kuppingercole ANALYSTS

Access Management

Alejandro Leal

August 16, 2023

This report provides an overview of the market for Access Management products and services and presents you with a compass to help you to find the product or service that best meets your organization's needs. We examine the market segment, vendor product and service functionality, relative market share, and innovative approaches to providing Access Management solutions.

Contents

Figures

Introduction / Executive Summary

The combined impact of the pandemic driven shift to remote work with a connect-anywhere paradigm and the ongoing digital business transformation has inspired a higher awareness of cybersecurity concerns, requiring a profound change in the way we define access management. The term “Access Management” refers to the group of capabilities targeted at supporting access management requirements of organizations ranging from authentication, authorization, single sign-on, and identity federation traditionally found within Web Access Management (WAM) & Identity Federation solutions. These access management capabilities are well-established areas in the broader scope of Identity and access management (IAM), in which they are continuing to gain attraction due to emerging requirements for integrating business partners and customers.

Web Access Management & Identity Federation began as distinct solutions. (Web) Access Management is a traditional approach which adds a layer in front of web applications and takes over authentication and – usually coarse-grained – authorization management. Tools also increasingly support APIs for authorization calls to the system. Identity Federation allows splitting authentication and authorization between an IdP (Identity Provider) and a Service Provider (SP) or Relying Party (RP). Although Identity Federation can be used in various configurations, most vendors today provide integrated solutions that support centralized access management based on federation protocols such as SAML v2, OAuth, and OIDC.

The selection of an appropriate IAM solution is crucial for organizations as it plays a vital role in effectively managing, securing, and controlling access across their various entities. As a result, the adoption of Identity-as-a-Service (IDaaS) has become the preferred choice of customers and organizations for IAM purchases globally. The IDaaS market, with its ease of adoption and cloud-native integrations, is quickly overtaking the on-premises IAM market. The IDaaS market combines access management functions with Identity Governance and Administration (IGA) and Access Governance capabilities all delivered and managed as a service. Today, all IDaaS vendors predominantly deliver a cloud-based service in a multitenant or dedicatedly hosted fashion to serve the common IAM requirements of an organization's hybrid IT environment.

As an alternative to organizations managing the access management solutions themselves, some vendors provide Managed Services offerings, either by delivering per-tenant installations of on-premises solutions as a service, or by operating Software as a Service (SaaS) offerings. The first type of IDaaS Access Management vendors involve the traditional single sign-on (SSO) vendors that evolved to support web access management and handle web-centric cases along with identity federation but lacked the ability to address IAM

requirements for cloud-based infrastructure. The second type of IDaaS Access Management vendors include those that are born in the cloud to manage access management requirements of SaaS and IaaS applications and services but have architectural limitations in how these could be extended to address access management for on-premises deployments.

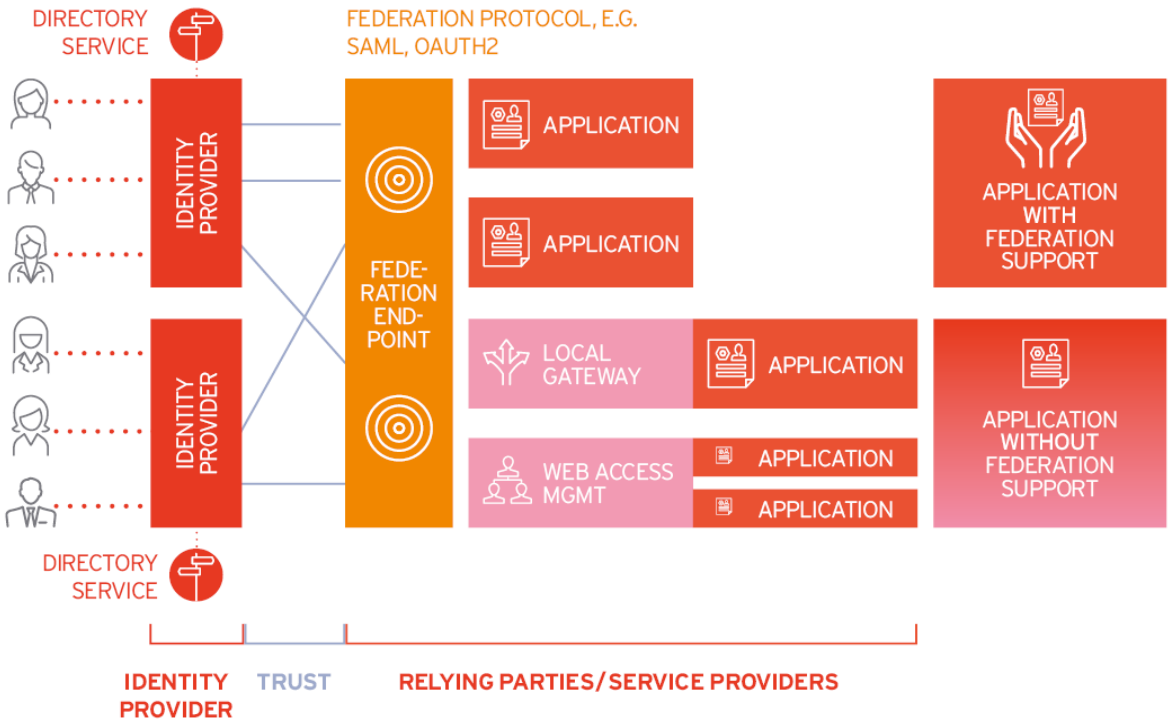


Figure 1: Access Management

Over the last few years, these vendors have made significant changes to their product architecture to become cloud-ready or support extended on-premises applications. These methods include delivering a SSO experience to users across multiple web sites and allow for centralized user management, authentication, and access control. Although traditional on-premises access management solutions was a focus of previous WAM & Identity Federation Leadership Compasses, KuppingerCole sees a convergence of this market with Access Management focused IDaaS solutions. Therefore, this Leadership Compass will consider solutions deployed on-premises, in the cloud, or as a hybrid model. Additionally, solutions offered as a managed service will also be considered, if the technology is owned by the MSP (Managed Service Provider).

As the access management and IDaaS markets continue to evolve and gain maturity, well-established players and innovative start-ups are starting to improve and deliver similar but unique solutions for consumer and enterprise use cases. Fundamental changes and improvements include simplified design of user journeys and enhanced authentication flows. In addition, new contact-free onboarding experiences from the workforce to the customers, the need for managing human-to-device relationships, passwordless authentication as the new normal, decentralized identities as a way of dealing with identities, the impact of policy-

based access, and the convergence of IGA and access management are just some of the current trends that we are seeing.

Figure 2: Access Management Trends

A few challenges organizations face, however, include the inability to integrate different authenticators, leverage existing technologies, support hybrid scenarios, and work with fraud detection solutions. In the future, seeing more support for fine-grain policy-based access management might become an expectation of ours. Finally, innovative features such as the ability to incorporate decentralized identities and support for onboarding flows involving identity verification would be a requirement as well. It is therefore important that businesses and organizations pursue greater use of access management solutions as they modernize their authentication systems.

Highlights

- The access management market provides several options to organizations and continues to evolve beyond the traditional capabilities seen in the past.
- Access management and Identity Federation should not be seen as separate segments in the IT market.
- Access management is used in any industry or sector that requires secure access to data and resources, and compliance with regulatory requirements.
- The impact of Covid-19 has accelerated innovation, rapid cloud adoption, and remote work, making the traditional approach of providing access less relevant as employees now access corporate data and resources from multiple locations.
- By implementing a modern access management solution, organizations are likely to reduce maintenance costs and instead rely on a modern platform that will provide organizations with the right tools to manage digital identities.

- The introduction of passwordless authentication solutions and decentralized identities will continue to drive innovation in the access management space.
- The Overall Leaders (in alphabetical order) are CyberArk, ForgeRock, IBM, Microsoft, Okta, One Identity, OpenText, Oracle, Ping Identity, and Thales.
- The Product Leaders (in alphabetical order) are 1Kosmos, Broadcom, Cloudentity, Cross Identity, CyberArk, EmpowerID, Exostar, ForgeRock, IBM, Microsoft, Okta, One Identity, OpenText, Oracle, Ping Identity, SecureAuth, and Simeio.
- The Innovation Leaders (in alphabetical order) are 1Kosmos, Cloudentity, CyberArk, ForgeRock, IBM, Microsoft, Okta, OpenText, Ping Identity, SecureAuth, and Simeio.
- The Market Leaders (in alphabetical order) are Broadcom, CyberArk, ForgeRock, IBM, Microsoft, Okta, One Identity, OpenText, Oracle, Ping Identity, RSA, and Thales.

Market Segment

Access management and Identity Federation should not be seen as separate segments in the IT market, but these technologies are inseparable. The business challenge is to support the increasingly growing "Connected and Intelligent Enterprise." Businesses require support for both external partners and customers. They need access to external systems, rapid onboarding, and request for access to external services such as Cloud services. Mobile devices are needed for organizations to support their workforce's desires to work anywhere from any device. These are only a few of the challenges organizations must face today.

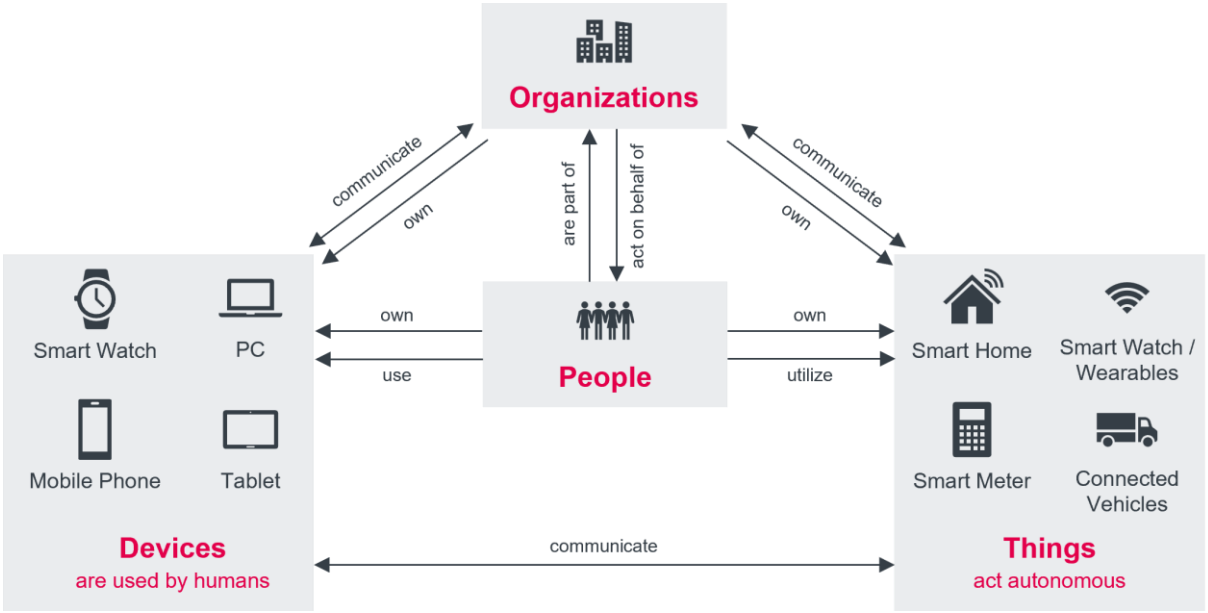


Figure 3: The increasingly connected enterprise ecosystem

The support for open identity standards continues to shape the direction of access management implementations. Some of the most popular authentication and identity federation standards include support for LDAP, Kerberos, OpenID, OAuth, SAML, and

RADIUS. Organizations with a need for dynamic authorization management might require support for OPA, XACML or UMA. User provisioning services commonly require support for SCIM. And having access to the Access Management solution's functionality via APIs or other programmable interfaces will go a long way in keeping your IAM flexible and sustainable. API-based platforms typically require a developer-ready solution, providing API toolkits such as Webhooks or SDKs that facilitate rapid development.

Access management continues to evolve beyond the traditional capabilities seen in the past. Increasingly, we see access management solutions providing security for APIs becoming more readily available and driven by the need to meet emerging IT requirements that include hybrid environments that span across on-premises, the cloud, and even multi-cloud environments. And although Fraud Detection solutions, also referred to as Fraud Reduction Intelligence Platforms (FIPS), is often considered a different market with their separate offerings, there has been a noticeable up-tick in access management solutions providing some level of fraud detection capabilities ranging from the detection of identity fraud through Identity Proofing to the detection of unauthorized account takeover, response mechanisms, or support for user and device profiling as some examples. More recently, there has been some indication and interest of access management support for passwordless authentication and verifiable credentials. This Leadership Compass evaluates and reports on the level of fraud detection, passwordless authentication, and verifiable credentials support for each vendor, giving the reader an indication of the extent of this trend in the access management market.

Besides these technical capabilities, we also evaluate participating access management vendors on the breadth of supported capabilities, operational requirements such as support for high availability and disaster recovery, strategic focus, partner ecosystem, quality of technical support, and the strength of market understanding and product roadmap. Another area of emphasis is providing access management capabilities out-of-the-box, rather than delivering functionality partially through 3rd party products or services. Finally, we also assess their ability to deliver a reliable and scalable access management service with desired security, UX, and TCO benefits.

Delivery Models

There is a clear trend in the market to move access management solutions from an on-premises delivery model to a cloud delivery model. Even though vendors are helping customers to make this transition easier, there will still be valid reasons that organizations will need to maintain an on-premise presence, such as the continued use of legacy and sometimes in-house developed custom systems, among other reasons. Because of this, it is safe to assume that a hybrid delivery model will be a viable option for the foreseeable future. Therefore, this Leadership Compass will consider all delivery models.

Although all delivery models are looked at in this Leadership Compass, it is worth considering each delivery model's pros and cons against the use cases for access management solutions. For instance, some customers still focus on on-premise products due to specific internal organizational reasons such as security policy requirements. It is also

good to be aware that public cloud solutions are generally multi-tenant in most cases, while some cloud services are single tenant. Other approaches use container-based microservice deployments to provide consistent delivery of a vendor's solution, whether cloud-hosted or on-premises. An alternative approach offered is a managed service by a Managed Service Provider that outsources the responsibility for maintaining access management. Ultimately selecting the right access management solution delivery model will depend on the customer requirements and their use cases.

Required Capabilities

When evaluating the products, we start by looking at standard criteria such as:

- Overall functionality
- Size of the company
- Number of customers
- Number of developers
- Partner ecosystem
- Licensing models
- Platform support

Each of the features and criteria listed above will be considered in the product evaluations below. We've also looked at specific USPs (Unique Selling Propositions) and innovative product features that distinguish them from other market offerings.

When looking at this market segment, we evaluate solutions that support a broad range of features that span the access management capabilities within the portfolios of a wide range of vendors in the market. Aside from the baseline access management characteristics such as federation, authentication, authorization, reporting, etc., we expect to see at least some of the capabilities listed in the required qualifications below as necessary features. Furthermore, access management solutions must support centralized management of user access to various types of applications and services and the overall configuration of the solution itself.

Features such as mobile support, governance, and integration with ITSM solutions are also considered but are not mandatory for this category of products. However, delivering a very comprehensive set of capabilities will influence our ratings. In the case of fraud detection, the level of ability will be measured and reported but weighted to a lesser extent.

Expected features include, amongst others:

- Authentication, including:

- Flexible support for different types of authenticators
- Strong authentication (e.g., 2FA, MFA)
- Risk- and context-based authentication
- Adaptive, step-up, and continuous authentication
- Device Authentication (for instance, IoT)
- Toolkits for adding additional authenticators
- Passwordless Authentication options
- A level of analytical and intelligent capabilities
- Decentralized Identities
- Authorization Management
- Access management automation
- Password Management
- Session Management (e.g., Single Sign-On, Secure Token Translation)
- Support for inbound and outbound federation
- Support for all major Identity Federation standards, including SAML and OAuth
- Support for non-federation-enabled applications and other legacy application/services
- Support for a broad range of deployment models, including on-premise deployments
- Integration to existing directory services
- Support for access protocols (OAuth, OIDC etc.) and open identity standards such as FIDO, etc.
- Support for user self service
- User onboarding and registration
- Self-services for credentials and user profiles
- Integration and/or synchronization to directory services
- Support for federated provisioning

- Centralized management of users, authorization policies, dashboards, etc.
- A comprehensive set of APIs, exposing capabilities via APIs and not just UI/UX
- Support for audit, forensics, compliance, and reporting
- Solution architecture (e.g., how modern is the architectures and the technologies used)
- Support for Administrators and DevOps

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

Other comprehensive capabilities to be considered, that are highly valued and will influence our ratings, but are not mandatory for this category of products are:

- Mobile support
- API Security
- Analytics and access intelligence
- Fraud detection
- Security orchestration
- Managing access to Container repository/registry
- Integration with ITSM solutions
- Integrations with threat intelligence solutions
- Access Governance

Inclusion criteria:

- A baseline level of support for the capabilities listed above
- On-premises, cloud, or hybrid solutions
- Support for both Access Management & Identity Federation capabilities
- IAM suites providing a comprehensive feature set for Access Management and Identity Federation

Exclusion criteria:

- Point solutions that support only isolated capabilities such as 2FA or Enterprise SSO centric solutions, but little support the other expected features

- MSP solutions that are based on technology of other vendors, with the MSP not owning the IP on the technology
- Vendors without active deployments at customers (e.g., start-ups in stealth mode) will not be considered.
- Solutions that lack a comprehensive set of APIs will not be considered.

We cover vendors from all regions, from start-ups to large companies. In the end, picking the right vendor will always depend on your specific requirements and your current and future IT landscape that will be managed.

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

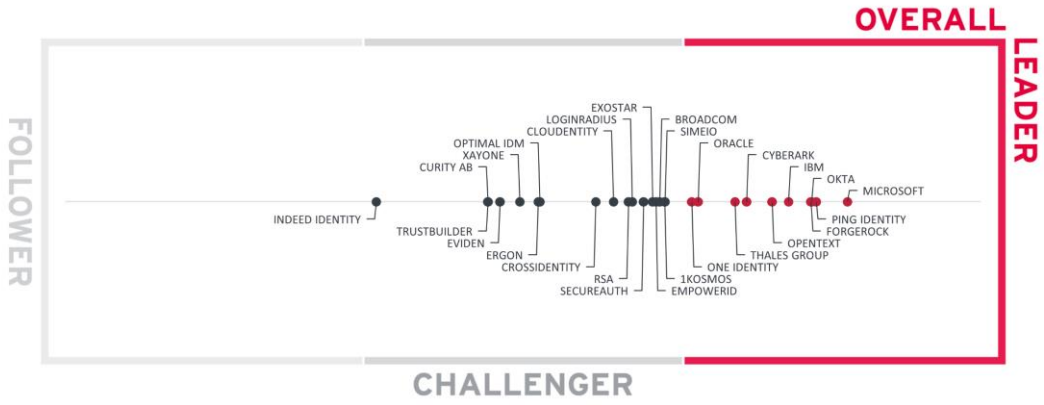


Figure 4: The Overall Leadership rating for the Access Management market segment

Overall Leaders are (in alphabetical order):

- CyberArk

- ForgeRock
- IBM
- Microsoft
- Okta
- One Identity
- OpenText
- Oracle
- Ping Identity
- Thales

The Overall Challengers are (in alphabetical order): 1Kosmos, Broadcom, Cloudentity, Cross Identity, Curity, EmpowerID, Ergon, Eviden, Exostar, Indeed Identity, LoginRadius, Optimal IDM, RSA, SecureAuth, Simeio, TrustBuilder, and XAYone.

Product Leadership

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

Figure 5: The Product Leaders in the Access Management market segment

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services. All vendors in the Product Leadership deliver leading-edge capabilities across the depth and breadth of the Access Management capability spectrum evaluated for the purpose of scoring the vendors in this Leadership Compass. However, we can also observe several much smaller vendors among the leaders, which nevertheless are able to offer their solutions with comprehensive capabilities, flexible deployment options and lower operational complexity than the market giants.

Product Leaders (in alphabetical order):

- 1Kosmos
- Broadcom
- Cloudentity

- Cross Identity
- CyberArk
- EmpowerID
- Exostar
- ForgeRock
- IBM
- Microsoft
- Okta
- One Identity
- OpenText
- Oracle
- Ping Identity
- SecureAuth
- Simeio

The Product Challengers are (in alphabetical order): Curity, Ergon, Eviden, Indeed Identity, LoginRadius, Optimal IdM, RSA, Thales, TrustBuilder, and XAYone. All these vendors have striking offerings but lack certain advanced capabilities that we expect to see, either in the depth or breadth of functionalities seen in the Leadership segment offerings. There are no Followers in the Product Leadership rating.

Innovation Leadership

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

Figure 6: Innovation Leaders in the Access Management market segment

Innovation Leaders are those vendors that deliver cutting edge products, not only at customer request 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 strong 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.

Innovation Leaders (in alphabetical order):

- 1Kosmos
- Cloudentity
- CyberArk
- ForgeRock
- IBM
- Microsoft
- Okta
- OpenText
- Ping Identity
- SecureAuth
- Simeio
- Thales

The Innovation Challengers are (in alphabetical order): Broadcom, Cross Identity, Curity, EmpowerID, Ergon, Eviden, Exostar, LoginRadius, One Identity, Optimal IdM, Oracle, RSA, TrustBuilder, XAYone. These companies also have some specific innovations that make their solutions attractive to their customers but lack the breadth of innovation that other vendors demonstrate. Indeed Identity appears as a Follower.

Market Leadership

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

Figure 7: Market Leaders in the Access Management market segment

Market Leadership is a combined measure of customers, managed users, partners, the geographic distribution of customers, support, and partners, and overall financial position. These vendors have financial strength, geographic distribution of customers and partners, and extensive ecosystems of system integrators.

Market Leaders (in alphabetical order):

- Broadcom
- CyberArk
- ForgeRock
- IBM
- Microsoft
- Okta
- One Identity
- OpenText
- Oracle
- Ping Identity
- RSA
- Thales

The Market Challengers are (in alphabetical order): 1Kosmos, Cloudentity, Cross Identity, Curity, EmpowerID, Ergon, Eviden, Exostar, Indeed Identity, LoginRadius, Optimal IdM, SecureAuth, Simeio, TrustBuilder, and XAYone. Some of these vendors are relatively young, lack a comprehensive global presence, focus mainly on their home markets, or are still in their growth phase.

Correlated View

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

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

The Market/Product Matrix

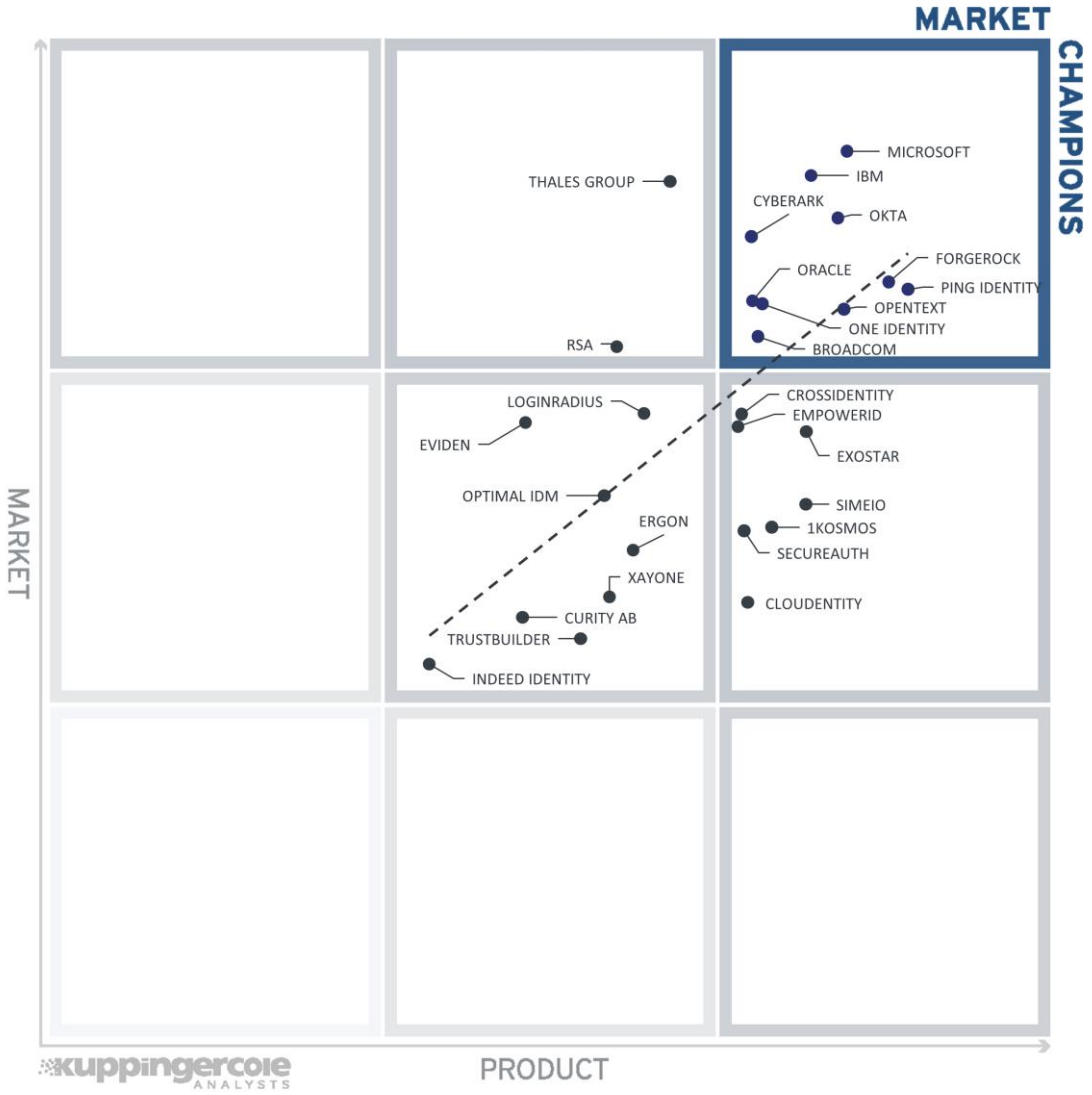


Figure 8: The Market/Product Matrix

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

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

This comparison shows which vendors are better positioned in our Product Leadership analysis than their position in the Market Leadership analysis. Vendors above the line are somewhat “overperforming” in the market. It comes as no surprise that these are often very

large vendors, while vendors below the line may more often be innovative but focused on specific regions as an example.

In the upper right segment, we find “Market Champions.” Given that the access management market is mature but still evolving in areas, we see Microsoft and IBM as market champions positioned in the top right-hand box. Close to this group of long-established AM players in the same box are (in alphabetical order) Broadcom, CyberArk, ForgeRock, OpenText, Okta, One Identity, Oracle, and Ping Identity.

The Thales Group and RSA are positioned in the box to the left of market champions, depicting their stronger market success over product strength.

In the middle right-hand box, we see a number of vendors that deliver strong product capabilities for access management but are not yet considered Market Champions. EmpowerID, Exostar, Cross Identity, Cloudentity, Simeio, SecureAuth, and 1Kosmos have a strong potential to improve their market position due to the more robust product capabilities they are already delivering.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not market leaders. They also have moderate market success as compared to market champions. These vendors include (in alphabetical order): Curity, Ergon, Eviden, Indeed Identity, LoginRadius, Optimal IdM, TrustBuilder, and XAYone.

The Product/Innovation Matrix

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

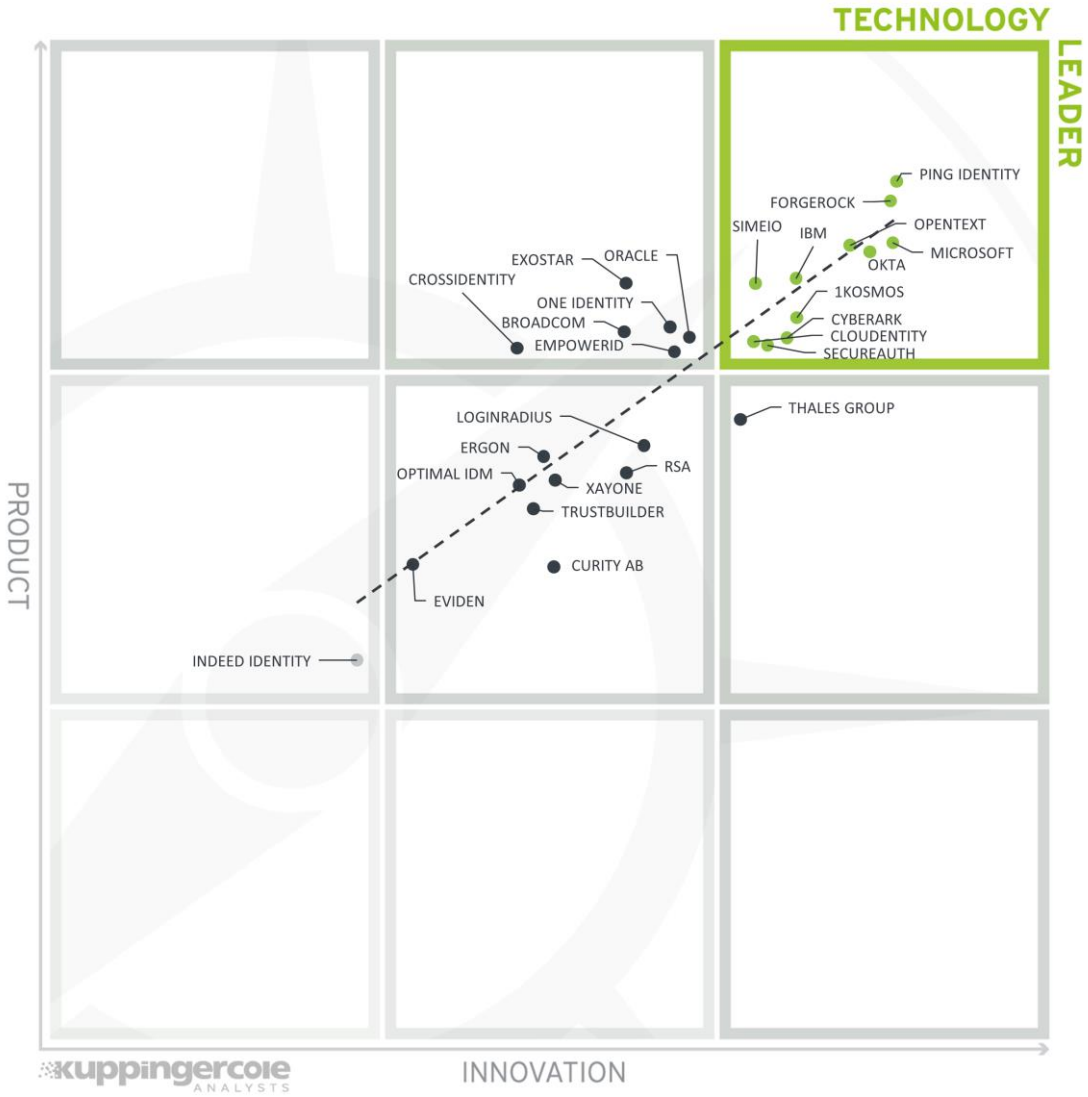


Figure 9: The Product/Innovation Matrix

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

Here, we see a good correlation between the product and innovation rating. Many vendors placed close to the dotted line, indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find most leading vendors

scattered throughout the box in the upper right corner. The leading vendors are Ping Identity, followed by ForgeRock, Microsoft, Okta, IBM, OpenText, Simeio Solutions, Cloudentity, CyberArk, 1Kosmos, and SecureAuth.

Four vendors appear in the top middlebox with good products but less innovation than the leaders, including Broadcom, Cross Identity, EmpowerID, Exostar, One Identity, and Oracle.

Over a third of the vendors appear in the middlebox, showing both innovation and product strength, which includes (in alphabetical order): Curity, Ergon, Eviden, LoginRadius, Optimal IdM, RSA, Thales Group, TrustBuilder, and XAYone.

One vendor, Indeed Identity, appear in the middle-left box, showing stronger product capabilities than innovation.

The Innovation/Market Matrix

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

Figure 10: The Innovation/Market Matrix

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

Vendors above the line perform well in the market compared to their relatively weaker position in the Innovation Leadership rating. In contrast, vendors below the line show, based on their ability to innovate, have greater potential for improving their market position.

In the upper right-hand corner box, we find the “Big Ones” in the access management market. We see Microsoft, IBM and Thales Group on top, with the remainder of the vendors towards the bottom half of the same box, which includes (in alphabetical order) ForgeRock, Okta, CyberArk, Ping Identity, and OpenText, indicating that they haven’t yet reached the same market position as the more established players.

Oracle, Broadcom, One Identity, and RSA are shown in the top middlebox with a stronger market, although less innovation than the leaders.

Four vendors, Cloudentity, SecureAuth, Simeio Solutions, and 1Kosmos, are shown in the middle right box showing good innovation with slightly less market presence than the vendors in the “Big Ones” category.

The segment in the middle of the chart contains a third of the vendors rated as challengers both for market and innovation, which includes (in alphabetical order) Cross Identity, Curity, EmpowerID, Ergon, Eviden, Exostar, LoginRadius, Optimal IdM, TrustBuilder, and XAYone.

Only Indeed Identity appears in the middle-left box, indicating market presence with lower innovation. However, Indeed Identity has the potential to become more innovative, increase market presence, or both.

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Access Management Platforms. 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
1Kosmos	Strong Positive	Positive	Positive	Positive	Strong Positive
Broadcom	Strong Positive	Strong Positive	Strong Positive	Positive	Positive
Cloudentity	Strong Positive	Positive	Strong Positive	Positive	Strong Positive
Cross Identity	Strong Positive	Strong Positive	Positive	Positive	Positive
Curity	Positive	Positive	Positive	Positive	Neutral
CyberArk	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
EmpowerID	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
Ergon Airlock IAM	Strong Positive	Positive	Positive	Positive	Positive
Eviden	Strong Positive	Positive	Positive	Neutral	Positive
Exostar	Strong Positive	Positive	Positive	Neutral	Positive
ForgeRock	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
Indeed Identity	Positive	Neutral	Weak	Neutral	Neutral
LoginRadius	Positive	Positive	Positive	Positive	Positive

Microsoft	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Okta	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
One Identity	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
OpenText	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
Optimal IDM	Strong Positive	Positive	Positive	Positive	Positive
Oracle	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
Ping Identity	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
RSA	Strong Positive	Positive	Strong Positive	Positive	Strong Positive
SecureAuth	Strong Positive	Positive	Strong Positive	Positive	Strong Positive
Simeio	Strong Positive	Positive	Positive	Strong Positive	Positive
Thales	Strong Positive	Positive	Positive	Strong Positive	Strong Positive
TrustBuilder	Positive	Neutral	Neutral	Positive	Positive
XAYone	Positive	Positive	Neutral	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
1Kosmos	Strong Positive	Neutral	Positive	Neutral
Broadcom	Positive	Positive	Strong Positive	Strong Positive
Cloudentity	Strong Positive	Positive	Neutral	Positive
Cross Identity	Strong Positive	Positive	Neutral	Positive
Curity	Positive	Positive	Neutral	Neutral
CyberArk	Strong Positive	Strong Positive	Positive	Strong Positive
EmpowerID	Strong Positive	Neutral	Positive	Neutral
Ergon	Positive	Positive	Positive	Positive
Eviden	Neutral	Positive	Positive	Positive
Exostar	Neutral	Strong Positive	Strong Positive	Positive
ForgeRock	Strong Positive	Strong Positive	Strong Positive	Strong Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Indeed Identity	Weak	Neutral	Neutral	Neutral
LoginRadius	Positive	Positive	Neutral	Positive
Microsoft	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Okta	Strong Positive	Strong Positive	Strong Positive	Strong Positive
One Identity	Strong Positive	Positive	Positive	Positive
OpenText	Strong Positive	Positive	Strong Positive	Strong Positive
Optimal IDM	Positive	Neutral	Positive	Neutral
Oracle	Positive	Strong Positive	Strong Positive	Positive
Ping Identity	Strong Positive	Strong Positive	Strong Positive	Strong Positive
RSA	Neutral	Strong Positive	Strong Positive	Strong Positive
SecureAuth Corporation	Strong Positive	Positive	Positive	Positive
Simeio	Strong Positive	Positive	Positive	Neutral
Thales Group	Strong Positive	Strong Positive	Strong Positive	Strong Positive
TrustBuilder	Neutral	Neutral	Neutral	Positive
XAYone	Neutral	Positive	Neutral	Positive

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 the LC Access Management, we look at the following six categories:

- **Federation, SSO, & Session Management:** The depth in which solution supports Identity Federation, Session Management & SSO is provided and its support of standards. Identity Federation ability to supply Service Provider (SP) and/or Identity Provider (IdP) functionality and federation provisioning to cloud services, for example. The solution's use of APIs/ SDKs to expose federation services, consume third-party identities, and social media integration are also considered. Session Management & SSO looks at the depth to which the solution can handle user web sessions, session protection, ability to detect session attacks as examples. Also, the solution's ability to provide Web SSO, Enterprise SSO, and supported SSO mechanisms and secure token translation are evaluated as well.

- **Authentication:** The breadth of authentication support for multiple form factors and support for step-up authentication is measured, as well as the depth of contextual and risk-adaptive authentication. Also considered are various aspects of contextual attributes at each interaction channel and layer, for example.

- **Authorization & Policy Management:** This category looks at the solution's level of policy management and the ability to manage access using authorization features. Examples include the types of policies available using ABAC, RBAC, and/or CBAC principles for example, dynamic vs. coarse-grained policies, the capability to make rule-based decisions, and the ability to define and test policies using authoring/editing tools as examples.

- **API Security:** This section evaluates the level of API security such as protecting APIs against other attacks such as API authentication & authorization, validating API calls against API schema, scanning and/or filtering traffic, or API key management, to name a few API security features.

- **Analytics and Access Intelligence:** This looks at the level of analytics and access intelligence is used within the Access Management solutions.

- **Fraud Detection:** This category measures the solution's level of fraud detection and mitigation abilities. Some capabilities include collecting and analyzing information for

fraud prevention, User and Entity Behavior Analytics (UEBA), detecting unauthorized account takeover, user and device profiling, orchestration of fraud signals, and identity proofing.

- **UI, Dashboards & Reports:** This section looks at the solution's overall user interface usability as well as its ability to provide a consolidated view and management of all access, regardless of where the solution is deployed. Centralized visibility often features a single pane view via a dashboard and provides visibility to users, threats, policy management, licenses, configuration, etc. Also elevated is the solution's ability to demonstrate compliance, support auditing, and forensic activities through capabilities such as logging a user's access to resources or administrators' changes to the system and running out-of-the-box, ad-hoc, or custom reports in various formats.

- **Admin & DevOps Support:** This category measures the ability to provide IT environmental assistance options for administrators and the operations team to support their tools, automation, and continuous integrations. Also evaluated is the vendor's ability to support developers using the solution's APIs through documentation, tutorials, tools, knowledgebase, and community support/platform for developers.

1Kosmos – BlockID Workforce and BlockID Customer

1Kosmos was founded in 2018 and is headquartered in New Jersey. They address the consumer and workforce identity management markets with their blockchain ID solution aimed at giving secure identity control back to the user, with a focus on reducing fraud. It leverages cutting-edge technologies such as biometrics, passwordless authentication, decentralized identity, and distributed ledger technology to ensure a high level of identity assurance and protection. The BlockID platform provides a suite of products for enterprise use (BlockID Workforce), private consumer use (BlockID Customer), and identity verification (BlockID Verify). Coverage includes North America, Middle East, United Kingdom, India, Singapore, and Australia.

For their workforce offering, BlockID Workforce introduces identity proofing and onboarding features which allow employees to enroll their biometric credentials to login. The solution encrypts each user's biometric data with their own cryptographic key pair, storing the private key in their device's secure enclave. BlockID Customer provides biometric passwordless authentication with optional identity proofing that can adjust to flexible levels of identity assertion to support the evolving needs of customers while maintaining access to multiple accounts via one consistent experience.

In addition, BlockID has a real biometrics capability called LiveID, which uses a proprietary 3D modelling technique for face detection. It is Patent Pending and captures the live motion, emotion as well as 3D map of a user’s face, including depth detection, and checking the distance between ears and nose to ensure that a complete map of a user's face is taken while enrolling the user. This is immediately followed by asking the user to provide a government-issued document such as a driver's license or a passport to ensure that the user enrolling the LiveID is the same user who has enrolled into BlockID.

BlockID as SaaS supports public and private cloud and hybrid deployment models. The platform is delivered as container-based on Kubernetes, which is deployed to multiple cloud providers, such as AWS, GCP, Azure, IBM Cloud, and Oracle Cloud. Furthermore, BlockID integrates with existing identity management systems and platforms, allowing for seamless integration into the organization's infrastructure. It offers a range of APIs and connectors to facilitate easy integration and customization based on specific business requirements. Supported API protocols include REST, RADIUS, JSON-RPC, gRPC, Google Pub/Sub, and Webhooks, as some examples. To strengthen security and support compliance, 1Kosmos has been independently certified with the ISO/IEC 27001 and EIDAS standards, as well as certified by FIDO2, SOC 2 Type II, and PAD2 by iBeta. The company is also certified to the NIST 800-63-3 standard by Kantara.

BlockID has recently improved its developer experience, sandbox environment, and admin dashboard to effectively leverage its digital identity solutions. 1Kosmos also provides its own authenticator, which is FIDO2 certified but also supports Yubico, Trust Key, Feitian, OneSpan, Thetis, Google Titan, and others. The platform has also enabled authentication using the FIDO key on the 1Kosmos mobile app itself. Moreover, the company recently partnered with Arculus, a provider of advanced encryption solutions, to address the growing demand for reliable identity verification across multiple industries and provide customers with enhanced security and user experience.

Overall, BlockID by 1Kosmos offers a robust and innovative approach to Access Management, combining advanced biometric authentication, strong fraud detection features, support for verifiable credentials, and seamless integration capabilities. It empowers organizations to enhance their security posture, streamline access control processes, and ensure a frictionless user experience. 1Kosmos customers are primarily in North America with a growing presence in Europe and the APAC region supporting mid-market to enterprise organizations. 1Kosmos appears in both the product and innovation leadership categories which should be of interest to organizations in North America and the APAC.

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

Table 3: 1Kosmos' rating

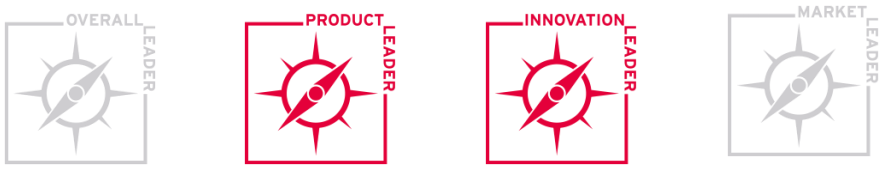
Strengths

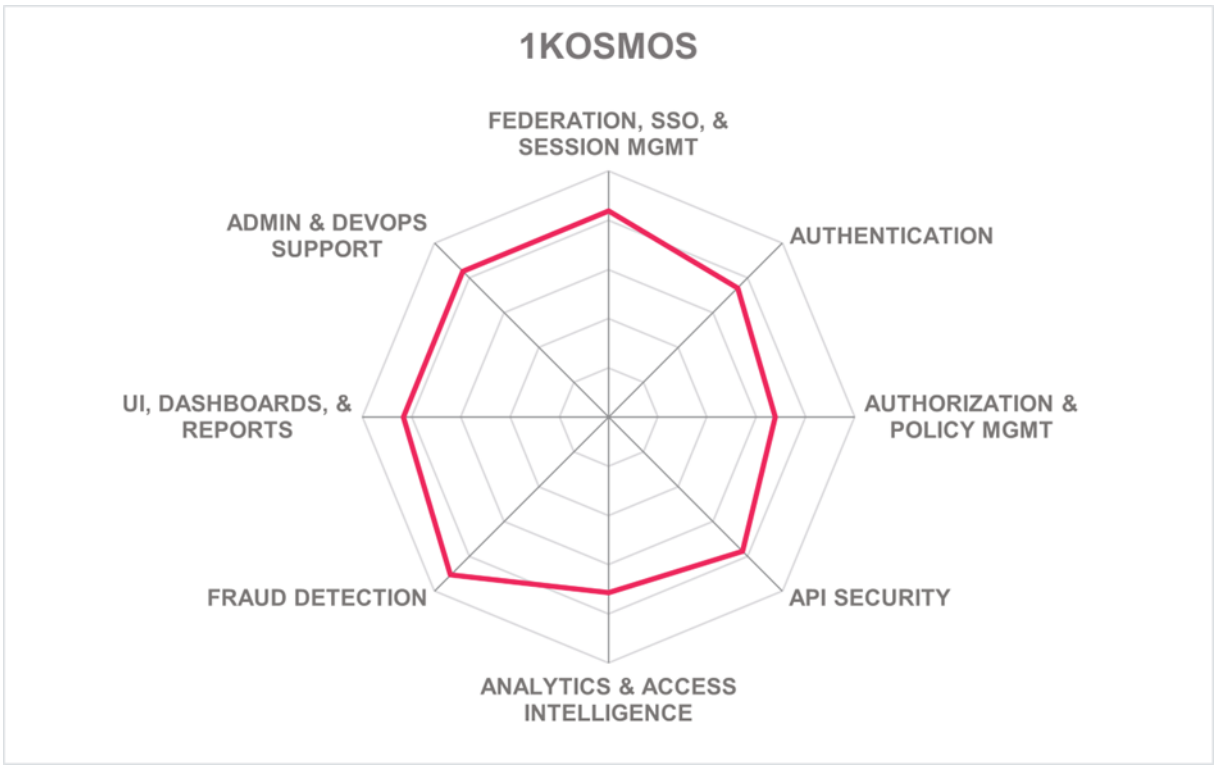
- Identity proofing and onboarding capabilities
- Strong and well-documented set of APIs
- Risk-adaptive authentication
- SSO and session management
- Verifiable credential support
- Passwordless support
- Identity federation
- Admin UI, dashboard features
- Fraud detection
- Innovative features on the roadmap

Challenges

- Small, but growing partner ecosystem
- Moderate API Security capabilities
- SCIM based provisioning to cloud services is not supported
- Little market visibility outside of North America and the APAC regions

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


1KOSMOS
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Broadcom – Symantec Access Management

Broadcom is a world leader in business-critical software designed to modernize, optimize, and protect the world's most complex hybrid environments. The company acquired CA Technologies in 2018, and the Symantec Enterprise business in November of 2019.

The Symantec Identity Service thus comprises multiple solutions for access management, authentication, IGA, and PAM. The Symantec Access Management suite consists primarily of Symantec SiteMinder and components of the Symantec VIP, Symantec IGA, and Symantec Advanced Authentication offerings.

Symantec SiteMinder is a robust access management platform designed to secure modern enterprises. It applies appropriate authentication mechanisms to positively identify users, enable SSO and identity federation for seamless access to applications, enforce granular security policies to prevent unauthorized access to sensitive resources, and monitor and manage user sessions to prevent session hijacking. SiteMinder has a proven history and has been successfully deployed in some of the world's largest IT environments. It provides both scalability and flexibility for large, complex access management deployments.

To enhance its capabilities, the VIP Authentication Hub, built in a microservice containerized format, acts as an authentication policy engine. It enables SiteMinder to incorporate and use various authentication methods and improve its functionality. A good breadth of authentication methods that includes basic password, OTP, QR Code, apps, biometric, passwordless MFA, and hardware tokens is supported, as well as contextual and risk-adaptive authentication as part of its Advanced Authentication portfolio. Essentially, the VIP Authentication Hub extends the capabilities of SiteMinder by providing advanced authentication features and expanding the range of authentication methods available to organizations using the Symantec IAM solution.

Broadcom SiteMinder is primarily software-based that can be deployed to supported operating systems on-premises or in IaaS. Symantec VIP (MFA) is delivered via SaaS. Additionally, Symantec IGA provides an optional Virtual Appliance for deployment. The Symantec IAM Fabric Security Services Platform is micro-service based, containerized, and supports K8s. Managed service offerings, which encompass any of Broadcom's IAM capabilities, are available through partners.

Furthermore, the platform offers a range of APIs and connectors to facilitate easy integration and customization based on specific business requirements. Supported API protocols include SOAP, REST, RADIUS, GraphQL, Webhooks, and LDAP. Symantec SiteMinder handles all federation use cases and supports most related standards such as SAML, OAuth2, OIDC, WS-Federation, JWT, and SCIM. SCIM support is provided by Symantec Directory and Symantec IGA. Good support for 3-party services such as Threat Intelligence or EPP solution via API or SDKs is given.

Broadcom positions itself as a provider of enterprise solutions for large global multinational organizations. In that context, the Symantec access management suite is an interesting option for organizations seeking a comprehensive, flexible, scalable, and modern solution. The company has enterprise-level support globally in both pre-sales and support. The largest proportion of customers are primarily focused on North America.

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

Table 4: Broadcom's rating

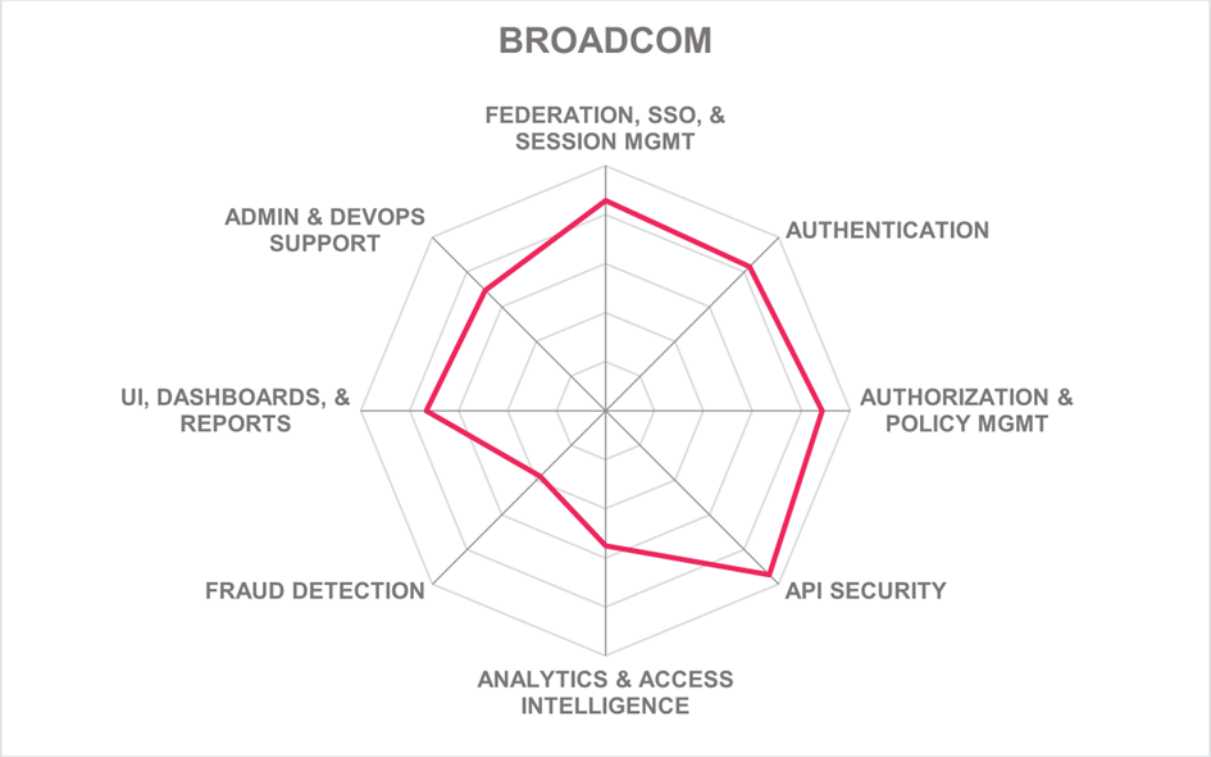
Strengths

- Large global customer base
- Breadth of authentication methods
- High level of flexibility
- API-based approach
- Proven scalability
- Utilizes a modern IAM Security Fabric platform
- Contextual and risk-adaptive authentication
- Strong federation and session management capabilities
- Third-party verifiable credential providers can be used in Government use cases

Challenges

- FIDO supported but not certified
- Fraud detection capabilities have room for improvement
- Analytics and other access intelligence rely on third party solutions
- The solution is more geared towards enterprise-level organizations rather than mid-market or SMB organizations

Leader in


BROADCOM
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Cloudentity – Cloudentity

Cloudentity is a privately held identity and access management company headquartered in Seattle, WA. In 2021, the company introduced its SaaS CIAM platform referred to simply as "Cloudentity". This platform is a cloud-native identity, authorization and consent solution designed to meet the demands of hybrid-cloud services and complex partner ecosystems. Cloudentity focuses on dynamic authorization and authorization as code to secure APIs, microservices, and traditional application workloads. Cloudentity offers its platform for traditional and API-driven access management solutions. The company has a presence in North America and a growing number of customers in EMEA, APAC and Latin America.

Cloudentity offers a significant advantage with its ability to create multiple workspaces (subtenancy), organizations, and identity pools within a single tenant. This feature allows organizations to effectively model different user populations and their unique authentication processes. Additionally, the platform provides the flexibility to define self-service journeys for various user groups, such as employees, customers, contractors, partners, and more. This versatility makes it suitable for both B2B and direct consumer use cases, setting it apart in the market. In addition, by aggregating data from multiple identity providers and API-based systems (including Cloudentity's own Identity Pools and Permission System), Cloudentity enhances the context of identities and requests fed into its policy engine, ensuring that authorization tokens and associated claims are granted only to authorized parties and transactions. This approach enables organizations to generate finer scoped authorization tokens at higher performance levels while reducing the potential attack surface.

The Cloudentity platform is built as a set of highly scalable, distributed microservices that can be delivered in a SaaS, customer deployed or hybrid model providing customers with flexible deployment options for cloud and edge protection. Cloudentity is entirely API-driven, so 100% of the Cloudentity functionality is available via APIs and its UI. SDKs are generated on the fly to provide SDKs for over 40 different programming languages and variants. Leveraging Cloudentity's JavaScript extension capability allows customers to extend functionality via authorization-based orchestration with external APIs or microservices.

The platform recently made significant improvements to its next-generation permissions service, an advanced solution that enables organizations to manage and enforce fine-grained access control and authorization policies within their applications and systems. It provides a flexible and scalable framework for defining permissions, roles, and entitlements, allowing organizations to efficiently manage access to resources based on user identities and their relationships. The next-generation permissions service leverages technologies such as the Zanzibar relational graph to enable organizations to manage complex entitlement objects and effectively control access across their entire ecosystem.

Cloudentity serves mid-market to enterprise organizations, with customers in various regions in the world. The platform could be considered unorthodox from other traditional access management solutions, although it provides a modern Zero-Trust approach to access management use cases for APIs and legacy Apps. Cloudentity, being a rather young vendor in IAM space, has a still relatively small global partner ecosystem, compared to many of the other vendors. On the other hand, Cloudentity is very innovative and provides a modern solution that fits well to the architecture requirements of a modern access management solution. Cloudentity appears in both the product and innovation leadership categories.

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

Table 5: Cloudentity's rating

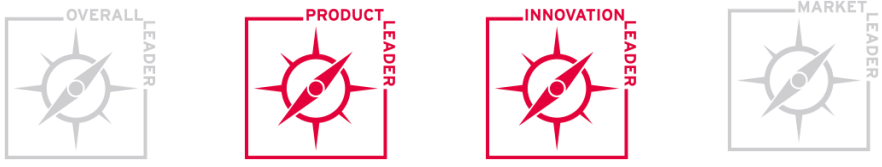
Strengths

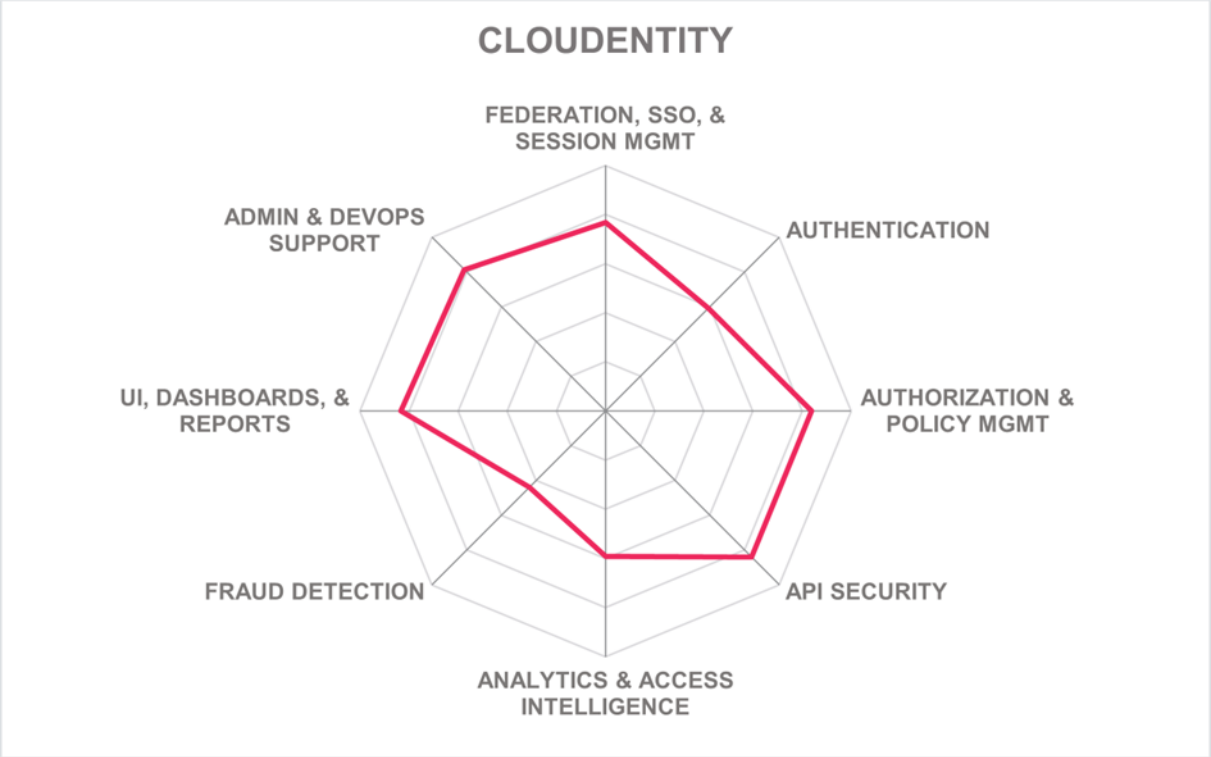
- Modern architecture
- Proven scalability
- Good Admin and DevOps support
- Strong API Management and API Security with integrated policy-based access control
- Rich extension and third-party integration capabilities
- Extensive branding customization options
- Advanced OAuth (mTLS, DPoP, PAR, RAR, FAPI 1.0 & 2.0, OAuth step-up) support
- Federation, SSO, and session management support
- Delegated administration for organizations and user populations
- Innovative authorization and policy management features

Challenges

- Lacks depth of out-of-the-box features in certain areas, such as fraud detection
- Customers may initially find the platform daunting without adequate assistance
- Solution cannot integrate with policy management tools other than OPA, but improvements are on the roadmap

Leader in




CLOUDENTITY
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Cross Identity – Cross Identity

Cross Identity, formerly known as Ilantus Technologies, has been in the IAM domain since 2000, with a focus on delivering IGA and access management capabilities on a single platform with multiple services. The product services include IGA, access management, PAM, and CIAM features. Apart from its headquarters in Schaumburg, Illinois, Cross Identity has additional offices in Bangalore, India. Coverage is primarily focused on North America and the APAC region, but with a growing presence in EMEA and Latin America.

Cross Identity provides a comprehensive IAM solution in a single platform. It includes access management, IGA, PAM, and passwordless authentication. Cross Identity is a lightweight and user-friendly solution with a single source code that includes the aforementioned services. Admins can easily navigate and configure features using the platform's self-guided option, eliminating the need for external searches or documentation. Cross Identity offers various ways to create identities, including a universal directory, integration with external applications such as HRMS, and the ability to import user details from CSV files. These features simplify identity management and integration processes. Cross Identity also supports various authentication mechanisms, MFA and SSO, and certificate-based authentication. MFA requires administrators to provide additional authentication factors, such as a one-time password (OTP) generated by a mobile application or a hardware token. With SSO, administrators can log in to multiple applications with a single set of credentials.

Cross Identity offers a range of authenticator options such as Windows Hello, Mac Touch ID, Android Biometrics, iOS Biometrics, FIDO UAF & U2F, and FIDO2. It also supports risk-adaptive authentication, considering device, user, and network contexts. The solution provides centralized policy management that supports various access principles like ABAC, PBAC, RBAC, CBAC, RAdAC, ReBAC, and user-group access, complemented by basic role management features. Password management supports password syncing across multiple identity repositories and a range of password recovery options. Cross Identity also supports passwordless authentication on the Web and Desktop access.

Cross Identity supports on-premises, public and private cloud, multi-cloud, and hybrid deployment models, delivered as SaaS or software deployed to a server or managed service. A pay per use model/consumption-based model is also supported by the company. A container-based delivery option supports Docker and Red Hat container-based platforms. For IaaS installations, Cross Identity supports most cloud platforms such as AWS, GCP, Azure, etc. Most features and capabilities are available via REST APIs. Other API protocols such as SOAP, Webhooks, SCIM, JSON-RPC, and XML-RPC are supported, although gRPC is not. In addition, Cross Identity Client SDKs can provide various authentication mechanisms that make it easier to authenticate and call API endpoints.

The company started in 2000 with decades of global IAM implementation experience. Cross Identity differs from many of the other offerings in the IAM market in both the flexible deployment options, and the breadth of supported capabilities. It comes as a full IAM package, covering IGA, Access Management, PAM, and other capabilities that businesses require. While some of the capabilities are more at the baseline level, for both IGA and Access Management comprehensive capabilities are supported and that will be sufficient for most businesses. Cross Identity appears in the product leadership category.

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

Table 6: Cross Identity's rating

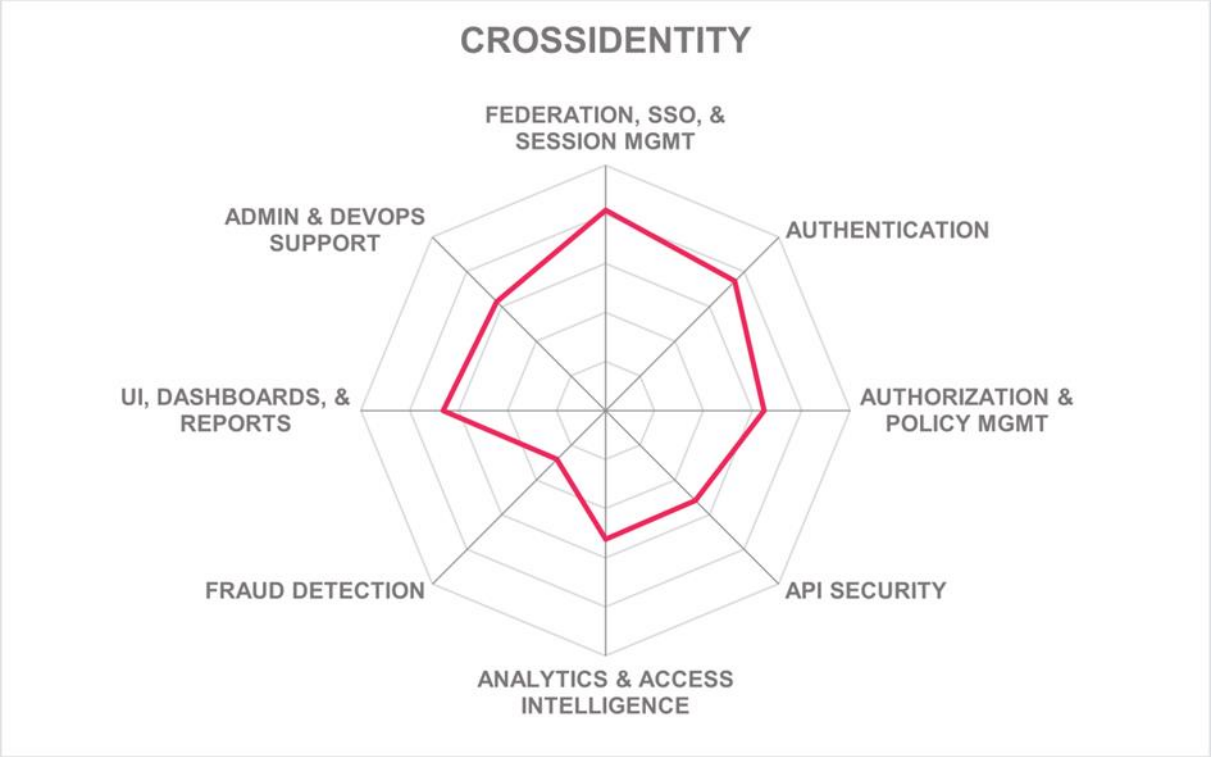
Strengths

- Flexible solution
- Strong UEBA capabilities
- Modern UI and dashboards
- FIDO 2 authentication options
- Good reporting capabilities
- Authorization & policy management
- Single platform with multiple services
- User-friendly solution with a single source code
- Good support for in-built MFA with contextual attributes
- Increased focus of enhancing user and administrative experience

Challenges

- Focused on the mid-market
- Moderate partner ecosystem focused on NA and APAC regions
- Somewhat limited fraud detection capabilities, but risk scoring, and risk-based authentication is supported
- Managing market perception and maintaining a positive reputation throughout the rebranding process is crucial

Leader in


CROSSIDENTITY
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Curity – The Curity Identity Server

Curity is a provider of API-focused identity management solutions based in Stockholm, Sweden. Launched in 2015, the company is focused on providing identity services for APIs and microservices and removing complexity by externalizing and centralizing access control across any API. The Curity Identity Server adheres to many identity standards, to promote interoperability and to make it easier for clients to deploy necessary new features while shielding users from complexity. The company is primarily focused on the EMEA region, but with a growing number of customers in North America and Latin America.

The product has a strong focus on DevOps, with an API-focused approach and a user interface designed for developers and operators. By using the Curity Identity Server, organizations can secure their digital services in configuration and not in code, thus reducing the complexity of development and maintenance. It is composed of three major modules: Authentication Service, Token Service, and User Management Service. The Authentication Service provides a wide range of authenticators, including SSO for web and mobile devices. It offers customizable login and registration pages and supports Hypermedia Authentication API (HAAPI), which allows creating native clients that use OAuth and OpenID Connect flows without relying on browser support. The platform also allows password resets, account creations, and other authentication methods such as social logins, e-IDs, and more.

The foundation for app and API security is the Token Service. The Token Service issues security tokens like OAuth Access Tokens, Refresh Tokens, and OpenID Connect ID Tokens. Curity is an OpenID Foundation certified implementation and supports various OAuth 2 and OpenID Connect sub-standards, allowing customization of tokens with different claims and scopes. Furthermore, the User Management Services enables users to manage their accounts via a protected graphical and programming interface and allows admins to handle user accounts and permissions, manage delegations, and revoke tokens; to accomplish this using programmatic means, customers may leverage the products SCIM standard interface as well as a GraphQL API. The Curity Identity Service's User Management module is designed to integrate with existing customer portals and user data repositories, including noSQL and SQL databases as well as LDAP. The platform supports over 30 types of authentication methods for admin access including but not limited to: Passkeys/WebAuthn, OpenID Connect federation, SAML Federation, Email OTP, SMS OTP, TOTP, BankID, Duo, and username and password. The Curity Identity Server can be deployed on-premises or in any cloud platform; it can also be deployed across multiple clouds if needed. It supports OAuth 2, OpenID Connect, and SCIM, offering a modern solution for both internal and external users. Supported API protocols include REST, GraphQL, Webhooks, and LDAP. It is compatible with containerized environments like Docker, Kubernetes, and Helm, and offers integrations and guides for cloud platforms such as AWS, Azure, and GCP. The solution supports various access principles like ABAC, PBAC, RBAC, CBAC, RAdAC, ReBAC, and user-group access.

Overall, the Curity Identity Server's advanced features, extensive support for industry standards, comprehensive token management capabilities, and robust documentation and resources makes it a good alternative for medium and mid-market organizations. The company's API-driven approach enables seamless integration and interoperability with other systems and applications, allowing for efficient data exchange and communication. The Curity Identity Service should be of interest to organizations around the world who are providing digital services to apps and websites.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Neutral

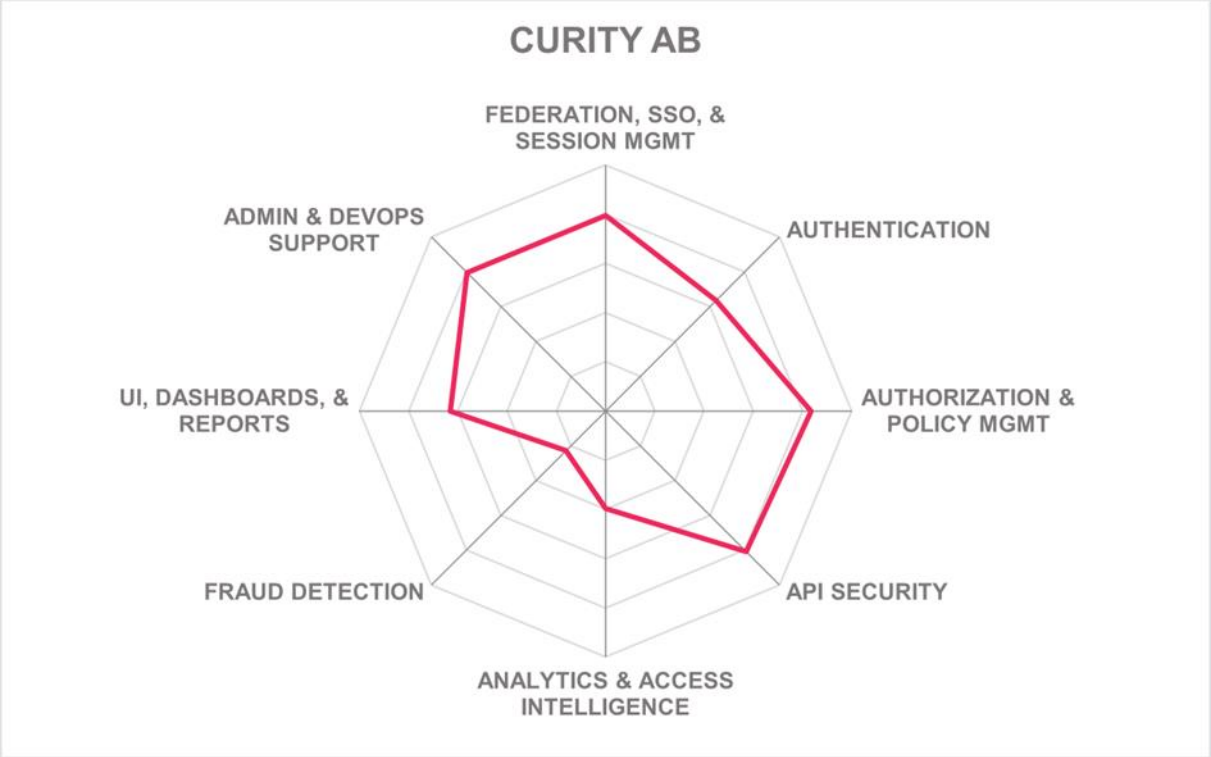
Table 7: Curity's rating

Strengths

- Modern architecture
- Friendly user experience
- Modular API-focused approach
- SSO and session management
- Good Admin and DevOps support
- Cutting edge support for verifiable credentials
- Comprehensive support for OAuth and OIDC open standards
- Combines flexible authentication with token-based API security controls
- API security solution focusing only on identity and access management

Challenges

- Reporting not supported
- Lack of fraud detection capabilities
- Limited analytics and access intelligence features
- Relatively small market presence outside of EMEA


CURITY AB
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

CyberArk– CyberArk Identity

Having been in the market since 1999, CyberArk has established itself as a leader in Identity Security. CyberArk helps companies protect their highest-value information assets, infrastructure, identities, and applications. Headquartered in Israel and the US, CyberArk has offices in over 15 countries including the U.K., France, Germany, the Netherlands, India, and Singapore and serves customers in more than 65 countries. Since the acquisition of Idaptive in May 2020, a spin-off of Centrify, the company has continued to add technical functionalities to its broad suite of products in response to changing market demands.

The CyberArk Access Management solution is CyberArk Identity, which unifies Workforce and Customer Access and Identity Management capabilities in a single offering. CyberArk Identity is an integral part of the CyberArk Identity Security Platform, which provides capabilities across workforce and customer access, endpoint privilege security, PAM, secrets management, cloud privilege security, and identity management. The CyberArk Identity Security Platform stands out because it goes beyond just a collection of products. It offers a cohesive set of solutions that work together and share key components, creating a unified platform for various use cases. Workforce and customer access capabilities include SSO, app gateway, adaptive MFA, UBA, endpoint security, workforce password management, secure web sessions, and B2B identity. Identity management solutions include identity lifecycle management, identity flows, and identity compliance. A central CyberArk Identity Cloud Directory serves as the foundation for the platform, enabling seamless configuration and deployment of downstream solutions. CyberArk's focus is on providing a comprehensive experience for different types of users, such as employees, customers, partners, and more.

CyberArk Identity is a fully cloud-hosted SaaS-delivered service that runs on the AWS platform. It supports public cloud and hybrid deployment models with its App Gateway service, enabling VPN-less, Zero Trust access, SSO, and access management capabilities back to on-premises applications and services. The cloud service supports a Managed Service Provider mode, where MSPs can manage the entire lifecycle of customer tenants. In addition, CyberArk Identity supports REST APIs, which include standards-based authentication and directory services based on LDAP, RADIUS, etc. SDKs are publicly available on CyberArk's developer-focused portal supporting the C/C+, .NET, Python, Ruby, and Go programming languages.

CyberArk Identity offers a modern UI that is easy to navigate and use. Its User Behavior Analytics (UBA) service, which powers Adaptive MFA provides built-in reports and dashboards with a flexible and customizable widget framework. CyberArk Identity also allows users to easily register their devices via email, SMS, or QR code scan in a completely passwordless fashion for all possible applications. Moreover, CyberArk supports hardware tokens, CAC/PIV card, Duo, Feitian, Google Titan, Kensington Security Key, OneSpan Digipass, RSA SecurID, Smartcards, Symantec VIP, Thetis, and YubiKey tokens. In addition, CyberArk supports FIDO2 standards and integrates with many other vendors through other standards such as OATH HOTP/TOTP, RADIUS, SAML, and OIDC.

CyberArk has a strong offering for access management, with CyberArk Identity serving primarily mid-market to enterprise organizations. The company's primary focus is on North America, but it has also experienced significant growth in the EMEA, APAC, and Latin America markets, which is bolstered by a robust partner ecosystem. This makes CyberArk a good option for organizations seeking a comprehensive, feature-rich, and modern solution.

CyberArk appears in all Leadership segments with a well-balanced set of features for access management.

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

Table 8: CyberArk's rating

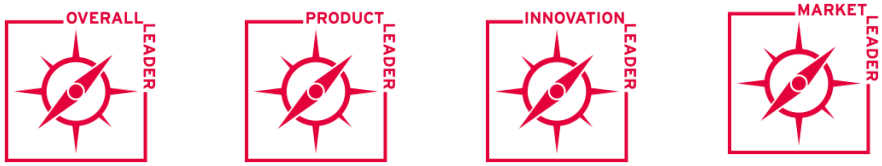
Strengths

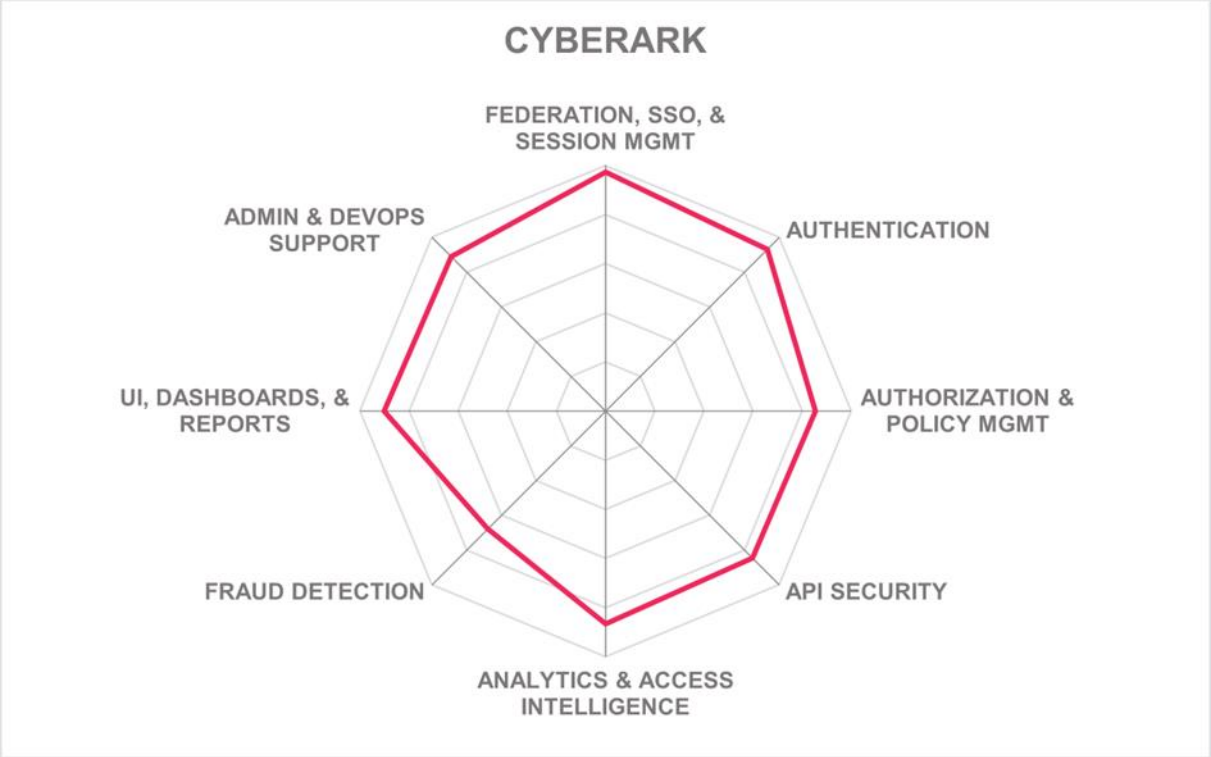
- Strong partner ecosystem
- Friendly user experience
- Good API Security
- Proven scalability
- Fraud detection features
- Admin & DevOps support
- Large selection of authenticators accepted
- Good use of analytics and access intelligence
- Strong federation, SSO, and session management
- Convenient solution for remote access and BYOD scenarios

Challenges

- High modularity of solution could be unfavorable for certain deployments
- Missing decentralized identity & verifiable credentials support
- Limited third-party integrations to fraud detection & protection solutions OOB
- Additional integrations with 3rd party UBA vendors would be beneficial but enhancements are on the roadmap

Leader in




CYBERARK
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

EmpowerID– EmpowerID Suite

Founded in 2005 and based in Ohio (US), EmpowerID offers multiple products in a suite which includes EmpowerID password management, group management, dynamic group management, lifecycle management, advanced lifecycle management, SSO, MFA, access recertification, risk management, advanced risk management, and policy-based access control (PBAC) as components of its access management portfolio. Coverage includes North America, Europe, and the APAC region.

The company aims to streamline and automate identity management and access, following a zero-trust framework as the guiding principle. Its primary focus is serving large and complex enterprises in the European and North American markets, although it also caters to consumer use cases. With a strong emphasis on B2B and B2E scenarios, the product specializes in authorization policies that align well with European market requirements. From an architecture perspective, EmpowerID benefits from its approach for providing an integrated set of solutions. All solution components are mature, having undergone substantial modernization and improvements in recent years. It also integrates well with Microsoft Azure Active Directory, utilizing the aforementioned access management capabilities

EmpowerID offers a modern UI with a visual workflow editor and can be deployed as software deployed on-premises, a cloud service, or a managed service. EmpowerID is completely containerized using Docker, RedHat, SUSE and runs on Azure AKS, making it Kubernetes compatible. EmpowerID provides a fully integrated directory, although standard LDAPs and Microsoft AD/AAD are supported. All EmpowerID functionality is exposed via REST API. SCIM support is given too. The company also offers out-of-the-box reports, including many that support major compliance frameworks like GDPR, PDS2, HIPAA, SOX, etc.

EmpowerID provides users with a wide selection of authentication methods, such as OTPs, QR Codes, SMS codes, popular authenticator apps like Duo, Google, LastPass, and Microsoft, as well as mobile biometrics for both Android and iOS devices. Additionally, FIDO 2 and a variety of hardware tokens are available as options. EmpowerID also supports password-less authentication via the WebAuthn standard. The company offers an innovative drag and drop MFA as a workflow feature that can seamlessly integrate into any process. For instance, if a user initiates a process, the system can analyze the risk and prompt MFA verification if necessary. This capability provides the flexibility to incorporate MFA into any process or perform risk analysis within workflows while maintaining a user-friendly experience.

Furthermore, the management of authorizations and policies is one of their particular strengths. EmpowerID supports ABAC, RBAC, CBAC, RAdAC, ReBAC, and user group-based controls, EmpowerID has implemented the full UMA 2.0 Specification within the product and extended its authorization engine with PBAC. In addition, the company provides PBAC support along with APIs for real-time external authentication, allowing for dynamic and context-aware access control decisions. Fraud detection, as part of the EmpowerID Access Management, is limited. However, EmpowerID can trigger adaptive authentication workflows, which can force identity verification or proofing. Verifiable credential support is currently not supported but is on the roadmap.

Overall, EmpowerID has demonstrated its ability to serve customers in different geographies and at different scale. EmpowerID makes a suitable candidate for organizations looking for

an integrated solution that can be run both on-premises or cloud-native as-a-service. With its modern architecture and integrated approach, it is a good access management solution specifically for mid-market companies, but also for larger organizations looking for a comprehensive, feature-rich, and modern solution. EmpowerID appears in the Product leadership category.

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

Table 9: EmpowerID's rating

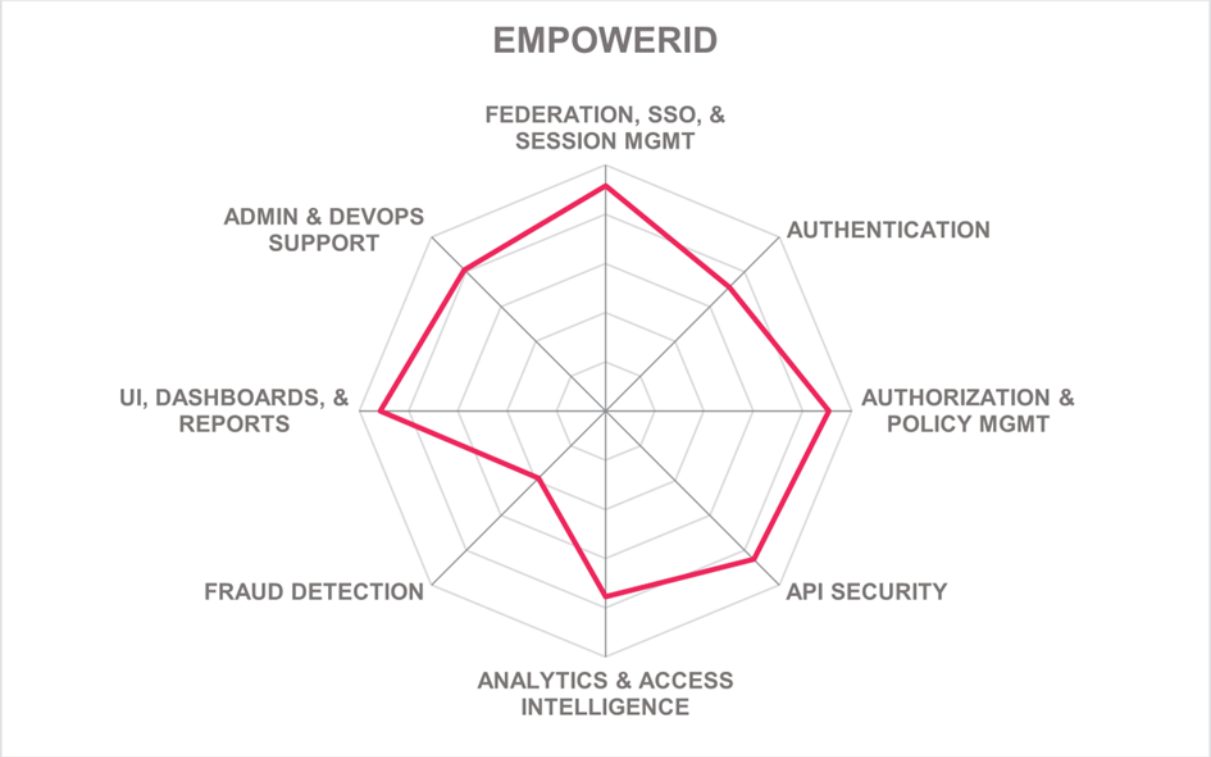
Strengths

- Modern architecture
- UI, dashboard & reporting
- Admin & DevOps support
- Innovative MFA drag and drop feature
- Full UMA 2.0 capabilities
- Strong authorization & policy management
- Certified compliant with multiple standards
- Good federation, SSO, & session management

Challenges

- Limited fraud detection capabilities
- Global partner ecosystem is growing, but still not very large
- ISO/IEC 27001 certification in work
- Missing verifiable credential support, although it is on the roadmap

Leader in


EMPOWERID
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Ergon– Airlock

Ergon Informatik is on the verge of its 40th anniversary and currently has over 400 employees in Switzerland and a small sales office in Germany. The product has a strong presence in the DACH region (Germany, Austria, Switzerland) and serves customers in the financial industry as well as banking software vendors. They also have a small but growing number of customers in the Middle East, North America, and the APAC region. Airlock is a single security product by Ergon with multiple services within the Secure Access Hub. The Secure Access Hub includes a Web application and API protection (WAAP), 2FA, and IAM. Both the Airlock 2FA and Airlock IAM will be considered in this access management leadership compass.

The Airlock IAM login app is an integral component of Ergon Airlock that focuses on end-user interactions. It offers a feature-rich set divided into three categories: authenticated users, users going through authentication, and already authenticated users. Some of these features include self-registration, public self-services, authentication, authorization, protected self-services, and transaction approval. The login screen supports multiple languages and dynamic step activation through checkboxes, enabling users to customize their flow experience.

Airlock IAM supports many authentication methods that may be combined into authentication flows. Some of the authentication options include Digipass OTP, mTAN/eTAN, QR Code, X509 client certificates, mobile push notifications, a few select authentication apps such as Google and OneSpan Mobile ES, Token auth via RADIUS, Android and iOS mobile biometrics, and several popular hardware token options such as Airlock 2FA hardware tokens. Passwordless authentication is accomplished using FIDO2 and Airlock 2FA support. Airlock IAM can both provide digitally signed credentials as well as receive and verify for verifiable credentials support. Ergon’s approach acts as an abstract layer for self-sovereign identity (SSI), providing the ability to receive, extract, verify, and issue verifiable credentials.

Furthermore, the integration of WAAP (Web Application Access Proxy) and IAM by Ergon aims to provide a seamless and secure access control solution for web applications. It strengthens access control, simplifies management, and enhances security for web applications, helping organizations protect their sensitive data and resources. In addition, Airlock’s Continuous Adaptive Trust is an innovative feature which focuses on providing dynamic and context-aware security measures to protect digital assets and ensure secure access to resources based on the continuously evolving risk landscape.

Ergon Airlock can support on-premises, full multi-tenancy for cloud, and hybrid deployment models. The product is not available for IaaS installations, although both Ergon and partner companies provide a SaaS and managed service. The Airlock Gateway is available as a virtual appliance while Airlock IAM is delivered as a self-contained application. The Microgateway version of the Airlock Gateway is delivered as a Docker container focused on security features such as deny rules, JWT validation and processing, OpenAPI specifications, and uses DSL for configuration. The solution's functionality is primarily available via REST-based APIs, although LDAP, RADIUS, and Java are supported. Strong

API security is given and derived from its long history in the WAF market, focusing on content security.

Ergon's Airlock has a well-established and mature set of access management capabilities with a strong focus on WAF, API Security, CIAM, and strong authentication in one solution. Its customers and their partner ecosystem primarily focused on DACH, although growing across the EMEA and the APAC regions. Ergon Airlock Secure Access Hub continues to grow its feature set and remains an interesting alternative to other solutions within the DACH EMEA region.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

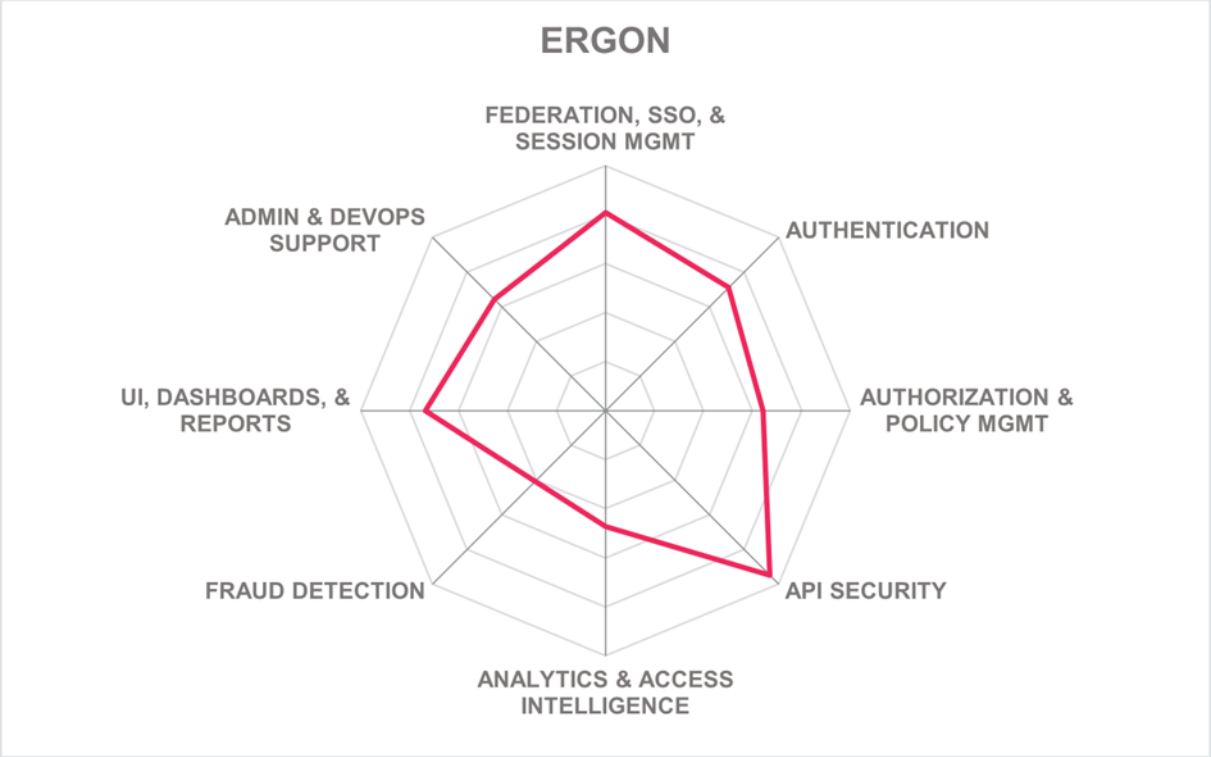
Table 10: Ergon's rating

Strengths

- Friendly user experience
- Good MFA support
- Strong API security
- Verifiable credential support
- Innovative list of capabilities on roadmap
- Modern product deployment & delivery options
- SSO & session management
- Continuous Adaptive Trust feature
- Good UI, dashboards, user self-service

Challenges

- No integration with ITSM products
- Small partner ecosystem & limited global reach
- Limited fraud detection capabilities
- Moderate analytics and access intelligence


ERGON
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Eviden– Evidian WAM, Evidian IDaaS

Eviden is an Atos business that brings together their digital, cloud, big data, and security business lines. Evidian IAM is a software solution of Eviden. Evidian is an established IAM business and has more than 900 customers with over 5 million users within the finances services, manufacturing, retail, transport, telecom, media, utilities, and public health sectors. The Evidian Suite includes multiple products such as Evidian WAM, and Evidian IDaaS as its Access Management portfolio evaluated in this Leadership Compass, although some capabilities are possible via integrations with Evidian IGA, and Evidian Analytics and Intelligence (A&I). The company is primarily focused on Europe but has a small and growing number of customers in North America, Latin America, and the APAC region.

Evidian WAM is a comprehensive solution designed to control and secure access to web and mobile applications, whether they are deployed on-premises, in the cloud, or as SaaS. It follows the principle of least privilege, allowing authenticated users to access only the public and protected services they are authorized to use. It includes a comprehensive set of features, including strong authentication, adaptive authentication, identity federation, SSO, access authorization, and user profile management. Evidian WAM incorporates robust analytics features, empowering administrators with valuable insights through intuitive dashboards and reports on identity and access activity.

Evidian IDaaS Access is an integral part of Evidian's "as a Service" portfolio, which includes Evidian e-SSO as a Service and Evidian IDaaS. It serves as an Identity Provider (IdP) and provides SSO and MFA for various SaaS applications such as Office 365, Salesforce, Box, Jira, Teams, and many more. The solution adheres to industry-standard protocols including SAML 2.0, OpenID Connect, and OAuth 2.0. Evidian offers a wide range of authentication methods including OTP options, QR codes, client-side certificates, popular authenticator apps, Android & iOS mobile biometrics, hardware tokens, and supports controlled devices as well as BYOD (Bring Your Own Device) scenarios. Push notification-based authentication is also supported, via the “Evidian Authenticator” app. Evidian supports full FIDO compliance, and can be used with Kensington, Feitian, Yubico, Duo, and Google (Titan) authenticators, for example. Adaptive authentication supports the device, network, and user-based contexts. The solution also provides identity federation services, including SAML, OIDC, and OAuth, facilitating seamless integration with external systems. Support for verifiable credentials includes integrations with regional third-party verifiable credential providers such as FranceConnect, SwissID, itsme ®, Belgium’s eID card, and Pro Santé Connect.

Eviden’s customers and partner ecosystem are primarily focused in the EMEA region serving mid-market to enterprise-sized organizations. Eviden is a solid option in this market segment, despite the need for further modernization. Evidian is not directly targeting the fraud detection and prevention market, however, a partnership approach has been taken. Overall, Evidian delivers good Access Management capabilities, making it an interesting alternative to the leading vendors in specific industry verticals, particularly in highly regulated industries.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Positive

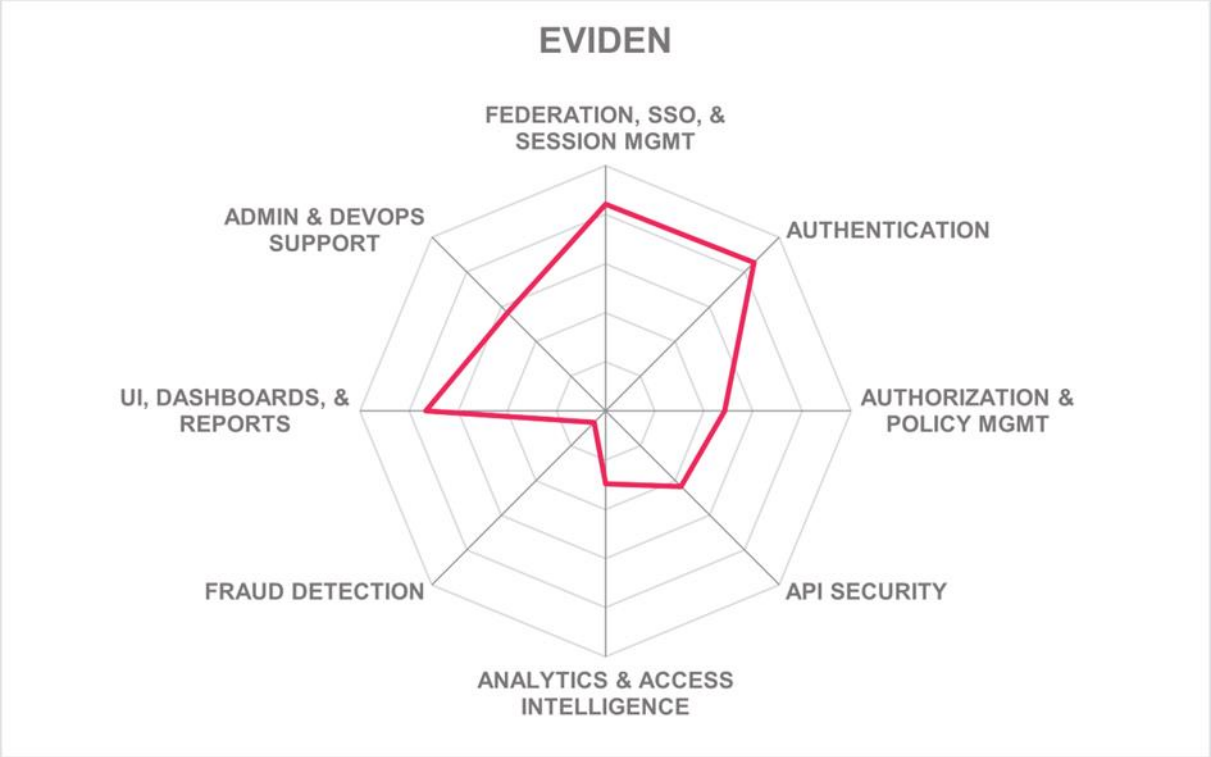
Table 11: Eviden's rating

Strengths

- Identity Federation
- Evidian Authenticator app
- Mature Web Access Management
- Tightly integrated suite of products
- Good breadth of supported authenticators
- Good set of features for reporting and analytics
- Innovative plans and features on the roadmap
- Integrates with regional third-party verifiable credential providers

Challenges

- Limited API security
- Weak fraud detection options
- Limited Admin & Devops support
- Support for Policy-Based Access Control (PBAC) would be beneficial
- Managing market perception and maintaining a positive reputation throughout the rebranding process is crucial


EVIDEN
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Exostar– Access One

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

Access One offers an access management platform that can be delivered as a service or deployed on-premises. The platform prioritizes security, time to value, and flexibility, providing a range of packaged services for both consumer and enterprise access management. Additionally, it allows easy creation and publication of custom IAM services and user journeys using a no-code workflow builder and secure plugin integration service. Access One stands out by targeting highly regulated and adhering to the latest security standards, including OpenID Connect, OAuth, Financial Grade API, Consumer Data Rights, NIST-800-63-B, FIDO 2, and WebAuthn. Key features include user journey orchestration through a graphical workflow builder, seamless integration with third-party interfaces via the plugin architecture, pre-built services for various enterprise and consumer use cases, versatile API access management capabilities, and the ability to create custom IAM APIs using the platform's workflow and plugin interfaces.

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

Exostar is different than the other vendors because they are focused on highly regulated industries. They might do fewer things but do them well and are much more focused. The company continues to add innovative features to their roadmap. Exostar and its identity proofing, passwordless, and credentialing capabilities provide a good alternative for customers in complex and highly regulated industries. Exostar appears in the Product leadership category.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Positive

Table 12: Exostar's rating

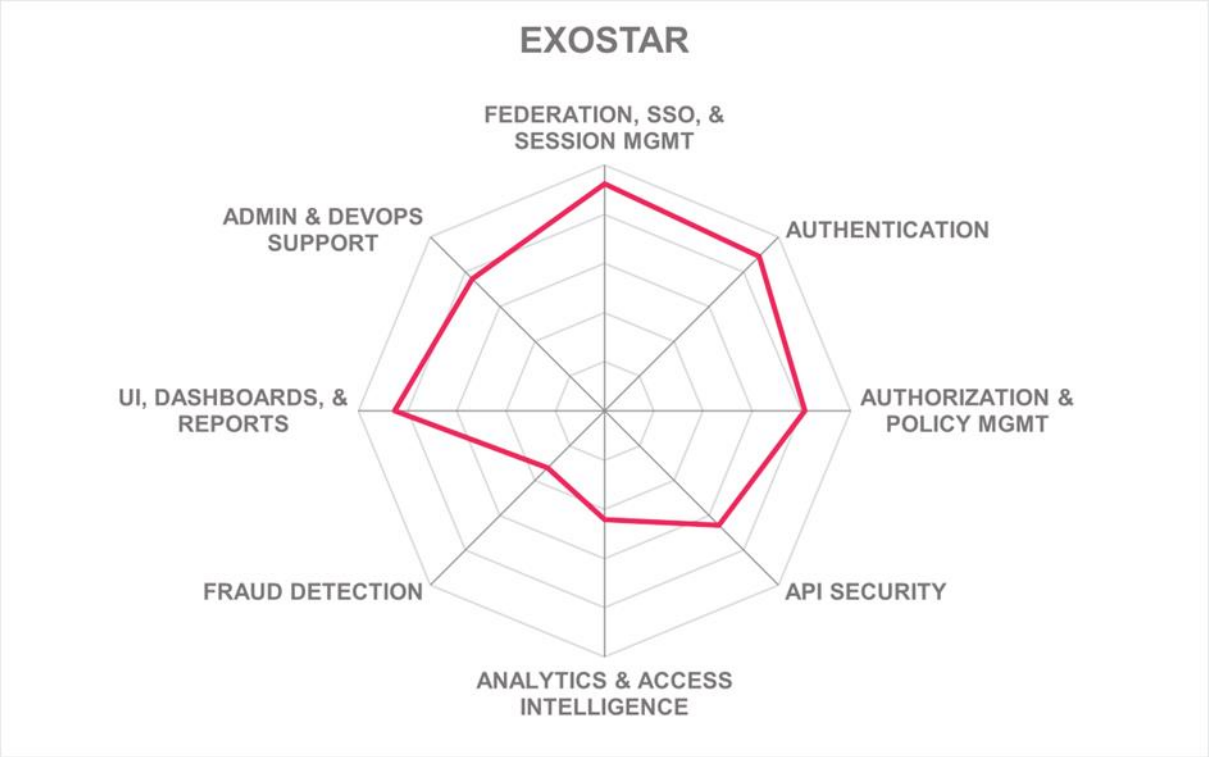
Strengths

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

Challenges

- Remote access is currently not supported
- Lack of analytics and access intelligence capabilities
- Encourage customers in highly regulated industries to adopt standards

Leader in


EXOSTAR
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

ForgeRock– Identity Platform

ForgeRock was founded in 2010 and is headquartered in San Francisco and has many offices located around the world. The ForgeRock Identity Platform unifies the various IAM solutions provided by ForgeRock, such as access management, identity management, IoT/Edge Security, identity gateway, identity governance, privacy & consent management, and other components including directory services. ForgeRock has a strong expanding partner ecosystem. In addition, ForgeRock is a significant contributor to several international standards organizations, such as Open ID Foundation, Open Identity Exchange, OASIS, etc. The company targets large enterprise customers primarily in North America, followed by EMEA, and a growing presence in the APAC region.

The ForgeRock Identity Platform is highly scalable, modular, and easy to deploy, capable of being implemented across various environments such as on-premises, multi-cloud, hybrid, and as-a-service. It incorporates intelligent access, which provides flexibility and security in the authentication journey through an authentication trees framework. In addition, fraud detection capabilities are integrated through the intelligent access orchestration platform. Fraudulent account creation is detected through third-party detection solutions, proofing services, and bot protection. Authorization capabilities include a GUI-based editor for creating context-based policies, allowing fine-grained entitlements, and extension of logic during policy evaluation. Adaptive Risk assesses risks during authentication to determine the need for additional steps. With the breadth and depth of functionality and the architecture,

The platform's SSO mechanisms facilitate easy and secure access across domains and organizations, while Social Sign-On integrates with popular social identity providers. User Self-Service empowers users through easy self-registration and password reset, and User-Managed Access (UMA) provides centralized control over digital resources and access delegation. Furthermore, Transactional Authorization enhances security through event-based approvals, and Identity Federation enables seamless federation across organizations using standard identity protocols. Decentralized Identity is not a product focus; however, ForgeRock continues to integrate through partners to enable DI and digital wallet solutions.

Also, ForgeRock's orchestration capabilities make it easy to facilitate a journey to passwordless authentication. Three WebAuthn authentication nodes are included in the platform; one for creating credentials, one for using those credentials, and one for adding information about the FIDO2 device to a user's profile for later authentication. Passkeys is based on WebAuthn, and ForgeRock supports it out-of-box. ForgeRock also supports CAC/PIV card, Duo, Feitian, Google Titan, Kensington, OneSpan Digipass, RSA SecureID, Symantec VIP, Smartcards, Thetis, YubiKey tokens, and any OATH compliant hardware tokens. All the ForgeRock platform functionality is exposed through SOAP, REST, gRPC, Webhooks, LDAP, and RADIUS APIs, with half of the functionality available through a CLI. Both APIs and CLI are documented on ForgeRock's developer portal. Available SDKs support Android, iOS, and JavaScript programming languages.

With the breadth and depth of functionality and the architecture, ForgeRock positions itself as one of the market leaders. The ForgeRock Identity Platform and its Access Management component offer a comprehensive set of IAM capabilities, enabling organizations to manage

identities, secure access, and enforce policies across diverse environments and identity types. ForgeRock provides a well-balanced solution for access management and continues to invest in product development. This investment shows their rapidly improving capabilities, placing them in all Leadership segments. Overall, ForgeRock is amongst the leading-edge vendors in the IAM space and should be considered in product evaluation.

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

Table 13: ForgeRock's rating

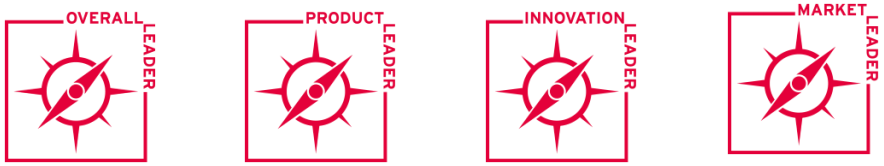
Strengths

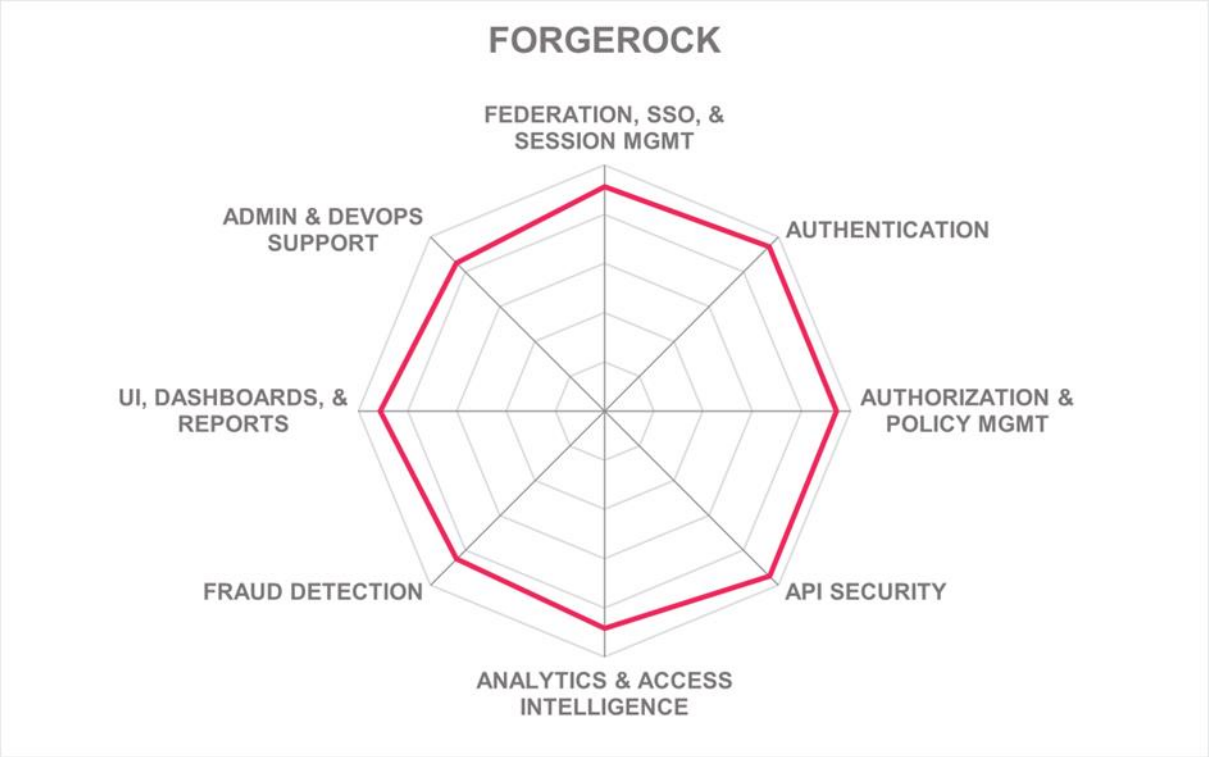
- Fraud detection
- API Security
- Good DevOps support
- Strong federation capabilities
- Broad partner ecosystem support
- Good reporting capabilities
- Strong features for orchestration
- Wide range of authentication options
- Good analytics and access intelligence
- Strong adaptive/risk-based authentication
- Highly scalable microservices architecture
- Innovative features on the roadmap

Challenges

- ForgeRock Identity Platform components have Java runtime dependencies, but provide alternative methods such as file stores to protect Java secrets in the cloud
- Missing direct support for verifiable credentials, although third-party integration support is available

Leader in




FORGEROCK
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

IBM– IBM Security Verify

IBM Corporation is a multinational technology and consulting company headquartered in Armonk, New York, USA. Founded in 1911, IBM has evolved from a computing hardware manufacturer into offering a broad range of software solutions, infrastructure hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, cybersecurity, and IAM. With a strong global presence and customers and partners across the globe, IBM is a major player in the market.

IBM Security Verify provides both depth and breadth in feature support. IBM Verify delivers a modern web UI with dashboards with various activity and usage widgets. The solution provides fully cloud based deployments for SSO, MFA, adaptive access, privileged access, lifecycle management, and passwordless authentication. Administration is facilitated through a modern web application, allowing users to configure applications for SSO and provisioning, manage user records from various sources, define access policies, and fine-tune platform settings for enhanced user security. The offering is a multi-tenant containerized and highly scalable solution built on microservices providing Identity use cases as a service. Components can run on-prem in traditional datacenters or private clouds, in cloud-based IaaS services like Alibaba, Azure, AWS, Google Cloud, IBM Cloud, and PaaS by way of Docker-based deployments.

IBM accepts a long list of authentication mechanisms, including hardware tokens, CAC/PIV card, Duo, Feitian, Google Titan, Kensington Security Key, OneSpan Digipass, RSA SecurID, Smartcards, Symantec VIP, Thetis, and YubiKey tokens. Passwordless authenticators are supported natively via passkeys and QR Code, along with other biometric authenticator mechanisms using the IBM Verify authenticator app. The solution also integrates with 3rd party authenticator vendors. Good contextual and risk-adaptive authentication functionality is with contextual support using user, device, network, location, and a range of available fraud factors. All user access principles such as ABAC, RBAC, CBAC, RAdAC, and user-group are possible. All IBM Security Verify functionality is available via APIs, in which SOAP, REST, Webhooks, SCIM, LDAP, and RADIUS protocols are supported.

IBM Security Verify proprietary fraud detection uses fraud reduction intelligence sources and supports Online Fraud Detection (OFD). The solution uses in-network fraud reduction intelligence sources. The unauthorized account takeover detection is accomplished with a Trusteer integration on-premise or natively within the SaaS offering. Support for verifiable credentials is currently a technology preview, but the solution supports integrations with third-party verifiable credential providers such as Evernym, Trinsic, and others.

IBM positions itself as a leader in the IAM space and provides a feature-rich and modern solution. IBM also benefits from its integration into other IBM services such as IBM QRadar. Organizations that are looking for mature, highly scalable, and secure enterprise authentication solutions built on state-of-the-art micro-services architecture should put IBM on the list of solutions to consider. IBM appears in the overall, product, market, and innovation leadership categories.

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

Table 14: IBM's rating

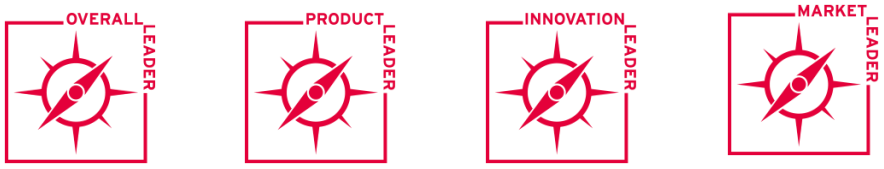
Strengths

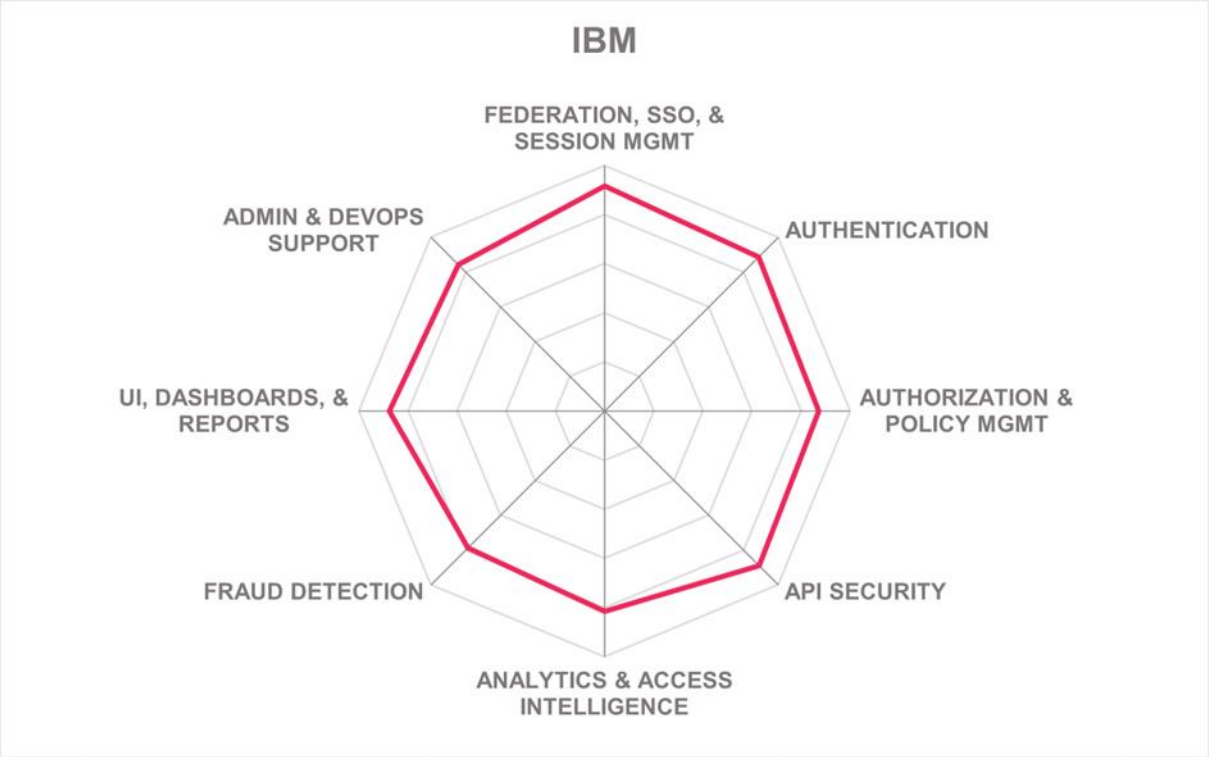
- Proven scalability
- Strong API Security
- Fraud detection
- Admin & DevOps support
- Strong global partner ecosystem
- Good analytics and access intelligence
- Strong and adaptive authentication
- Modern microservice-based architecture
- Wide selection of authentication mechanisms supported
- Authorization and policy management

Challenges

- Lack of focus on the mid-market segment
- Requires integration with other IBM products for some more advanced features
- Limited verifiable credential support, but improvements are on the roadmap
- Missing OOB reports for major compliance frameworks, although supported through QRadar

Leader in




IBM
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Indeed Identity– Indeed Access Manager

Founded in 2011, Indeed Identity is an IT security vendor with headquarters in Dubai, UAE and offices in Lithuania and Singapore. The company provides solutions for MFA, PAM, and PKI management based on a unified modular IAM platform that can be adapted to various use cases. Indeed Identity is currently serving enterprise customers primarily in the EMEA, APAC and GCC as well as across the EECA countries. Although Indeed Identity does not yet have enough prominence outside of its home markets, the company is currently actively expanding its partner network ecosystem.

Indeed Access Manager is an advanced IAM solution designed to deliver secure and efficient control over user access to resources within an organization. It offers a comprehensive set of features and functionalities to manage identities, enforce access policies, and streamline authentication processes. Some of the key features of the platform include authentication management, MFA, web SSO, and out-of-band mobile authentication. Indeed Access Manager also provides sophisticated Enterprise single sign-on for legacy applications, which makes every newly issued smart card or security token immediately available for securing access to enterprise applications. For custom integrations, the product exposes a set of REST APIs as well.

The solution can support on-premises and private cloud deployment models. A virtual appliance is also provided. Docker support for deployment is currently not available. However, it is on their roadmap. Most of the authenticators evaluated are supported, including authentication method options with biometrics for Android and iOS. Some popular authentication apps and hardware token options are given, such as Digipass, Thales eToken Pass, OATH, and Feitian. Nevertheless, FIDO UAF, FIDO U2F and FIDO2 are currently not supported. The platform does not currently support contextual and risk-adaptive authentication, but improvements are on the roadmap. Centralized policy management supports PBAC, and user-group based access.

Indeed Identity’s flexible approach towards designing its whole product portfolio as a highly modular open application platform allows the customers to pick and choose the modules as needed and grow in the future as their business needs expand. The Indeed Key mobile app provides a secure means of accessing corporate resources. Users verify their access using the app on their smartphones, which also displays their access information and the system name they are attempting to log in to. Additionally, the system incorporates one-time password technology through the TOTP protocol.

Indeed Identity makes a good access management platform choice for organizations in the financial, manufacturing, insurance, and energy industries in the EMEA and APAC regions. The solution is well designed, however, enhancements in fraud detection, analytics, access intelligence, and API security would greatly contribute to its competitiveness. Although there is room for improvement, it is worth noting that Indeed Identity has outlined innovative features on their roadmap, indicating potential for further advancement.

Security	Positive

Functionality	Neutral
Deployment	Weak
Interoperability	Neutral
Usability	Neutral

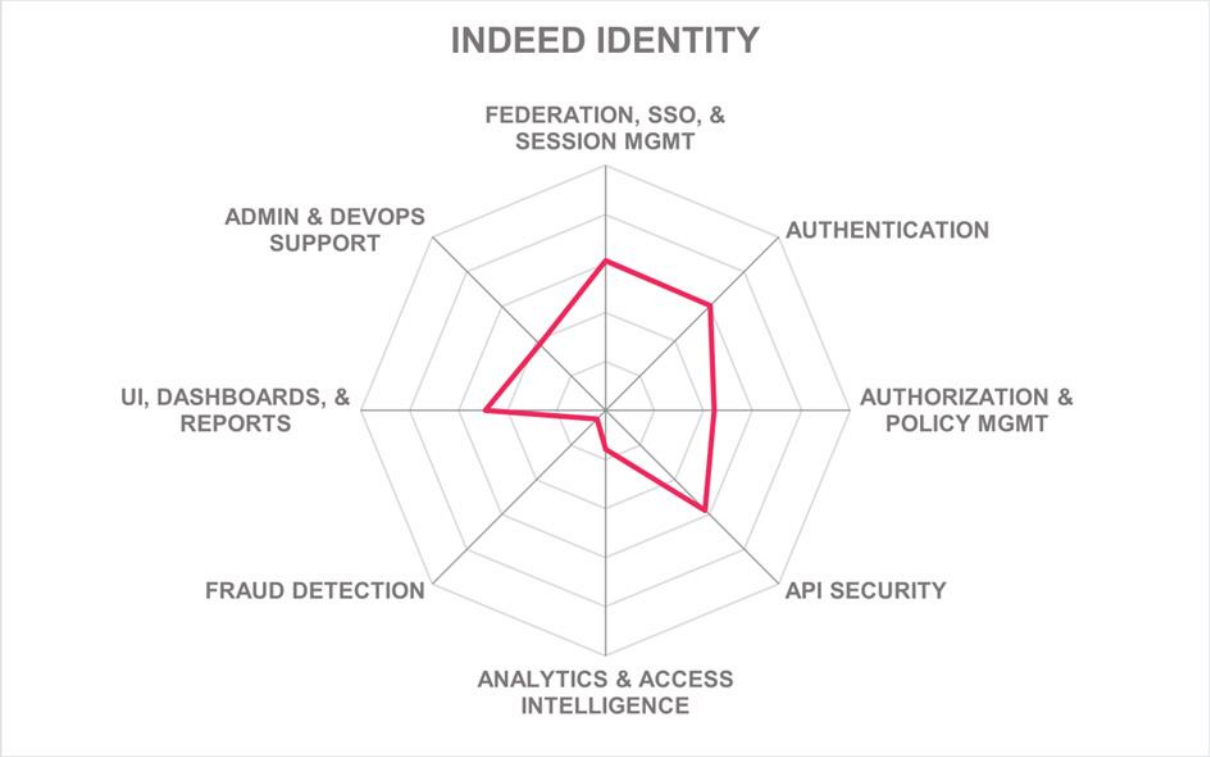
Table 15: Indeed Identity's rating

Strengths

- Flexible solution
- Identity Federation
- Supports legacy systems
- Friendly user experience
- Good reporting capabilities
- SSO and session management
- Good option for remote access
- Innovative list of capabilities on roadmap
- Modular architecture allows adding support for new devices quickly
- Company has good knowledge of IAM technologies which will be useful for future development

Challenges

- FIDO support would be beneficial
- Limited market presence outside of EMEA and APAC regions
- Risk-adaptive authentication is not supported
- Moderate Admin and Devops support
- Lack of fraud detection and access intelligence capabilities
- Limited API protocol support outside of REST
- Missing verifiable credential support


INDEED IDENTITY
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

LoginRadius– CIAM Platform

Founded in 2012, LoginRadius is a VC-backed CIAM vendor based in San Francisco, California. The company is a leading provider of cloud-based digital identity solutions. The LoginRadius CIAM platform includes a suite of solutions designed to address various IAM needs. It enables organizations to efficiently manage customer identities, ensure secure access to applications and data, and deliver personalized experiences across all digital channels. The company's primary focus is on small and mid-market sized organizations in North America, EMEA, APAC, and Latin America.

The platform offers a range of functionalities to enhance the customer experience. Customer Registration streamlines the process by enabling customers to create a unified identity across multiple channels, simplifying their interactions. Social Login is another convenient feature that allows customers to effortlessly log in using their social media accounts, eliminating the need for separate credentials. Additionally, the platform provides a variety of MFA options, including SMS, email, OTPs, and push notifications, ensuring enhanced security and flexibility during the authentication process. SSO allows customers to log in once and access multiple applications while the Customer Profile Management feature allows customers to update their profile information, view their activity, and manage their preferences. The platform also provides role-based access control, risk-based authentication, and detailed analytics and reporting capabilities. Furthermore, the platform integrates seamlessly with popular marketing and CRM platforms, enabling businesses to leverage customer data for targeted campaigns and enhanced customer experiences.

The company provides CIAM as SaaS via a multi-cloud model hosted in globally distributed data centers. The CIAM platform is containerized using Docker, RedHat, and Rancher Labs. Customers can deploy on-premises on CentOS, RHEL, Solaris, or Ubuntu; or run it in any of the major IaaS providers. Additionally, LoginRadius Provides a CLI tool which can be integrated into Devops Processes. API protocols supported include REST and Webhooks. LoginRadius Access Management capabilities give good support for basic, popular authentication apps and hardware token authenticators. Both Android and iOS biometric authenticators are supported, although more advanced voice authentication or iris scan biometric authentication capabilities are not. FIDO UAF is not supported, but good support for FIDO U2F and FIDO 2 is available. In addition, the CIAM platform supports a variety of mobile authentication apps such as Aegis Authenticator, Authy, DeepNet, Duo Security, Google Authenticator, LastPass Authenticator, and Microsoft Authenticator. LoginRadius offers advanced fraud detection features which include user behavior analytics, risk-based authentication, user account verification, and IP address blocking. These features work together to analyze user behavior patterns, evaluate risk levels, and verify user identities to detect and prevent fraudulent activities. LoginRadius is designed as a turnkey CIAM solution. APIs are exposed and the platform is extensible, but it is not a developer-focused platform. Their multi-cloud, global data center deployment strategy provides excellent availability and scalability. Any organization that is looking for a straightforward, easy-to-maintain CIAM solution should think about LoginRadius.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

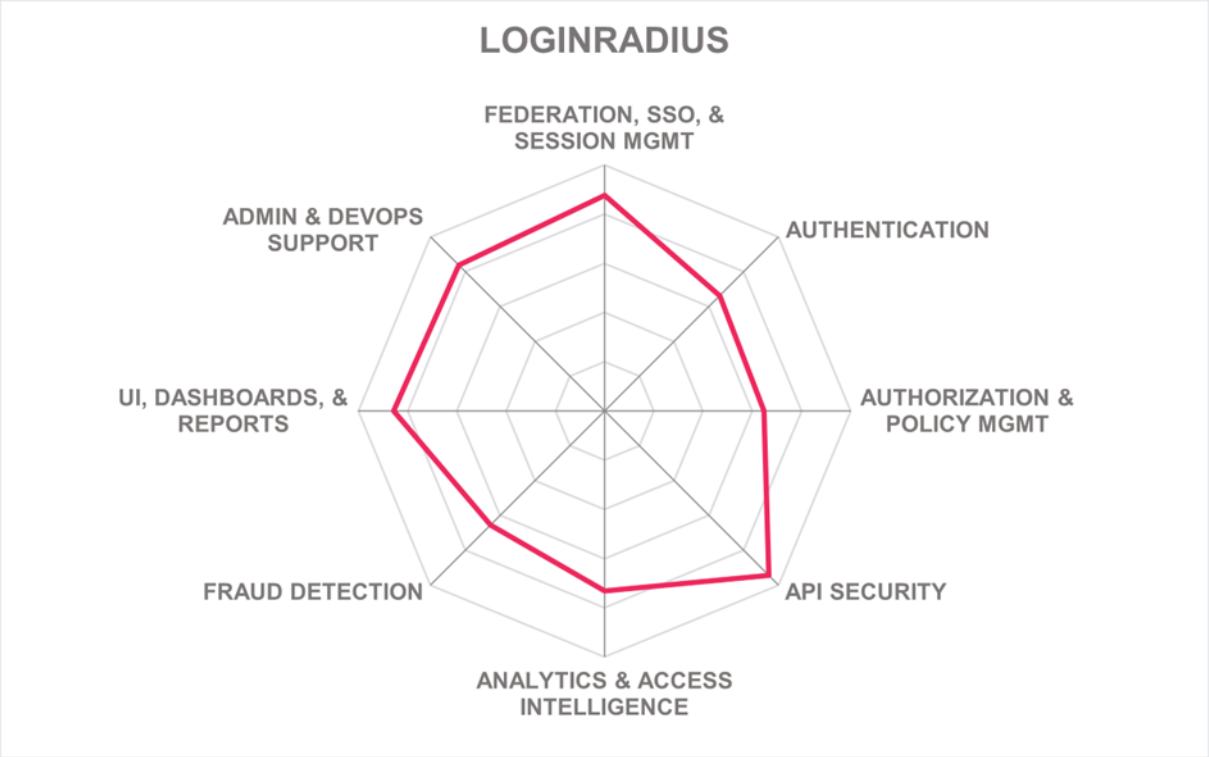
Table 16: LoginRadius' rating

Strengths

- API security
- Fraud detection capabilities
- Admin UI, dashboard capabilities
- Session management and SSO
- Many connectors for marketing analytics/automation and other SaaS tools
- Multi-cloud / global data center deployment for high availability and scalability
- Integration with threat intelligence sources further strengthens the platform's security measures.

Challenges

- FIDO supported but not certified
- Limited verifiable credential support
- No integration to VPN solutions
- No support for policy-based access control


LOGINRADIUS
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Microsoft– Azure AD / Microsoft Entra ID

Microsoft Entra ID, formerly Azure Active Directory (Azure AD) is a cloud-based identity and access management service focused on facilitating business to consumer applications and providing enterprise authentication capabilities. Microsoft Entra ID is one of the global leaders in the cloud infrastructure market and it is delivered via dozens of data centers operating globally. Microsoft offers Entra ID as its primary IDaaS Access Management platform. The solution provides directory services, identity federation, and access management from the cloud in a single integrated platform with extensive integrations as well as the ability to address traditional IAM (B2E), B2B, and B2C use cases.

Microsoft Entra ID offers a comprehensive range of key functionalities to empower organizations in managing identities and access securely. With Microsoft Entra ID, businesses can benefit from adaptive access and conditional access capabilities that provide flexible control over user access based on context and risk assessment. It enables organizations to efficiently create and manage user accounts, while SSO simplifies the user experience by allowing seamless access to multiple applications with a single set of credentials. MFA strengthens security with various authentication methods. Identity Governance ensures compliance and reduces unauthorized access risks. Microsoft Entra ID also incorporates UEBA to detect and protect against identity compromise. Microsoft Entra ID supports Passwordless Authentication, enhancing security and user convenience. It also supports Microsoft Entra Verified ID which enables customers to issue and verify credentials based on open standards for decentralized identifiers and verifiable credentials.

Microsoft Entra ID supports applications, hosted in any public or private cloud. It also supports any SaaS application and offers pre-integrated SaaS application gallery. Additionally, integration with on-premises web-based applications is also provided. In addition, Microsoft Entra ID has obtained an impressive list of security certifications, such as CSA Star, ISO 27001/27018, SSAE 18 SOC 2 Type 1/2, and many country-specific security certifications. FIDO 2 and OpenID profiles are certified as well. Microsoft Entra ID gives strong support for Access Management capabilities, including hardware authenticators such as CAC/PIV cards, Duo, Feitian, OATH (any), OneSpan Digipass, Thetis, Smartcards, Symantec VIP, and YubiKey tokens. CBAC, RBAC, ABAC, PBAC, RAdAC, and ReBAC principles are supported, and Microsoft Entra ID roles can be assigned to users, groups, and service principals. Microsoft Entra ID also works with JWT, Kerberos, OAuth, OIDC, and SAML. Microsoft Entra ID functionality is available via REST, JSON-RPC, XML-RPCSCIM, LDAP, RADIUS, Java, AMQP, and UDP Socket API.

Microsoft Entra ID is a leader in the product, market, innovation, and overall segment of this Access Management Leadership Compass. The company continues to move Microsoft Entra ID in a positive direction with innovative capabilities. Microsoft Entra ID should be considered for cloud-based access management and extending on-premises AD infrastructures to the Cloud.

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

Table 17: Microsoft's rating

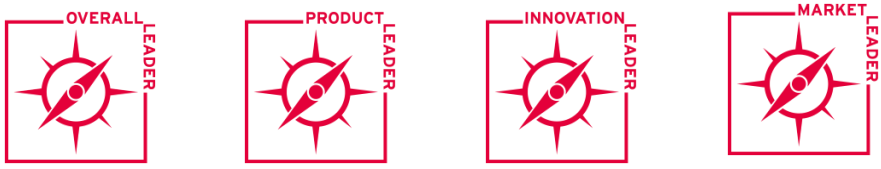
Strengths

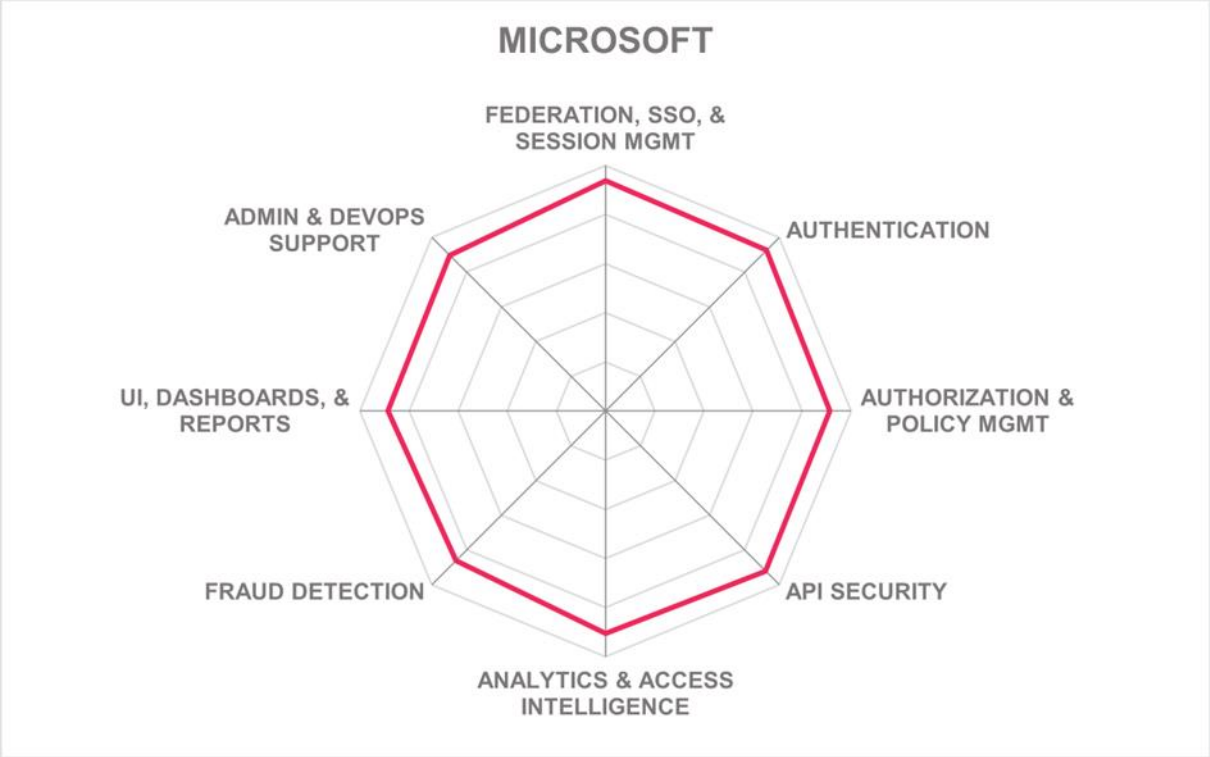
- API security
- High scalability
- Flexible deployments
- Identity federation
- Fraud detection
- Verifiable credential support
- SSO & session management
- Good authorization and policy management
- Good overall authentication support
- FIDO2 and app-based passwordless MFA options
- Global partner ecosystem and strong geographical presence

Challenges

- No support for voice recognition and iris scan biometrics
- Ensuring that Microsoft Entra ID is recognized as a standalone identity offering separate from the broader suite of Microsoft products

Leader in




MICROSOFT
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Okta– Okta Identity Cloud

Based in San Francisco, California (US), Okta's cloud identity platform is targeted at the workforce and customer identity management. Okta's acquisitions of Auth0 (CIAM, developers) and atSpoke (IGA) broadened Okta's portfolio in 2021. Okta's Identity Cloud is a cloud-based identity platform that provides organizations with a secure and scalable solution for managing user identities, controlling access to applications and data, and enabling seamless user experiences across various devices and platforms. The platform is used by customers, developers, and businesses to address complex identity problems which is covered by its authentication, policy management, authorization, and extensibility capabilities. Features that stand out include SSO, MFA, workflows, user provisioning, lifecycle management, API access management, and adaptive security policies.

Okta's Identity Cloud provides a secure and modern infrastructure, including a universal directory service, integration network, system log and analytics engine, and access policies based on various factors. The solution includes bot detection capabilities and adaptive MFA, which further enhances security by providing additional layers of protection and authentication to combat automated threats and prevent unauthorized access. In addition, the recently launched Security Center and Log Streaming features provide valuable insight for analysis and threat detection. Okta Identity Cloud supports authentication, federation, authorization, device management, data integration, API access management, advanced server access, insights, workflows, and platform services. Okta also offers out-of-the-box user experiences for admins and end-users, including an admin console, end-user dashboard, and native mobile/desktop apps. Okta Verify and Okta FastPass are available through the same app which can be deployed via mobile and desktop platforms. This app provides several features, including passwordless and FastPass capabilities. FastPass also offers MFA phishing resistant capabilities. Moreover, on-premises agents called identity bridges are available for connecting to systems behind the firewall. Okta Access Gateway serves as a reverse proxy for on-premise app SSO and authorization.

Okta offers a multi-tenant cloud service for private (Auth0) and public cloud (Okta or Auth0 on AWS and Azure) with SaaS, IaaS, and IDaaS deployment options. On-premise integration is available through the Okta Access Gateway (OAG), an on-prem virtual appliance deployed on-prem or by using public IaaS services. Additionally, customers can use DevOps tools to automate the deployment and configuration of Okta. Okta provides a good set of web UIs for administration and user self-service. Insights, real-time behavior graphics, and easy-to-use drag and drop no code/low code workflow capabilities are given. Additionally, Okta provides good support options for authentication methods, including OTPs, popular authenticator apps, mobile biometrics for iOS, Android, full FIDO support, and a wide range of hardware tokens. Missing are more advanced biometric options such as iris scan or voice recognition, although Okta can integrate with iris, voice, and face recognition software. With the incorporation of Auth0, Okta has added further versatility to its authentication methods, demonstrating a commitment to evolving in line with the changing needs and expectations of users and cutting-edge features like Passkey. Good risk-adaptive authentication is given with device, network, user, and contextual location support for risk-based authentication decisions via access policies. Centralized ABAC, RBAC, CBAC, PBAC, RAdAC, and user-group

access policy management are given with delegated policy management and policy testing tools. API protocols supported include REST, Webhooks, RADIUS, and SCIM and LDAP.

While headquartered in North America, Okta has increased its year over year revenue by 23% internationally. Okta provides a feature-rich and mostly cloud-based solution with strong federation, SSO, authentication, and policy management for both CIAM and workforce use cases with good DevOps support. Okta appears in all leadership segments of this Leadership Compass. Organizations contemplating a move to the cloud for their access management services might consider Okta.

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

Table 18: Okta's rating

Strengths

- Verifiable credential support
- Strong identity federation
- Session management and SSO
- Passwordless support
- Authorization and policy management
- Analytics and access intelligence
- No code/low code workflow editor
- Good Admin and DevOps support
- API Security
- Advanced CIAM capabilities through Okta's robust offerings
- Fraud detection via advanced bot detection and adaptive MFA
- Range of third-party integration options

Challenges

- Need to integrate with on-premises appliances, containers, or software delivery options from partners or third parties.
- Okta should raise awareness of its complete identity offering beyond SSO and MFA.

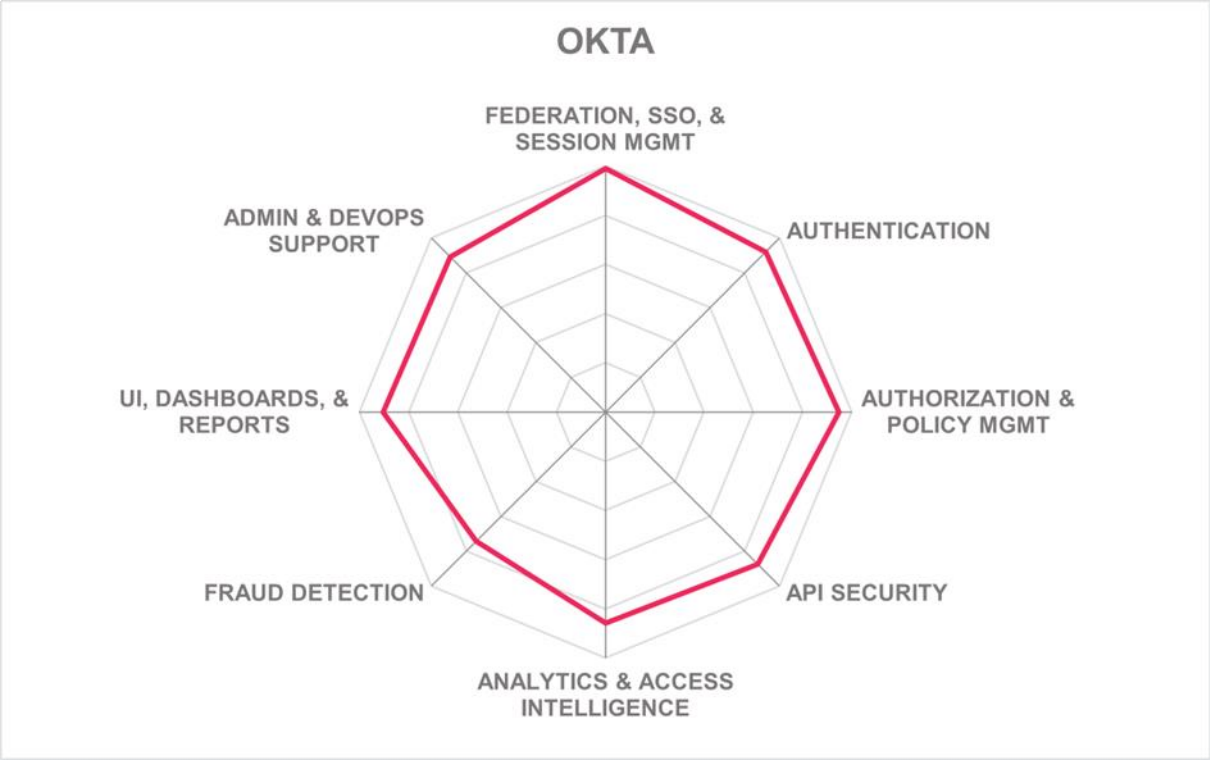
Leader in


OVERALL
LEADER


PRODUCT
LEADER


INNOVATION
LEADER


MARKET
LEADER


OKTA
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

One Identity– OneLogin Platform

One Identity brings together IGA, IAM, PAM, and active directory management capabilities. It acquired OneLogin in October 2021 to support its vision to help customers shift from a fragmented to a holistic approach to identity management and security. OneLogin by One Identity offers workforce and customer identity and access management solutions with real-time actionable intelligence and automated configurations. OneLogin supports many pre-configured cloud services that can be easily connected and provides services for access management, single sign-on, user provisioning, mobile identity, compliance, and both multi-factor and adaptive authentication with various passwordless authentication options to choose from. One Identity has a strong presence across all geographical regions.

With OneLogin Workforce Identity, organizations can establish a modern and efficient identity strategy that prioritizes security and user experience. Moreover, it promotes best practices by offering features like OneLogin Enterprise Sandbox, enabling teams to test application changes and updates in a controlled environment before deploying them to production, minimizing the risks associated with implementation. OneLogin Customer Identity facilitates the management of customer identities at a large scale, offering a robust and dependable CIAM solution. By utilizing advanced machine-learning capabilities, OneLogin Customer Identity streamlines and predicts customer identity lifecycle management, facilitating efficient operations and ensuring customer satisfaction.

OneLogin has a modern multi-tenant SaaS micro-services architecture based on immutable infrastructure and infrastructure as code, with an on-premises reverse proxy available as a Docker container. On-premises components of the platform are IaaS agnostic, supporting a wide range of IaaS platforms. OneLogin provides a modern, easy-to-navigate administrative UI and user self-service. Good graphics dashboards and reporting options are given with some out-of-the-box (OOB) support for some significant compliance frameworks like GDPR, PDS2, and PCS DSS. OneLogin's federation-related capabilities include support for SAML 2.0, OAuth 2, OIDC, WS-Federation, WS-Trust, JWT, and SCIM.

OneLogin’s core access management capabilities include strong authentication support for a wide range of soft MFA authenticators, passwordless authentication, and most hardware tokens. In addition, OneLogin SmartFactor Authentication uses its proprietary Vigilance AI™ threat engine which leverages risk insights to automatically configure login flows and determine whether to prompt users for MFA while communicating anomalies in real-time. OneLogin also provides a Bring Your Own Authentication Factor Option, Trusted IDP as Factor. This feature gives customers the ability to use any authentication factors that they have configured through their own IDP that they are using to log in to OneLogin. All OneLogin policies reside in the OneLogin Admin console and support ABAC, RBAC, CBAC, RAdAC, ReBAC, and both user and policy groups access policy models.

OneLogin offers a modern and feature-rich solution in the market and would likely be suitable for any type of organization looking to adopt a scalable platform. One Identity appears in the product and market categories in this Leadership Compass for access management and should be considered by organizations worldwide.

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

Table 19: One Identity's rating

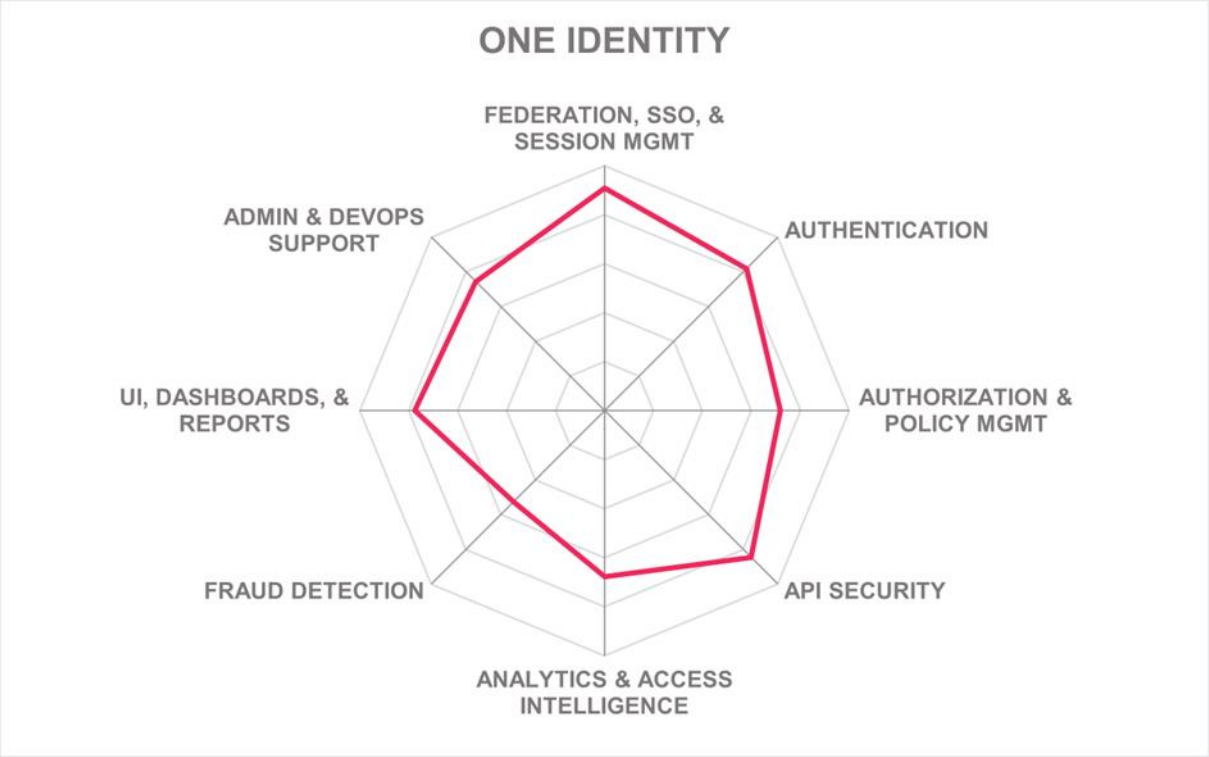
Strengths

- Proven scalability
- Identity Federation
- API Security
- Modern architecture
- Strong MFA capabilities
- Passwordless support
- UI, dashboards, reporting
- User friendly platform
- Verifiable credentials support
- SSO and session management

Challenges

- Deep integration with legacy on-premises systems can be a challenge
- The solution does not currently integrate with other policy management tools

Leader in


ONE IDENTITY
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

OpenText– NetIQ Access Management

Following the acquisition of Micro Focus by OpenText, the NetIQ portfolio has become part of the OpenText Cybersecurity division. OpenText offers an IAM platform as a set of solutions which includes IGA, access management, advanced authentication, data security, PAM and SIEM. The company is one of the world's largest enterprise software providers and offers mission-critical technology and consulting services to thousands of customers. NetIQ Access Management is a mature and widely deployed product on the market and was the first solution in the market to integrate identity federation capabilities with WAM.

The NetIQ Access Management Solution is a tightly coupled, loosely integrated set of products that can be purchased individually or as a full suite. It offers various functionalities such as authentication, SSO, authorization, adaptive access, API Security, and remote access to web and API-based applications. It also integrates with external systems such as CASB, WAFs, and other third-party platforms to support Zero Trust security models. The platform includes CIAM capabilities, providing customizable end-user interfaces, onboarding, profile management, and privacy management. Furthermore, NetIQ Access Management provides integration APIs and workflows for validation of decentralized identities with external systems and Government digital identity services.

NetIQ Access Management can support both on-premises and cloud deployment use cases. The hybrid model has some components that can be deployed on-premise and in a cloud service. Delivery options include virtual appliances, containers, and multi-platform software installations. The product is implemented as a microservices architecture with all components in the SaaS offering as microservices and cloud software offerings are a mix of microservice and traditional architectures. Support is also given for a range of container-based platforms such as Docker, Red Hat, SUSE, Amazon Kubernetes Services, Azure Kubernetes Services, and RHEL OpenShift. Access Management is also available via a managed service provided by OpenText partners. All major product functionalities are exposed via REST interfaces with documentation, scripts, and examples for DevOps support. SOAP, SCIM, LDAP, and Java APIs are also available. CLI is supported for administrative functions, updates, automation tasks, etc. SDKs are available for a wide range of programming languages.

OpenText’s customers are evenly spread across medium to large enterprise organizations, focusing on North America and EMEA, with a growing presence in the APAC region. Still, they have an extensive partner ecosystem on a global scale. Overall, NetIQ Access Management is one of the leading products in the Access Management market segment. They remain in the leadership categories for the product, market, and innovation segments, as well as in the overall leadership category. OpenText NetIQ Access Management is recommended for consideration for mid to enterprise organizations in North America and the EMEA region.

Security	Strong Positive

Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

opentext™

Table 20: OpenText's rating

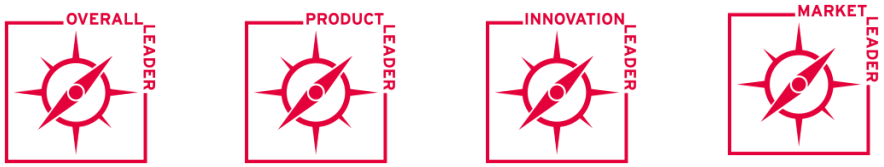
Strengths

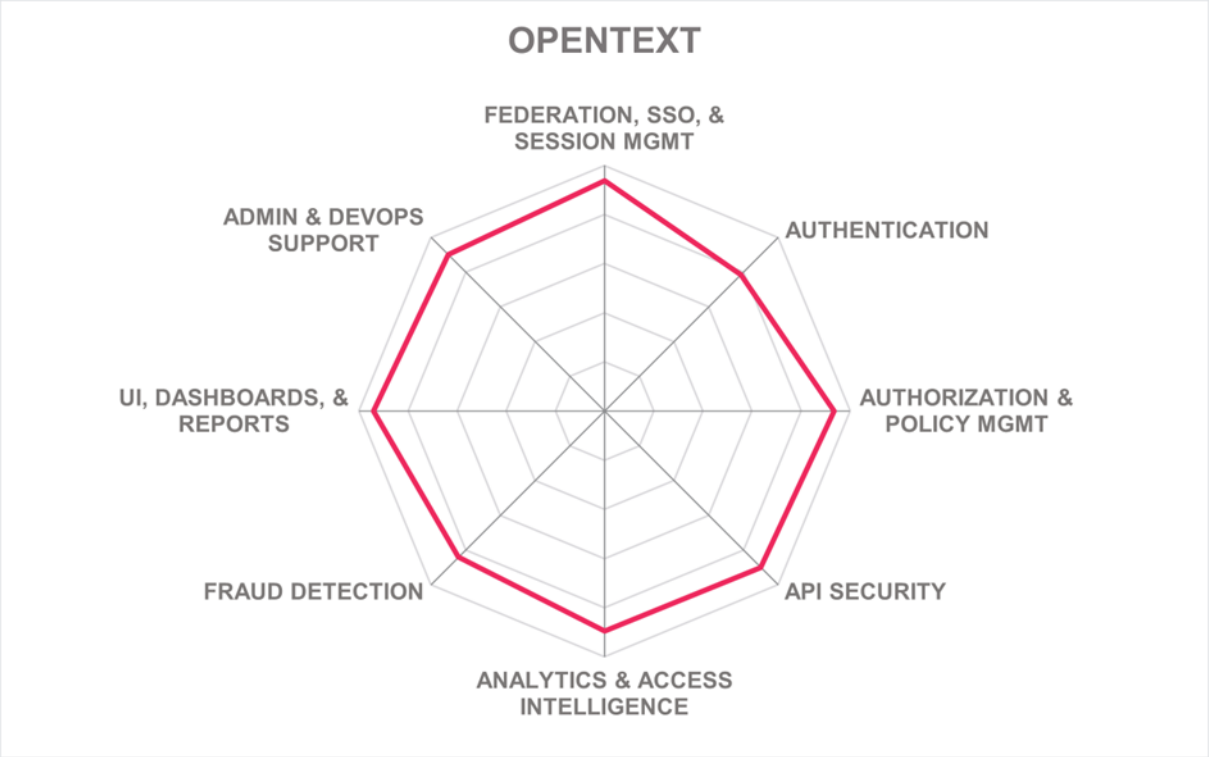
- Verifiable credentials support
- Identity federation
- Session management and SSO
- Authentication support
- Authorization and policy management
- API security
- Fraud detection
- Good use of analytics and access intelligence
- Strong UI, dashboards, and reporting
- Third-party integration options
- Strong partner ecosystem

Challenges

- Continue making the platform adaptable and easy to deploy
- Enterprise-level product solution may exceed small-to-medium company requirements
- Ensuring customers maintain the necessary skillset to effectively operate the infrastructure
- Limited presence and partner ecosystem outside North America and the EMEA regions

Leader in




OPENTEXT
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Optimal IdM– The OptimalCloud

Established in 2005, Optimal IdM is a privately held company headquartered in Lutz, Florida, in the U.S, with other regional offices in the U.S. and Melbourne, Australia. Their product, OptimalCloud, is focused on providing access management capabilities such as SSO, MFA, CIAM, IGA, Federated Identity, and IDaaS use cases. Optimal IdM's sweet spot is large enterprises in North America in the retail, finance, insurance, manufacturing, healthcare, travel, and utilities industries. The solution combines security, flexibility, scalability, and comprehensive features to meet the diverse needs of organizations.

The OptimalCloud administrative UI provides tab-based navigation with some good color-based action indicators making it simple and easy to use. The dashboard gives widgets that can display a variety of stats and basic graphics. Optimal IdM OptimalCloud is delivered a SaaS and offers a Virtual Identity Server to support on-premises, as well as a managed service. Container-based delivery options are not available. Optimal IdM OptimalCloud is a dedicated multi-tenant cloud offering built on .NET and hosted on Windows servers. IaaS platform support includes Amazon AWS, GCP, Azure, and Oracle Cloud. Almost all the OptimalCloud functionality is available via SOAP and REST APIs. RADIUS, SCIM, LDAP, and Webhooks are also supported. Native CLI capabilities are not supported, although most other CLI frameworks can invoke OptimalCloud APIs. Popular programming languages support a wide range of SDKs. It is based on standard protocols and offers many downloadable code samples for programming languages such as C#, VB.NET, Java, JavaScript, and Swift.

Optimal IdM OptimalCloud gives moderate support for authentication methods and a few popular authenticator apps and hardware tokens. Optimal IdM offers its own device-based authenticator, the Optimal Authenticator. Support for Android and iOS biometric authenticators for core Access Management capabilities is also given. FIDO support includes FIDO U2F and FIDO 2, for compliant authenticators, and FIDO UAF. Risk-adaptive authentication provides some device, user, network, and location contexts to be used in access policies. The OptimalCloud central policy management offers a user interface for the administrator or delegated administrator to view, edit, and test all access policies supporting ABAC, RBAC, CBAC, PBAC, RAdAC, ReBAC, and user-group access principles. Fraud detection support includes several third-party integrations to fraud detection, and prevention tools are available. Fraud reduction intelligence sources can be in-network or use connectors to third-party providers. Support for verifiable credentials is not given currently. However, the solution offers a plug-in framework that can be used to support any third-party identity proofing service.

Optimal IdM is a company with customers in enterprise-level organizations that are primarily focused on North America, but with a growing presence in the EMEA and APAC regions. Although Optimal IdM appears as a Challenger in this Leadership Compass, it does show some core strength in Access Management capabilities such as identity federation, SSO, and a particular strength with authorization & policy management support. In sum, organizations should consider Optimal Cloud for access management if their requirements align with the vendor's strengths.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

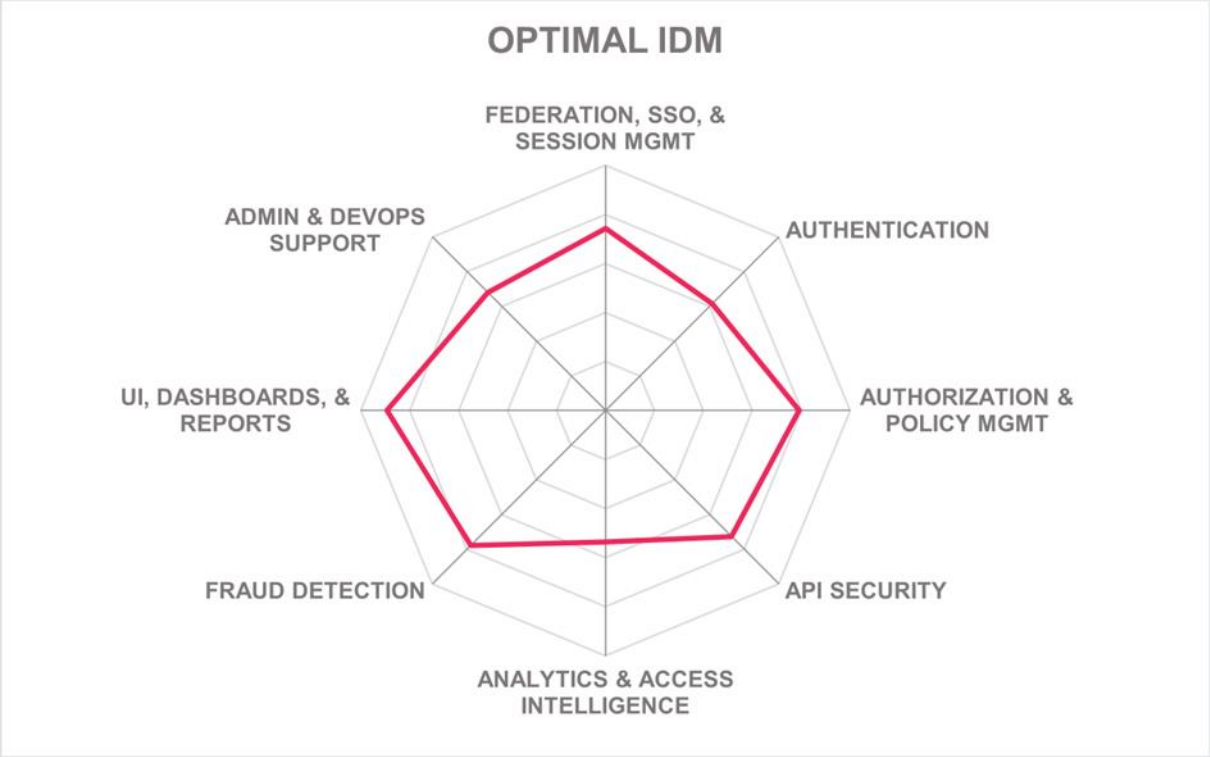
Table 21: Optimal IdM's rating

Strengths

- Easy-to-use admin interface
- Identity federation
- Session management
- Single Sign On
- Some API security capabilities
- Admin and DevOps support
- Authorization and policy management
- UI, dashboards, and reports
- Well-designed dashboards for both customer admins and consumers

Challenges

- Moderate API Security
- A small but well-selected partner ecosystem
- Contextual and risk-adaptive authentication is not supported
- No specific support for device trust on multiple devices
- Limited analytics and access intelligence capabilities


OPTIMAL IDM
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Oracle– Oracle Cloud Infrastructure Identity and Access Management

Based in Texas, Oracle, is one of the leading providers of cloud infrastructure, database management, and enterprise resource planning software. In 2021, Oracle Identity Cloud Services (IDCS) merged into Oracle Cloud Infrastructure Identity and Access Management (OCI IAM). Oracle's IDaaS service, OCI IAM, delivers IAM capabilities from the cloud. OCI IAM is intended to meet organizations' needs in a range of typical use-case scenarios. It enables organizations to define and enforce granular access policies, ensuring secure and controlled access to cloud resources and services.

OCI IAM is a robust and comprehensive solution that caters to diverse IAM needs. One of its key features is the provision of SSO, simplifying user access to multiple applications. It supports popular federation protocols such as SAML, OIDC, and OAuth, ensuring seamless access to federated applications across different platforms. For audit and compliance, the solution provides good auditing capabilities, allowing organizations to track user activities, access requests, and changes to access policies. Also, the solution offers disaster recovery capability. For example, if an entire OCI region becomes unavailable, traffic is routed to the disaster recovery region to speed service recovery and retain as much data as possible. OCI IAM integrates well with other Oracle Cloud services, including networking, storage, and database services. This ensures consistent and centralized management of access controls across the entire cloud environment.

Security is further enhanced with the inclusion of MFA, offering users some factors to choose from, including mobile app OTP or push notifications, SMS, email, phone call, and FIDO2. Both Android and iOS biometrics authenticators like fingerprint and facial recognition are available. Limited hardware token support is given and includes YubiKey, Duo, OATH, as well as any FIDO2 enabled authenticators. Centralized ABAC, RBAC, CBAC, PBAC, RAdAC, and user-group access policy management are supported. Additionally, OCI IAM incorporates risk adaptive-authentication, utilizing a context-aware risk engine that calculates risk scores by considering factors such as device, network, location, and user behavior. Moreover, OCI IAM supports identity verification or proofing via partner solutions such as Singular Key, 1Kosmos, and TruU.

OCI IAM is implemented in a microservices architecture and provides a fully integrated standalone SaaS solution that offers all the core IAM capabilities through a multi-tenant cloud platform. OCI IAM runs on the Oracle Cloud Infrastructure (OCI), however, installations on other IaaS platforms are not possible. OCI IAM cannot be delivered as software or via containers, although Oracle offers software- and container- based AM solutions via OAM. A managed service option is also available. OCI IAM can also be augmented by Oracle Access Manager to support scenarios where customers prefer on-prem deployment or Access Management hosted in third-party clouds. API protocols supported include REST, SCIM and LDAP, and RADIUS.

Oracle OCI IAM provides a strong offering in the access management market and provides a solution that will be attractive to existing Oracle customers. It is tightly integrated with other Oracle business products as well as other Oracle security products. Organizations

considering cloud-based access management can consider OCI IAM for a product evaluation. Oracle appears in the product and market leadership categories.

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

Table 22: Oracle's rating

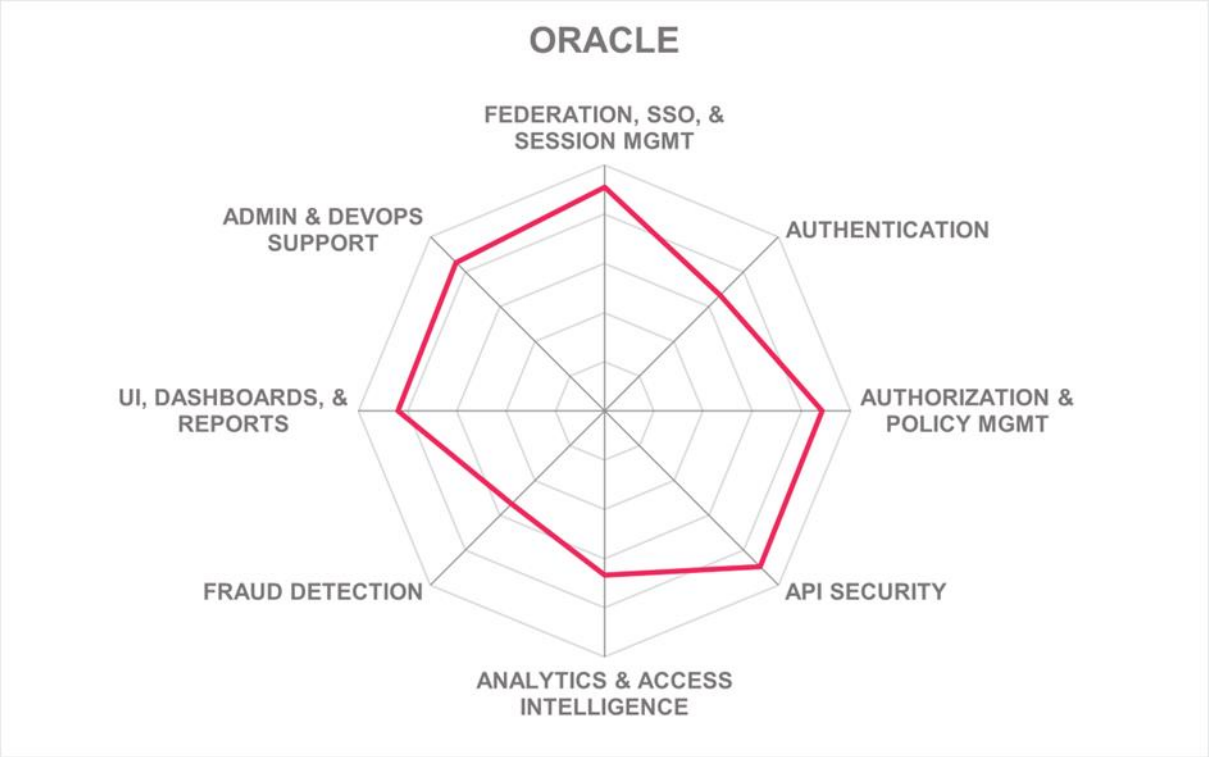
Strengths

- API-based approach
- Identity federation
- Audit and compliance features
- Session management and SSO
- Good API security
- Admin and DevOps support
- Adaptive authentication
- Full FIDO support
- Disaster recovery
- Integration with other Oracle security products

Challenges

- Limited reporting OOB
- Moderate range of authenticators offered
- Limited fraud detection capabilities
- Ensuring OCI IAM is recognized as an identity offering beyond the broader suite of Oracle products

Leader in


ORACLE
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Ping Identity– PingOne Cloud Platform

Ping Identity was founded in 2002 and is based in Denver, Colorado. Ping Identity was among the first of the enterprise IAM vendors to adapt to consumer-facing requirements. Ping Identity started with a primary focus in identity federation. Since then, Ping Identity has continued to grow and accelerate innovative capabilities, acquiring Symphonic Software for policy-driven authorization and ShoCard for decentralized identity in 2020, and more recently SecuredTouch to add fraud prevention capabilities and Singular Key, now known as PingOne DaVinci, for user experience orchestration across the platform. These acquisitions augment the other areas of their identity portfolio. The PingOne Cloud Platform offers a complete portfolio of access management functions for B2B, B2E, and B2C scenarios.

Ping Identity products can be licensed standalone, as well as through solution packages. Integration is made easy with a wide range of integration kits, connectors, and templates, enabling quick implementation of identity verification, digital credentials, profile management, SSO, MFA, authorization, and threat protection. SaaS delivered products include PingOne DaVinci (no-code identity orchestration), PingOne SSO (cloud authentication and directory), PingOne MFA (cloud MFA for customers), PingID (cloud MFA for workforce), PingOne Protect (risk and threat detection), PingOne Verify (identity verification for customers), PingOne Authorize (fine-grained, real-time authorization decisioning and web/API access controls), and more. During the past year, the company released PingOne Neo which is comprised of PingOne Verify and PingOne Credentials, as well as the native Neo Mobile SDK which includes digital wallet and verification functions. PingOne Neo is a multi-standard, decentralized identity management solution that can be implemented for employee, consumer, and supply chain use cases.

The PingOne Cloud Platform’s access management capabilities offer strong authentication methods, including hard and soft authenticators, good biometrics authenticator support and FIDO U2F, and FIDO 2 certified authenticators. However, their legacy FIDO support includes U2F, but UAF capabilities are not offered. Contextual and risk-adaptive authentication are well supported as part of its base authentication service. The solution supports managing users' access based on ABAC, RBAC, CBAC, RAdAC, ReBAC, and user-group principles. Its PBAC offers a graphical policy administration for fine-grained P/ABAC to address Web, API, and Data use cases. The solution's functionality is available via APIs and supports SOAP, REST, Webhooks, SCIM, LDAP, and RADIUS. All platform functionality is also available via CLIs. SDKs are provided for a wide range of popular programming languages. Third-party integrations are well supported, which includes integration to popular ITSM, threat intelligence, EPP, EDR, and UEM solutions.

Ping Identity's cloud-ready software and SaaS solutions are highly scalable and offer maximum flexibility to customers in terms of support for standards as well as innovation for cutting-edge use cases. Ping Identity has a strong presence in North America and good representation in EMEA and APAC regions with a suitable partner ecosystem. They appear in all leadership categories in this Leadership Compass and continue to move in a positive direction. As such, Ping Identity’s platform should be included in any shortlist for access management platform solutions to consider.

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

Table 23: Ping Identity's rating

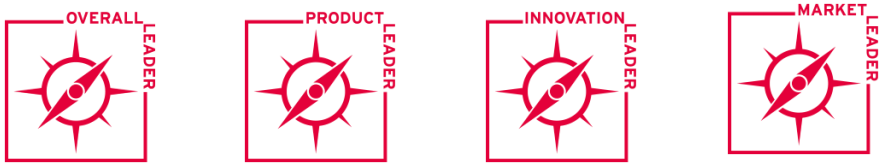
Strengths

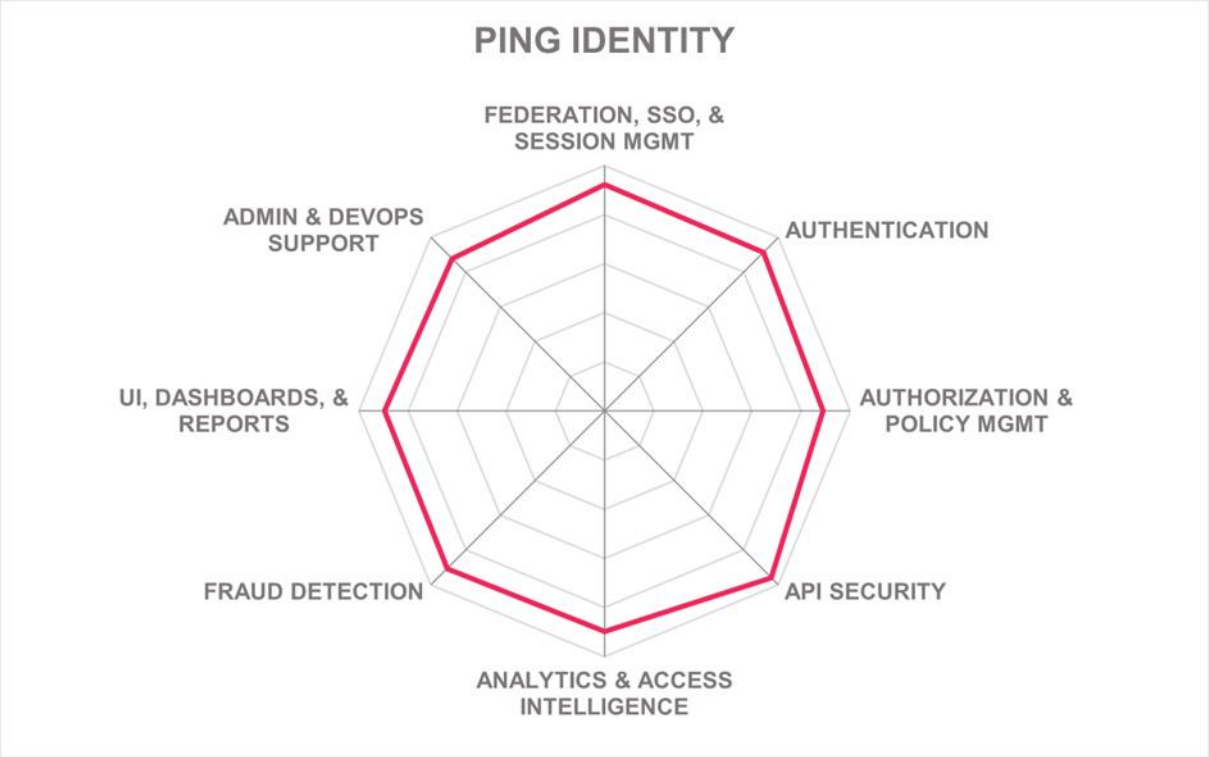
- Proven scalability
- Good API Security
- Lots of authentication options
- Excellent orchestration capabilities
- Authorization and policy management
- Good use of analytics & access intelligence
- Strong fraud detection
- Identity verification capabilities
- UI, dashboards, and reporting
- Admin and DevOps support
- Delegated administration support
- Strong federation, SSO, & session management
- Verifiable credentials support

Challenges

- FIDO UAF capabilities are not offered
- Simplify Ping's offerings to address complexity and enhance accessibility
- Primary customers are focused on North America, but with growth in EMEA and APAC

Leader in




PING IDENTITY
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

RSA– SecurID and ID Plus

RSA Security provides various IAM solutions, both for IGA and Access Management. The company was founded in 1982 and is headquartered in Bedford, MA. RSA was divested from Dell Technologies and acquired by a consortium of private investors led by Symphony Technology Group in September 2020. RSA again operates independently and has a focus on identity. The company offers industry-leading solutions in identity assurance, access control, encryption, key management, compliance, security information management, and fraud protection. RSA is also a board member of the FIDO Alliance.

RSA ensures convenient and flexible access to applications for all users across different environments. RSA provides a fully integrated service available on-premises with SecurID or hybrid cloud with ID Plus, consisting of a Cloud Authentication Service, RSA Authentication Manager (AM), and innovative self-service Single Sign-On with integrated self-service portal. Not only can users access all their web-based OIDC resources, but they can also access all other protected web (SAML) and legacy on-prem resources from the same place with the convenience of SSO.

The cloud components of RSA are multi-tenanted. The cloud service can stand on its own, but it can also be deployed as an additional layer of services and protection on top of the traditional on-prem authentication services. This enables their customers to adopt cloud services and migrate from on-prem to cloud at their own pace. The new Unified Directory provides a Local Identity (ID) Source to enable fully cloud-only deployments without the need for external ID sources like LDAP or on-premises Active Directory. It also improves ease of integration with external ID sources by adding SCIM API support for creating and managing users. RSA Authentication Manager (AM) is an optional component that enables on-premises redundancy for certain cloud authentication services and acts as a proxy for legacy on-prem technology. It is deployed as a virtual or hardware appliance that includes out-of-the-box components.

RSA Risk AI uses identity intelligence to analyze user access activities for anomalous behavior. It then reports the results of the analysis as Identity Confidence scores. The higher the Identity Confidence scores, the more likely it is that this is the same user that is accessing a protected resource. Admins can add Identity Confidence to conditional access policies and assign them to protect access to resources.

RSA recently introduced the DS100 authenticator which is a hardware authenticator that marries the cryptographic advantages of FIDO protocols with the security benefits of a disconnected one-time password (OTP) solution. The DS100 firmware can be securely updated by customers so that end users do not need to replace their authenticators to receive new features and bug fixes.

RSA Mobile Lock protects organizations from threats that could compromise mobile devices. Embedded within the RSA Authenticator mobile application, Mobile Lock can be configured to detect multiple threats on mobile devices and prevent a user from authenticating, until the threats are resolved.

RSA supports a broad range of authentication methods. These include a variety of ways for mobile authentication, including push to approve, OTP, SMS voice, FIDO2, and support for a range of biometric authenticators including Apple FaceID and TouchID, and Samsung Fingerprint. RSA offers passwordless MFA, machine learning enhanced risk analytics, and hardware and software tokens that can be purchased separately or as part of the ID Plus solution subscription plan. In addition to their own well-known authenticators, RSA is FIDO certified as a relying party/server, and therefore supports any FIDO2 or FIDO U2F authenticators, such as Feitian, Google Titan, Kensington, Thetis, Yubikey, or any others FIDO certified credentials. Smart cards and other third-party authenticators can be supported via 3rd party IdP integration. The solution supports managing users' access based on ABAC, RBAC, CBAC, PBAC, RAdAC, and user-group principles. API protocols supported include REST, SCIM, LDAP, and RADIUS.

RSA security maintains a substantial global customer base in mid to enterprise-level organizations. With the breadth and depth of functionality, RSA solutions are scalable and provide good hardware-based authentication methods. In addition, RSA's hybrid deployment enables a unified experience across cloud and on-prem resources while facilitating the organization's cloud journey. Backed by a global ecosystem, the company can readily deploy such solutions. For organizations that broadly utilize RSA products, SecurID and ID Plus are good options for organizations wishing to adopt a secure and user-friendly solution. RSA appears in the market leadership category.

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

Table 24: RSA's rating

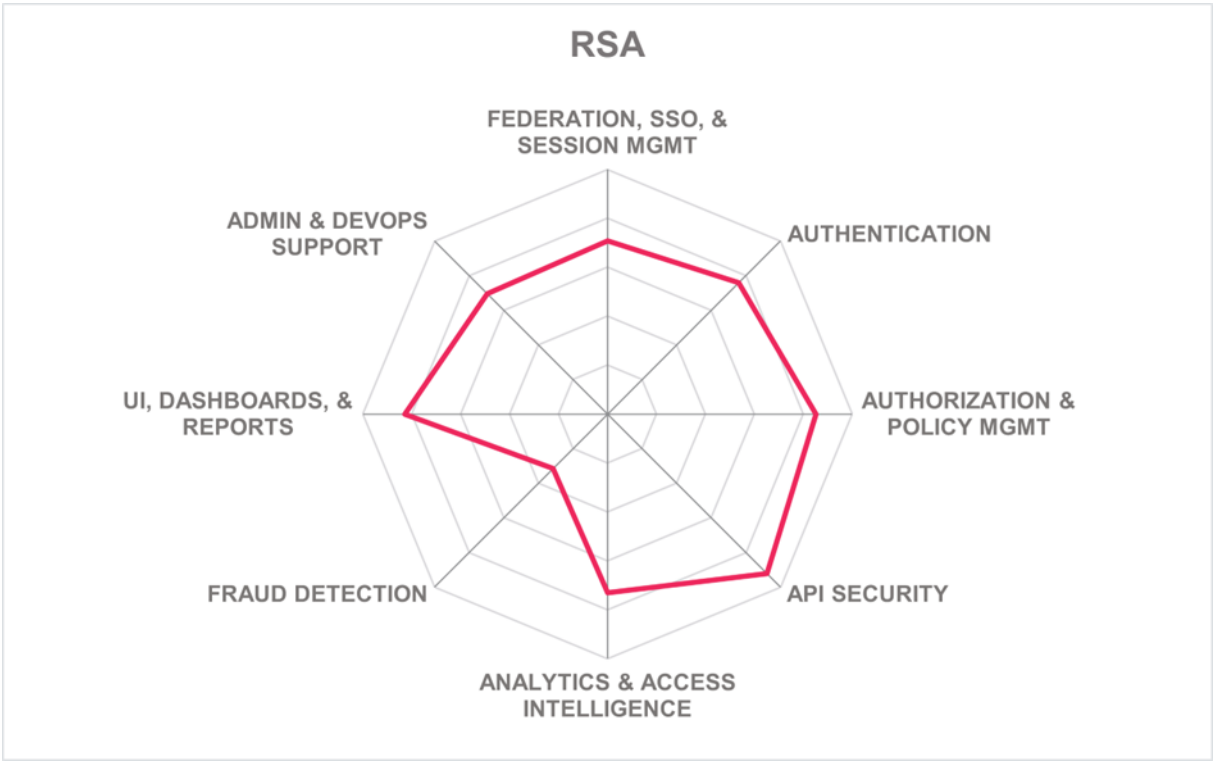
Strengths

- API Security
- Proven scalability and flexibility
- Auditing and compliance
- Good option for remote access
- UI, dashboards, and reporting
- Broad range of authentication methods
- FIDO U2F & 2.0 certified server
- Scales well for large enterprises with many users, entitlements, and policies
- Flexible integration to full suite of RSA security products
- Hybrid deployment addresses on-premises and cloud models

Challenges

- FIDO UAF capabilities are not offered
- Limited fraud detection capabilities
- No support for delegated administration
- Integration with third party EPP platforms and UEM tools would be beneficial
- Missing direct support for verifiable credentials, although third-party integration of identity proofing support is available

Leader in



SecureAuth– Arculix and SecureAuth Identity Platform

SecureAuth has been in the market since 2005 and is headquartered in Irvine, CA. The company is dedicated to staying ahead through continuous modernization and innovation. In late 2021, SecureAuth's acquired Acceptto and added contextual behavior threat intelligence to its list of capabilities. Last year, the company launched Arculix, a next generation platform that combines orchestration, passwordless, and continuous authentication capabilities. The solution delivers MFA, risk-based adaptive authentication, SSO, authorization and policy management, and user self-service capabilities. SecureAuth has a large customer base in medium to enterprise organizations, predominantly in North America, with some growth in the EMEA and APAC regions. The company serves organizations in the financial, manufacturing, government, healthcare, insurance, retail, and energy industries

The Arculix platform caters to both IAM and CIAM needs. Users can access a diverse set of features on the platform. There are numerous functionalities offered by the platform. It delivers risk-based adaptive authentication policies and advanced data science methods, allowing for continuous authentication and offering a comprehensive set of capabilities. Arculix also uses its risk engine to establish a level of assurance (LOA) that begins before the first login and continuously adjusts the LOA score post-authentication throughout the user journey. In addition, the MFA feature enhances security by evaluating access post-authorization using push notifications or verification codes, even offline. The solution also supports SSO and federation using standard protocols, while also accommodating on-premise custom applications.

SecureAuth's solution is implemented in a microservice architecture that can support on-premises, cloud, and hybrid deployment models as well as air-gapped environments. The product can be delivered SaaS, software deployed to a server, virtual appliance, or Docker container. CLI support is not given. SDKs are given that support Java, .NET, Python, Go, Ruby, and JavaScript programming languages and SDKs for Android and iOS platforms. API protocols supported include REST, Webhooks, SCIM, LDAP, and RADIUS. Third-party integrations are well supported, which includes integration to popular ITSM, threat intelligence, EPP, EDR, and UEM solutions. SecureAuth's Access Management capabilities include good authentication support for OTPs, many popular authenticator apps, and hard tokens with support for Android and iOS biometric authenticator options. Also supported are fingerprint sensors for Windows Hello and macOS Touch ID. However, advanced voice recognition and iris scan biometrics are not provided. Full FIDO support includes UAF, U2F and FIDO 2 / WebAuthn authenticators, which includes Windows Hello, Mac OS, Android OS, YubiKey, Kensington, RSA SecureID, Google Titan Key, as examples.

SecureAuth solutions also provide an innovative approach with its Universal Authentication Fabric (UFA) that encompasses Device Trust (for root of trust) and an AI/ML driven Risk Engine that tracks over 200 variables and integrates third party intelligence. This approach enables continuous authentication that allows users to log-in one time with biometric or other passwordless methods and after that they can log-in passwordlessly into other apps, VPN, VDI etc. By continuously authenticating users every few minutes with Invisible MFA, the solution provides an easy-to-use experience while securing access.

The solution has been modernized over the past years and suits our requirements for a modern, microservices-based architecture. SecureAuth continues to move in a positive direction and appears in both the product and innovation leadership categories of this Leadership Compass and shows particular strength in API security, identity federation, and authentication, making it an appealing access management for an organization in North America, focusing on these capabilities.

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

Table 25: SecureAuth's rating

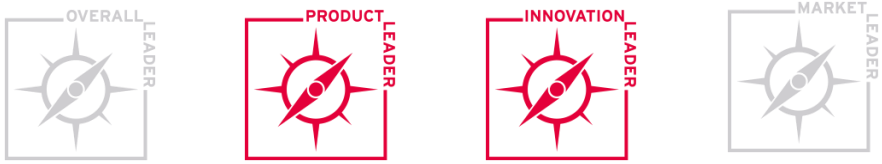
Strengths

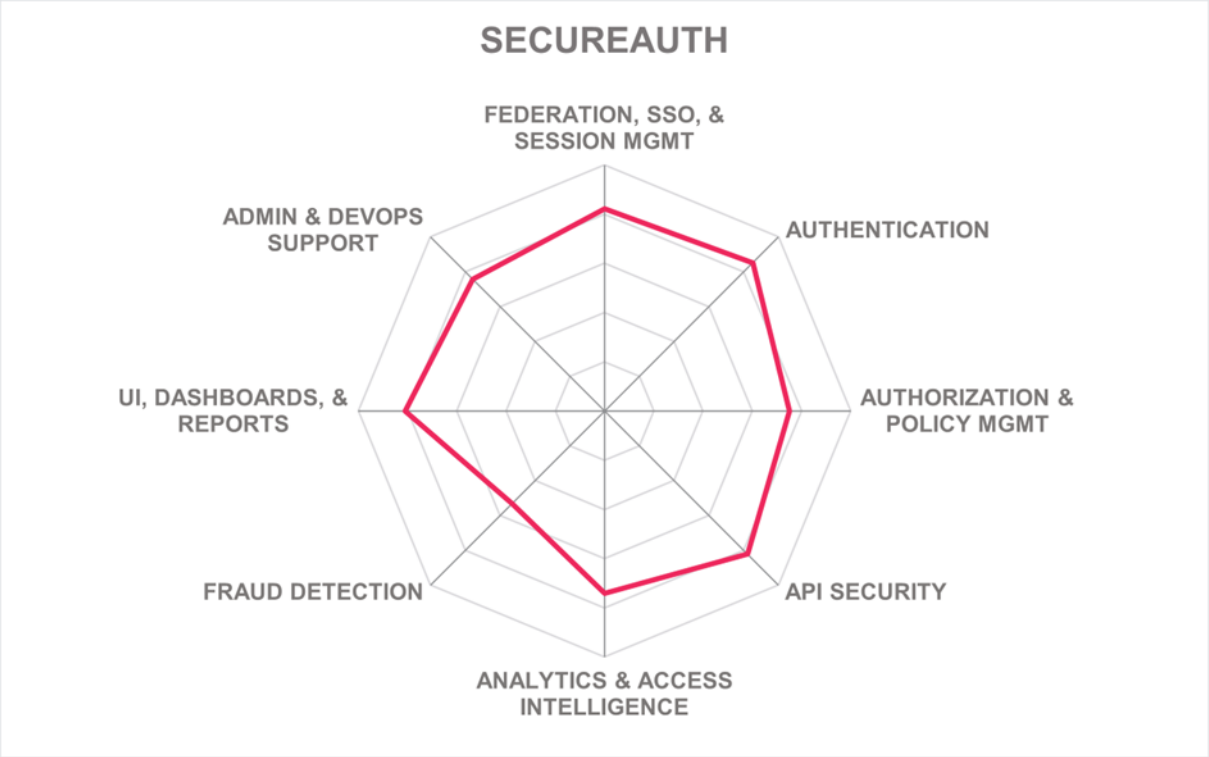
- API security
- Continuous authentication
- Identity federation
- Good device trust features
- Strong MFA capabilities
- SSO and session management
- Good authentication support
- Full FIDO support
- Contextual and risk-based authentication
- Passwordless support
- Third-party identity proofing support
- Good orchestration

Challenges

- Primarily focused in the North American market
- Limited fraud detection capabilities
- Promote the adoption of continuous authentication among customers

Leader in




SECUREAUTH
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Simeio– Simeio Access Management

Simeio Solutions, based in Atlanta, Georgia (US), began in IAM system integration business. Since then, Simeio entered the mainstream IAM market as a full-fledged IDaaS service provider with Simeio Identity Orchestrator. The Simeio Access Management Service is its primary service comprising authentication, authorization, SSO, and identity federation for a hybrid IT environment. Also, Simeio Identity Orchestrator comes with fully integrated PAM, and IGA capabilities. For this Leadership Compass, Simeio offers the access management component of its Simeio Identity Orchestrator.

The solution offers a wide range of features and capabilities to ensure secure and streamlined access to applications and resources. It provides organizations with the tools they need to manage identities, control access, and protect sensitive data effectively. During the past year, Simeio made several enhancements, including analytics improvements, new onboarding capabilities, and customer self-help desk management. The solution provides a modern UI framework with dashboard widgets displaying various customizable security metrics and graphs. Good reporting capabilities are available, including IGA and AG-related reports and strong support for reports based on major compliance frameworks out-of-the-box. Online Fraud Detection (OFD) is a part of the access management solution, in which third-party fraud detection and prevention tools can be used such as Akamai, Arkose, BehavioSec, ID DataWeb, Imperva, iovation, Preempt Security, Telesign, and ThreatMetrix.

Simeio Identity Orchestrator is implemented in a microservices architecture and supports primarily the cloud with an on-premises option and a hybrid deployment model. Its SaaS offering is fully multi-tenant, providing isolation at the network layer, not the application layer, and is hosted on AWS, Azure, Oracle, and Google cloud platforms. Both virtual appliance and container-based delivery options are provided. Supported container-based platforms include Docker, Rancher Labs, and Pivotal. A managed service option is also offered with a range of services. A wide range of operating systems, application servers, and directory services are supported on-premises when delivered as software deployed to a server. All Access Management functionality is available via the UI via REST APIs, and LDAP, SCIM, and Webhook APIs can be enabled upon customer request. Only some access is available via CLI. Only SDKs for Java and .NET are available. Integrations to third-party services include ITSM, Threat Intelligence, EPP, EDR, and UEM solutions. The solution supports managing users' access based on ABAC, RBAC, CBAC, PBAC, RAdAC, and user-group principles.

Overall, Simeio counts amongst the leading-edge solutions for access management. The company is a leader in the product and innovation categories of this Leadership Compass. Simeio combines its IAM development experience and systems integration expertise to give a viable alternative to several established vendors. Organizations that lack IAM knowledge and expertise internally will require detailed guidance and support for transitioning existing on-prem access management to the cloud. Simeio should be considered by organizations primarily in the North American and EMEA regions.

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

Table 26: Simeio's rating

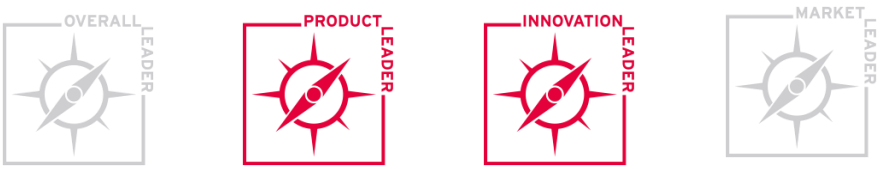
Strengths

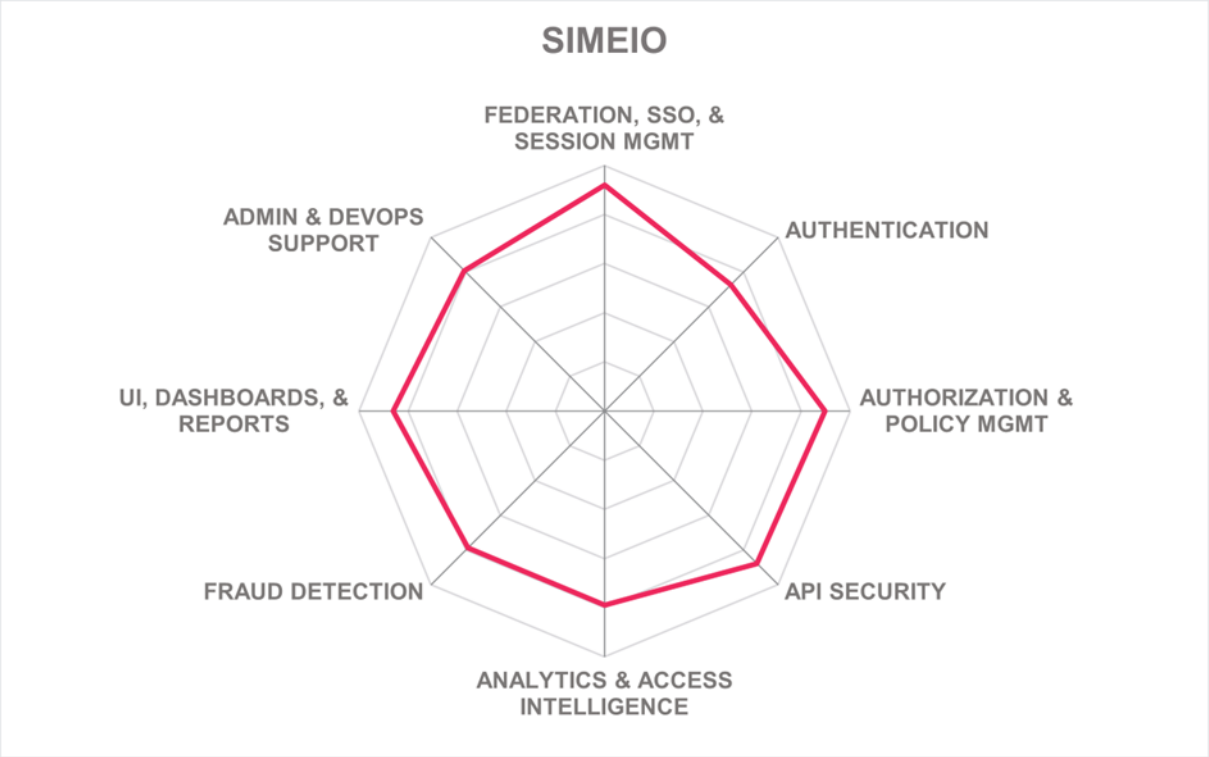
- Identity federation
- Reporting features
- Analytics and access intelligence
- Good third-party integration options
- Session management and SSO
- Authorization and policy management
- Good onboarding capabilities
- API security
- Good use of analytics and access intelligence
- Full FIDO support
- Good reporting support
- Admin and DevOps support
- Fraud detection capabilities

Challenges

- Lack of focus on the SMB market
- Continue making the platform adaptable and easy to deploy
- Missing verifiable credential support, but it is on their roadmap
- Good ability to execute in North America, but limited system integrator partner network on a global scale

Leader in




SIMEIO
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Thales Group– OneWelcome Identity Platform

Thales is a French global company and leader in the aerospace, transportation, and defense and security markets. Its Digital Identity & Security division has approximately 15.000 people worldwide and sells through a large network of distributors and resellers, Thales has a unique capability to design, develop and deploy equipment, systems and services that meet the most complex security requirements. In 2022, the company acquired Dutch CIAM company OneWelcome, one of the leading European providers of CIAM. As a result, Thales offers a comprehensive suite of integrated IAM products and services designed to address various identity use cases for customers, partners, and external identities for different verticals like insurance, banking, government, and telco.

Thales OneWelcome Identity Platform consists of a collection of flexible identity applications that cater to diverse identity use cases, including customers, partners, suppliers, and other external identities. The platform is built as identity fabric on an open and extensible architecture, ensuring its compatibility with current IAM practices while also accommodating future trends like Self Sovereign Identity (SSI) for both customers and the workforce of tomorrow. The platform also includes the workforce access management component, previously known as SafeNet Trusted Access (STA). This service offers highly accessible access management and authentication capabilities, specifically designed for common enterprise workforce scenarios like remote access and cloud application access. It ensures the highest levels of identity assurance for organizations, bolstering security and minimizing risks associated with workforce-related access. Verifiable credentials support is offered through the User Journey Orchestration module, to connect to national identity schemes for identity validation or natively verify the identity via various methods incl. liveness detection, ID photo to selfie matching, NFC eID capture, AML checks, manual verification. The Thales Digital ID Wallet also offers in-person verification.

Thales OneWelcome Identity Platform supports a public cloud deployment that is fully multi-tenant SaaS implemented in a microservice architecture. Support for IaaS installation is not available. Depending on the product component, on-premises and private cloud components are delivered as software deployed to a server or a Docker container. A managed, white-labeled cloud service is also offered. The platform is API-first for interoperability and to serve the developer community. CLI access capabilities is not given, although professional services can provide API-based PowerShell scripts when requested. SDKs provide access to most product functionality and are available for the Android, iOS, Java, C/C++, .NET, and Python programming languages. The product has been independently certified to support compliance with a wide range of standards, including FIPS, ISO, PSD2 and eIDAS, to name a few. Thales OneWelcome includes phishing resistant and passwordless authentication options, covering both backend and client, supporting all relevant authentication technologies, namely PKI, OATH and FIDO. On the client side, Thales offers a very wide range of software and hardware authenticators. Software authenticators include a PKI virtual smart card and Mobile SDKs for both OATH and FIDO, as well as support for FIDO/passkeys native platform authenticators. Hardware options include a wide range of PKI, OATH and FIDO tokens, smart cards, and smart card readers.

Overall, Thales offers a comprehensive solution, combining the OneWelcome Identity Platform, password-less authentication options through OneWelcome Authenticators, and secure workforce access management capabilities. This suite enables organizations to enhance their identity management practices, adapt to evolving technologies, and safeguard their systems and data effectively. Organizations with strong multi-factor and API security access management requirements with a useful UI, dashboards, and reporting capabilities should consider Thales. Thales appears in the market leadership category.

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

Table 27: Thales Group's rating

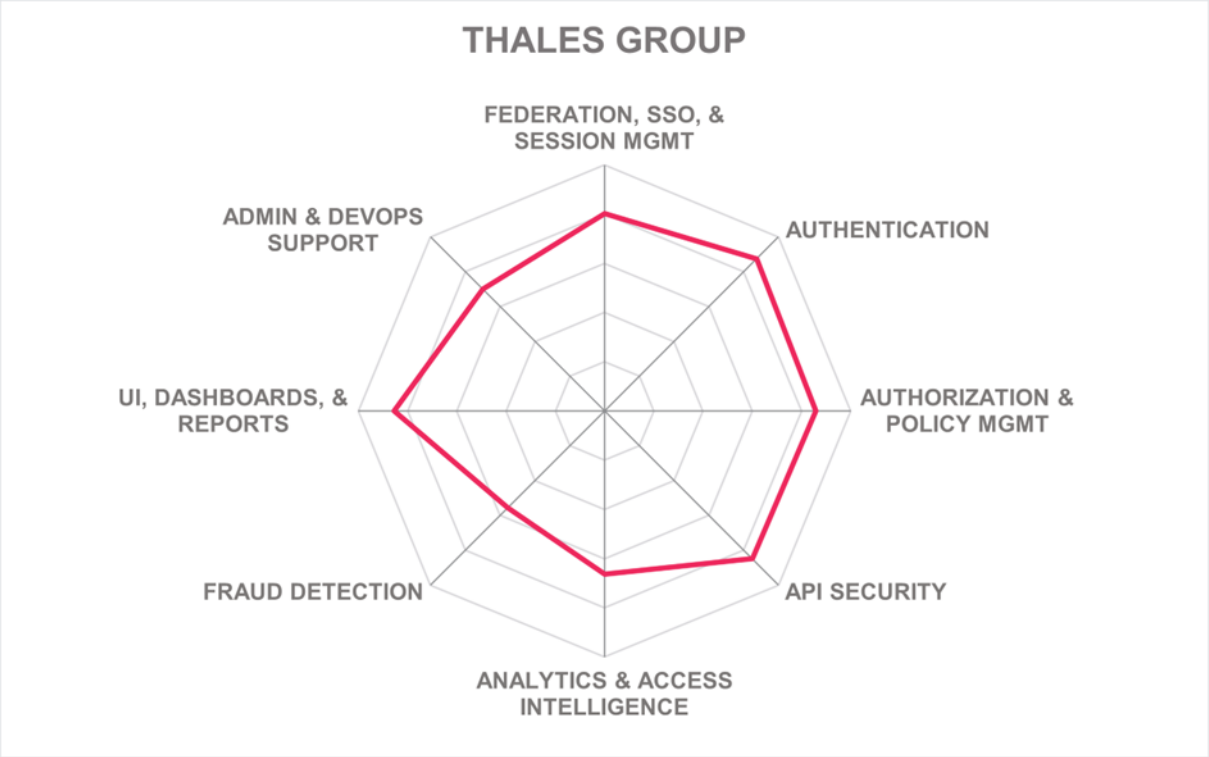
Strengths

- API security
- Flexible deployments
- Strong partner ecosystem
- Good OOTB selection of connectors
- Modern UIs and dashboards
- Good reporting capabilities
- Authorization and policy management
- Broad range of authenticator types supported
- Ability to comply with country-specific regulatory requirements

Challenges

- Moderate analytics and access intelligence

Leader in


THALES GROUP
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

TrustBuilder– TrustBuilder.io Suite

TrustBuilder is based in Gent, Belgium and was founded in 2017 with development beginning in 2016. The company delivers a cutting-edge SaaS CIAM solution that is specifically tailored for the European market. It provides a full-service identity solution consisting of onboarding, verification, authentication, and authorization. TrustBuilder.io Suite currently consists of three products: TrustBuilder.io, TrustBuilder ID Hub and TrustBuilder Mobile Authenticator. The company has other offices in Netherlands, Germany, the UK, and US. Today, TrustBuilder has joined the inWebo Group, an independent vendor of MFA solutions.

TrustBuilder places a strong emphasis on prioritizing identity-centric policies for access management. The solution provides a comprehensive end-to-end solution to customers, ensuring a seamless and secure experience throughout their entire journey. It includes a wide range of capabilities such as SSO, MFA, Federated Identity Management, adaptive authentication, and more. MFA is provided, consisting of TrustBuilder's Bring Your Own Authentication (BYOA) integration with numerous IdPs, push notification, and/or biometrics. It also supports passwordless authentication and offers multiple MFA methods, available on mobile, desktop, and web.

A distinctive feature of the product, however, is its support for verifiable credentials. Document verification and biometric onboarding is completed by partners and are embedded in the product, providing regional coverage of over 100 countries. Customers may choose custom identity verification vendors to integrate the product with. Additional identity attributes can be verified by checking against national registries, by verifying verifiable credentials, and through data aggregation with credit bureaus, telecom, banks, universities, insurance, and employers. The solution has connectors for EU IdPs such as Itsme, eHerkenning, and BankID; and identity and attribute providers including Experian, HID Global, ID.me, OneSpan, Signicat, Thales, etc.

The solution is delivered as a SaaS solution for MFA and CIAM, with a local component called TrustBuilder Connect which connects the SaaS solution with customers' applications and sensitive data that can remain in their dedicated environments. The product is also delivered as a virtual appliance, container-based, or managed service by 3rd Party service providers. Docker, SDUSE, Rancher Labs and Red Hat container-based platforms are supported. All of the TrustBuilder functionality is available via APIs, in which SOAP, REST, Webhooks, JSON-RPC, LDAP, Google Pub/Sub, TCP Socket API, and RADIUS protocols are supported. The MFA solution and web components for self-service are available through SDK's. TrustBuilder capabilities give good support for basic, popular authentication apps and hardware token authenticators such as Duo, Feitian, OATH, OneSpan Digipass, RSA SecureID, Symantec VIP, and YubiKey. FIDO UAF is not supported, but good support for FIDO 2 is available. Good contextual and risk-adaptive authentication functionality is with contextual support using user, device, network, and location. All user access principles such as ABAC, RBAC, CBAC, PBAC, RAdAC, ReBAC, and user-group are possible.

TrustBuilder positions itself as a good alternative to the established offerings supporting mid-market to enterprise organizations in the European market. However, being a rather small vendor, the company still has a relatively small global partner ecosystem. On the other hand,

the company is innovative and provides a secure and user-friendly solution. TrustBuilder is a solid option in this market segment, although it needs to improve its fraud detection, analytics, and API Security capabilities.

Security	Positive
Functionality	Neutral
Deployment	Neutral
Interoperability	Positive
Usability	Positive

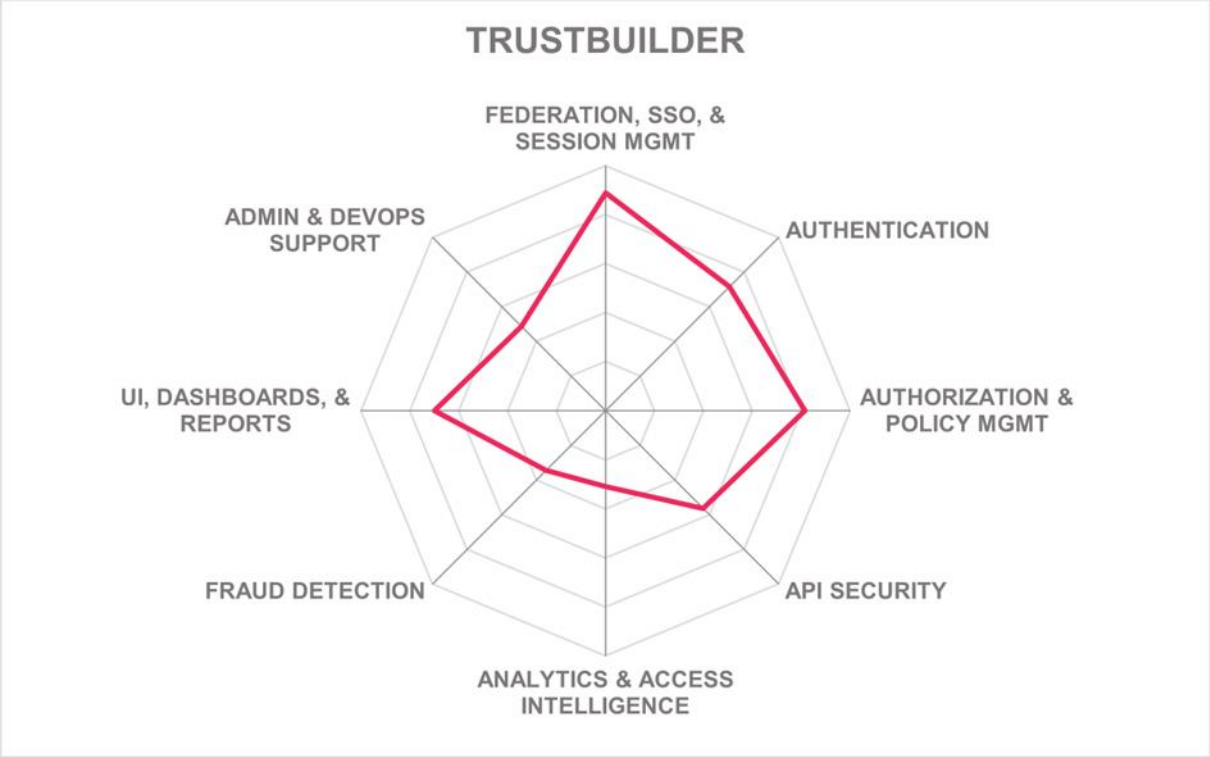
Table 28: TrustBuilder's rating

Strengths

- User friendly solution
- Lots of connectors
- Flexible and scalable solution
- Various options for MFA
- Strong orchestration capabilities
- SSO and session management
- Verifiable credentials support
- Pre-integrated IdPs and connectors
- Strong federation model for European IdPs
- Compelling use of persona-based access control

Challenges

- Moderate API Security
- A small but growing company
- Limited fraud detection capabilities
- Currently focuses on the EU market only
- The solution does not integrate with 3rd-party ITSM solutions, but improvements are on the roadmap


TRUSTBUILDER
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

XAYone– XAYone Platform

XAYone Solutions was founded in 2012 as Oxyliom Solutions. They are headquartered in Luxembourg and have offices in Casablanca and Dubai. In addition to CIAM services, XAYone Platform has B2E IAM, API Security, authentication, authorization, identity federation, session management, fraud detection, and key management features. Mid-market organizations in finance, insurance, manufacturing, defense, and government in EMEA and North America are the company's sweet spot. The platform incorporates advanced features such as self-service device authentication, passwordless authentication, and SSO, which not only enhance security but also improve the user experience for partners and employees alike.

XAYone has strong support for relevant regulations in the financial industry, including AML, eIDAS, GDPR, KYC, and PSD2. XAYone has a connector for Broadcom for fraud prevention. A good range of identity activity reports are available through the customer dashboard, including anonymized metrics related to regulatory compliance. XAYONE offers a remote identity verification app that can scan any ICAO passport and perform hologram verification, facial recognition, NFC reads against chipped documents, and passive liveness and spoofing checks. The platform also features user dashboards for self-service consent and privacy management, including the abilities to view/edit/export/delete personal information. Family management can be configured via roles and a delegated admin model.

XAYone Platform can be delivered as SaaS, container-based, or managed as a service. It can also be installed on-premises on Linux or Windows or in most Tier 1 IaaS platforms. The solution is based on microservices which should enable scalability, but the service is run from a single data center. Most sales and support are currently in Africa, the Middle East, and the Benelux region of the EU. Multiple licensing/subscription models are available. API protocols supported include REST, Webhooks, SCIM, LDAP, RADIUS, UDP Socket API, and TCP Socket API. SDKs programming languages supported include JavaScript, Android, and iOS. Integration with 3rd-party Threat Intelligence solutions, EPP platforms, and EDR solutions is also provided.

XAYone capabilities give good support for basic, popular authentication apps and hardware token authenticators such as Duo, Feitian, Google Titan, Kensington, OATH, and YubiKey. FIDO UAF is not supported, but good support for FIDO 2 is available. Good contextual and risk-adaptive authentication functionality is with contextual support using user, device, network, and location. All user access principles such as ABAC, RBAC, CBAC, PBAC, RAdAC, ReBAC, and user-group are possible.

With a strong, feature-rich solution built on modern architecture, broad standards support, and a well-thought-out roadmap, XAYone is well-positioned to serve customers in the financial services and other sectors, as well as in various regions. Therefore, organizations in the finance industry should review XAYone’s capabilities when searching for access management solutions.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Positive
Usability	Positive

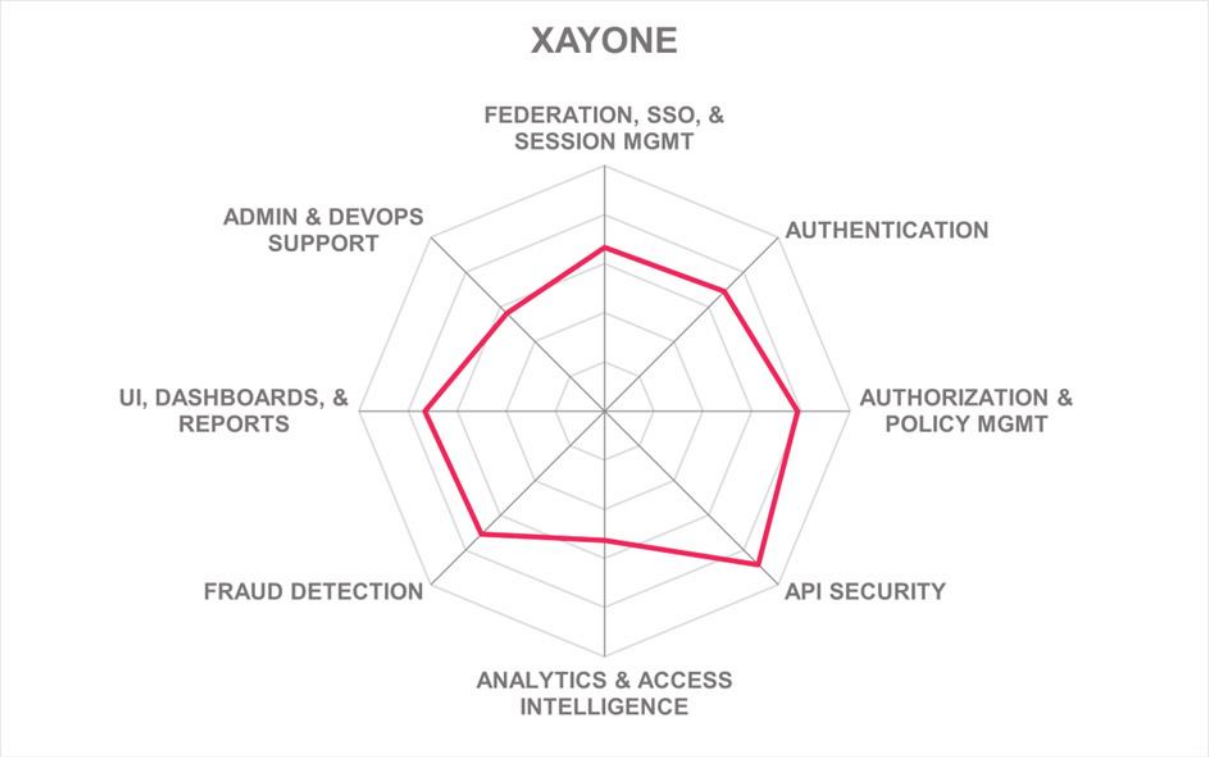
Table 29: XAYone's rating

Strengths

- API Security
- User friendly experience
- Good option for remote access
- Above average range of authenticators accepted
- Authorization and policy management
- UI and dashboards
- Highly flexible remote identity verification app for identity proofing
- Strong support for relevant regulations in the financial industry, including AML, eIDAS, GDPR, KYC, and PSD2

Challenges

- FIDO supported but not certified
- Limited analytics and access intelligence features
- Moderate Admin and Devops support
- Small vendor but with a growing customer base, mostly in Africa at present


XAYONE
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS & ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS, & REPORTS
ADMIN & DEVOPS SUPPORT

Vendors to Watch

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

Authlete

Founded in 2015, Authlete is a small company located in Tokyo, Japan. Authlete offers OAuth 2.0 and OpenID solutions by giving developers the ability to implement API authorization and identity federation services. Its developer-centric solution allows OAuth and OIDC token processing and management with a reference implementation of OAuth/OIDC servers that can forward requests to their Authlete cloud solution.

Authlete is highly specialized, focusing on a narrow segment of Access Management capabilities. Authlete takes a modern API approach and uses the latest OAuth/OIDC standards, suitable for new implementations but may not fit some legacy system requirements. Although Authlete is considered a niche player in the Access Management market, watch for Authlete to give viable OAuth/OIDC implementation options to organizations looking to take a more modern approach to API authorization and identity federation services.

Why worth watching: Watch for Authlete to continue to provide developers with good API authorization solutions for the OAuth and OIDC standards.

AvocoSecure

AvocoSecure is a privately-owned UK company offering Cloud services. The Avoco Identity API platform is a toolkit providing extended ecosystem functionality to deliver multiple components, including IDPs, hubs, brokers, verification, and support for Open Banking. AvocoSecure is available on G-Cloud 12 as well as on-premises hosting.

The AvocoSecure Identity API Platform is an interesting offering considering its ability to support SAML, OpenID Connect, OAuth, DIDs, Lambda Extensions, and Identity orchestration workflows, as well as the tools to secure transactions and create verified identities for Open Banking.

Why worth watching: AvocoSecure Identity API toolkits, Trus-T service, and support for Open Banking move in a positive direction of assuring identities and securely connecting business to customers.

F5 Networks

Established in 1996, F5 Networks has a strong presence with large companies in North America with a presence in other countries. F5 Networks' offers the F5 BIG-IP Access Policy

Manager (APM) as is its Access Management proxy solution. F5 BIG-IP APM provides their Identity Federation, Web Access Management / Identity Aware Proxy, Remote and Application Access, and API protection capability. F5 BIG-IP APM also extends to meet Virtual Application Access and Enterprise Mobility Management use cases.

F5 BIG-IP APM offers context-based remote access to private applications and centralized SSO / federation with desktop and mobile platform security posture capabilities for on-premises and private cloud deployments. Also given are authentication and authorization such as Kerberos, Header-based, RADIUS, NTLM, OAuth/OIDC, MFA, step-up authentication, and protocol translations once the user has logged in from on-premises or a SaaS identity provider. A new capability introduced is the ability to protect an organization's public APIs. Support is given for ingesting APIs using the OpenAPI specification, such as a Swagger file. The solution protects all API endpoints using the same F5 BIG-IP APM authentication and authorization capabilities, as well as rate-limiting and throughput protection.

Why worth watching: Watch F5 BIG-IP APM continue moving in a positive direction to meet the evolving use case of Access Management

Identity Automation

Founded in 2004 and headquartered in Huston, Texas, Identity Automation introduced its RapidIdentity IAM solution later in 2010. In 2018, Identity Automation acquired HealthCast, a vendor specializing in IAM solutions for the healthcare industry. By combining the two portfolios, Identity Automation now delivers a comprehensive IAM solution for healthcare organizations that spans all core IAM capabilities, including automated Identity Lifecycle Management, Identity Governance, Multi-Factor Authentication, and Single Sign-On.

The RapidIdentity platform focuses on SSO and MFA for the Access Management segment. Their Single Sign-On (SSO) is standards-compliant, allowing integration with on-premises and cloud-based applications using SAML 2.0, OAuth, OpenID Connect, and WS-Federation. SSO mobile access support to cloud applications for iOS and Android devices. Various authentication options include support for Duo Authentication and MFA for Windows.

Why worth watching: Watch Identity Automation RapidIdentity as it focuses on the education market providing core Access Management within the user lifecycle with future capabilities towards more intelligence and insight features on the roadmap.

Nevis Security

Until early 2020, Nevis was a part of Adnovum Informatik AG, but was then spun off as a separate company. Nevis Security protects many banking, insurance, healthcare, and government portals and secures a large percentage of e-banking transactions in Switzerland making it one of the leaders in identity and access management solutions in the country. Nevis recently expanded into the UK market and has a strong presence in Germany and Singapore. In addition to its headquarters in Zurich, Nevis operates offices in Germany and Hungary.

Why worth watching: Nevis has demonstrated its ability to serve customers in different geographies and at different scales. Their CIAM offering provides core account recovery and device management capabilities with strengths in omni-channel experience and transaction confirmation.

Ory

Ory is a private company headquartered in München, Bayern, Germany. Ory offers an open-source identity infrastructure for modern cloud-native solutions and provides authentication and authorization capabilities. The Ory identity platform allows organizations to authenticate and manage users, set and check permissions, and protect customer APIs, applications, and data.

The Ory identity platform is built with developers in mind. It provides CLIs and SDKs for programming languages, documentation, tutorials, and community support for its open-source identity platform. It gives custom/white-labeled branding and flows, OAuth 2.0, OIDC, IAP, RBAC, and the ability to integrate.

Why worth watching: Ory offers a developer-centric identity platform that provides hardened open-source alternative in the cloud.

Radiant Logic

Radiant Logic, headquartered in Novato, California, United States, is a leading virtualization-based federated identity services provider. Its RadiantOne provides Access Management with Integrated Identity. The RadiantOne Identity Platform components include the Cloud Federation Service (CFS), which provides a federation layer to the target applications with SAML, WS, OIDC, and OAuth support. The Federation/Access Management contains the identity integration engine supporting a wide range of protocol standards and consumer-specific views. The Synchronization Layer interfaces with various data source types and synchronizes across legacy and cloud systems.

Why worth watching: Watch for Radiant Logic to continue to build out its RadiantOne Identity Platform with additional features and Access Management capabilities.

Signicat

Founded in 2006, Signicat has offices in the Netherlands and throughout Europe. Signicat customers are based in the EMEA region, such as the Nordics, Benelux, DACH/GSA, and Southern Europe. The Norwegian company, Signicat, offers a set of solutions that support customers in creating seamless processes for Identity Proofing, Authentication, and Electronic Signatures, in tight integration with their existing IT infrastructure. Signicat recently acquired the Dutch company Connectis in 2020, ENCAP Security, eID, and Dokobit in 2021. Signicat offers its Signicat Authentication and User Management as an Access Management offering.

Signicat offers a range of authenticator options, and Signicat Authentication and User Management do not provide policy management. Instead, it offers the necessary inputs such

as attributes or other data to support external policy management solutions. Role management and role mining capabilities are available via a SCIM API and is meant to manage access controls, not as core user management SSO is fully integrated into the solution and supports SSO across IdPs, even if the IdP does not support SSO natively. One of the Signicat Identity Platform's strengths in Access Management is its identity federation capability. Support for identity federation-related standards includes SAML, OAuth 2, OIDC, WS-Federation, SCIM, and UMA. Support for other proprietary interfaces used primarily by governmental schemes and banks is also given. The Signicat Authentication and User Management is a SaaS-only offering that supports public, private, and multi-cloud or hybrid deployment models and is fully multi-tenant.

Why worth watching: With Signicat's many acquisitions over the last couple of years, watch for Signicat to integrate more capabilities into its product offerings.

Silverfort

Silverfort is a private company based in Tel Aviv, Israel, delivering authentication and access policies across corporate networks and cloud environments. It offers to provide visibility and protection to assets within an organization. Its agentless authentication platform applies a layer of protection to existing authentication protocols, thereby removing the need to deploy agents and proxies or make any changes to existing servers and applications. The platform also monitors all access requests across systems while providing risk analysis capabilities. Support is given for both legacy and cloud IAM solutions.

Why worth watching: Watch for the expansion of Silverfort's unified identity protection platform on top of IAM solutions.

Soffid IAM

Founded in 2013 and based in Spain, Soffid provides a IAM platform that brings access management, SSO, IGA, Identity Risk and Compliance (IRC) and PAM in one single platform. Soffid IAM caters to organizations in the government, retail, insurance, energy, and financial sectors by providing an integrated platform with access management capabilities. Soffid IAM offers a flexible IAM solution that provides organizations with the ability to efficiently manage user identities, secure access to resources, and maintain compliance with regulatory standards. Soffid's access management capabilities give support for basic, popular authentication apps and hardware token authenticators. However, both Android and iOS biometric authenticators are not currently supported. Soffid's sweet spot is the mid-market and large enterprises in Latin America and the EMEA region.

Why worth watching: The company's continuous expansion and its standing as a captivating alternative among solutions in the Latin America and European region make it an appealing choice.

SSO Easy

SSO Easy is a privately owned US-based company headquartered in Quincy, Massachusetts, with offices in New York and Australia. EasyConnect is SSO Easy's core

enterprise SAML solution that supports both SAML 1.1 and 2.0 standards. EasyConnect can act as either an Identity Provider (IdP) or Service Provider (SP) and offers multi-factor SSO options. EasyConnect doesn't require any coding or customization but rather offers pre-configured drop-in templates that can support Google Apps or Salesforce SAML connections, as some examples. Easy SSO can be implemented on-premises or in the cloud. For cloud deployments, Easy SSO provides Amazon EC2 support. EasyConnect also includes a set of built-in REST APIs to facilitate integrations with any client environment. Out-of-the-box support is given for AD and LDAP, Kerberos/IWA/NTLM, popular applications, web servers, and form-based authentication support.

Why worth watching: Watch for SSO Easy continued support for SAML-based SSO use cases and the expansion of pre-configured drop-in templates for other common SAML connections.

WALLIX

France-based WALLIX provides a range of cybersecurity solutions, including WALLIX Bastion for Privileged Access Management (PAM) and WALLIX Trustelem as its Identity & Access Management-as-a-Service solution. WALLIX Trustelem Identity Management features include a centralized directory, SSO, MFA, and self-service capabilities. Its Central Directory allows for the import of other directories and provides support for Active Directory, Azure AD, LDAP directories, and Google G Suite directory. Its SSO identity federation provides good standard support for SAML, OpenID Connect, and OAuth protocols, gives pre-integrated application support to popular services such as Office 365, G Suite, and Salesforce, to name a few, and provides a dashboard of user rights to application along with integrated Window Authentication, and X.509 client certificates support. Trustelem offers its own mobile application authenticator as well as support for SMS OTP, FIDO 2, and Google authenticator. Trustelem also provides a user self-service with Active Directory self-service password reset and MFA enrollment capabilities.

Why worth watching: Look for WALLIX Trustelem to continue good integrated support of some key Access Management features to customers in the EU.

Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

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

Types of Leadership

We look at four types of leaders:

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

For every area, we distinguish between three levels of products:

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Deployment
- Interoperability
- Usability

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

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

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

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

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

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

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

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be

of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly, and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

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

Rating scale for products and vendors

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

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

Positive	Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.
Neutral	Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.
Weak	Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.
Critical	Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

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

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

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

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

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

Related Research

Leadership Compass: Access Management - 80757

Leadership Compass: Access Governance & Intelligence - 80098

Leadership Compass: API Management and Security - 80477

Leadership Compass: Passwordless Authentication - 81215

Leadership Compass: Enterprise Authentication Solutions - 80062

Leadership Compass: IDaaS Access Management - 79016

Leadership Compass: Identity API Platforms - 79012

Copyright

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

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

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