve the somewhat outdated interface, along with expanding its limited IGA and security orchestration features. Optimal IdM also lacks PAM support. Addressing these areas could significantly enhance Optimal IdM's value proposition in the market.

Optimal IdM operates primarily in North America, with some influence in the EMEA and APAC regions. Businesses seeking a reliable IAM component for access management, with strong federation capabilities and compliance with standards such as ISO 27001 and PCI-DSS, will find Optimal IdM appealing. Its solution is particularly advantageous for organizations with identity environments requiring integration across multiple directories without full consolidation.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Neutral
Usability	Positive



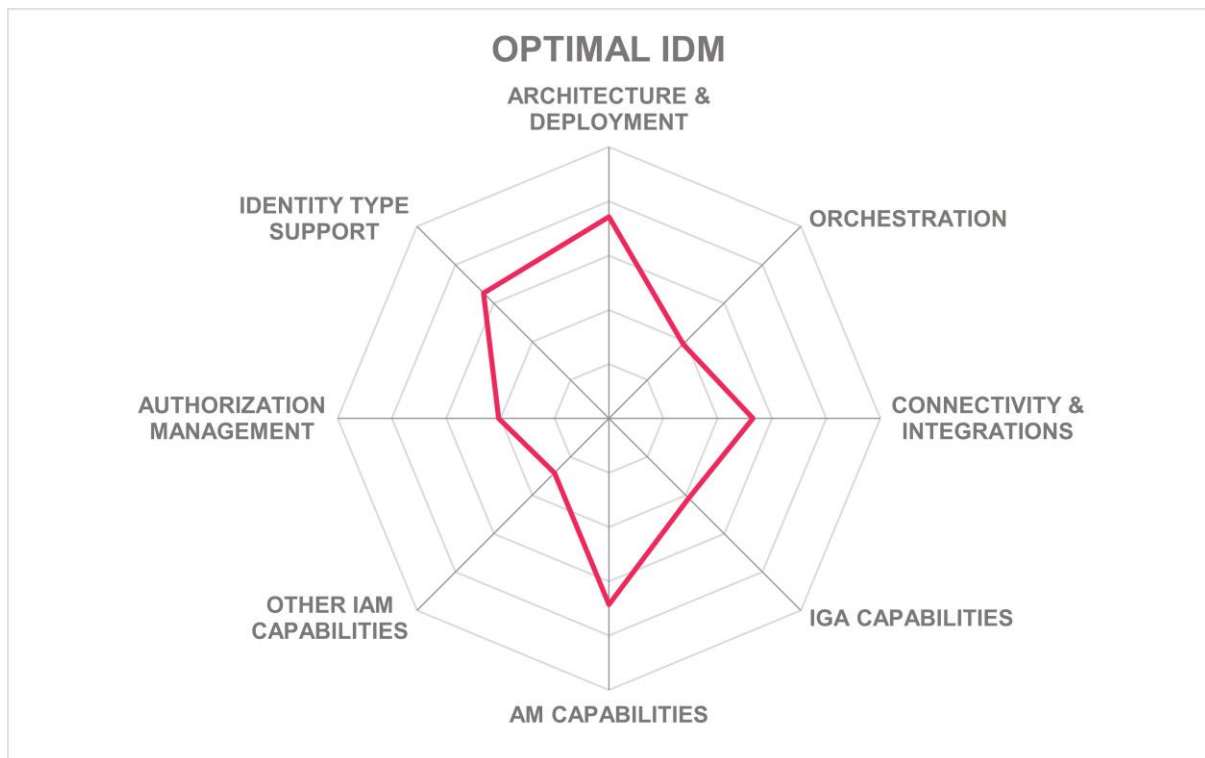
Table 15: Optimal IdM's rating

Strengths

- Strong federation support and standards.
- Flexible directory integration capabilities.
- Innovative virtual directory services.
- Dynamic access controls.
- Wide range of MFA methods are available at no extra charge
- Delivering virtual directory capabilities also to large enterprises.

Challenges

- Outdated user interface.
- Very limited IGA capabilities.
- Lack of PAM support and other broader IAM capabilities.
- Needs broader security orchestration features.
- Limited support for out-of-the-box target system connectivity.



Oracle – OCI IAM

Oracle, founded in 1977 and headquartered in Redwood Shores, California, is an established player in the IAM market. Oracle's portfolio integrates both traditional and modern IAM solutions. The Oracle Cloud Infrastructure Identity Access Management (OCI IAM) and Oracle Access Governance demonstrate the vendor's commitment to delivering modern IAM solutions, from authentication to lifecycle management. Oracle's IAM solutions cater to both its existing vast customer base and new enterprises, in particular Oracle enterprise customers, seeking identity solutions.

OCI IAM provides a strong coverage across various IAM areas, offering strong authentication supporting most common authenticators including FIDO2, Single Sign-On (SSO), and lifecycle management. Supporting over two million identity domains and aiming to manage a billion users, OCI IAM provides a powerful backbone for Oracle Cloud as well as other heterogeneous environments. Its 100% API-first approach enables integration with a wide range of solutions, ranging from line of business applications such as the Oracle eBusiness Suite to office solutions such as Microsoft 365, and customization, aligning with regulatory standards including HIPAA and GDPR. The integration with Oracle's extensive cloud and application ecosystem further enhances its capability to meet enterprise IAM requirements.

Oracle Identity and Access Management (IAM) differentiates itself by its flexible cloud and hybrid deployment scenarios, supporting major platforms such as Microsoft, Google Workspace, and AWS. It supports ABAC, RBAC, and PBAC. While the IDaaS modules come with a modern UI, the interface design and user experience of the on-premises component (Oracle Identity Governance) could benefit from modernization. There also is room to improve AI integration. Getting the full set of capabilities may require the use of Oracle legacy IAM solutions, leading to hybrid deployments and additional complexity. We expect this to change with Oracle continuing their IAM modernization journey. Oracle lacks integrated support for extended IAM capabilities such as PAM, CIEM, or NHI management, but provides a wide range of integrations to 3rd party solutions. Despite these areas for development, the platform's strengths lie in its broad target application support and strong integration capabilities across Oracle and non-Oracle applications.

Oracle's IAM solutions primarily cater to large enterprises with substantial cloud infrastructures. Its approach to identity management is of interest for organizations that require scalability and extensive integration capabilities in both Oracle-exclusive and multi-cloud environments. Particularly, enterprises that rely heavily on Oracle applications or seek heterogeneous IAM solutions will find Oracle's solutions appealing. The geographic deployment in multiple regions ensures that its services can meet the needs of global enterprises requiring high availability and compliance with various regulatory standards.

Security	Strong Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

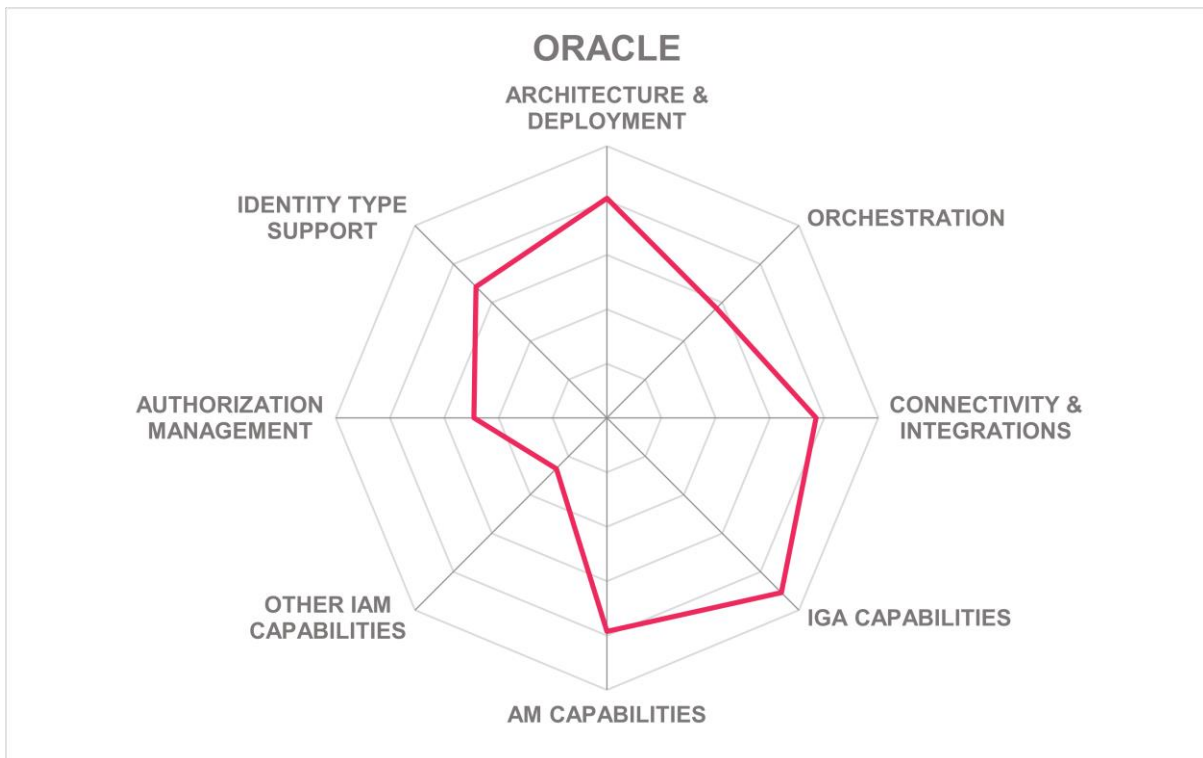
Table 16: Oracle's rating

Strengths

- Partially based on modern IDaaS solution, for instance for access management use cases.
- Good IGA capabilities, available as native cloud service.
- Strong support for Oracle and third-party environments.
- Experienced vendor in IAM.
- Good API support and orchestration capabilities.
- Robust legacy support.
- Broad authenticator support and SSO capabilities.

Challenges

- Interface modernization is needed.
- AI integration is limited.
- No out-of-the-box support for PAM use cases, but partnership with Arcon.
- Primarily oriented towards Oracle enterprise customers.
- Legacy components may still be required for some features.



Ping Identity – Platform

Ping Identity, established in 2002 and headquartered in Denver, Colorado, leads the market in Identity Fabrics. Their products and services are covering a wide range of identity and access management capabilities as well as orchestration of IAM solutions. With a complete suite of identity solutions, Ping Identity supports a variety of deployment models including single-tenant SaaS, multi-tenant SaaS, and on-premises software.

Key capabilities of Ping Identity's platform include extensive identity lifecycle management and access management features. The platform excels in orchestration, providing customers with No-Code visual flows, allowing for secure and seamless user journeys. Additionally, comprehensive integration with technology partners such as ITSM vendors and FRIP solutions supports a wide array of applications, enhancing interoperability. The AI-driven threat detection and adaptive authentication services deliver context-aware risk analysis, increasing security against evolving threats. Moreover, the platform has IGA capabilities. In access management, Ping Identity counts amongst the vendors with the broadest standards support and set of capabilities, engaging in the further development of standards. They also provide policy-based orchestration capabilities.

A standout feature of Ping Identity is its DaVinci orchestration capabilities, which offer unparalleled flexibility and control in configuring user journeys. The platform integrates features from the ForgeRock heritage, enhancing support for complex relationships and non-human identities. However, some legacy components are not fully aligned with the newer microservices architecture, suggesting room for improvement in integration and modernization. Overall, the platform's strengths across all major IAM capability areas and AI-driven operations solidify its position as a product, innovation, and market leader.

Ping Identity caters to large enterprises and organizations requiring secure identity management solutions across complex environments. Its strong presence in multiple regions ensures support for global enterprises. Key customer segments include service providers and businesses with diverse user bases, both workforce and consumer identities. The platform's flexibility makes it suitable for companies seeking to modernize identity infrastructure without extensive changes to existing systems. Ping Identity proves valuable for those needing sophisticated identity solutions and orchestration capabilities.

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

Table 17: Ping Identity's rating

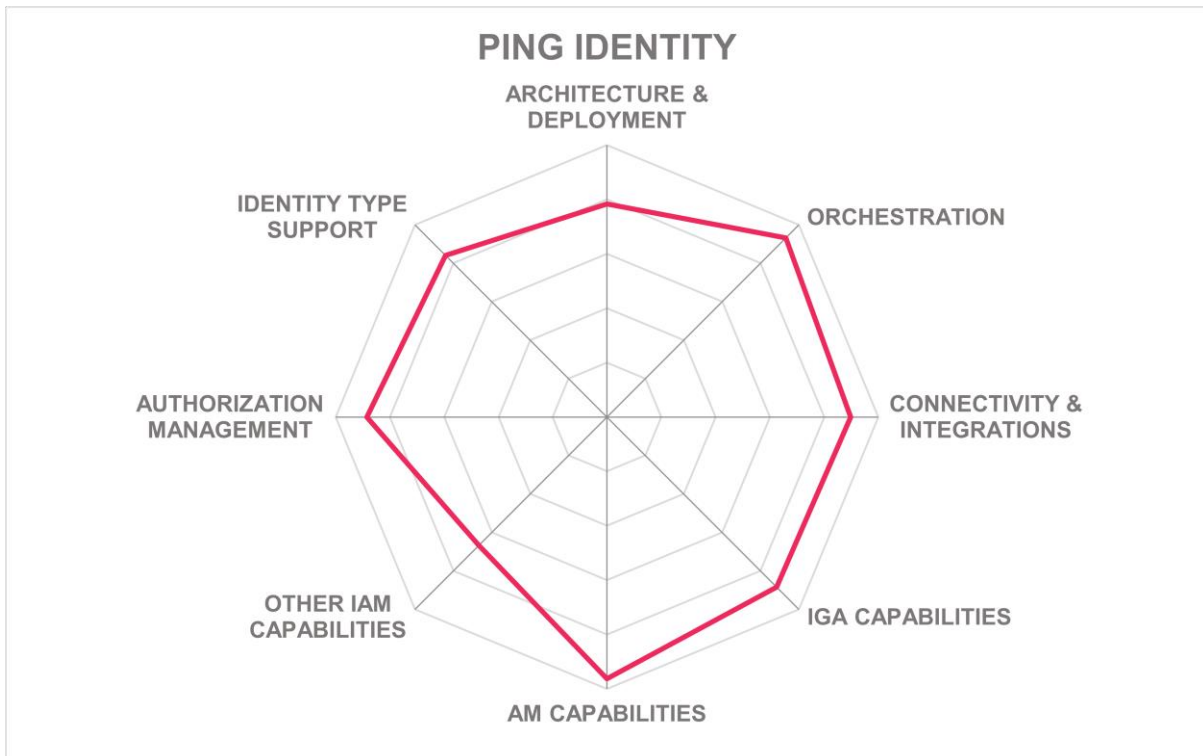
Strengths

- Comprehensive suite of IAM services.
- Leading orchestration platform.
- Strong integration with technology partners.
- AI-driven threat detection and analytics.
- Support for complex identity relationships.
- Flexible deployment options.
- Support for decentralized identity.
- Well-documented API and SDK solutions.
- Well-thought out acquisition strategy.

Challenges

- Legacy component integration not fully complete.
- Microservices alignment needed for older software components.
- Requires planning for solution component overlap.
- Broader CIEM and NHI management support would add further value.

Leader in



RSA Security – Unified Identity Platform

RSA Security was established in 1982 and is headquartered in Burlington, Massachusetts. The company holds a strong position in the identity security domain, focusing on identity protection throughout the user lifecycle. RSA has a broad identity security strategy, addressing the evolving landscape where point solutions are insufficient. Their Unified Identity Platform integrates three main product lines: ID Plus, SecurID, and Governance & Lifecycle, designed to meet the needs of organizations across a spectrum of environments including cloud, on-premises, and hybrid. This approach allows RSA to serve a wide clientele with varying identity security requirements globally.

RSA's Unified Identity Platform offers a broad range of key capabilities. ID Plus provides a comprehensive cloud-native, multi-tenant identity management solution with both access management and lifecycle management capabilities. The solution supports OAuth2, FIDO2, OATH, SAML, and SCIM standards. This platform has its strengths in areas such as risk-based authentication, a unified directory, and support for passwordless authentication. Governance & Lifecycle delivers full featured identity governance and administration (IGA) including access certifications, automated provisioning, role-based access controls (RBAC), segregation of duties (SoD), and advanced workflow orchestration. RSA also supports a secure enrollment process for third-party ID verification.

What sets RSA apart is its innovation backed by a strong foundation in IAM. RSA's integration of Automated Identity Intelligence delivers identity insights using AI, machine learning, and advanced analytics, not only to enhance process automation, but also to help organizations clearly understand what their identity data reveals, including potential security gaps. This is complemented by RSA Mobile Lock, which provides mobile threat detection and helps in identifying attack vectors targeting mobile devices. However, while well-equipped with modern authentication methods including FIDO2, the current interface of Governance & Lifecycle is somewhat traditional; improvements planned for 2025 aim to align it with ID Plus's modern UX. Moreover, an opportunity exists to boost the maturity of lifecycle management within ID Plus, particularly for more complex use cases typically seen in large enterprises. RSA lacks advanced IAM capabilities such as PAM, but can integrate with 3rd party PAM solutions.

RSA Security's solutions can meet the needs of organizations with complex identity requirements and offer hybrid deployment options to support high availability. At the same time, RSA's portfolio is well-suited to organizations of all sizes. With thousands of customers and ID Plus alone serving clients in 90 countries, RSA serves a global market. Particularly within sectors including finance and manufacturing, where uninterrupted authentication is critical, RSA's solutions are valuable, also highlighted by its proven uptime. Organizations seeking a proven IAM solution that demonstrates innovation would find RSA worth considering.

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

Table 18: RSA Security's rating

Strengths

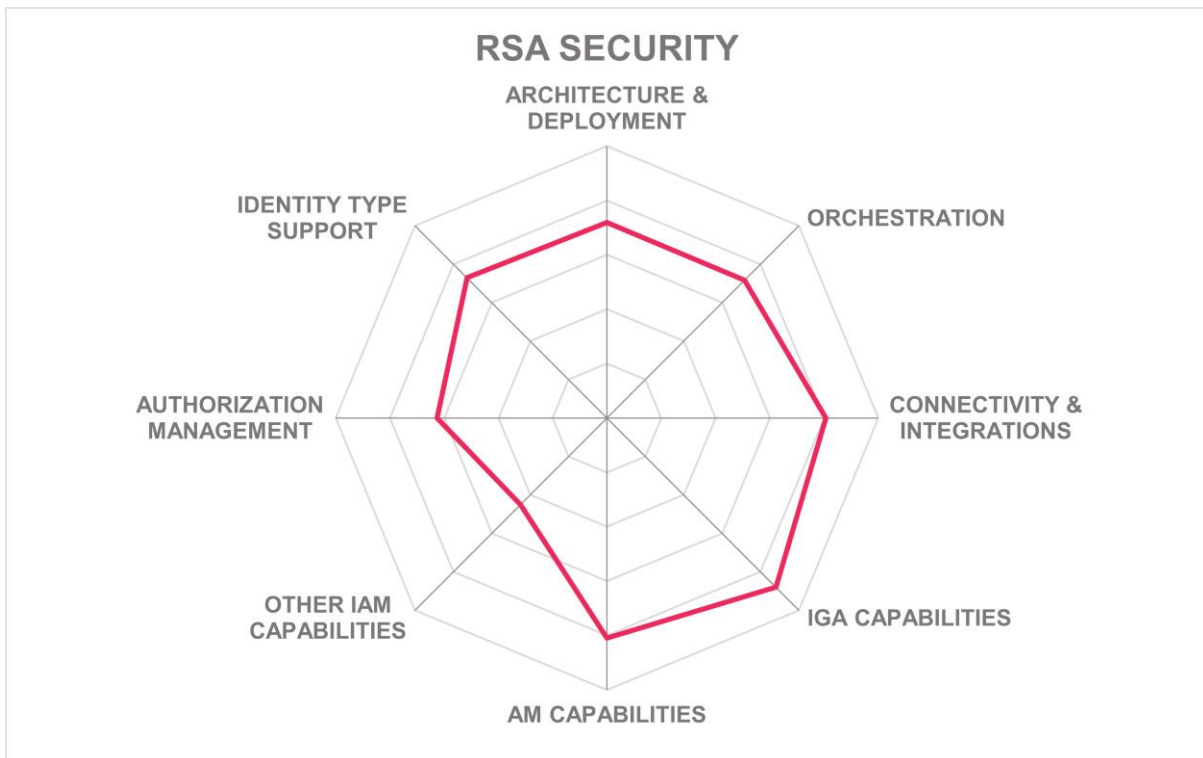
- Broad standards support including OAuth2 and FIDO.
- Innovative mobile threat detection with RSA Mobile Lock.
- Extensive customer base across 90 countries.
- Many integration capabilities with other IAM solutions.
- High uptime availability and robust support infrastructure.
- Detailed risk-based access and authentication controls.
- Strong support for hybrid deployment requirements.
- Good level of AI support across the various features.

Challenges

- Governance & Lifecycle's user interface needs modernization.
- Further acceleration needed in platform modernization towards full IDaaS support.
- Lack of PAM and CIEM capabilities.

Leader in





SailPoint – Identity Security Platform

SailPoint, headquartered in Austin, Texas, since 2005, is a prominent player in IGA. While they do not provide their own Access Management capabilities, which slightly constrains their overall rating, they can serve as a strong foundation for an Identity Fabric in combination with other vendor's Access Management solutions. Their position in IGA continues to be a significant strength, alongside strategic investments in PAM and CIEM that are focused on delivering a comprehensive governance across all types of identities. SailPoint is making a decisive shift towards cloud-based services, effectively moving away from their traditional platform.

SailPoint excels in providing a feature set beyond IGA that includes Privileged Task Automation, data access security, and machine identity governance. Their Identity Security Cloud (ISC) offers a high degree of flexibility, based on over 300 microservices, driven by a focus on API orchestration. Their capabilities encompass user activity monitoring, privilege management, and identity risk scoring, all underpinned by their Atlas Platform, which delivers the common services across the platform. The solution benefits from a strong developer community and a flexible set of APIs, enabling integration with third-party No-Code platforms and enhancing the scope for automation and extensibility.

One of SailPoint's standout innovations is their connectivity fabric, which allows for dynamic extensibility and interoperability with third-party systems. This alongside their AI for identity and access analytics, and graphical workflow capabilities positions SailPoint as a forward-thinking identity solutions provider. However, the lack of native Access Management functionality and ongoing UI modernization efforts highlight areas for improvement. For Access Management, SailPoint has integrations to all major players in the market. Their roadmap shows promising enhancements, such as broader SAP integration, which is gradually being rolled out.

SailPoint's solutions are particularly compelling for enterprises transitioning to the cloud, engaging in leading-edge IGA, identity risk management, and seeking extensive PAM and CIEM functionalities including a holistic governance approach. Their solutions serve a diverse client base, ranging from large corporations to mid-market organizations embracing a cloud-first approach. SailPoint's products are especially beneficial for firms looking to enhance governance across complex IT environments and multi-vendor cloud services, supporting AWS, Azure, Google Cloud, and VMware, thus meeting regulatory compliance standards such as GDPR and SOC 2. SailPoint thus, despite not providing Access Management as part of their portfolio, can serve as a foundational element in an Identity Fabric architecture.

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



Table 19: SailPoint’s rating

Strengths

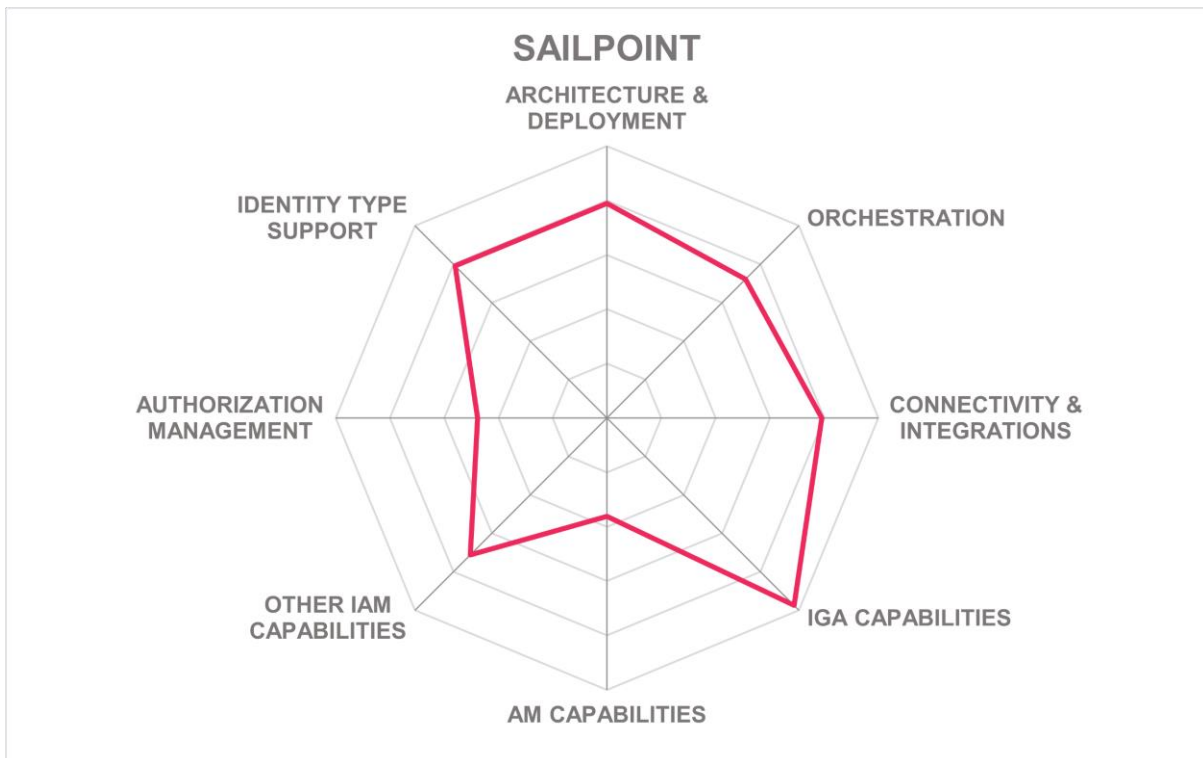
- Excellent identity lifecycle and access governance capabilities.
- Comprehensive governance across all types of identities, human and non-human identities as well as privileged and standard users.
- Well-designed API orchestration and workflow tools.
- Dynamic extensibility through connectivity fabric.
- Innovative agentic AI features.
- Innovative approach on complementing IGA with PAM and CIEM features.
- High interoperability with enterprise systems, many connectors for line-of-business systems.
- Strong analytics and risk management tools.
- Global partner ecosystem.

Challenges

- Lack of native Access Management functionalities.
- UI modernization still in progress.
- Some limitations in PAM features such as session management, but modern and lean approach on PAM.
- Integration of acquisitions not yet fully done.

Leader in





SAP – Cloud Identity Services

SAP SE, established in 1972, is a renowned enterprise software company headquartered in Walldorf, Germany. It offers a suite of identity services under the SAP Cloud Identity Services. As a part of SAP's Business Technology Platform (BTP), these solutions are designed to enhance identity and access management capabilities, particularly for SAP environments. The solutions include Identity Authentication Services, Identity Provisioning Services, and Access Control, tailored to meet a diverse range of enterprise identity needs.

SAP Cloud Identity Services provide access management, identity analytics, and integration capabilities. They support a wide array of authentication mechanisms including multi-factor authentication with FIDO standards and various user attributes analytics through SAP Enterprise Threat Detection. Additionally, the solutions embrace a microservices architecture, allowing for flexible deployment and scalability. While they ensure strong integration within SAP ecosystems, some limitations exist in supporting heterogeneous environments, which are primarily supported via open standards such as SCIM.

A key strength of SAP's solution is its tailored approach to SAP applications, providing tight integration and native support. This also means that some components such as SAP Access Control, while supporting hybrid landscapes, rely on mature, scalable, but SAP specific architectures, and that specific SAP knowledge is required for administration, configuration, and operations. Moreover, advanced user analytics and comprehensive access governance capabilities stand out as unique selling points. However, the absence of certain features, such as CIEM capabilities or PAM support beyond SAP environments, suggests room for expansion. With the end-of-life of SAP Identity Management, there also remains a gap in broader IGA support. SAP addresses this via a broad integration strategy with leading IGA vendors. The product could also benefit from enhanced support for non-SAP environments to broaden its market.

SAP Cloud Identity Services primarily cater to customers entrenched in the SAP landscape across regions including North America and EMEA. The solution is well-suited for use cases requiring strong identity governance and compliance, making it attractive to industries such as finance and manufacturing. Enterprises heavily utilizing SAP solutions will find significant value in SAP's identity solutions, enhancing both operational security and compliance efficiencies.

Security	Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Neutral	
Usability	Positive	

Table 20: SAP's rating

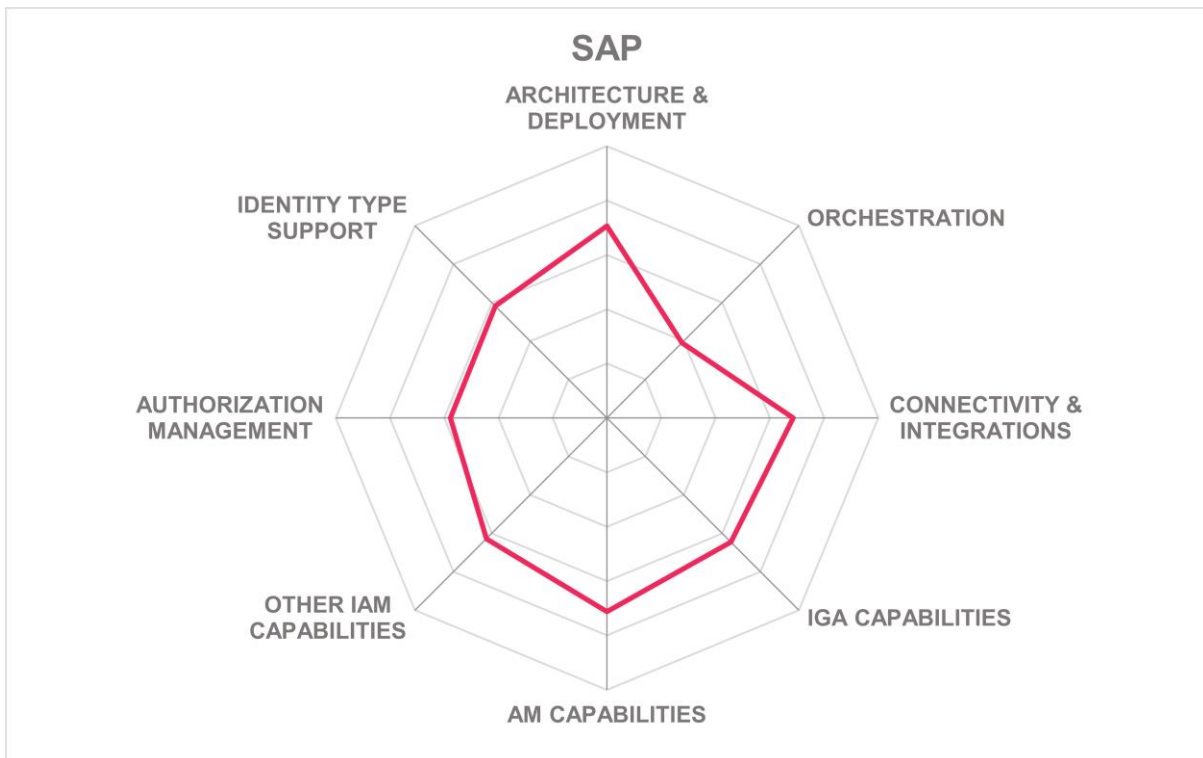
Strengths

- Comprehensive support for SAP environments.
- Good multi-factor authentication options.
- Integrated identity analytics with AI capabilities.
- Microservices architecture for flexible deployment.
- Secure and scalable access management solutions.
- Extensive integration within SAP's Business Technology Platform.
- Advanced identity governance features for SAP environments.

Challenges

- Limited PAM and CIEM capabilities.
- Expansion needed for non-SAP environments.
- Integrations primarily based on open standards such as SCIM, limiting deep integration and legacy integration.
- End-of-life of SAP Identity Management leaves a gap in broader IGA capabilities.
- Requires deep SAP skills for optimal use.

Leader in



Saviynt – Identity Cloud

Saviynt, founded in 2010 and headquartered in Los Angeles, California, has evolved to become a leading IAM player. Specializing in IGA, Saviynt expands its portfolio to include Non-Human Identity Management, Access Control for Line of Business (LoB) applications, PAM, and ISPM (Identity Security Posture Management). Positioned as a Product and Innovation leader, Saviynt has consistently achieved product leadership recognition, demonstrating a dedication to advancing secure identity management capabilities across various sectors.

The product’s capabilities are based on their leading-edge IGA capabilities and embed AI and machine learning, enabling automation in provisioning/de-provisioning and identity analytics with features such as anomaly and outlier detection. The policy framework supports dynamic access entitlements and role management, enforcing the least privilege principle. Saviynt’s architecture is designed to integrate with a wide array of third-party tools, supporting interfaces including REST and SCIM, and providing out-of-the-box integrations with notable systems, such as Microsoft Entra ID, SAP, and Amazon AWS. ISO/IEC 27001, PCI-DSS, and FedRAMP certifications offer a solid compliance foundation for global deployments.

Saviynt distinguishes itself with its identity security data lake architecture, facilitating intelligent access recommendations through AI/ML-driven insights. This model allows for nuanced, risk-based identity postures but has room for growth by adding Access Management capabilities as well as in further modernization of the internal security model towards policy-based access controls. Noteworthy differentiators include integration frameworks and the capacity to discover peer groups for managing access entitlements. The solution’s intuitive design and strong dashboard features deliver significant user benefits, though expanding support towards access management and for identity federation standards could broaden reach.

Saviynt caters primarily to medium to large enterprises across North America, EMEA, and APAC regions, supporting all industry sectors. The platform’s rich feature set is particularly valuable for organizations undergoing digital transformations that necessitate advanced data governance and operational intelligence. Those seeking to enhance identity management processes with flexible, scalable, and secure solutions should consider Saviynt an option, in combination with other vendor’s Access Management solutions.

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



Table 21: Saviynt’s rating

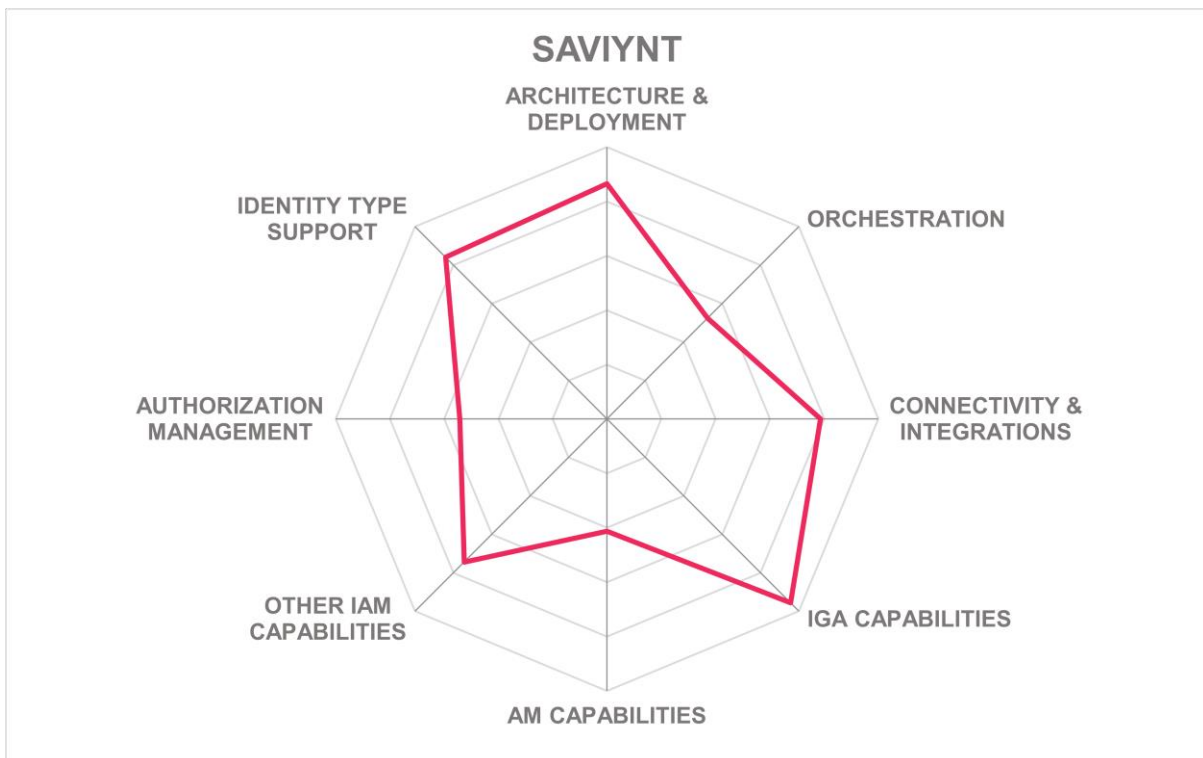
Strengths

- Leading-edge IGA capabilities.
- Advanced AI/ML-based identity analytics.
- Extensive third-party integration capabilities.
- Strong compliance with recognized standards.
- Good set of Privileged Access Management features.
- Evolving into the NHI management market segment.
- Notable identity security data lake architecture.
- Intuitive and powerful dashboard insights.
- Wide support for enterprise-grade connectors.

Challenges

- Very limited Access Management capabilities.
- Enhanced support for identity federation standards needed.
- Additional language support for documentation could improve accessibility.

Leader in



SecureAuth – SecureAuth CIAM & SecureAuth Workforce

SecureAuth Corporation, established in 2005 and headquartered in Irvine, California, specializes in Identity and Access Management (IAM) solutions across the spectrum from workforce to partner and customer IAM. The SecureAuth platform incorporates the functionalities of their IdP with passwordless device trust, AI/ML risk management, and advanced CIAM authorization technologies. The recent acquisition of SessionGuardian (December 2024), which provided continuous facial authentication, underscores their commitment to enhancing session security. SecureAuth provides a modern IAM approach with significant weight on interoperability and dynamic authentication across different types of applications for diverse use cases, including B2B, B2C, and B2B2C scenarios.

Key capabilities of SecureAuth’s platform include fine-grained access management, orchestration across multiple identity providers such as Ping and Okta, and strong authentication mechanisms. It supports flexible deployments tailored to enterprise needs, supporting both monthly active users (MAU) and transaction-based licensing models. The platform excels in delivering a frictionless experience, leveraging broad support for various applications with a dynamic authorization concept embedded. Furthermore, their Identity Hub supports identity pools such as cloud directories.

SecureAuth’s strength lies in its leading-edge authentication support, integrated with strong authorization capabilities, and in their advanced orchestration capabilities that do not require storing identities within the SecureAuth system, thereby providing flexibility in scenarios involving multiple identity providers. All of SecureAuth’s technologies are available for SaaS, hybrid or on-premises deployment; including air-gapped operation for highly secured environments. Another unique aspect is their multi-tier tenant model, serving complex organizational structures as well as supply chain and distributed network integrations. However, SecureAuth must partner with other vendors to fill gaps in areas such as IGA and PAM via product integration, reflecting a need for enhancement in these domains to deliver a complete IAM solution.

Predominantly serving the North American market, SecureAuth’s solutions have gained traction in the following industries: finance, retail, and healthcare. Their focus on identity orchestration combined with advanced authorization functionalities makes SecureAuth particularly appealing for organizations requiring complex B2B2C identity scenarios and dynamic user journeys. Retail, finance, and other industries dealing with complex identity hierarchies may find their deep orchestration and API integrations particularly beneficial.

Security	Strong Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

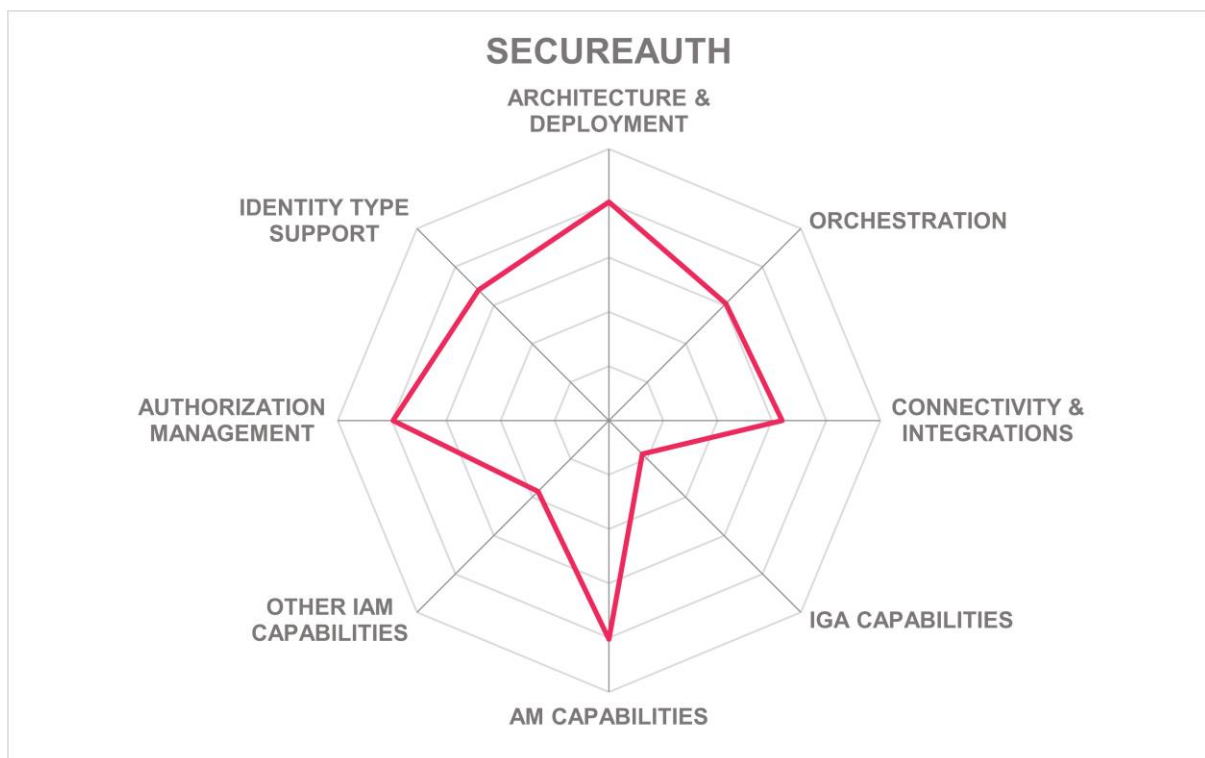
Table 22: SecureAuth's rating

Strengths

- Strong access management capabilities for diverse use cases.
- Interesting approach to identity orchestration with flexible integration but lacking advanced workflow support.
- Multi-tiered tenant model for complex organizational needs.
- Strong interoperability with major IdPs including Microsoft, Google, Okta and Ping.
- Supports many authentication methods with dynamic, granular authorization.
- Recent enhancements in session security.
- Strong position in the CIAM market.

Challenges

- Lack of capabilities in Identity Governance and Administration.
- Lack of Privileged Access Management features.
- Orchestration features would benefit from expanded workflow support.
- Strong authorization management, but focused on access management use cases only, not expanding into IGA modernization.



Simeio – Identity Orchestrator

Simeio, established in 2007 and headquartered in Atlanta, Georgia, has distinguished itself as a leading player in the Identity and Access Management (IAM) space. Simeio started as an identity services provider, and has developed identity orchestration products and services based on their extensive customer engagement experiences. The company is positioned in the Identity Fabrics market segment with its Simeio Identity Orchestrator, which offers a strong orchestration platform that can integrate multiple IAM solutions to streamline identity management operations for its clients. With a significant footprint in North America and a growing presence in Dubai and London, Simeio is well-positioned to become a global solution provider.

Simeio's Identity Orchestrator stands out with its integration functionality across various IAM domains, including IGA, AM, PAM, and CIEM. The platform utilizes a modern microservices architecture with container-based deployments on prominent platforms including OCI, Kubernetes, and AWS. It excels in automated user and application lifecycle management, offering its own sophisticated entitlement management and privilege control features. This solution ensures thorough compliance with industry standards such as AICPA SOC 2 and ISO 27001.

The company's clear differentiators lie in its expansive integration capabilities, allowing orchestration with solutions from major IAM vendors such as Saviynt and SailPoint. While Simeio's unified user interface is a positive feature, it still requires refinement to enhance user experience consistently across deployments. Focusing on facilitating application onboarding and improving dashboard interfaces could further improve their solution. Additionally, expanding native support for specialized IAM features would strengthen their market position.

Simeio's solutions appeal particularly to large enterprises and mid-market companies that already have various IAM solutions and are seeking integration combined with professional services. With a strong presence in industries such as finance, manufacturing, and healthcare, and a regional customer base predominantly in North America, Simeio is well-suited to organizations with complex IAM environments. Those requiring unified security and compliance management across diverse identity tools will find in Simeio a valuable partner.

Security	Strong Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

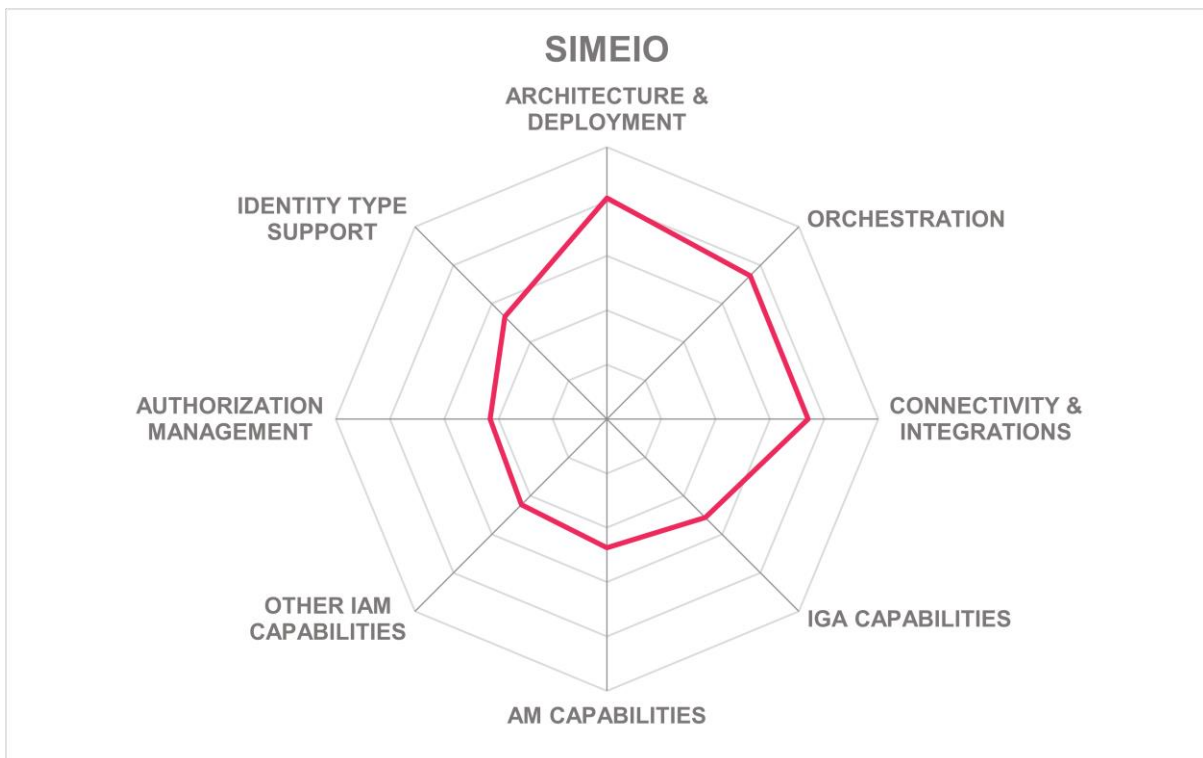
Table 23: Simeio's rating

Strengths

- Excellent IAM orchestration platform.
- Strong integration with leading IAM vendors.
- Large number of identity specialists for delivering professional/managed services.
- Products developed with extensive experience helping customers with IAM integrations.
- Compliance with global standards such as SOC2 and ISO 27001.

Challenges

- Some user interface components need refinement.
- Native support for own or specialized IAM capabilities is very limited, focus is on integrating and expanding other vendor’s solutions.
- Application onboarding still needs streamlining.
- Dashboard interface can improve in detail and usability.
- Focused on customers looking for a managed IAM.



Soffid – IAM

Established in 2011, Soffid is a European-based IAM vendor headquartered in Spain, providing an increasingly comprehensive Identity and Access Management (IAM) platform in an open-source model. The company provides a converged IAM platform, delivering enterprise-grade solutions that span across IGA Access Management, and PAM. By covering these areas, Soffid aims to support both workforce and CIAM needs. The solution is available both as an IDaaS and on-premises, adapting to various deployment models to suit customer requirements.

Soffid impresses with its wide range of integrated features. The platform delivers strong MFA including good authenticator and FIDO2 support, SSO, password management, and adaptive access controls. Additional capabilities include password vaulting and strong authentication for secure access to privileged credentials, user activity monitoring, and user behavior analysis. The solution supports integration with common IT infrastructures including AWS, Microsoft Azure, Kubernetes, and more. Additionally, Soffid supports REST, SOAP, and SCIM.

Soffid’s strength lies in its integrated platform, combining IGA, Access Management, and PAM functionalities with an open-source approach. This makes it interesting for organizations looking to manage many different types of identities with a single solution. Innovations such as the identity analytics platform, which has support from threat intelligence sources including HavelBeenPwned and SpyCloud, further enhance its solution. However, areas for improvement remain, the need for more built-in connectors and a more intuitive workflow automation.

Soffid targets organizations looking for powerful open-source IAM platforms, including government organizations seeking a feature-rich IAM platform as well as smaller organizations requiring baseline capabilities. The platform is particularly attractive to European clients seeking compliance with regional regulations including eIDAS and GDPR. The company’s strategic focus on partnering with implementation service providers broadens its market reach, especially in regions where local partnership models are vital for successful market entry.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive



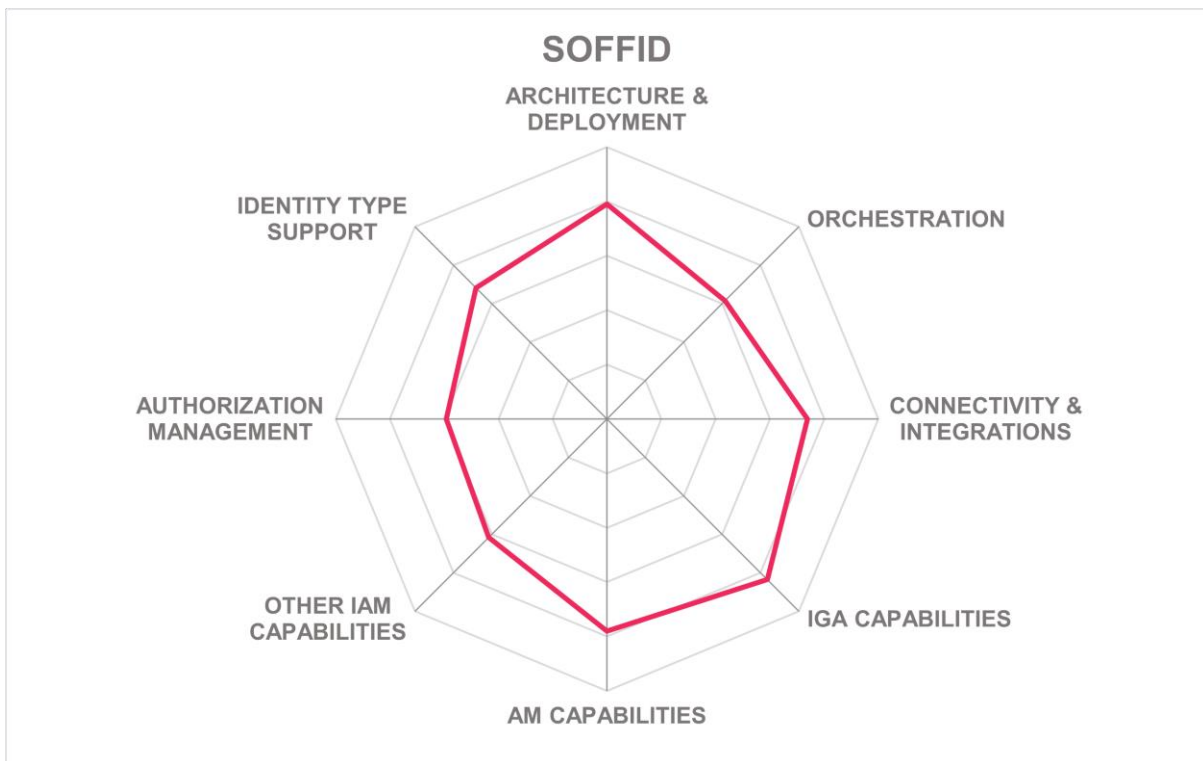
Table 24: Soffid's rating

Strengths

- Integrated IGA, Access Management, and PAM functionality.
- Modern architecture and native converged platform.
- Open-source approach offers customization flexibility.
- Strong support for AWS, Azure, and Kubernetes.
- Identity and user behavioral analytics are built-in.
- Supports adaptive and multi-factor authentication including FIDO2 support.
- Includes third-party compromised credential intelligence.

Challenges

- Good number of connectors, but room for further growth.
- Interface could benefit from more workflow automation.
- Growing but still limited partner ecosystem.
- Small vendor, but growing presence also in very large organizations.



Strata Identity – Mavericks Identity Orchestration Platform

Strata Identity, established in 2019 and headquartered in the US, has carved out a distinct niche in the Identity Fabrics sector. While it does not present a complete Identity Fabric suite, Strata Identity focuses on integrating existing access management solutions and identity silos. With a solid capital backing, Strata Identity has developed a strong partner ecosystem, including major players Microsoft and CyberArk, which enhances its market presence. Their Mavericks platform acts as an orchestrator that efficiently maps Identity Providers (IdPs) and directories to protected applications, offering integration for both legacy and modern applications.

The Mavericks Identity Orchestration Platform stands out for its ability to act as an abstraction layer between identity components and applications. Strata Identity excels in Low-Code integration, presenting a versatile solution that supports continuous access evaluation and ensures IdP resilience for disaster recovery scenarios. The platform is designed for high scalability, supporting flexible deployment models such as Kubernetes and load balancers. Moreover, it can integrate easily with third-party systems such as Active Directory, AWS, and CyberArk, and more, enabling orchestration across cloud and on-premises environments.

Strata Identity's differentiation is in its ability to integrate identity silos at runtime, supporting Identity Continuity and application modernization without extensive recoding efforts. The Mavericks platform also enables identity continuity across diverse IdPs and supports cross-IdP failover and fallback. However, the platform's narrow focus on access management orchestration means it lacks comprehensive IGA and PAM capabilities.

The Mavericks platform is particularly beneficial for large enterprises dealing with legacy IdP solutions and non-standard applications. It supports a wide array of identity types, making it suitable for organizations looking to modernize their authentication processes for non-standard applications. Its capability to handle both cloud and on-premises environments makes it an attractive option for those needing continuity in identity management across varied infrastructures. Strata Identity targets industries requiring complex orchestration, making it an important complementary solution to existing Identity Fabrics.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Positive
Usability	Positive



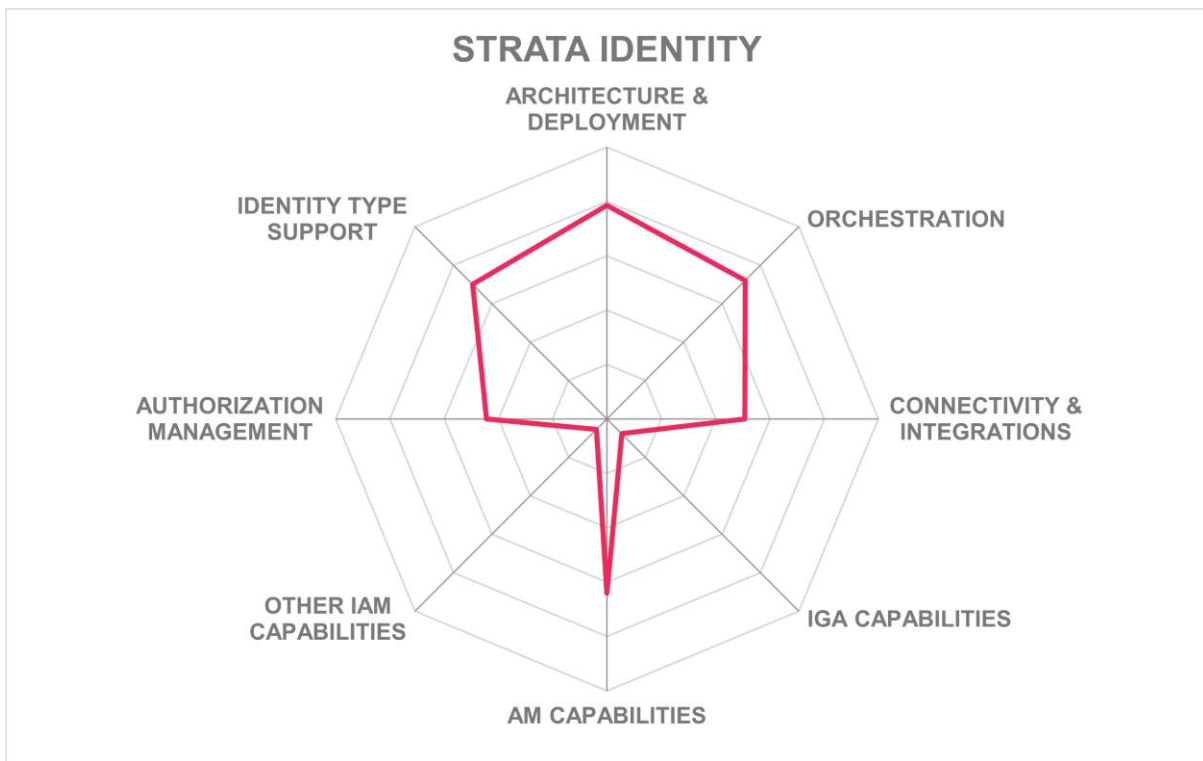
Table 25: Strata Identity's rating

Strengths

- Unique identity silo integration capabilities.
- Well-selected partner ecosystem, including industry leaders.
- Flexible, Low-Code/No-Code integration.
- High scalability with excellent orchestration features.
- Extensive interoperability with major legacy access management systems.
- Secure, air-gapped architecture.
- Supports resilience and disaster recovery initiatives.

Challenges

- Lack of PAM and IGA capabilities.
- Small customer base.
- Focused on a subset of Identity Fabric capabilities.
- Requires further integration of orchestration workflows.



TrustBuilder – TrustBuilder.io

TrustBuilder, a result of the merger between inWebo and TrustBuilder, is a European access management company headquartered in Paris. Established in 2008, it emphasizes EU sovereignty and has customers in over 90 countries. The company has hundreds of clients globally, integrating strong authentication with a focus on CIAM for B2B2X use cases. The company is led by a proven executive team and a commitment to innovation, channeling a significant share of its revenue into R&D.

The TrustBuilder.io SaaS platform is a solution offering features such as passwordless authentication for resilience against phishing attacks, and thorough fine-grained authorization controls. Its capabilities in access management, including support for B2B, government, and application identities, make it a compelling choice for organizations looking for solutions in that area. Notably, it supports standards such as XACML, while ensuring interoperability with systems such as Azure Entra ID and LDAP. TrustBuilder's deviceless browser-based MFA as well as its authenticator app exhibit strong user-centric design, combining accessibility and ease of integration.

TrustBuilder's strengths lie in its adaptability and innovation within the access management area of identity fabrics, with features such as a dynamic persona model that supports complex use cases and B2B2X scenarios by reflecting identity relationships. However, while their authentication capabilities are strong, FIDO2 and WebAuthn are not yet supported. They also lack support for the broader IAM feature set, including IGA and PAM. They have recently improved the admin and user interfaces, yet they would still benefit from further modernization.

TrustBuilder.io is well-positioned for customers seeking authentication, authorization, and access management for CIAM and B2B use cases. Built for the European market but with a growing global reach, it is ideal for organizations looking for EU-hosted services, with specific interest in regions where compliance with regulations such as EU eIDAS and GDPR is essential. Those managing extensive external relationships, requiring delegated administration, and sophisticated access control mechanisms will find significant value in examining TrustBuilder's solution.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Neutral
Usability	Positive



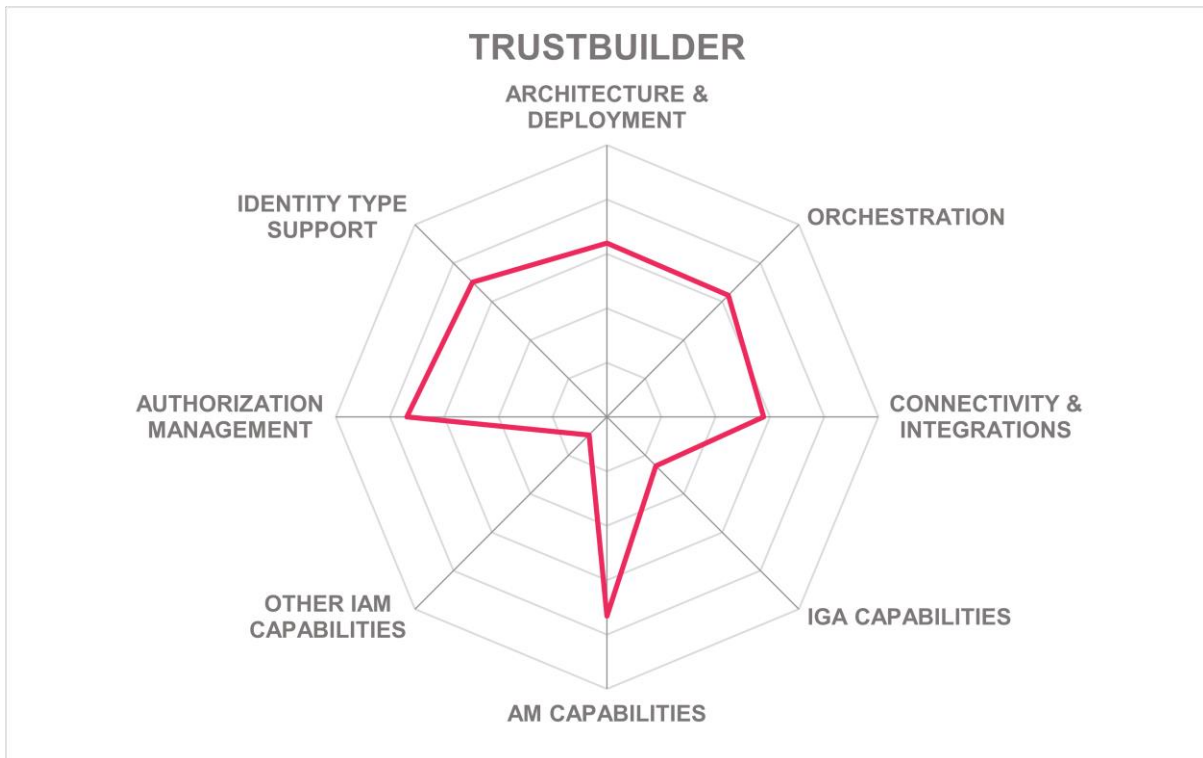
Table 26: TrustBuilder's rating

Strengths

- Strong focus on EU sovereignty and data residency.
- Robust authentication options with phishing resistance.
- Strong B2B2X and consumer identity management features.
- Strategic investment in R&D.
- Supports a wide range of identity types and relationships.
- Advanced persona and delegation features.

Challenges

- Lack of support for IGA and PAM use cases, complementary to full Identity Fabrics approaches.
- UI requires further modernization.
- Gaps in FIDO2 support.
- Limited customization in reporting.



XAYone – XAYone Platform

XAYone provides a modern IAM platform tailored primarily for CIAM, along with additional trust services such as identity verification and electronic signature management. Designed to help customers meet regulatory compliance requirements, XAYone is built on a microservices architecture, enabling deployment both on-premises and in IaaS environments. Despite being a newer entrant in the market, the company has already gained recognition by securing notable customers across government, finance, and other sectors. The XAYone platform provides numerous key capabilities that position it well in the IAM market. It delivers outstanding identity verification support, covering a wide range of identification documents globally, with integrations for standards such as OpenID Connect and SAML. The platform also includes customizable reporting, adaptive security measures, and an interface that offers detailed insights through dashboards for the state of identities, their access, and the associated risk. These capabilities are delivered through a policy-driven model that incorporates MFA.

The platform features identity orchestration and administration of various types of identities and their relationships across different organizational entities, making it a good choice for complex organizational structures. Noteworthy differentiators include their customizable UI alongside extensive support for automated Identity Verification based on a variety of globally recognized ID documents. However, areas such as deeper graphical visualizations for authentication flows and legacy system integration could be improved. Also, PAM features are lacking and IGA for workforce users is just at a basic level. The upcoming addition of AI-powered analytics could further enhance the solution.

Their customers are primarily in the finance and government sectors, specifically in regions such as EMEA with some expansion into North America. Due to its tailored CIAM and trust services, XAYone is particularly viable for regulatory-intensive industries that demand advanced digital identity solutions, endorsing its suitability for medium and large enterprises. Organizations with a significant focus on customer identity cases and the specific features provided by the solution will find the XAYone platform a solution worth evaluating.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive



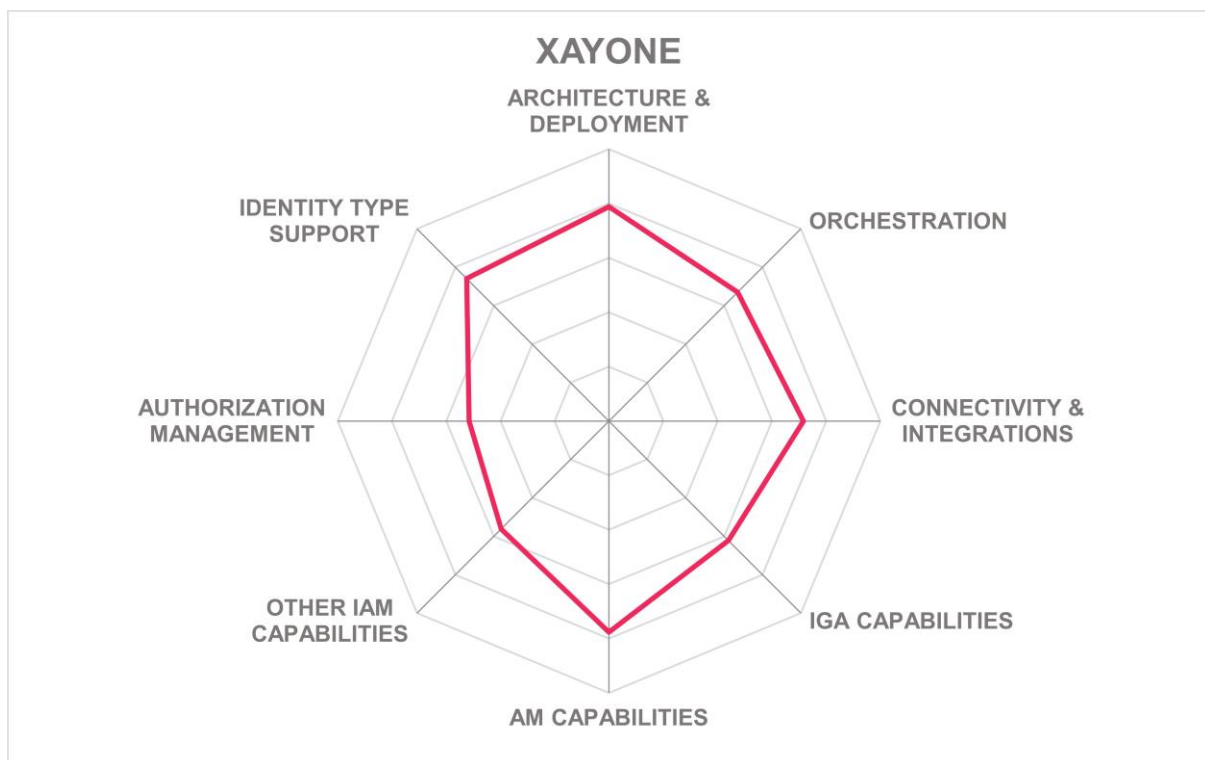
Table 27: XAYone's rating

Strengths

- Modern and adaptable UI.
- Comprehensive identity verification capabilities.
- Strong support for regulatory compliance.
- Extensive standards support including FIDO2, RADIUS, and others.
- Policy-based administration, beyond role-based access controls for administrative access.

Challenges

- Limited legacy system integration.
- No graphical visualizations for authentication flows.
- Small customer base relative to larger competitors.
- Small partner ecosystem.



Vendors to Watch

Besides the vendors covered in detail in this document, here are some other vendors worth considering.

Authlete

Authlete is a vendor specializing in offloading authentication and protocol specifics for the OAuth and OIDC protocol. This is a unique solution, which is of specific interest for organizations creating their own digital services.

Why worth watching – complements other solutions with its specialized support for complex authentication use cases and thus adds to an Identity API layer.

Avatier

Avatier is a 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 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. Dynamic Authorization Management capabilities are becoming increasingly important and should be included if applications are built against a central Identity API Layer.

Why worth watching – delivers additional, leading-edge authorization capabilities to an Identity Fabric.

Baar-ID

Baar-ID is a provider of identity verification and authentication solutions, offering services that combine biometrics, AI-driven risk assessment, and compliance-focused identity proofing. The company focuses on delivering good user experiences while maintaining strong security measures across digital transactions. Baar-ID's approach integrates liveness detection, document verification, and behavioral analysis to reduce fraud and streamline identity verification.

Why worth watching - Baar-ID's focus on advanced biometric authentication and AI-powered risk assessment positions it as a relevant player in identity verification and fraud prevention.

cidaas

cidaas has a cloud-based customer identity and access management (CIAM) platform designed for secure authentication, identity verification, and access control. The platform includes adaptive authentication, consent management, and API security to support digital transformation initiatives. cidaas helps organizations provide secure and user-friendly access to digital services while ensuring compliance with privacy regulations. They are increasingly expanding into workforce IAM.

Why worth watching - cidaas' focus on CIAM and adaptive authentication positions it as a strong choice for businesses aiming to enhance security while improving user experience.

Eviden

Eviden is part of Atos, and they offer 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 built on proven technology and has the ability to deliver IDaaS services from a European cloud.

Fischer International

Fischer International is a US based vendor of IDaaS solutions. Their products are available on-premises and cloud, 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.

Identity Automation

Identity Automation is a US-based provider of an IAM solution covering both Access Management and IGA requirements. Their focus is on the higher education market, but they also serve other market segments. They were recently acquired by JAMF.

Why worth watching – Identity Automation is a provider of a solution for IAM that is well-suited for higher education and mid-market companies.

Ilex

Ilex is a European IAM provider specializing in access governance, authentication, and privileged access management. With a strong presence in regulated industries, Ilex provides solutions that integrate with existing IT environments while addressing compliance and security requirements. The solution can be deployed on-premises or in the cloud.

Why worth watching - Ilex's focus on access governance and regulatory compliance makes it a strong option for organizations with complex security requirements.

Imprivata

Imprivata is a provider focusing on the healthcare industry; however their solutions can also serve customers in other industries. Aside from their traditional strength in Enterprise Single Sign-On, Imprivata has created an IAM portfolio through acquisitions.

Why worth watching – specifically for healthcare organizations, Imprivata provides a leading-edge solution with specific support for specialized industry applications.

Memory

Memory is a spin-off from Accenture and delivers an integrated solution that supports most areas of IAM, specifically IGA and Access Management. Memory is based in France, and has a large French customer base that includes some very large installations.

Why worth watching – The solution has 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 a specialist in IGA and specifically Access Governance. The product has close integration with Microsoft Azure Active Directory and Microsoft 365 as well as support for other Access Management solutions.

Why worth watching – It can serve as a complement to Microsoft Entra ID with good IGA solutions, specifically for mid-market customers.

Netwrix

Netwrix provides identity security and governance solutions, with capabilities spanning identity analytics, privileged access management, and risk assessment. The company offers tools for monitoring user activity, detecting anomalies, and enforcing security policies across hybrid IT environments. Netwrix's solutions are designed to enhance visibility and control over identities, reducing the risk of unauthorized access.

Why worth watching - Netwrix's approach to identity security and risk-based access control aligns with the growing need for visibility and governance in modern IT environments.

Pathlock

Pathlock provides identity governance and application access security, with a focus on securing business-critical applications such as ERP, CRM, and financial systems. Its platform enables organizations to enforce access controls, monitor user activity, and automate compliance reporting. Pathlock integrates with enterprise applications to manage segregation of duties, detect insider threats, and streamline access certification. The company's approach combines risk-based access management with automation to reduce security gaps and compliance burdens.

Why worth watching - Pathlock's focus on securing application access and enforcing governance makes it relevant for enterprises looking to strengthen controls around business-critical systems.

PlainID

PlainID is a specialist vendor for Dynamic Authorization Management and policy-based authorizations. Though it is not a complete IAM portfolio, it can be a complement to other solutions, adding the authorization capabilities for building new digital services.

Why worth watching – PlainID delivers leading-edge authorization capabilities to an Identity Fabric.

Omada

Omada has an IGA solution aimed at helping organizations manage access, enforce security policies, and meet regulatory requirements. The company's platform includes role-based access controls, automated provisioning, and risk-based decision-making to streamline identity lifecycle management. Omada's solutions cater to enterprises seeking to balance security, compliance, and operational efficiency.

Why worth watching - Omada's focus on identity governance and automation makes it relevant for organizations looking to improve security and compliance while reducing administrative overhead.

OpenText

OpenText provides identity and access management solutions that integrate with enterprise information management platforms. Their solution includes authentication, access control, and identity governance capabilities designed to secure data and manage user identities across complex IT environments.

Why worth watching - OpenText's integration of IAM with enterprise content management provides organizations with a comprehensive approach to securing identities and information.

Radiant Logic

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.

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

Systancia

Systancia supports both Access Management and IGA use cases, as well as ZTNA (Zero Trust Network Access) and other capabilities. Their solution comes with strong support in certain areas such as workplace integration.

Why worth watching – Combining ZTNA and workplace access is their product emphasis.

Teleport

Teleport provides an identity-based access management platform designed for securing infrastructure, including cloud environments, Kubernetes clusters, and on-premises servers. The platform emphasizes passwordless access, certificate-based authentication, and session recording to enhance security without adding operational complexity. Teleport's approach aligns with modern zero-trust security principles, ensuring that access is both seamless and verifiable.

Why worth watching - Teleport's emphasis on identity-driven infrastructure access and zero-trust security aligns well with the increasing demand for secure, passwordless authentication in enterprise IT.

Thales

Thales, following its acquisition of OneWelcome, offers a strong portfolio in customer and business partner identity and access management (CIAM and B2B IAM). Its platform provides identity verification, delegated administration, consent management, and adaptive authentication, helping organizations manage complex identity relationships across customers, suppliers, and partners. The solution supports compliance with privacy regulations while enabling secure and seamless digital interactions. In addition to its CIAM and B2B IAM capabilities, Thales provides a broader IAM portfolio covering authentication, access management, and identity governance. Beyond that, they provide data security and data governance solutions, as well as delivering further capabilities.

Why worth watching - Thales' capabilities in CIAM and B2B IAM, strengthened by OneWelcome's technology, address the growing need for secure and scalable digital identity management.

Transmit Security

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

Why worth watching – modern solution with strong authentication, identity verification and Fraud Reduction Intelligence Platform 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 – Their broadening portfolio of IAM capabilities with PAM features are appealing to some organizations.

WSO2

WSO2 is an established vendor in the IAM market, and their portfolio also comprises an Enterprise Integration Platform and API Management and Security. For IAM, the solution is WSO2 Identity Server, which primarily handles Access Management. Together with its other solutions, the company provides a strong foundation for identity fabrics.

Why worth watching – WSO2 is a strong platform for building digital services with good support for IAM, targeting primarily developers.

Related Research

[Advisory Note The 2025 Identity Fabric and IAM Reference Architecture](#)

[Buyer's Compass Identity Fabrics](#)

[Leadership Brief Leveraging Identity Fabrics on Your Way Towards Cloud Based IAM](#)

[Leadership Brief Connecting Anyone to Every Service](#)

[Leadership Compass Identity and Access Governance](#)

[Leadership Compass Privileged Access Management](#)

[Leadership Compass Passwordless Authentication for Enterprises](#)

[Leadership Compass Identity Governance and Authentication](#)

[Leadership Compass Customer Identity and Access Management \(CIAM\)](#)

[Leadership Compass Passwordless Authentication for Consumers: Securing Fast Business Online](#)

[Leadership Compass Identity Threat Detection and Response \(ITDR\): IAM Meets the SOC](#)

[Executive View Microsoft Entra Suite](#)

[Executive View Oracle Access Governance](#)

[Executive View Sailpoint Atlas – Unified Identity Security Platform](#)

[Executive View Microsoft Entra ID Governance](#)

[Executive View Cidaas Access Management](#)

[Executive View Omada Identity Cloud](#)

[Executive View Saviynt Application Access Governance](#)

[Executive View XAYone Best Practice: Combatting Identity and Document Fraud at Border Control](#)

[Executive View Pathlock Cybersecurity Application Controls](#)

[Executive View IBM Security and Compliance Center](#)

[Executive View Ping Identity Workforce Identity Governance](#)

Copyright

© 2025 KuppingerCole Analysts AG. All rights reserved. Reproducing or distributing this publication in any form is prohibited without prior written permission. The conclusions, recommendations, and predictions in this document reflect KuppingerCole's initial views. As we gather more information and conduct deeper analysis, the positions presented here may undergo refinements or significant changes. KuppingerCole disclaims all warranties regarding the completeness, accuracy, and adequacy of this information. Although KuppingerCole research documents may discuss legal issues related to information security and technology, we do not provide legal services or advice, and our publications should not be used as such. KuppingerCole assumes no liability for errors or inadequacies in the information contained in this document. Any expressed opinion may change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Their use does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole 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 technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

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