KuppingerCole Report

LEADERSHIP COMPASS

By Richard Hill
February 02, 2021

Access Management

This Leadership Compass provides insights to the leaders in innovation, product features, and market reach for Access Management on-premises, cloud, and hybrid platforms. Your compass for finding the right path in the market.

By **Richard Hill**
rh@kuppingercole.com

Content

1 Introduction

Access Management refers to the group of capabilities targeted at supporting an organizations' access management requirements traditionally found within Web Access Management & Identity Federation solutions, such as:

- Authentication
- Authorization
- Single Sign-On
- Identity Federation

These access management capabilities are well-established areas in IAM's broader scope (Identity and Access Management). They are continuing to gain attraction due to emerging requirements for integrating business partners and customers.

Web Access Management (WAM) & Identity Federation started as distinct offerings. (Web) Access Management is a rather traditional approach that puts a layer in front of web applications that takes over authentication and – usually coarse-grained – authorization management. That type of application can also provide HTTP header injection services to add authorization information to the HTTP header used by the back-end application. Also, tools are increasingly supporting APIs for authorization calls to the system. Identity Federation, on the other hand, allows splitting authentication and authorization between an IdP (Identity Provider) and a Service Provider (SP) or Relying Party (RP). The communication is based on standard protocols. Back-end systems need to be enabled for Identity Federation in one way or another, sometimes using the Web Access Management tool as the interface. Identity Federation can be used in various configurations, including federating from internal directories and authentication services to Cloud Service Providers or different organizations. However, most vendors today provide integrated solutions that support both a centralized access management based on federation protocols such as:

- SAML v2
- OAuth
- OIDC

Access Management focused IDaaS vendors vary from the traditional SSO vendors. Overtime, WAM vendors progressed to address most internal web-centric use-cases with greater customization flexibility according to business-specific requirements. Further progressions included vendor solutions born in the cloud that address standardized access management requirements for SaaS and IaaS applications.

However, this came with some architectural limitations in how their solutions could be more easily extended to address access management for on-prem applications. Over the last few years, these vendors have made significant changes to their product architecture to make them cloud-ready or support extended to on-premises applications.

However, support for web applications without federation support through traditional approaches such as Http header injection or credential injection must still be considered. Both methods deliver a single sign-on (SSO) experience to the users across multiple web sites and allow for centralized user management, authentication, and access control.

These technologies are enabling technologies for business requirements such as agility, compliance, innovation (for instance, by allowing new forms of collaboration in industry networks or by adding more flexibility in the R & D supply chain), and the underlying partnership & communication.

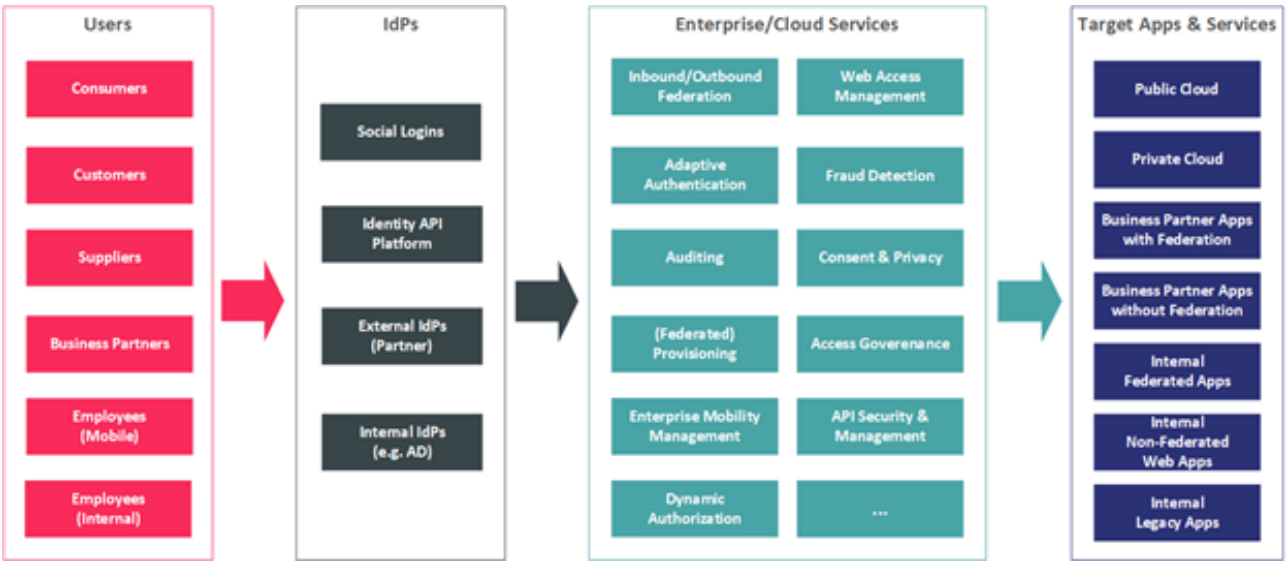


Figure 1: The enterprise requires access to systems, either on-premise or in the cloud, for all types of user populations

Although traditional on-premises Access Management solutions have focused on WAM & Identity Federation solutions in the past, KuppingerCole sees a convergence of this market with Access Management focused IDaaS solutions. Therefore, this Leadership Compass considers Access Management solutions deployed on-premises, in the cloud, or as a hybrid model. Solutions offered as a managed service are also be considered when the technology is owned by the MSP (Managed Service Provider).

1.1 Market Segment

Access Management and Identity Federation are still frequently seen as separate segments in the IT

market. However, when looking at the business problems to be solved, these technologies are inseparable. The business challenge to solve is how to support the growing “Connected and Intelligent Enterprise.” Businesses require support for business processes incorporating external partners and customers. They need access to external systems and rapid onboarding of externals for controlled and compliant access to internal systems. They request access to external services such as Cloud services, as well as capabilities to use their acquired access data to drive intelligence within their systems. The required use of mobile devices is also leveraged onto organizations as the changing workforce desires to work anywhere from any device. IT has to provide an infrastructure for this increasingly connected and intelligent enterprise, both for incoming and outgoing access, both for customers and other externals such as business partners, including existing and new on-premise applications, cloud services, and mobile devices.

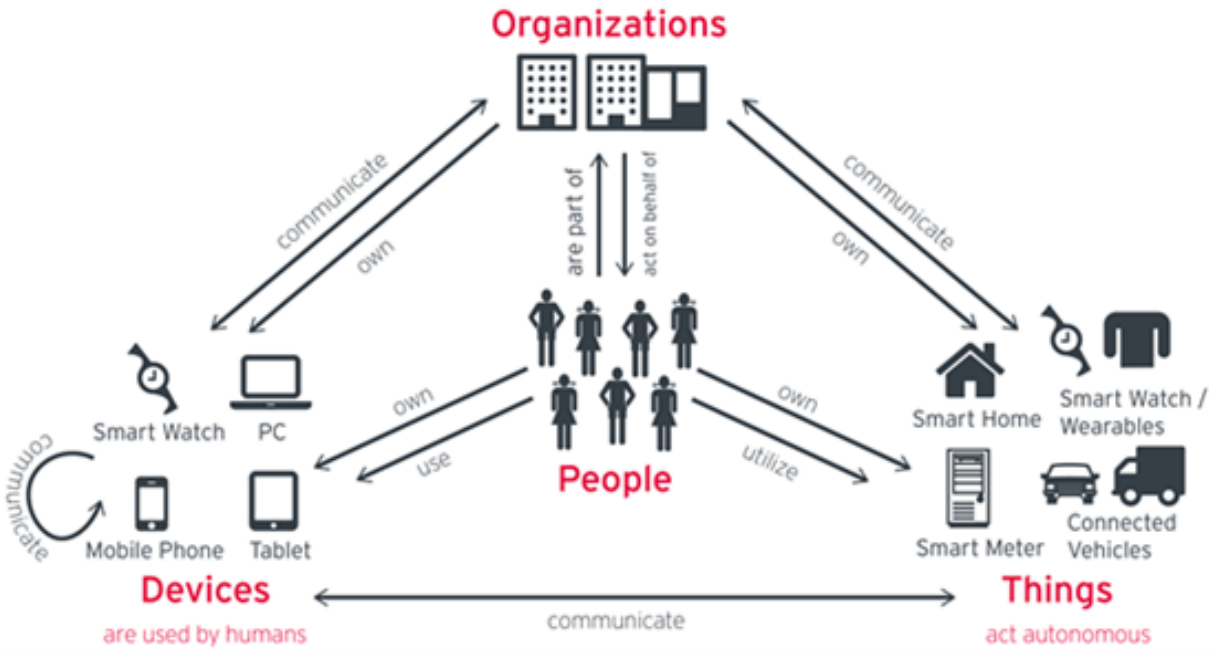


Figure 2: The increasingly connected enterprise ecosystem

IDaaS Access Management (AM) offers a springboard for most organizations to start using foundational IAM elements delivered from the cloud and move the rest of the IAM functions, as they find it appropriate and at a pace that matches the organizational security maturity and cloud strategy. The IDaaS market, with its ease of adoption and cloud-native integrations, is slowly overtaking the on-premises IAM market.

The IDaaS AM market is continuing on a growth spree allowing these technology trends to speed up the adoption by aligning them to match the organization’s IAM priorities that security in which IAM leaders must take note. The IDaaS market continues to evolve with a significant push from organizations looking to adopt cloud-based delivery of security services, including IAM. With IDaaS vendors slowly bridging the gap with traditional on-premises IAM software in terms of depth of functionalities, they present a strong alternative for organizations to replace existing on-premises IAM deployments.

IDaaS is only delivered as SaaS, hosted, and managed by the IDaaS vendor itself. Vendors that use the on-premises software provided by other vendors to offer hosted and managed IAM services are not considered IDaaS vendors. Mostly combined in separate service bundles based on adoption and usage trends, most services are priced per managed identity or active users per month. Some functions such as user authentication or fraud detection can be charged on a per-transaction basis depending on the function's delivery and consumption.

As an alternative to organizations managing the Access Management solutions themselves, some vendors provide offerings described as Managed Services, whether on-premises or Software as a Service (SaaS) offerings. Pure-play SaaS solutions are multi-tenant by design. Customers can easily onboard, usually as simple as booking online and paying with a credit card. On the other side, Managed Service offerings are run independently per tenant. The two aspects of the high relevance are the elasticity of the service and a pay-per-use license model.

Providers of CIAM solutions increasingly understand the business use-cases requirements of managing privacy policies, terms of service, and data sharing arrangements that change frequently and adapt their services accordingly. For organizations doing business across borders, it is important to offer functions that allow them to comply with data sharing and privacy regulations, such as consumer notification and consent management. There's a varying level of support available from Access Management vendors to manage these CIAM functions.

The support for open identity standards shapes the direction and defines AM implementations' success increasingly. This also drills down to the sense that an organization's ability to support business requirements through IAM depends on the AM vendor's flexibility to support both open industry standards and protocols. Support for Open Banking presents a great validation of that observation. Most popular authentication and identity federation standards include support for LDAP, Kerberos, OpenID, OAuth, SAML and sometimes RADIUS and TACAS. Organizations with a need for dynamic authorization management might require support for XACML or UMA. User provisioning services commonly require support for SCIM and SPML. Security and IAM leaders are encouraged to understand whether the service supports these standards OOTB or require customizations using available SDKs or other programmable interfaces. This will go a long way in keeping your IAM flexible and sustainable.

Increasingly we are seeing security platform APIs becoming more readily available, exposing the platform's functionality to the customer for its use. It's 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. APIs are provided for the different functional requirements of IAM, Federation, IDaaS & CIAM, giving the ability to select these market segment capabilities a la carte as needed. Exposing key functionality via APIs allows for workflow and orchestration capabilities across environments and better DevOps support through automation. API-driven platforms diverge from the COTS solutions offered in the past and are defined by its use cases. Some use cases are targeted at organizations that, due to the complexity of internal processes and other operational reasons, are looking to build their own C/IAM platform, automate or enhance existing IAM capabilities. Also, where traditional turn-key COTS are primarily UI-driven, API-based platforms typically require a developer-ready solution, providing API toolkits such as widgets or SDKs that facilitate rapid development.

Fraud is a major cost to businesses worldwide. As one would expect, banking, finance, payment services, and retail organizations are some of the most frequent fraudsters' objectives. However, insurance, gaming, telecommunications, health care, cryptocurrency exchanges, travel and hospitality, and real estate are increasingly targeted as cybercriminals have realized that most online services trade in monetary equivalents. Moreover, after years in the sights of cybercriminals, banking, and finance, in general, are better secured than other industries, so fraudsters attack any potentially lucrative target of opportunity. Fraud perpetrators also continually diversify their Tactics, Techniques, and Procedures (TTPs). Although Fraud Detection solutions, also referred to as Fraud Reduction Intelligence Platforms (FIPS), is often considered a different market with its separate offerings, there has been a noticeable up-tick in Access Management solutions providing some level of Fraud Detection capabilities. These capabilities range 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. This Leadership Compass evaluates and reports on the level of Fraud Detection support for each vendor, giving the reader an indication of the extent of this trend in the AM market.

Besides these technical capabilities, we 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.

1.2 Delivery models

Increasingly there is a clear trend in the market to move Access Management solutions from an on-premises delivery model to a cloud delivery model. And 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 an organization's Access Management. Ultimately selecting the right Access Management solution delivery model will depend on the customer requirements and their use cases.

1.3 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, integration with ITSM solutions, or analytics, and intelligent capabilities 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 authenticators
  - Strong authentication (e.g. 2FA, MFA)

    - Some level of support for contextual, adaptive, or continuous authentication
    - Device Authentication (e.g. IoT)
- Authorization Management
- Policy Management and Security Orchestration
- Password Management
- Session Management (e.g. Single Sign-On, Secure Token Translation, etc.)
- Identity Federation
    - Including broad support for federation standards and related standards
- Support for non-federation-enabled applications
- Some level of support for on-premises 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
- Centralized management of users, authorization policies, dashboards, reporting, etc.
- Some level of access to the solutions capabilities via APIs
- API Security
- Support for audit, forensics, compliance, and reporting
- Support for Administrators and DevOps

Inclusion criteria:

- Support for the capabilities listed above
    - Although all expected features listed will be evaluated, some features will be weighted differently than others, for example:
    - Higher weighted features include, but not limited to, authentication, authorization, session, and password management, as well as identity federation
    - Lower weighting would include features such as API security and fraud detection
- 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:
    - MFA or SSO centric solutions, but little support the other expected features
- Solutions that only support Identity Federation via federation standards such as SAML and OAuth, but no non-federation-enabled web applications, or don’t support federation standards
- MSP solutions that are based on technology of other vendors, with the MSP not owning the IP on the technology

We’ve reached out to a large number of vendors for providing a comprehensive overview of the current state of the market. 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.

2 Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

Figure 3: The Overall Leadership rating for the Access Management market segment

When looking at the Leader segment in the Overall Leadership rating, we see a picture that is a typical representation of mature markets, where many vendors deliver feature-rich solutions. The market continues to remain crowded, with 28 vendors that we chose to represent in our Leadership Compass rating with a few other vendors that did not meet our essential evaluation criteria listed in the “vendors to watch” section or declined participation in this year’s edition.

ForgeRock holds the leadership position in the Overall Leadership evaluation of the Access Management (AM) market, closely followed by Microsoft. Next is IBM and Ping Identity close together, followed by Micro Focus. Following is a group of vendors that includes Okta, CyberArk, Oracle, OneLogin, Broadcom, RSA, and Ilantus. This group of vendors is a mix of established and emerging players, some being stronger in their market position and others in innovativeness. We strongly recommend further, detailed analysis of the information provided in this document for choosing the vendors that are the best fit for your requirements.

The Challenger segment is slightly more populated than the Leaders segment. It features established vendors, frequently being more regional focused, and several niche vendors with fit-for-purpose Access Management capabilities preferred by many organizations over the established players. Leading in this segment is Cloudentity, and Simeio Solutions near the upper borderline, with LoginRadius, EmpowerID, WSO2, and Ergon following in the upper half of the Challenger section. The Challenger section's lower half consists of Evidian, SecureAuth, Optimal IdM, Thales Group, Nevis Security, Soffid, Curity, and Forum Systems. Near the bottom border of the Challenger segment is Ubisecure having a good solution for its regional customers but having somewhat limited functionality and small market share and geographic coverage. All vendors within the Challenger section have good products with varying levels of Access Management capabilities, market presence throughout the world, or other market niche focus.

None of the vendors appear in the Follower segment.

Overall Leaders are (in alphabetical order):

- Broadcom
- CyberArk
- ForgeRock
- IBM
- Ilantus
- Micro Focus
- Microsoft
- Okta
- OneLogin
- Oracle
- Ping Identity
- RSA

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

Figure 4: Product Leaders in the Access Management market segment

Product Leadership is where we examine the functional strength and completeness of services. Since Access Management (AM) is continuously evolving product features, we find many vendors qualifying for the Product Leaders segment and some vendors adding Access Management capabilities to their product features portfolio. Because vendors offer a wide variety of Access Management capabilities and differ in how well they support these capabilities, organizations need to perform a thorough analysis of their Access Management requirements to align their priorities while evaluating an Access Management solution.

Leading from the front in Product Leadership is ForgeRock, very closely followed by Ping Identity with Microsoft, IBM, and Micro Focus close behind. Together, these vendors make up the top portion of the

Product Leadership section. A second group within the Product Leadership is evident in the lower half of this section. Leading this second group is Cloudentity, RSA, Broadcom, Oracle, Ilantus, CyberArk, Okta, OneLogin, Simeio Solutions, and EmpowerID, all of which deliver leading-edge capabilities across the depth and breadth of Access Management capability spectrum evaluated for the purpose of scoring the vendors in this Leadership Compass. IAM leaders must exercise appropriate caution while evaluating these vendors as subtle differences ignored in functionality evaluation of these products could translate into greater incompatibilities for business processes during implementation. Therefore, it is highly recommended that organizations spend considerable resources in properly scoping and prioritizing their Access Management requirements before an Access Management product evaluation.

In the challenger's product leadership segment are (in alphabetical order) Curity, Ergon, Evidian, Forum Systems, LoginRadius, Nevis Security, Optimal IdM, SecureAuth, Soffid, Thales Group, Ubisecure, and WSO2. All these vendors have interesting offerings but lack certain Access Management capabilities that we expect to see, either in the depth or breadth of functionalities seen in the Leadership segment offerings.

None of the vendors appear in the Follower segment.

Product Leaders (in alphabetical order):

- Broadcom
- Cloudentity
- CyberArk
- EmpowerID
- ForgeRock
- IBM
- Ilantus
- Micro Focus
- Microsoft
- Okta
- OneLogin
- Oracle
- Ping Identity
- RSA
- Simeio Solutions

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative

companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

Figure 5: Innovation Leaders in the Access Management market segment

We have rated roughly a third of the vendors as Innovation Leaders in the Access Management (AM) market. Given the maturity of Access Management solutions, the amount of innovation we see is somewhat limited. However, the vendors continue to differentiate themselves by innovating in several areas, such as strong adaptive authentication capabilities, dynamic authorization, access intelligence, providing APIs and

API security, fraud detection, automation, or using a more modern containerized and microservice-related product delivery that aligns with the KuppingerCole Identity Fabric framework, as well as delivering better flexibility. While the ease of deployment remains a fundamental capability for Access Management products, providing the desired levels of scalability and flexibility can considerably affect the ease of deployment for most large AM deployments.

The graphic needs to be carefully read when looking at the Innovation capabilities, given that the x-axis indicates the Overall Leadership, while the y-axis stands for Innovation. Thus, while some vendors are closer to the upper-right edge, others being a little more left score slightly higher regarding their innovativeness.

ForgeRock leads the Innovation Leadership evaluation, followed by a distinct grouping of Ping Identity, Microsoft, Micro Focus, and IBM. Another group occurs in the lower half of the Leadership segment. It includes Cloudentity, OneLogin, Okta, Ilantus, CyberArk, and Simeio Solutions that have made significant changes to their AM product portfolio to be in-line with other innovative vendors in the market. These vendors differ in many details when it comes to innovation and balancing it with overall product leadership. Therefore, a thorough vendor selection process is essential to pick the right vendor of all the AM players that best fit the customer requirements.

The majority of players in this Access Management Leadership Compass made it into the Innovation Challenger segment. Close to this segment's top border, we see Oracle with strong core AM functionality but less strength in innovative capabilities seen by the vendors in the Leadership section. Another distinct grouping is seen in the top third of the Challenger section are Broadcom, LoginRadius, EmpowerID, and RSA. Vendor groupings often indicate similar levels of capabilities. The remaining vendors in the lower half of this Challenger section (in alphabetical order) are Curity, Ergon, Evidian, Nevis Security, Okta, Optimal IdM, SecureAuth, Soffid, and WSO2. All these vendors have also been able to demonstrate promising innovation in delivering specific Access Management capabilities. Please refer to the vendor pages further down in the vendor's section of this report for more details.

Three vendors appear near the top border of the Follower segment and include Forum Systems, Thales Group, and Ubisecure. Although these vendors may provide their customers' necessary capabilities, they do not offer the same level of innovation feature sets as some of the other vendors.

Innovation Leaders (in alphabetical order):

- Cloudentity
- CyberArk
- ForgeRock
- IBM
- Ilantus
- Micro Focus
- Microsoft

- Okta
- OneLogin
- Ping Identity
- Simeio Solutions

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

Figure 6: Market Leaders in the Access Management market segment

With a strong market position, successful execution, and strengthened Access Management (AM) product features, Microsoft and IBM are out front leading the Market Leadership evaluation. Following these two vendors in the Market Leadership segment are (in alphabetical order) Broadcom, CyberArk, ForgeRock, Micro Focus, Okta, OneLogin, Oracle, Ping Identity, and RSA– all of which have several deep-rooted complex Access Management deployments across multiple industries.

We find WSO2, LoginRadius, Ergon, Evidian, Ilantus, Simeio Solutions, and EmpowerID close to the Leader segment in the Challenger section. While we count them amongst Market Leaders in other areas of the overall Access Management market, their position in the AM market is affected by several factors, including

limited global presence and a shortage of technology partners. Their Access Management product deployment is one of them. Following this group is (in alphabetical order) Cloudentity, Curity, Forum Systems, Nevis Security, OneLogin, Optimal IdM, SecureAuth, Soffid, and Ubisecure appear in the lower half of this Challenger segment.

No vendors appear in the Follower segment.

Market Leaders (in alphabetical order):

- Broadcom
- CyberArk
- ForgeRock
- IBM
- Micro Focus
- Microsoft
- Okta
- OneLogin
- Oracle
- Ping Identity
- RSA
- Thales Group

3 Correlated View

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

3.1 The Market/Product Matrix

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

Figure 7: The Market/Product Matrix.

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

In this comparison, it shows which vendors are better positioned in our Product Leadership analysis compared to their position in the Market Leadership analysis. Vendors above the line are sort of “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 (AM) market is somewhat mature but still evolving, 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, Micro Focus, Okta, OneLogin, Oracle, Ping Identity, and RSA. Being positioned closer to the axis, both ForgeRock and Micro Focus represent a slightly better market versus product leadership balance. Ping Identity is positioned under the axis representing its inclination for stronger product leadership compared to the market.

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

In the middle right-hand box, we see three vendors that deliver strong product capabilities for Access Management but are not yet considered Market Champions. Ilantus, Simeio Solutions, EmpowerID, and Cloudentity have a strong potential to improve its 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 as of yet. They also have moderate market success as compared to market champions. These vendors include (in alphabetical order) Curity, Ergon, Evidian, Forum Systems, LoginRadius, Nevis Security, Optimal IdM, SecureAuth, Soffid, Ubisecure, and WSO2.

3.2 The Product/Innovation Matrix

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

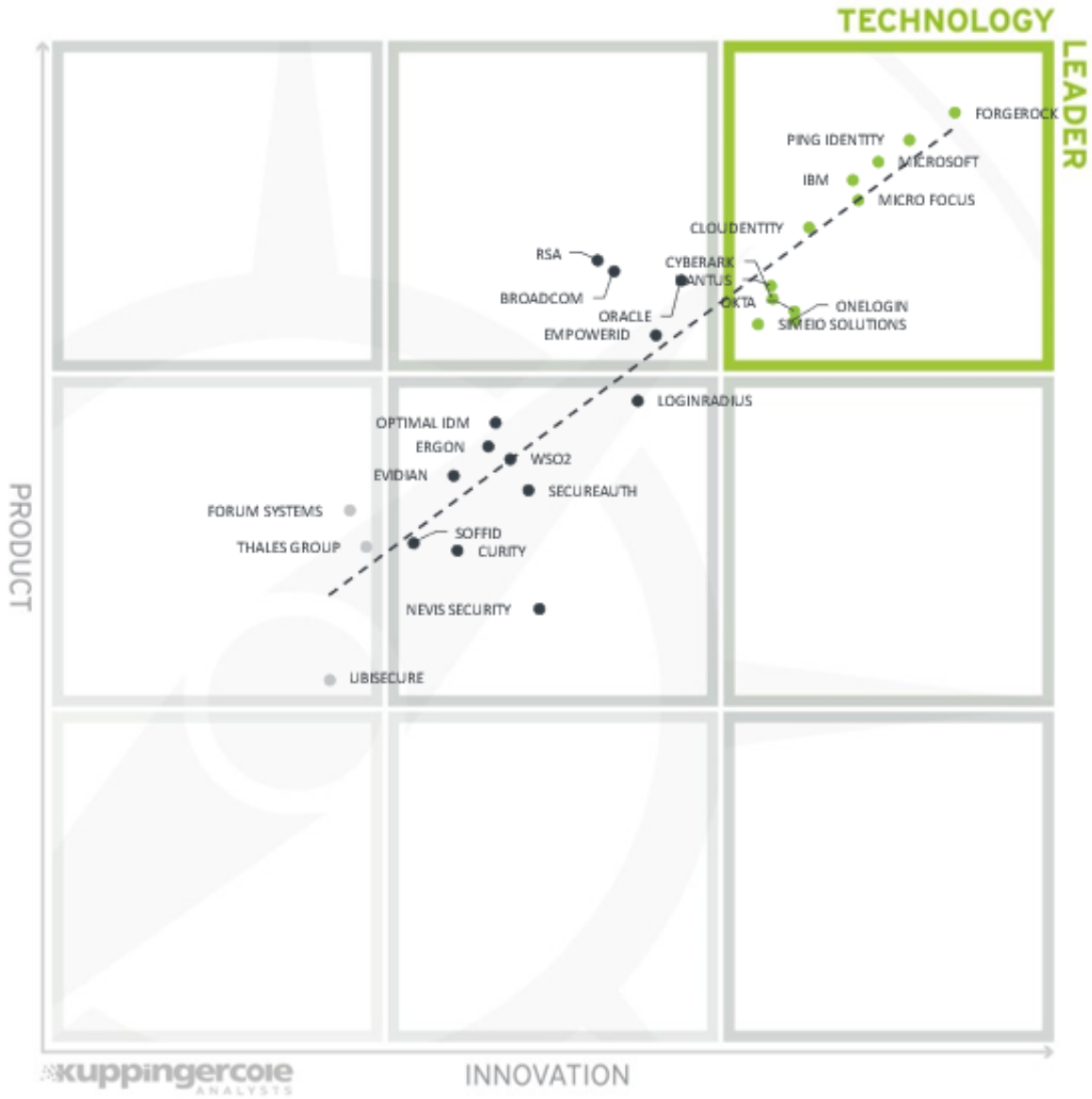


Figure 8: The Product/Innovation Matrix.

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

Here, we see a good correlation between the product and innovation rating, with 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 of the leading vendors in the upper right corner, scattered throughout the box. The leading vendors are ForgeRock, followed by Ping Identity, Microsoft, IBM, Micro Focus, and Cloudentity – all placing close to the axis depicting a good balance of product features and innovation. Ilantus, CyberArk, Okta, Simeio Solutions, and OneLogin are following found more towards the

bottom of the box.

Over a third of the vendors appear in the middle box vendors showing both innovation and product strength, which includes (in alphabetical order) Curity, Ergon, Evidian, LoginRadius, Nevis Security, Optimal IdM, SecureAuth, Soffid, and WSO2.

Three vendors, Forum Systems, Thales Group, and Ubisecure appear in the middle left box, showing stronger product capabilities than innovation.

3.3 The Innovation/Market Matrix

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

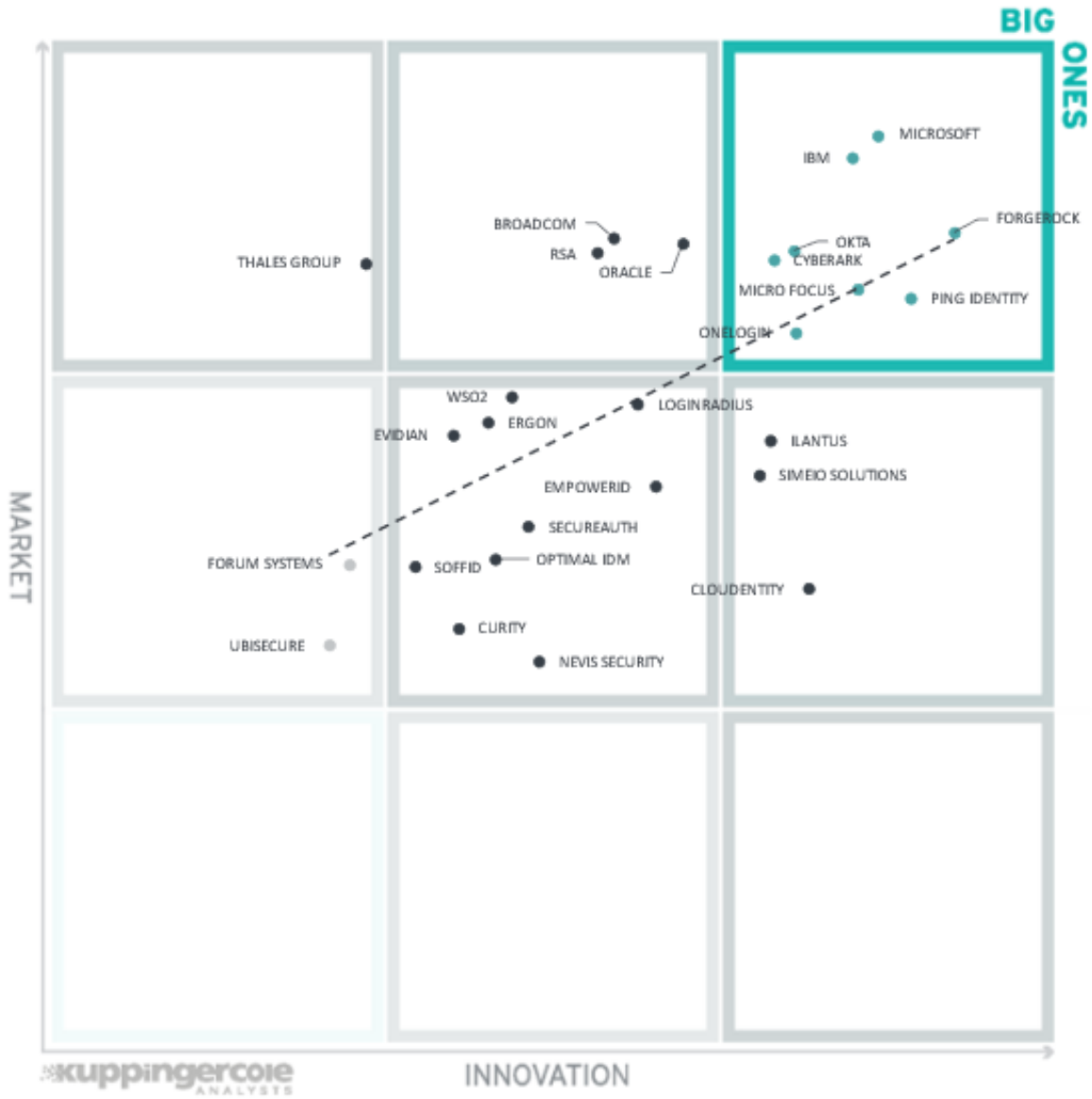


Figure 9: The Innovation/Market Matrix

Vendors 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 both Microsoft and IBM on top, with the remainder of the vendors towards the bottom half of the same box, which includes (in alphabetical order) CyberArk, ForgeRock, Micro Focus, Okta, Ping Identity, and OneLogin, indicating that they haven’t yet reached the same market position as the more established players.

Three vendors, Ilantus, Simeio Solutions and Cloudentity, appear in the middle right box showing good innovation with slightly less market presence than the vendors in the “Big Ones” category.

We find Oracle, Broadcom, and RSA with a strong market position in the box at the middle top but not scoring as much in Innovation Leadership.
The Thales Group appears in the top left box, indicating a strong market presence with fewer innovative features than the other vendors.

The segment in the middle of the chart contains about a third of the vendors rated as challengers both for market and innovation leadership, which includes (in alphabetical order) Curity, EmpowerID, Ergon, Evidian, LoginRadius, Nevis Security, Optimal IdM, SecureAuth, Soffid, and WSO2.

Only Forum Systems and Ubisecure appear in the middle left box indicating market presence with lower innovation. However, these vendors have the potential to become more innovative, increase market presence, or both.

4 Products and Vendors at a glance

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

Ratings at a glance

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

Product	Security	Functionality	Interoperability	Usability	Deployment
Broadcom Symantec Access Management	●	●	●	●	●
Cloudentity Cloud Identity Plane, Authorization Control Plane	●	●	●	●	●
Curity Identity Server	●	●	●	●	●
CyberArk Identity Security Platform	●	●	●	●	●
EmpowerID	●	●	●	●	●
Ergon Airlock Suite	●	●	●	●	●
Evidian Suite	●	●	●	●	●
ForgeRock Identity Platform	●	●	●	●	●
Forum Systems Forum Sentry	●	●	●	●	●
IBM Security Verify	●	●	●	●	●
Ilantus Compact Identity	●	●	●	●	●
LoginRadius CIAM Platform	●	●	●	●	●
Micro Focus NetIQ Access Management	●	●	●	●	●
Microsoft Azure Active Directory	●	●	●	●	●
NEVIS Security Identity Suite	●	●	●	●	●
Okta Identity Cloud	●	●	●	●	●
OneLogin Trusted Experience Platform	●	●	●	●	●
Optimal IdM OptimalCloud	●	●	●	●	●
Oracle Identity Cloud Service	●	●	●	●	●
Ping Intelligent Identity Platform	●	●	●	●	●
RSA SecurID Access	●	●	●	●	●
SecureAuth Identity Platform	●	●	●	●	●
Simeio Identity Orchestrator	●	●	●	●	●
Soffid IAM	●	●	●	●	●
Thales SafeNet Trusted Access	●	●	●	●	●

Product	Security	Functionality	Interoperability	Usability	Deployment
Ubisecure Identity Platform	positive	neutral	neutral	neutral	neutral
WSO2 Identity Server	strong positive	positive	positive	positive	strong positive
Legend	critical	weak	neutral	positive	strong positive

In addition, we provide in the second table 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
Broadcom Inc.	positive	strong positive	strong positive	positive
Cloudentity	strong positive	neutral	neutral	neutral
Curity	neutral	neutral	neutral	neutral
CyberArk	strong positive	positive	strong positive	positive
EmpowerID	strong positive	neutral	positive	neutral
Ergon	positive	positive	positive	positive
Evidian (was acquired by Atos)	neutral	positive	positive	positive
ForgeRock	strong positive	strong positive	strong positive	positive
Forum Systems	weak	neutral	positive	neutral
IBM	strong positive	strong positive	strong positive	strong positive
Ilantus Technologies	strong positive	positive	positive	positive
LoginRadius	strong positive	positive	positive	positive
Micro Focus	strong positive	positive	strong positive	positive
Microsoft	strong positive	strong positive	strong positive	strong positive
NEVIS Security AG	positive	weak	neutral	weak
Okta	strong positive	strong positive	strong positive	positive
OneLogin	strong positive	positive	positive	positive
Optimal IdM	positive	neutral	positive	neutral
Oracle	strong positive	positive	strong positive	strong positive
Ping Identity	strong positive	positive	strong positive	positive
RSA Security	positive	strong positive	strong positive	positive
SecureAuth	positive	neutral	neutral	positive
Simeio Solutions	strong positive	neutral	positive	neutral
Soffid	neutral	neutral	neutral	positive
Thales	weak	positive	strong positive	positive
Ubisecure	weak	weak	neutral	neutral
WSO2	positive	positive	positive	positive
Legend	critical	weak	neutral	positive	strong positive

This table requires some additional explanation regarding the “critical” rating.

In Innovativeness, this rating is applied if vendors provide none or very few of the more advanced features we have been looking for in that analysis, like strong adaptive authentication capabilities, dynamic authorization, access intelligence, providing APIs and API security, fraud detection, automation, or using a

more modern containerized and microservice-related product delivery.

These ratings are applied for Market Position in the case of vendors which have a very limited visibility outside of regional markets like France or Germany or even within these markets. Usually the number of existing customers is also limited in these cases.

In Financial Strength, this rating applies in case of a lack of information about financial strength or for vendors with a very limited customer base but is also based on some other criteria. This doesn't imply that the vendor is in a critical financial situation; however, the potential for massive investments for quick growth appears to be limited. On the other hand, it's also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding Ecosystem applies to vendors which have no or a very limited ecosystem with respect to numbers and regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that growth and successful market entry of companies into a market segment relies on strong partnerships.

5 Product/service evaluation

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

Spider graphs

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

- Identity Federation
  The depth in which standards support the Identity Federation solution can 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 Mgmt & SSO
  This category 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 Mgmt
  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, 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 Support & Security
  This section evaluates the solutions capabilities supported via APIs, API standards, and available

API DevOps support. Also looked at is the solution's ability to protect the solution's own APIs or APIs connected between applications and other services. Capabilities include 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.

- 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), detect unauthorized account takeover, user and device profiling, orchestration of fraud signals, and identity proofing.
- UI, Dashboards & Reporting
  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, knowledge-base, and community support/platform for developers.

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

5.1 Broadcom Inc.

Broadcom, a publicly-traded semiconductor and infrastructure software products company, acquired the Symantec Enterprise business in November of 2019. At the time of the acquisition, the Symantec division had a large number of customers worldwide but estimates that a small fraction of these customers uses products from the Symantec Identity Security portfolio, which includes its Access Management solutions. Symantec Access Management consists primarily of Symantec SiteMinder and components of the Symantec VIP, Symantec IGA, and Symantec Advanced Authentication offerings.

Broadcom's Identity Security portfolio includes Access Management, Authentication, Identity Management, and Privileged Access Management. Symantec SiteMinder handles all federation use cases and supports most related standards such as SAML, OAuth2, OIDC, WS-Federation, JWT, and SCIM. SCIM support comes from the Symantec IGA portion of the Broadcom offer, while the OAuth2 support is from the API Gateway part of the Broadcom offering.
SSO is available for web-based applications using reverse proxy or web server agents, although SSO for non-web (e.g., desktop & thick client) is not available without third-party integrations. Session management is also given for common use cases. SiteMinder session defense support the prevention of session stealing and stolen sessions, although detection of some common session attacks and session ID lifecycle monitoring are not given, as examples. Good breadth of authentication methods is supported, as well as contextual and risk-adaptive authentication as part of its Advanced Authentication portfolio. Good access management based on ABAC, RBAC, CBAC, or user-group based is available. Basic role management requires features of Symantec IGA, a separate, but complementary offering.

Broadcom provides good API security. SiteMinder's APIs require authentication that returns a bearer JWT token via SSL connections. All other API security is accomplished via its API Security Gateway and Broadcom's own Layer7 API Management offering. There is no direct Online Fraud Detection support without integrations with third-party offerings, such as identity proofing with their IGA offering or SiteMinder's eTelligent rules capability for reaching out to any third-party source of information.

Broadcom SiteMinder is primarily software deployed to a server with Symantec VIP component as its cloud-based service, which is FIPS 140-2 - Cryptographic module standards and SSAE 18 SOC 2 Type II certified compliant. However, its portfolio also includes other cloud products and services that can be used to augment its Access Management solution. SiteMinder can also be offered as a managed service by 3rd party service providers. SiteMinder provides REST interfaces that support Swagger Codegen and opensource tools to generate server stubs and client SDKs. Also, deployment scripts for DevOps tools like Chef and Puppet are given for deployments of SiteMinder environments.

Overall, Broadcom's Symantec Access Management solution is a mature and feature-rich product but may be more suitable for large complex Access Management deployments. Broadcom has a global presence with customers focused primarily in North America, but a relatively smaller number of specialized integration partners as compared to other international IAM suite vendors.

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

BROADCOM

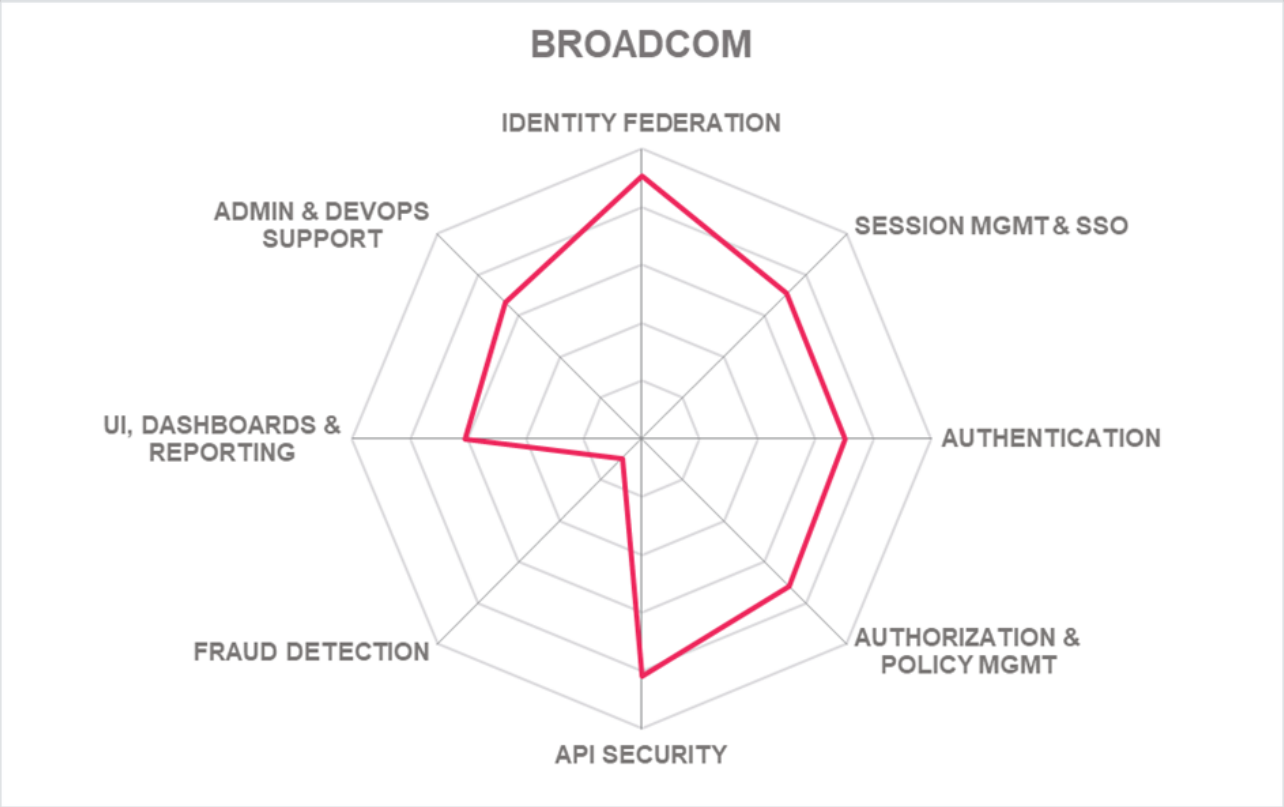
Strengths

- Good federation capabilities
- Breadth of authentication methods
- Contextual and risk-adaptive authentication
- Authorization and policy management
- API security
- DevOps support
- Integrates well with all Symantec IGA components
- Large global customer base
- Strong engineering and technical support

Challenges

- Customers primarily focused in North America, but also a presence in the EMEA and APAC regions
- Analytics and other access intelligence rely on third party solutions
- Somewhat limited product delivery options, although improvements on the roadmap
- Missing direct fraud detection support

Leader in


BROADCOM
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.2 Cloudentity

Cloudentity is a privately held identity and access management company headquartered in Seattle, WA. The company introduced its CIAM.next platform in 2017 as a cloud-native identity and authorization platform that separated Identity Management away from Access Management functions to meet the requirements of hybrid-cloud services. Cloudentity focuses on dynamic authorization and authorization as code to secure APIs, microservices, and traditional application workloads. Cloudentity offers its Cloud Identity Plane and Authorization Control Plane components of its Cloudentity Platform for API-driven Access Management solutions.

Cloudentity provides a Managed SaaS platform based on microservices and machine learning intended to automate the discovery, authorization, and governance of applications, services, and APIs. The platform leverages its REST or gRPC APIs for all intercommunication, allowing customers to extend functionality via orchestration with external APIs or microservices. Cloudentity features extend existing infrastructure through open standards to integrate identities beyond people to include workloads, applications, APIs, and IoT devices. Cloudentity Authorization Control Plane provides coarse to fine-grained data objects, consent, and gives centralized policy management that provides continuous and contextual transactional authorization. Cloudentity offers a good breadth of supported authentication methods, although there is some limitation of supported biometric authenticators. Good federation support is given, and for most federation-related standards with exceptions like WS-Federation and UMA. Cloudentity fully supports transactional authorization, where sessions are short-lived transactional tokens. Common session attacks and usage anomalies can be detected, and session protection is given for binding of session ID to user properties or session ID lifecycle monitoring as examples. SSO is achieved through a reverse proxy sidecars, existing API Gateway(s), or web server proxy for web-based applications, but SSO for non-web applications/ IT systems (Desktop apps, thick clients, etc.) are not supported.

Cloudentity features strong API security features using active security measures to protect APIs. Cloudentity supports MicroPerimeter Authorizers plug-ins for popular API Gateways, including Azure APIM, AWS API GW, Apigee, Axway, Kong, and Envoy. MicroPerimeter Authorizers provide API & service discovery, data tagging for sensitive information, IdP discovery for mapping to existing IAM infrastructure, and distributed PDP authorization. Cloudentity also offers some fraud detection related capabilities such as detecting unauthorized account takeover through transactional authorization with anomaly detection or endpoint device profiling fraud detection. Support for third-party fraud detection tools can be achieved through integrations with RSA and IBM. All report-related data is accessible via API queries. Policy Packs for specific verticals and major compliance frameworks are available out-of-the-box such as GDPR, PDS2, HIPAA, NIST SP 800-53, and CCPA.

Cloudentity supports SaaS and Managed SaaS deployment models and provides a fully distributed set of microservices for hybrid &multi cloud use cases. The cloud-hosted SaaS service is independently certified compliant with the EU GDPR. Cloudentity microservices are entirely API driven, so 100% of the Cloudentity functionality is available via APIs and its UI. Supported API related protocols include SOAP, REST, Webhooks, gRPC, and Kafka streams. SDKs are generated via Swagger to provide SDKs for over 60

different programming languages and variants.

Cloudentity serves mid-market to enterprise organizations, with customers primarily in North America with some EU & UK customers. The Cloudentity ecosystem of technology partners and integrators continues to grow rapidly. Although Cloudentity's identity and authorization platform could be considered unorthodox from other traditional Access Management solutions, it provides a more modern approach to API-driven Access Management use cases. It also provides a uniform service-level access policy enforcement that can significantly reduce the overall complexity of legacy and modern applications that rely heavily on APIs to exchange sensitive data across hybrid IT environments.

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

CLOUDENTITY™

CUSTOMER IDENTITY AT CLOUD SPEED

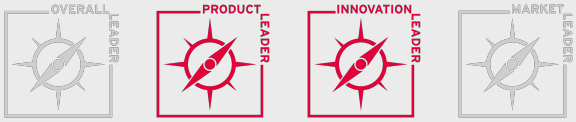
Strengths

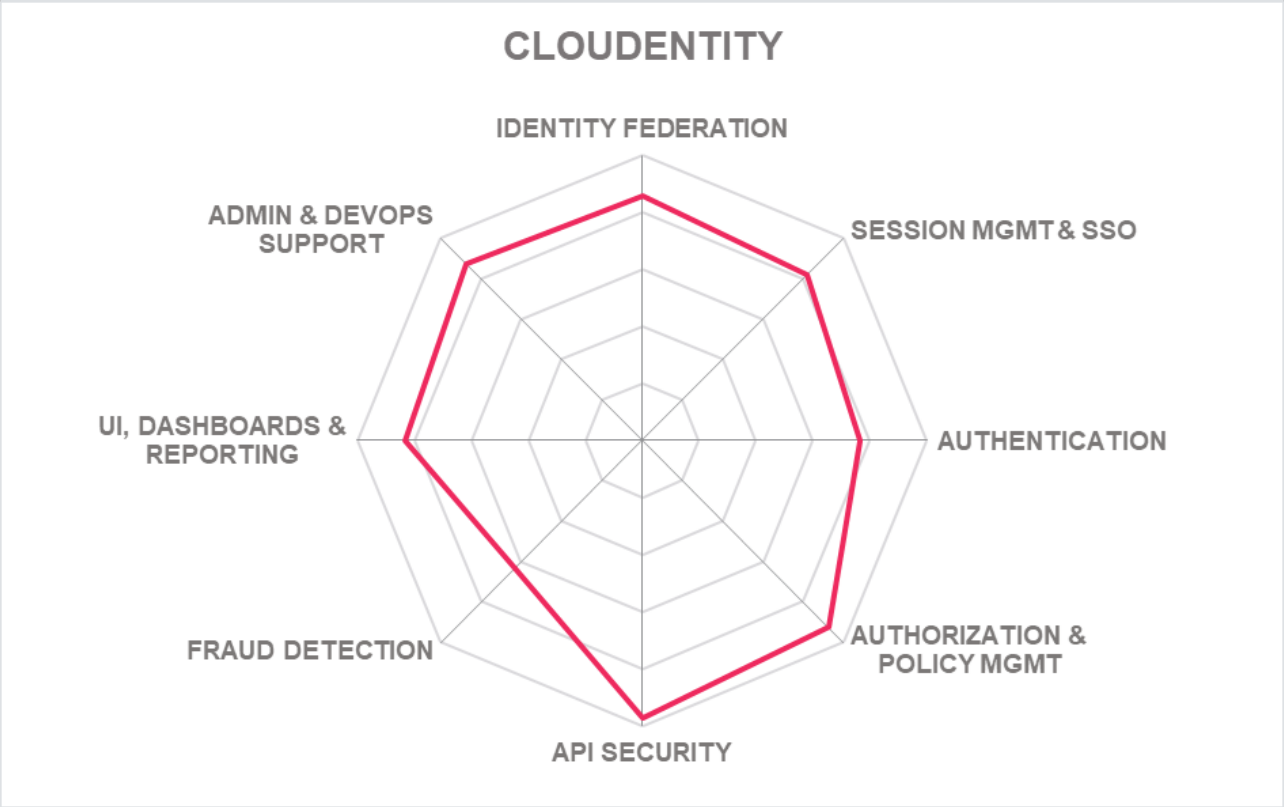
- Good federation support
- Session management
- Authorization and Policy Management
- Strong API security
- Admin and DevOps support
- Reporting API & OOB compliance framework support

Challenges

- Primarily North American customer base, with a presence in the EU & UK with a growing global support ecosystem
- Limited biometric authenticator support
- SSO for non-web-based applications not supported

Leader in




CLOUDENTITY
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.3 Curity

Curity is a provider of API-driven identity management solutions based in Stockholm, Sweden. The company focuses on providing identity services for APIs and microservices. Curity Identity Server is the company's flagship product for identity and access management and API security. The product has three core modular components that provide authentication, token, and user management services.

The Curity Identity Server is a modern solution designed for OAuth2, OpenID Connect, and SCIM to provide a modern platform for identity and access management for internal and external users and make it easy to manage very large deployments servicing millions of users. It is composed of three major modules: Authentication Service, Token Service, and User Management Service. SSO is accomplished using the same authentication service for all OIDC / OAuth clients. OIDC compliant session management is supported with the ability to detect session attacks such as brute force and session protection like the binding of session ID to user properties.

Multiple authentication methods are supported with some biometric authentication such as iOS Touch ID. FIDO support is given using YubiKey, macOS, iPhone, and other compliant authenticators. Encap SCA or Swedish BankID is provided via apps. Support for contextual and risk-adaptive authentication that includes contexts for device, network, user, and location-based that allows access decisions based on that contextual attribute information.

Curity provides a DevOps dashboard of clients in which runtime deployments, alarms, and profiles can be viewed, among other useful procedure screens. For a dashboard view of access or system activity overtime, Curity provides Prometheus compliant metrics data that can provide a historical view. API security can integrate with an API Gateway using token validation, split token approach, or phantom tokens. Curity's adaptive authentication can be integrated with fraud detection systems, although additional fraud detection capabilities are part of Curity's short term roadmap.

Curity Identity Server is a self-contained application that can support all deployment models and is delivered as a Zip file or as a Docker container. A Helm Chart is available to simplify deployment to a Kubernetes cluster. Curity can run in AWS, Azure, GCP, or a customer's own data center. Curity's partners can provide a managed service. The Curity Identity Server supports both REST, WebHooks and has a 100% Juniper-compliant CLI. For extending the capabilities or functionality of the product, SDKs are available for Java, Kotlin, or any other similar JVM-based language.

Established in 2015, Curity is the youngest of the vendors evaluated in this Leadership Compass. Although young, Curity builds on a solid foundation on a modern and modular API-driven architecture. Customers range from small to mid-market organizations focused primarily in the EMEA region with some North America presence. Although Curity has a relatively small system integrator ecosystem, it has a growing list of strategic technology partners, professional services, and on-site and remote support services globally.

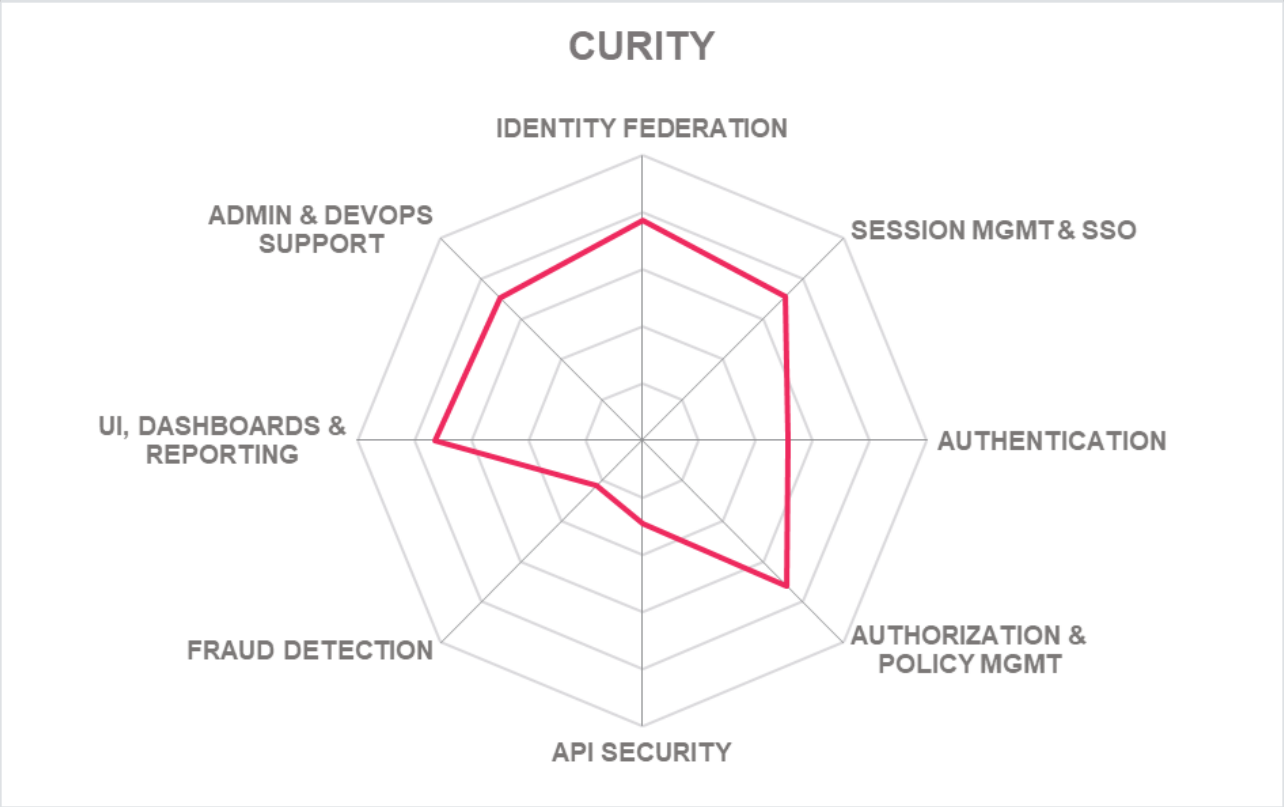
Security	●●●●○
Functionality	●●●○○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○

Strengths

- Identity federation
- Comprehensive support for OAuth and OIDC open standards
- Combines flexible authentication with token-based API security controls
- Authorization and policy management
- DevOps support
- Modular API-driven architecture

Challenges

- Customer base primarily in the EMEA region and some presence in North America with a relatively small partner ecosystem
- Limited support for on-premise legacy or non-federated applications or services, although its authentication API can integrate on-premise apps and services
- Limited fraud detection support, although more capabilities on near term roadmap


CURITY
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.4 CyberArk

CyberArk, known for its Privileged Access Management (PAM) solution, acquired the Idaptive identity platform in mid-2020. In January 2019, Idaptive was spun-out of Centrify. In this Leadership Compass, CyberArk offers its Identity Security Platform, which consists of CyberArk Single Sign-On, Adaptive Multi-factor Authentication, Lifecycle Management, and CyberArk Alero. Together, it provides the capabilities for Access Management.

CyberArk Idaptive has depth and breadth of authentication methods, including biometric support, except for voice recognition. Support for FIDO U2F and FIDO 2 is also given. CyberArk Idaptive leverages the WebAuthn API to enable passwordless authentication to the Identity Service. Risk-based authentication is part of the adaptive SSO and MFA offering, which covers all contextual use cases evaluated in this report. CyberArk Idaptive stores all its access policies centrally in its cloud directory. Support for ABAC, RBAC, CBAC, and risk-based policy controls. A risk score can also be sent as part of the SAML/OIDC payload for applications to enforce their respective authorization, allowing security teams to take immediate action when anomalous, risky, or suspicious behavior is detected. Password syncing across multiple identity repositories for on-prem and cloud directories are not supported. However, Idaptive does support user password generation during user onboarding, self-service password change, and forgot password flows for users residing in on-prem and cloud directories. Good session management, SSO, and federation related standards capabilities are given, including SAML, OAuth 2, OIDC, WS-Federation, JWT, and SCIM. Only FIPS 140-2 and SSAE 18 SOC 2 Type I & II standards are certified compliant.

CyberArk Idaptive services are 100% built upon RESTful APIs and support OData. None of the solution's functionality is exposed via CLI. SDKs are publicly available on CyberArk's developer-focused portal supporting the C/C+, .NET, Python, Ruby, Go, and PHP programming languages. CyberArk Idaptive's Online Fraud Detection (OFD) as part of the access management capabilities leverages a real-time event and user behavior analytics platform for fraud detection of logins and transactions via APIs.

CyberArk Idaptive is a multi-tenant SaaS cloud solution that runs in AWS. It supports both public cloud and hybrid deployment models with its App Gateway that enables VPN-less, Zero Trust access, SSO, and access management capabilities back to on-premises applications and services. However, the CyberArk Idaptive App Gateway is not part of its base AM products. Good built-in UEBA and integration support. The cloud service supports a Managed Service Provider mode, where MSPs can manage the entire lifecycle of customer tenants. The cloud-hosted service is independently certified to comply with US, Australian, and Asian specific laws and regulations.

CyberArk, established in 1999, has a strong offering for Access Management with its Identity Security Platform serving primarily mid-market to enterprise organizations. CyberArk mainly focuses on the US as the primary market with growth in the EMEA and APAC markets and has a good partner ecosystem. CyberArk appears in all Leadership segments with a well-balanced set of features for Access Management.

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

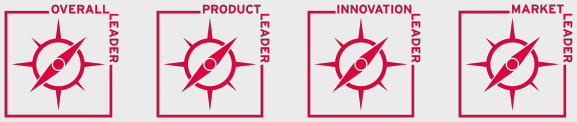
Strengths

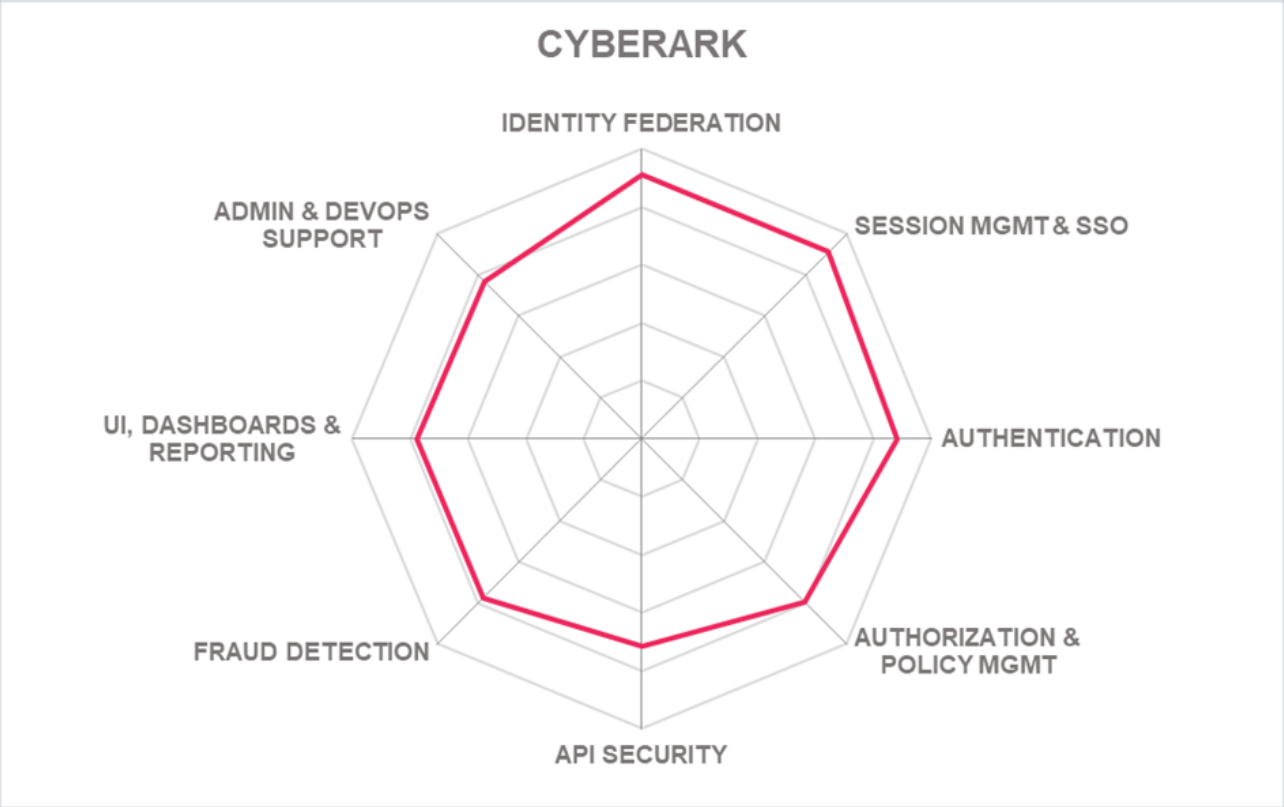
- Identity federation
- Session Mgmt. & SSO
- Authentication depth & breadth
- Authorization & Policy Mgmt.
- Fraud detection features
- User and Entity Behavior Analytics (UEBA)
- Good UI, dashboard and reporting
- DevOps support
- Partner ecosystem

Challenges

- Strong focus on the US as the primary market with growth in EMEA and APAC markets
- Gateway connection to on-premises AM capabilities not part of base AM product
- Password syncing across multiple identity repositories capability is not available, although user password generation support for several use cases regarding users residing in on-prem and cloud directories is given

Leader in




CYBERARK
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.5 EmpowerID

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, Single Sign-On, Multi-factor Authentication, Access Recertification, Risk Management (SoD), Advanced Risk Management (SoD), and Policy-Based Access Control as components of its Access Management portfolio.

EmpowerID provides a range of supported authentication methods, including biometrics, but excluding voice authentication. FIDO UAF and FIDO 2 U2F is supported with full WebAuthN/FIDO2 support on its short-term roadmap.
Support for contextual and risk-adaptive authentication is focused on device-based, user, location, with some network contexts, although these attributes cannot be added to access policies. EmpowerID's provides standard session management capabilities and some abilities to detect session attacks. SSO can be achieved by either reverse proxy or web-server agents. The solution supports managing access of users based on ABAC, RBAC, CBAC, PBAC, and user group-based controls. Role discovery and management are also given. Identity federation capabilities and standards are well supported. For WAM non-federated applications, a KONG/NGINX plugin is given for the microservice reverse proxy API gateway, which is free to protect EmpowerID but requires a license to protect other applications.

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. API security can be accomplished via an API Gateway, UMA, RBAC, ABAC, PBAC, and Scopes. Basic API protocol-specific attacks can be detected, as well as other features such as API key management, schema validation, rate liming, provides a Security Token Service.

EmpowerID can be deployed as software deployed on-premises, a cloud service, or a managed service. A couple of years back, EmpowerID shifted focus to a cloud-native and containerized approach. In fact, EmpowerID is completely containerized using Docker and runs on Azure AKS, making it Kubernetes compatible. Supported operating systems depends on which microservice is used. Most support Linux, but a few still require Windows. Microsoft SQL database server is required at deployment. Microsoft IIS and Azure application servers are also supported. Any IaaS platforms that support Docker containers or Kubernetes can be used. All EmpowerID functionality is exposed via REST API. SCIM support is given too. EmpowerID Workflow Studio IDE supports the ability to create customer APIs - to be published and run on EmpowerID or Azure as App Services or Functions.

EmpowerID provides Access Management functions and services that are largely targeted at meeting the common access management requirements of mid-sized enterprises. Overall, EmpowerID offers a good Access Management solution with few required on-prem components to better control data and applications on-premises. Several advanced access management features are available. 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.

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

empowerID

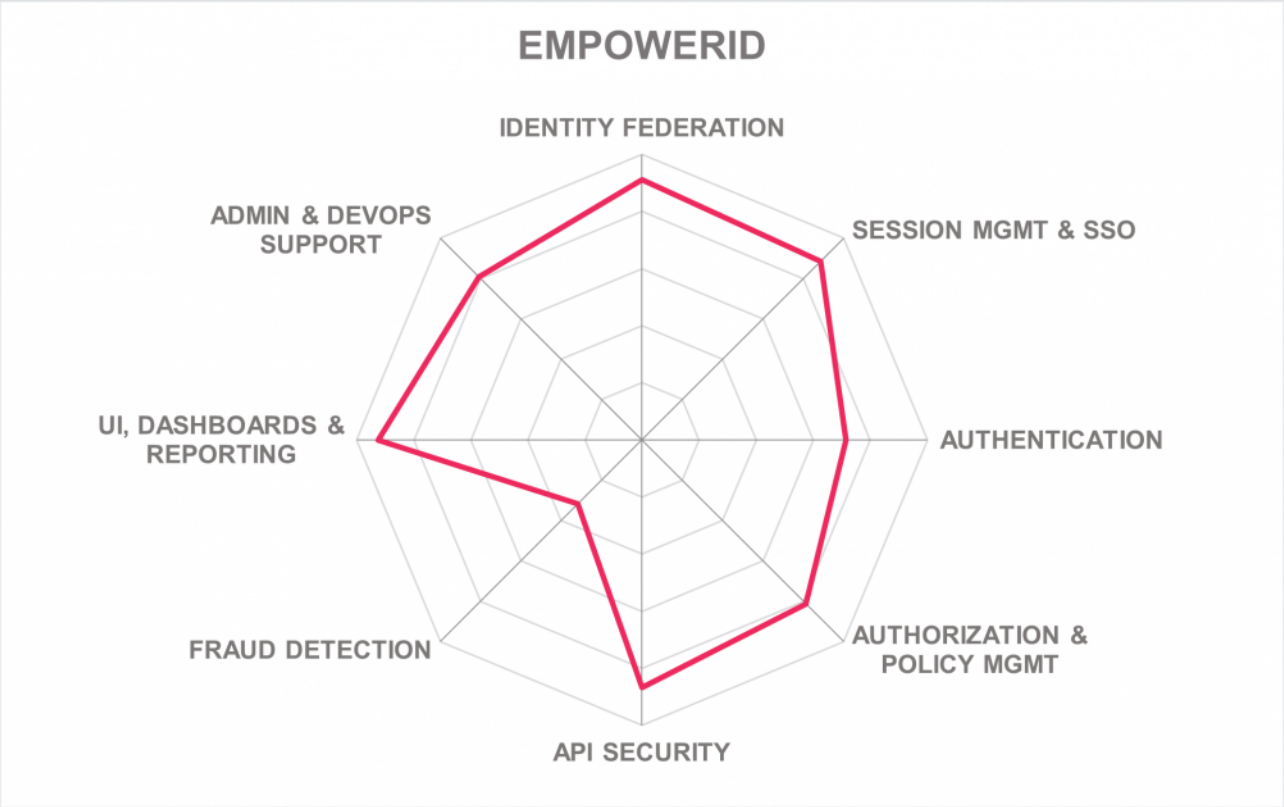
Strengths

- Identity federation
- Session management & SSO
- Authorization & policy management
- FIDO 2 support
- API support and security
- UI, Dashboard & reporting
- Admin & DevOps support
- Good support services
- Certified compliant with multiple standards

Challenges

- Runs and remains focused on Microsoft technology
- Smaller but selective partner ecosystem mostly concentrated across Europe
- Limited fraud detection capabilities
- API gateway has dependencies on third-party technology component

Leader in


EMPOWERID
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.6 Ergon

Ergon Airlock is a single product with multiple services within a suite. The suite includes a WAF, API Gateway, cIAM, and 2FA authentication that leverages the synergies from the close integration between components such as the Airlock WAF policy enforcement point for access decisions by Airlock IAM.

Common authentication methods are supported as well as Android and iOS-based biometric authenticators. FIDO authenticators are currently not supported, although FIDO support, including FIDO passwordless, will be released in the early part of 2021. Risk-based and adaptive authentication is also available supporting device, user, and location-based contexts that can be used within access policies. Access policies are managed and stored centrally, along with policy authoring tools provided that support ABAC, RBAC, CBAC, and user-group based access management. Basic role management is also given as well as good session management with some session attack detection capabilities. SSO is achieved through a reverse proxy that handles SSO across multiple web applications, although support for non-web applications is not. SSO secure token translation across multiple applications is available. A standard federation capability is given with the most recent federation related standards supported such as SAML 2, OAuth 2, OIDC, and JWT. SCIM support is not given. Good built-in reporting and connector to 3rd party reporting systems are supported.
Fraud detection capabilities have some dependencies on integrations with IBM Trusteer Pinpoint Solution and/or Webroot Threat Intelligence feeds, although a built-in scoring-based anomaly detection engine is provided. Good API security capabilities are available. API security enforcing specifications such as OpenAPI and WSDL, content filtering using blacklist filters via Airlock WAF can be applied to JSON attributes. Good support for analyzing protocol-specific API attacks, rate limiting, and schema validation is given. API statistics, monitoring, and reporting are available, as well as support for microservice architectures via a containerized micro gateway component.

Ergon Airlock can support on-premises, full multi-tenancy for cloud, and hybrid deployment models. Airlock can also be delivered as software deployed to a server, virtual appliance, or as a Docker container. Linux-based operating systems are supported, except Windows. The product is not available for IaaS installations, although a SaaS and managed service is provided through partner companies, but not directly by Ergon. Some of the solution's functionality is available via REST-based APIs, although SOAP, WebHooks, OData, or WebSocket protocols are not supported. Some functions accessible via CLIs and SDKs such as Android and iOS SDK are available for 2FA, and a Java API available for cIAM extensions and other types of customization.

Ergon is a Swiss-based company established in 1984 with customers primarily in the DACH EMEA region with some growth in the APAC and North American regions targeting medium and mid-market organizations, although Airlock has some enterprise presence. Their partner ecosystem is again focused in DACH but remains small in the other areas, with the exception of system integrator partners in North America. Airlock has a well-established and mature set of Access Management features and provides good support for API security. Ergon Airlock Suite continues to be an interesting alternative to other solutions within the DACH EMEA region.

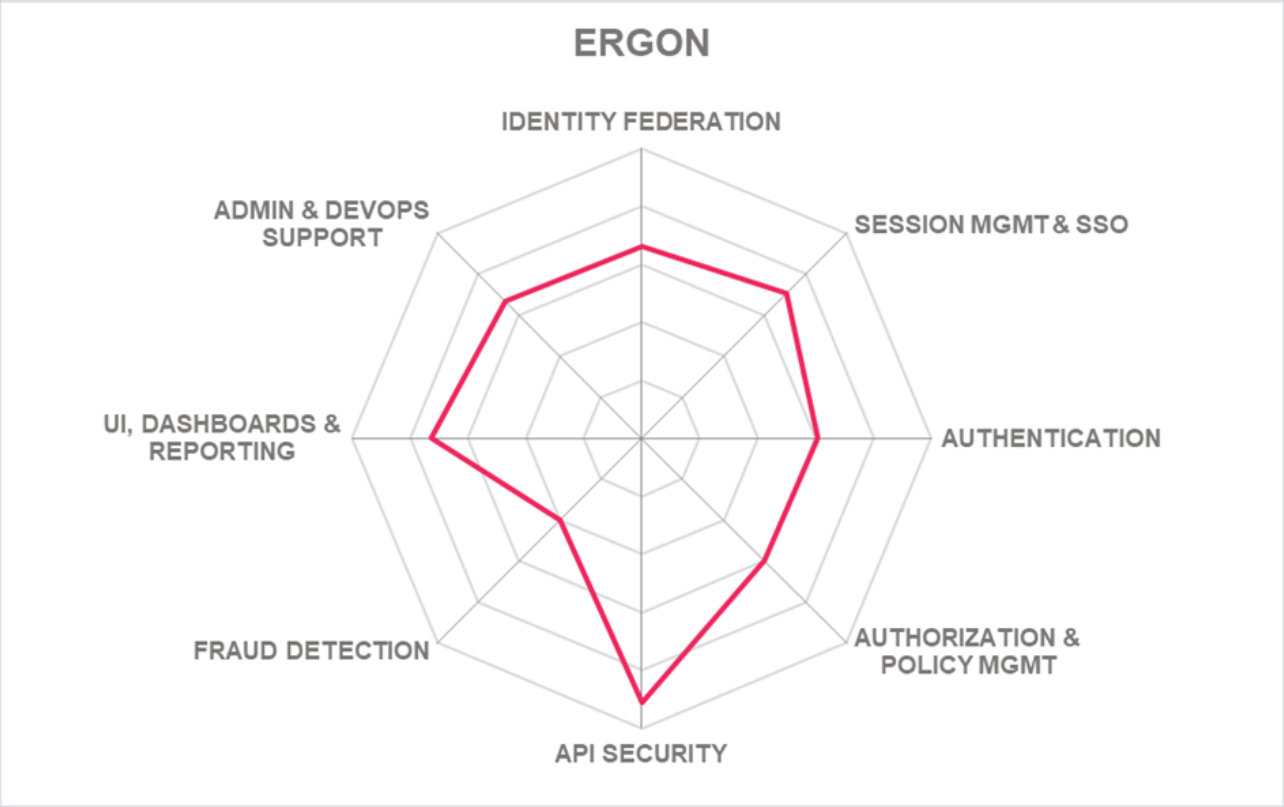
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○

Strengths

- API security
- Session management & SSO
- Identity federation
- MFA
- Adaptive Authentication
- User self-service
- Reporting and audit support

Challenges

- Small partner ecosystem & limited global reach
- Federation provisioning to cloud service is somewhat limited without additional configuration
- Limited fraud detection capabilities
- Limited API protocol support outside of REST


ERGON
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.7 Evidian (was acquired by Atos)

Based in France, Evidian is a dedicated business branch of the ATOS group within its Cybersecurity division since 2015, one of the leading IT service providers in Europe. Evidian offers multiple products within a suite, which includes Evidian Web Access Manager (WAM), Evidian IDaaS, as well as aspects of Evidian Identity Governance and Administration (IGA), and Evidian Analytics and Intelligence (A&I) as its Access Management portfolio evaluated in this Leadership Compass.

Evidian gives a good breadth of supported authentication methods and Android and iOS biometric authenticators. FIDO 2 is supported with compliant authenticators that include Yubico and Google.. Adaptive authentication supports the device, network, and user-based contexts. For location-based contexts, the Evidian WAM engine can determine the geocode of the IP of a user. These context attributes are used within access policies to determine a risk score for each new connection request. Access policies can be managed and stored centrally using Evidian WAM - IDaaS standalone or Evidian IGA but do not integrate with other policy management tools. Only ABAC and user-group access controls are available. Evidian WAM and IDaaS standalone offerings provide a coarse-grained authorization model, although fine-grained authorization can be achieved with an Evidian IGA integration. Good session management is provided with some session attack detection and protection. SSO is supported across multiple web applications, although Evidian WAM has to be used with Evidian eSSO for SSO of non-web applications or IT systems. Support for a range of identity federation use cases that include turning a regular Web application into Identity SP, IdP proxy with automatic redirection, partner scenarios, and token translation between federation protocols. Most federation related standards are also supported, except for UMA and SCIM, although a SCIM API is available to create (read/update/delete) users in the WAM component of the Evidian suite.

Fraud detection is limited to self-registration accounts creation and authentication that can be protected with Captcha and multiple login failures detection. Evidian WAM and Evidian IDaaS can act as an OAuth2.0 authorization servers providing authorization for API Management or Security Gateway solution. Evidian WAM can be used as a lightweight API Security Gateway that consumes OAuth tokens in reverse proxy mode. Still, it's not intended to replace a fully-feature API Management solution. Third-party integrations with Apigee have been achieved as part of the Atos Google Enhanced Alliance initiative.

Evidian supports on-premises, cloud, and hybrid deployment models that can be delivered as software deployed to a server, SaaS, or a managed service. Evidian managed service leverages Atos capabilities to host and manage its products. As software deployed to a server, Evidian supports CentOS, RHEL, and Windows operating systems. Evidian offers a fully integrated application server using Apache Tomcat. Evidian WAM could be deployed in containers on the most popular IaaS platforms. All administration actions can be performed via REST APIs or Java APIs as well as CLIs with Evidian WAM. Only JavaScript SDK is available to integrate user-facing functions such as authentication, self-service interface, registration, etc. into web pages.

Evidian has a somewhat larger share in the mid-market, localized mostly in the EMEA region. With a regional but healthy partner ecosystem across Europe, ATOS acquisition is likely to help Evidian gain

access to large customers and enter new geographies. European enterprises seeking Access Management solutions with good SSO, UI dashboards and reporting should look at Evidian Suite.

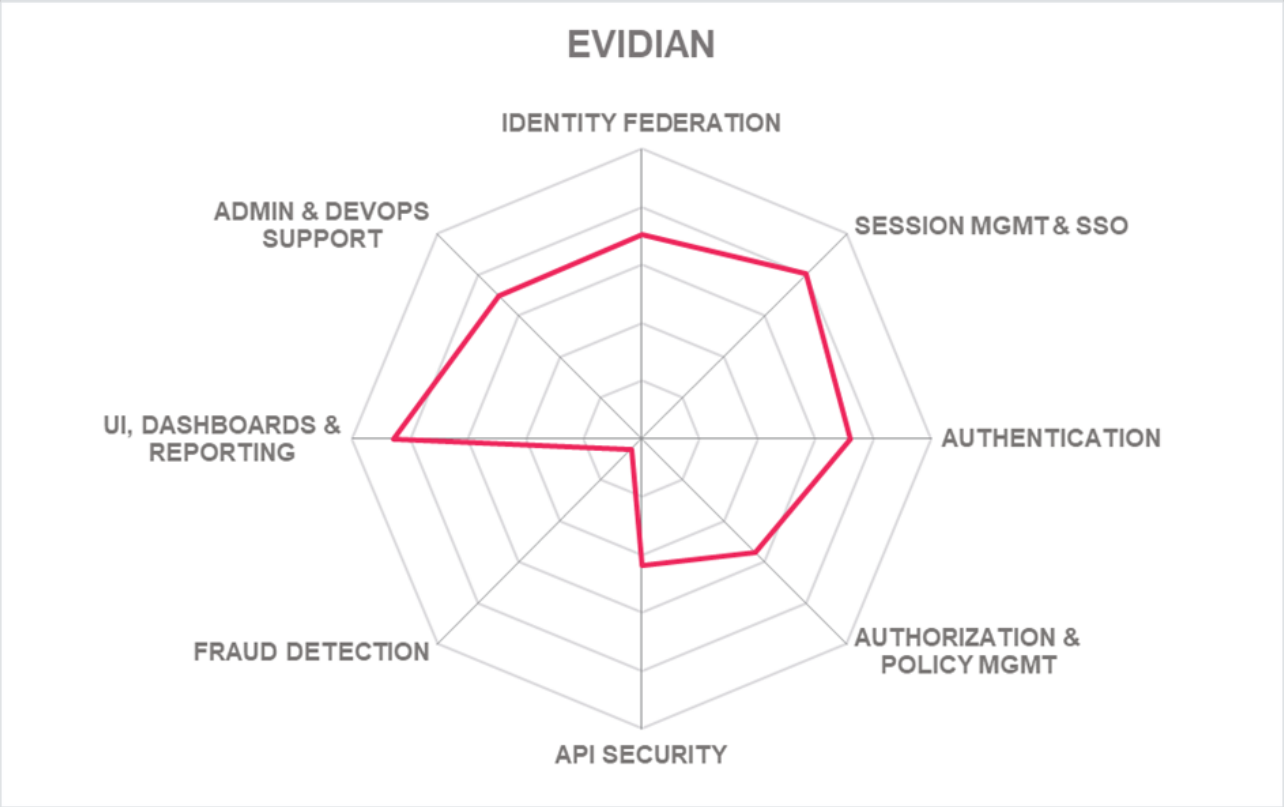
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●○

Strengths

- Mature Web Access Management
- Identity federation
- Session management & SSO
- Breadth of supported authenticators
- Adaptive authentication
- Good UI, dashboards, and reporting
- Tightly integrated suite of products

Challenges

- Limited presence and partner ecosystem outside Europe, and the APAC regions
- Limited, but effective access management control methods are supported
- Limited fraud detection
- Limited API security


EVIDIAN
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.8 ForgeRock

ForgeRock is a leader in the IAM space, providing a single integrated suite based on their Identity Platform. ForgeRock Access Management delivers core IAM functions such as authentication, authorization, user self-service, federation, entitlements, Single Sign-On (SSO), session management, and web services security.

ForgeRock supports most of the latest identity management and federation standards. In fact, ForgeRock is a significant contributor to several international standards organizations, such as Open ID Foundation, Open Identity Exchange, OASIS, etc. ForgeRock gives both depth and breadth of supported strong authenticators in including biometric and FIDO support. All adaptive authentication contexts evaluated are supported, including device, network, user, and location context attributes that can be used within access policies. ForgeRock Access Management supports many standard federation related protocols, such as SAML, XACML, OAuth2, OIDC, and SCIM, and can interoperate with other proprietary or non-standards-based WAM systems. SSO is achieved by reverse proxy or web-server agents. SSO is supported across multiple web or non-web applications. User web sessions are managed through browser cookies but not session HTTP headers. Good support for session detection and protection is also given.

The Intelligent Authentication Trees features allow customers to quickly build complex authentication policies leveraging state-of-the-art authenticators and risk intelligence sources to address high security and high assurance use cases. The graphical "Journey" workspace UI is straightforward to use, making it easy to see the entire flow graphically rather than paging through multiple configuration screens. ForgeRock Identity Platform gives a range of runtime services that assist with fraud detection and fraud management using validations at different points in the identity lifecycle from registration and proofing through to runtime checks using its Access Management services. Fraud detection capabilities are integrated through the ForgeRock Intelligent Access orchestration platform. ForgeRock also provides a Trust Network of different partner components that can be integrated into either on-premise or cloud deployments. ForgeRock offers strong API protection via the ForgeRock Identity Gateway, which provides a range of API security features. The ForgeRock platform can also be integrated with a range of gateway.

ForgeRock Identity Platform is a developer and administrator friendly product. ForgeRock solutions support on-premises deployments or deployments within IaaS providers. The ForgeRock cloud service is fully multi-tenant and is built on top of GCP, which aligns with a wide range of standards. For non-SaaS customers, ForgeRock supports DevOps through Kubernetes ready Dockers containers as well as scripted installers. All of the ForgeRock platform functionality is exposed through REST 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 Go, and JavaScript programming languages. ForgeRock Identity Platform components do have a dependency on Java technology requiring a Java runtime environment using either Oracle JDK 8 or 11, IBM SDK - Java Technology Edition (WebSphere only) 8, or OpenJDK 8 or 11.

ForgeRock is a privately owned company, established in 2010, that targets large enterprise customers split evenly across North America and EMEA, with a growing presence in the APAC region. ForgeRock provides a well-balanced solution for Access Management and continues to be venture-financed, allowing them to

invest in product development heavily. This investment shows by their rapidly improving capabilities, moving them up in the Innovation Leadership category. Overall, ForgeRock is amongst the leading-edge vendors in the IAM space and should be considered in product evaluations.

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

FORGEROCK

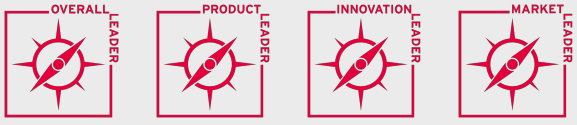
Strengths

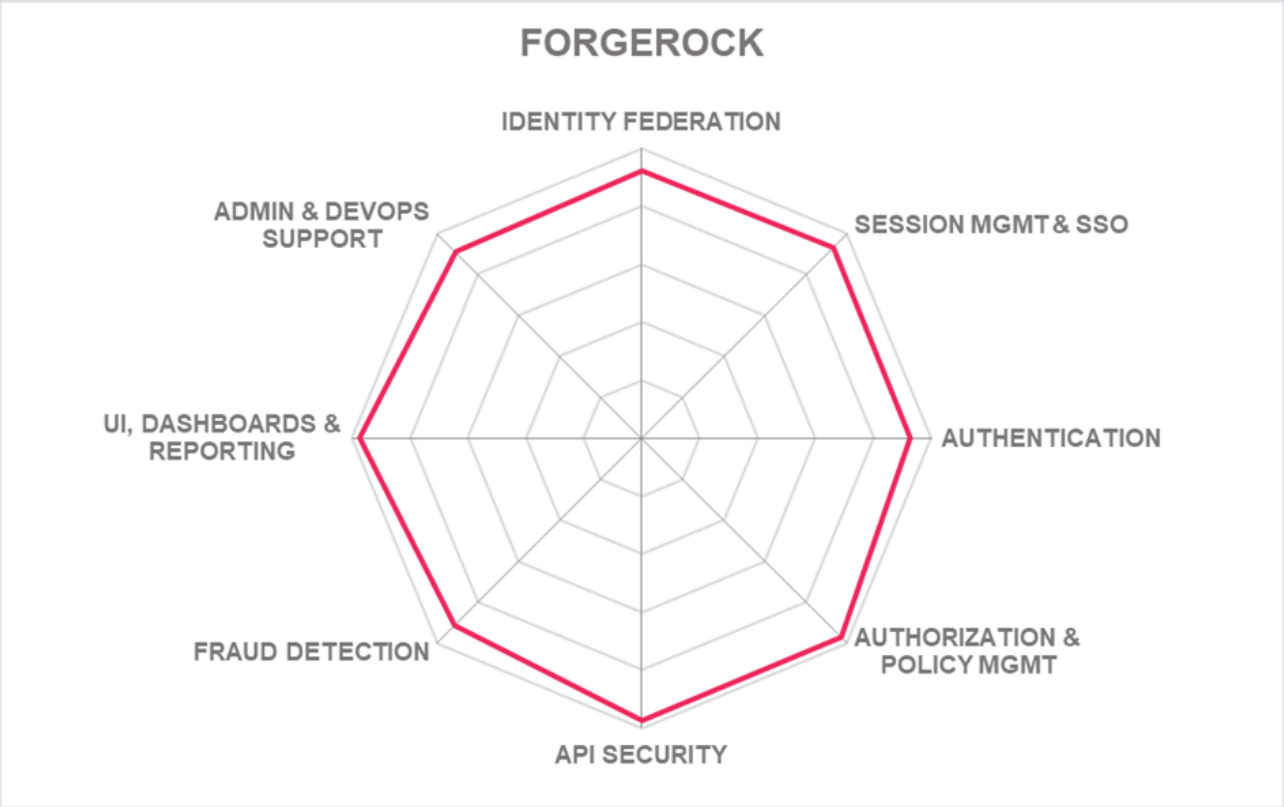
- Strong federation capabilities
- Wide range of MFA options out-of-the-box
- Strong Adaptive/Risk-based authentication
- All FIDO, FIDO2 - W3C WebAuthn standards supported
- Intelligent configuration flow UI
- Good reporting capabilities
- API security
- Fraud detection
- Good DevOps support
- Broad platform & partner ecosystem support

Challenges

- Java runtime dependencies
- Support for older versions of FIDO currently requires partner and community modules.
- Upgrades and configuration promotion from test to production require using command line tools and REST/JSON

Leader in




FORGEROCK
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.9 Forum Systems

Forum Systems is a privately held, employee-owned company with independent engineering based in Needham, MA. Since the very beginning, the company offers large-scale mission-critical solutions with a heavy emphasis on “Security by Design.” For this Leadership Compass report, Forum Systems provides its Forum Sentry platform as its Access Management solution.

Forum Sentry uses an administrative workflow capability and an agentless identity enforcement approach through built-in adapters to applications. Standard authentication support is available, but no FIDO options are given. Base adaptive authentication is available supporting device, user, location, and some network contexts that can be used in access policies. Centralized policy management is available both by a web interface or REST API, with some policy testing tools provided. Forum Sentry provides autonomous deployments and therefore does not integrate with other policy management tools. Access management allows for ABAC, RBAC, CBAC, and user-group based access controls. Basic role management and XACML are also supported. Password management supports password syncing across multiple identity repositories on-premises and cloud. SSO is achieved via a reverse proxy, which can support SSO across multiple web applications. Session management allows for some detection of session attacks and session protection mechanisms. Forum Sentry supports the most common identity federation use case with support for SAML, OAuth, OIDC, and WS-Federation. Federation related standards such as SCIM or UMA are not supported.

Forum Sentry uses its API Security Gateway with identity features built into the product capability set, providing the API firewall and DoS protection such as response caching, idle timeouts, concurrent connection limits. Content-based filtering and routing are also given. All OWASP XML and JSON attack threats can be analyzed. Secure token service and API key management is also provided. Fraud detection capabilities are not available within the Forum Sentry product but can be added via its API integration capabilities. Also, Forum Sentry provides the ability to selectively encrypt or redact data inside the message responses based on the identified user/system/device and their respective classification.

Forum Sentry supports on-premises, cloud, and hybrid deployments, in which the product can be delivered as either a hardware or virtual appliance, software deployed to a server, or Docker container that can be deployed to a Kubernetes cluster. For software delivered deployments, Forum Sentry can run on most Linux and Windows operating systems and support for most popular databases and application servers. Both AWS and Azure IaaS installations are possible. A managed service option is also available. Some of the solution's functionality is accessible via SOAP or REST APIs. CLIs are available for networking and provisioning. SDKs for any of the most popular programming languages evaluated are not available. Integrations with DevOps continual integration tools such as Puppet, Ansible, and Terraform are supported.

Founded in 2001, Forum Systems is a small company targeting mid-market to enterprise organizations, primarily in the USA and the UK, with a presence in other areas of Europe and the APAC region. Forum Systems maintains a relatively small partner ecosystem within its respective customer locations. Forum Systems should be of particular interest to organizations within the North American region requiring a U.S.

government standard support for Access Management.

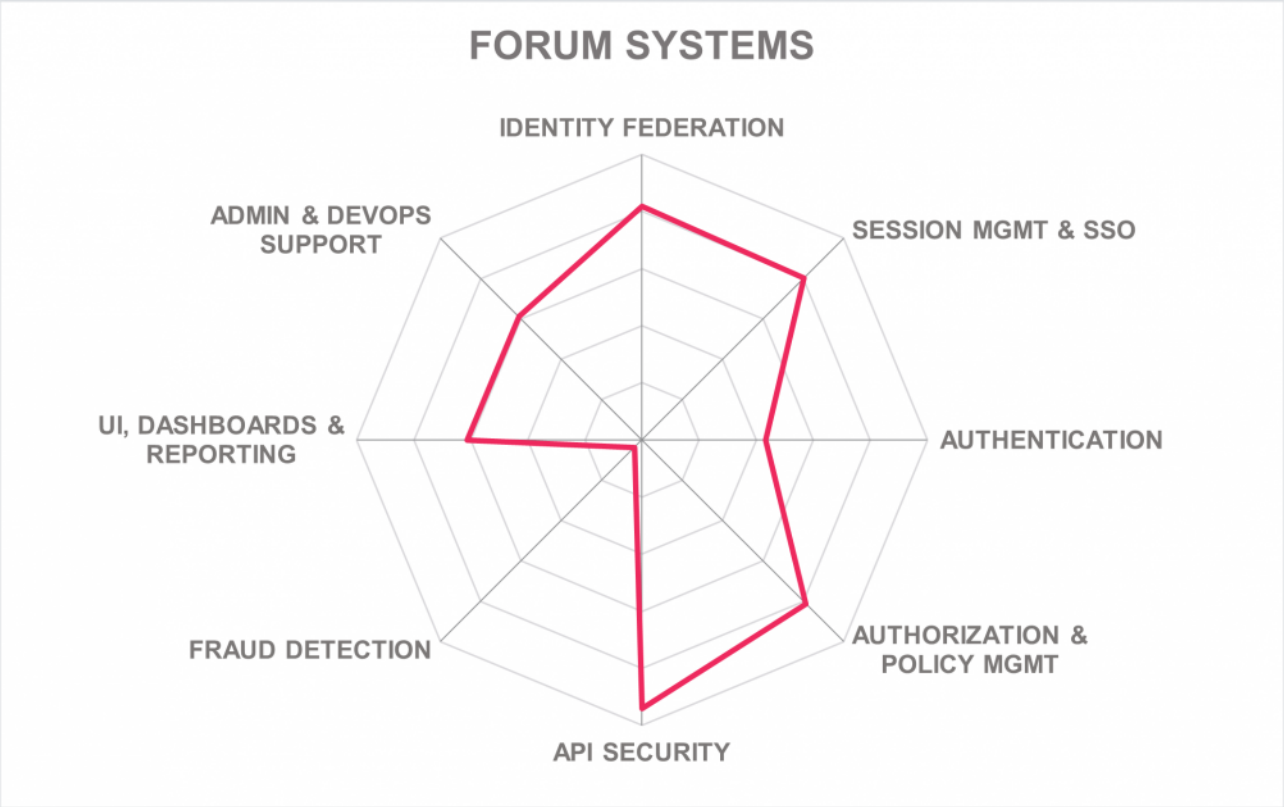
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●○

Strengths

- Identity Federation support
- Session management & SSO
- Standard authentication options
- Authorization & policy management
- API security capabilities
- Policy Enforcement Points (PEP)
- Dynamic user-based data redaction
- Wide range of product delivery options
- US government FIPS 140-2 & NIST standards support
- Support for US and UK government mission critical use cases

Challenges

- Focuses primarily on the North American and the UK regions, with a relatively small, but strategic partner ecosystem
- Rudimentary, but function UI
- Missing fraud detection capabilities


FORUM SYSTEMS
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.10 IBM

IBM Security Verify is a well-established product in the market. IBM also has one of the largest customer bases of all vendors in this market segment, with many substantial deployments of its products. More recently, IBM has rebranded its Identity portfolio. IBM Security Verify, formally IBM Cloud Identity, is offered as its Access Management solution for this Leadership Compass. IBM Security Verify is a cloud-based SaaS solution delivering SSO, MFA, adaptive access, provisioning, governance, and analytics capabilities.

IBM Security Verify Access Management capabilities give good support for basic, popular mobile app and hardware token authenticators. Both Android and iOS biometric authenticators are given, 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. For contextual and risk-adaptive authentication, functionality is provided as part of the Adaptive Access component in the SaaS offering and Advanced Access Control (AAC) component on-premise. Good contextual support is given for user, device, network, location, and a range of available fraud factors, which can be used with IBM Security Trusteer integrations. Access policies are managed and stored centrally with a policy authoring tool provided, although policy test tools are not. The solution cannot integrate with other policy management tools, and policy test tools are not provided. All user access principles such as ABAC, RBAC, CBAC, and user-group are possible, as well as support external risk engines like QRADAR UBA, Trusteer Pinpoint, and UEM solutions. Basic role management is available, although only account reconciliation and role synchronization for select applications are supported. Role mining requires IBM Security Identity Governance and Intelligence. Good web session management is available, except for session attack detection, although session protection can be accomplished through the binding of session ID to user properties. SSO across multiple web applications is achieved through a reverse proxy, and secure token translation for SSO across multiple applications is given. SSO support for non-web applications IT systems such as Desktop apps or thick clients requires IBM Security Access Manager for Enterprise Single Sign-On (ESSO) component addon. Good identity federation capabilities are given that supports SAML, OAuth 2, OIDC, WS-Federation, JWT, and SCIM federation related standards. Support for reporting is accessed through the SaaS native UI and QRadar on-premises. Although IGA or AG related reporting capabilities, only general reporting capabilities in Verify for major compliance frameworks are available out-of-the-box are given without QRadar capabilities.

IBM Security Verify proprietary fraud detection uses fraud reduction intelligence sources and supports Online Fraud Detection (OFD). Standalone OFD capabilities are provided via the IBM Security Trusteer offering. The unauthorized account takeover detection is backed with a Trusteer integration on-premise or available natively within the SaaS offering. IBM uses a range of technologies to detect fraudulent account creation. API security includes methods of DoS rate-limiting, content filtering, but not content-based routing. Good support for API protocol-specific attacks analysis is given as well as a WAF module that can detect a range of attack signatures. Also, the product includes a Security Token Service and some limited ability to use API key mechanisms such as to block anonymous traffic or control the number of calls made to an API.

IBM Security Verify is a single platform with multiple services in a suite, which can support primarily cloud as

well as on-premises and hybrid deployment models. IBM Security Verify is delivered as a SaaS solution, virtual or hardware appliance, or a managed service by 3rd Party service providers. IBM Security Verify components can run on-premises in an organization's datacenters or private cloud or in cloud-based IaaS services like Azure, AWS, and IBM Cloud. Also, PaaS is possible via Docker-based deployments. All of the IBM Security Verify functionality is available via APIs, in which SOAP, REST, and WebSocket protocols are supported. CLI support is given as well. SDKs for authentication & authorization APIs, configuration, DevOps, and mobile and web development include support for Android, iOS, Java, C/C++, Python, and JavaScript programming languages.

IBM offers a large number of system integration partners on a global scale and substantial experience in large-scale deployments. Although rebranded, IBM Security Verify steams from very mature products that have existed in the market. IBM Security Verify provides both depth and breadth in feature support. It is among the leading products in this Access Management Leadership Compass for enterprise product evaluation consideration.

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

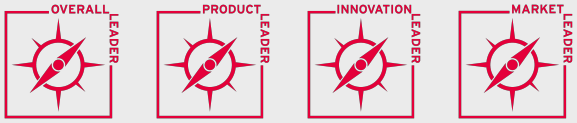
Strengths

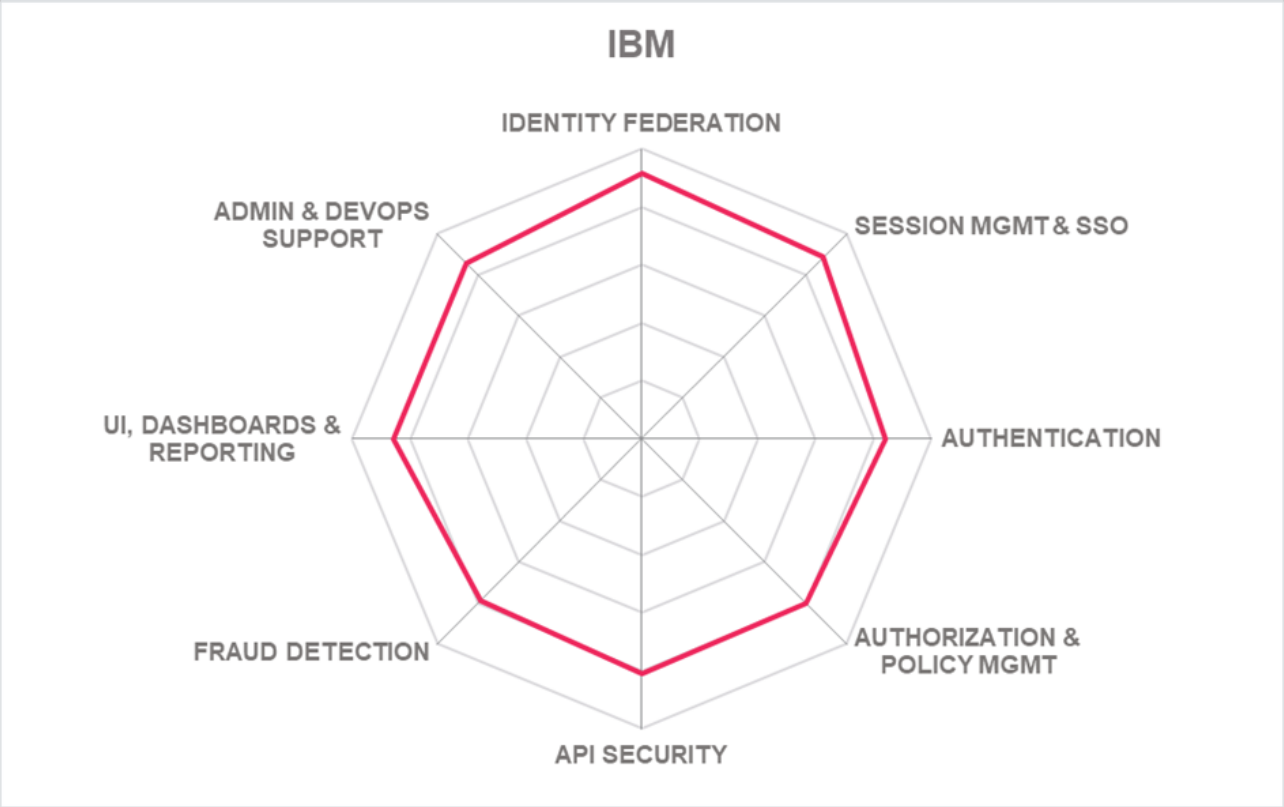
- Mature access management
- Strong and Adaptive authentication
- Session management and SSO
- Authorization and policy management
- API security
- Fraud detection
- Strong partner ecosystem globally
- Large installation base and professional services worldwide

Challenges

- Lack of focus on the mid-market segment
- Requires integration with other IBM products for some more advanced features
- Missing session attack detection capabilities
- Although good policy management is provided, delegated policy management and policy testing tools are missing.

Leader in




IBM
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.11 Ilantus Technologies

Ilantus, which started as a system integrator, has moved to provide offerings targeted at different customer types. Compact Identity is a fully integrated solution on a single platform with multiple services that can deliver IGA, Access Management, PAM, and CIAM capabilities from a single codebase that can meet more complex requirements on Access Management requirements in the market.

Of the core Access Management capabilities, Compact Identity offers good authentication support and includes good biometric authenticator options. FIDO 2 support is given with Windows Hello, Mac TouchID, Android Biometrics, iOS Biometrics, and FIDO UAF and U2F are also supported. Risk-adaptive authentication is available with some support for the device, user, and network contexts, and Compact Identity can be extended for additional location-based contexts. The available context attributes can be used with Compact Identity's access policies. Centralized policy management supports ABAC, RBAC, CBAC, and user-group access principles with basic role management support. A Risk score-based access control mechanism is also given. Password management supports password syncing across multiple identity repositories, as well as a range of password recovery options. Session management includes web browser management using cookies, which some session attack detection and protection capabilities. SSO is possible across multiple web and non-web applications through federation or credential replay techniques. Secure token translation for SSO across multiple applications is available. Identity federation for both SP and IdP use cases is offered, as well as good support for federation related standards, with the exception of UMA support.

Ilantus Compact Identity provides Online Fraud Detection (OFD) support as well as the detection of fraudulent account creation by flagging the access if it is not created via Compact Identity. Also, endpoint device profiling can be used for fraud detection. For API security, Compact Identity protects all APIs via the OAuth framework, as well as providing a means to protect against DoS attacks and using a WAF to identify other API abuses such as protocol specific attacks. Mechanisms for API keys can block anonymous traffic, revoke access token upon threat detection, or filter logs by API key identifier.

Ilantus supports on-premises, cloud, and hybrid deployment models, which can be delivered as SaaS, software deployed to a server, or as a managed service. When Compact Identity is delivered as software deployed to a server, Compact Identity supports both Linux and Windows operation systems and runs on any J2EE supported application servers. The product is available for IaaS installation on AWS and Azure platforms. A majority of features and capabilities are available via REST APIs. Other API protocols such as SOAP, WebHooks, or WebSockets are supported. CLIs arguments are available for all of the bulk import operations, and SDK support for a wide range of programming languages is available.

Ilantus started in 2000 with decades of global IAM implementation experience. Ilantus's customer base is primarily mid-market organizations in North America with growth in the APAC regions. Ilantus Compact Identity offers both Access Management and stronger IGA, Access Governance capabilities. Ilantus Compact Identity features continues to move in a positive direction with the completion of future capabilities on its roadmap.

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

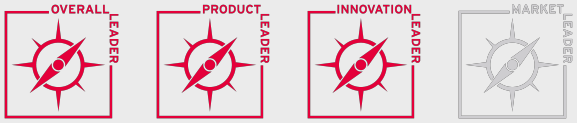
Strengths

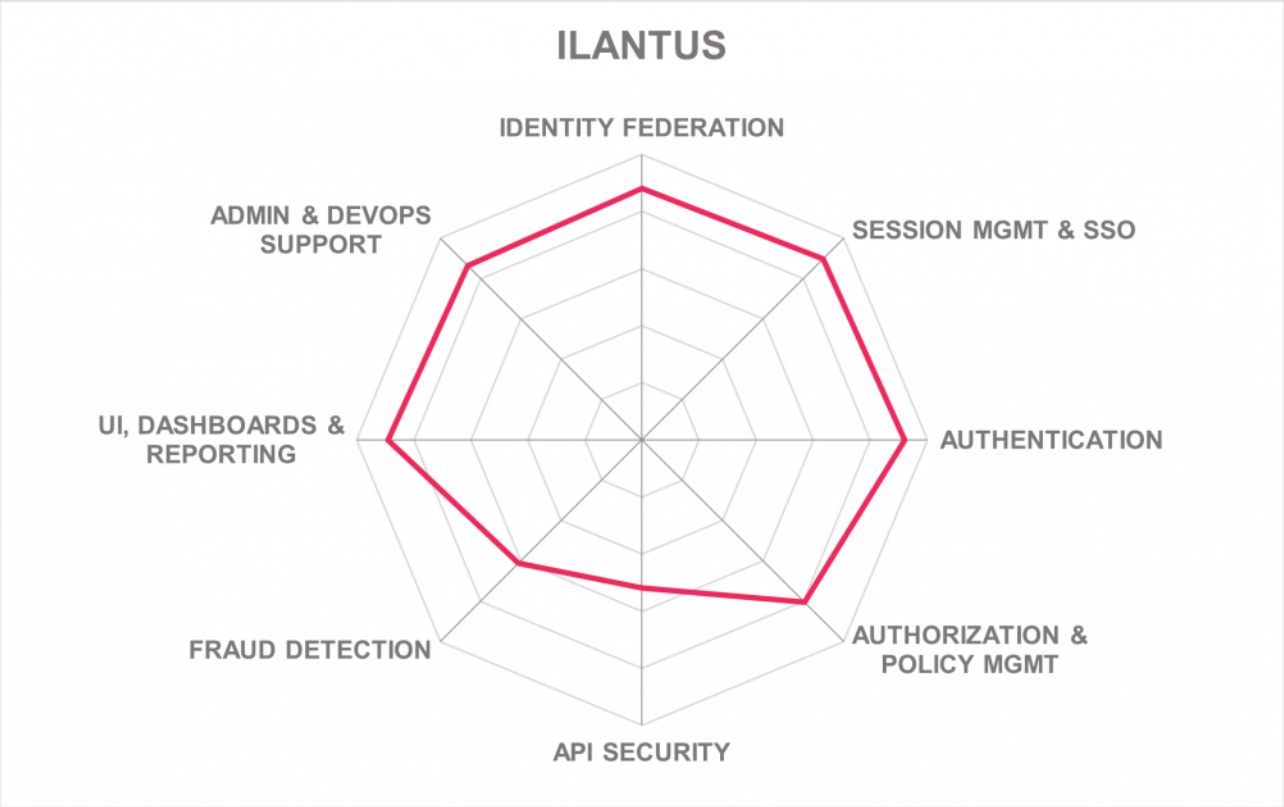
- Authorization & policy management
- Identity Federation support
- Session management & SSO
- Good authenticator options
- FIDO 2 authentication options
- Authorization & policy management
- Good reporting capabilities
- Modern UI and dashboards
- Admin & DevOps support

Challenges

- Customer presence is still primarily focused on the US and some APAC countries
- Only REST APIs are supported
- Limited API security capabilities

Leader in




ILANTUS
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.12 LoginRadius

LoginRadius is a VC-backed CIAM vendor based in Vancouver, Canada. LoginRadius has a full-featured CIAM offering that is continually adding capabilities to its platform over the last few years and is considered in this Leadership Compass for its Access Management capabilities.

Core Access Management capabilities include moderate authenticator options with biometric authenticators for Android and iOS. More advanced biometric (e.g., voice or iris) options are not given, although Duo, Yubico U2F, QR code, and support for IoT authenticators are given. Adaptive authentication is offered with support for some user, device, network, and location contexts that can be used in access policies. LoginRadius provides Risk-Based Authentication (RBA) capability as an add-on feature and allows for integrations with any 3rd party RBA provider. ABAC, RBAC, and user-group access controls can be used but missing CBAC capability. Delegated parent-child relationship policies can be configured. Also, context-based roles and attribute mapping are allowed. Good session management is available with some session attack detection, and protection is given. LoginRadius SSO is an entirely centralized session management system with no external dependencies. SSO is achieved through protocols that support browser, mobile, and server-side session management, and SSO. SSO for non-web applications is supported. Both SP and IdP federation use case is supported through SAML, OAuth 2, OIDC, and JWT federation related standards, although SCIM is not supported.

LoginRadius offers some proprietary fraud detection capabilities that can utilize fraud reduction intelligence sources, detect unauthorized account takeover. Detection of fraudulent account creation via integrations with 3rd party solutions, such as Trulio, performs identity verification. Endpoint device profiling for fraud detection is on the near-term roadmap. Of particular strength is the LoginRadius API security covering a wide range of capabilities found in most API gateways and includes rate limit, IP whitelisting, provide alerting and monitoring to identify anomalies in API transaction, protection from protocol-specific attacks, schema validation, API key management controls, as well as a security token service.

The LoginRadius cIAM Platform supports on-premises, Cloud, and hybrid deployments that is delivered software deployed to a server, containers for Kubernetes type of deployments, SaaS, or as a managed service. For software deployed to a server, both popular Linux and Windows operating systems are supported. LoginRadius uses .NET core, NodeJS, and Golang technologies for platform services that don't require specific web servers since they are self-hosted. At the infrastructure level, LoginRadius requires an HTTP reverse proxy and load balancers to be in place. The LoginRadius cIAM platform is Cloud agnostic with services supporting AWS, Azure, GCP, or Alibaba IaaS platforms. Both REST APIs and WebHooks can manage all components of LoginRadius, although CLI capabilities are not available. Its JavaScript SDK is compatible with popular client frameworks such as React, Angular, and Vue.

Established in 2012, LoginRadius customers range from small to mid-market organizations, with some presence in enterprises. The majority of LoginRadius's customer base resides in North America, followed by the EMEA and APAC regions. LoginRadius appears as a strong Challenger in Access Management with stronger features in the CIAM market. In general, LoginRadius provides a good set of Access Management

capabilities with a particular strength in API security.

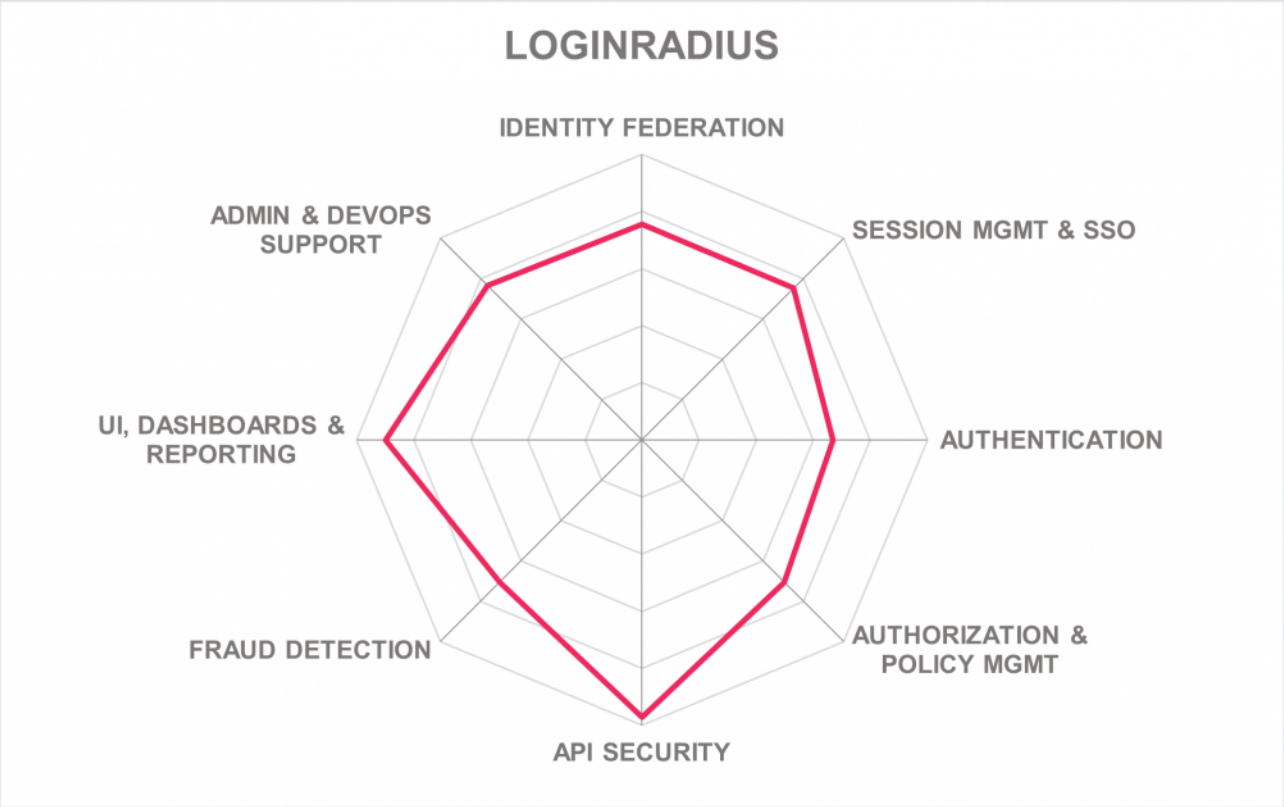
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●○

Strengths

- Identity federation support
- Session management & SSO
- Authorization & policy management
- API security
- FIDO 2 support
- Fraud detection
- Reporting
- Admin & DevOps support

Challenges

- RBA is an add-on feature, although support for 3rd party RBA providers is supported
- B2E may not be possible since its CIAM almost exclusively, although B2B use cases are possible


LOGINRADIUS
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.13 Micro Focus

Micro Focus NetIQ Access Manager is a mature and widely deployed product on the market and was the first vendor in the market to integrate Identity Federation capabilities with Web Access Management. They provide a fully integrated solution built on a consistent and modern architecture with improvements through the acquisition of Vertica through HPE and, more recently, Interset to provide AI/ML capabilities into its security product line.

Core Access Management capabilities include good authentication method support with biometrics options for Android, iOS, and voice recognition. FIDO U2F, FIDO UAF and FIDO2 are supported. The Access Management platform supports major open standards and is an open platform to build integrations to external and third-party authentication options. Risk-adaptive authentication is given with support for network, device, user, or location contexts, in which context attributes can be utilized with access policies. Access policies are managed and stored centrally, and integration with external policy management tools through API integrations are also possible. It provides a flexible policy definition UI, and extension capabilities can support a combination of ABAC, RBAC, CBAC, and user-group factors that can be used for access policies. SSO is achieved through a reverse proxy. Secure token translation for SSO across multiple applications for a wide range of supported protocols such as SAML, OAuth, Kerberos, and WS-Trust. Good session attack detection, if provided and protection from replay attacks, session renewal prevention, and device fingerprinting, is given. Good identity federation support is given for SP, IdP, as well as brokering capabilities. Also, good coverage of federation related protocols is supported. Micro Focus provides extensive out-of-the-box reporting that also support a wide range major compliance framework.

Fraud detection capabilities include coverage of financial fraud and compromised accounts. Additional capabilities are supported through the Micro Focus ArcSight platform. An integration with the third-party Lexis Nexis solution is also possible. Integrations with fraud detection and prevention systems are built-in through direct integration with Micro Focus' Interset solution. The integration includes provisions to gather and curate the data for the detection of fraud. Micro Focus NetIQ Access Manager offers both built-in API protection mechanisms as well as offering an API Security Gateway that includes token translation, encryption, traffic management, and rate-limiting. The API firewall type features are part of the API Gateway capability. Also, both JSON and XML schema validations are supported. API key mechanisms include API Key storage and workflow out-of-the-box.

Micro Focus NetIQ Access Manager can support on-premises and cloud deployment use cases. The hybrid deployment model has some components that can be deployed on-premise and in a cloud service. The NetIQ Access Manager consists of containerized components with feature parity between the SaaS with full multi-tenancy and on-premises offering. Kubernetes cluster support is currently on the near-term roadmap. Access Management is also available via a managed service provided by Micro Focus partners. All of the major product functionalities are exposed via REST interfaces with documentation, scripts, and examples for DevOps support. SOAP APIs are available for WS-Trust, STS, Webservice, and Windows/Azure integrations. APIs for administrative functions are currently on the roadmap. Access to product functionality via CLI is not supported. Available SDKs cover Android, iOS, Java, and JavaScript programming languages.

Also, a rapid connector builder tool is available to both customers and partners for creating custom application connectors.

Micro Focus was established in 1976 with its products widely deployed, with many large-scale implementations at customer sites. Customers are evenly spread across medium to large enterprise organizations, focusing on North America and EMEA, with a smaller presence in the APAC region. Still, they have an extensive partner ecosystem on a global scale. Overall, Micro Focus Access Manager is one of the leading products in the Access Management market segment. They remain in the leadership categories for both product and market segments, as well as the leadership category for innovation. Micro Focus NetIQ Access Management is recommended for consideration for mid to enterprise organizations.

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

MICRO FOCUS®

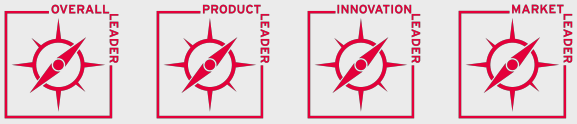
Strengths

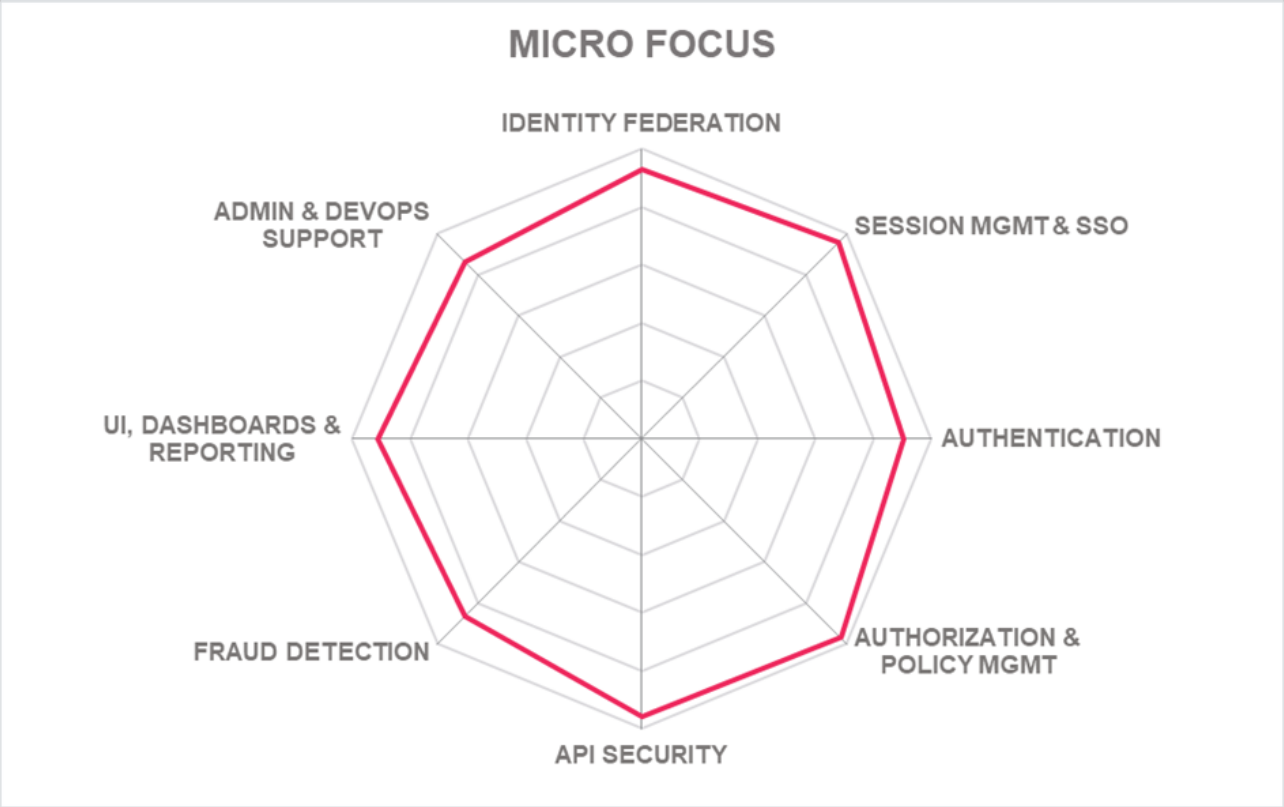
- Identity federation
- Session management & SSO
- Authentication support
- Authorization and policy management
- API security
- Fraud detection
- UI, Dashboards & Reporting
- Rapid connector builder tool for app on-boarding

Challenges

- Enterprise-level product solution may exceed small-to-medium company requirements
- APIs for administrative functions are currently not available, although on the roadmap
- Advance fraud detection may require additional ArcSight or third-party integrations through direct integration with Micro Focus' Interset solution

Leader in




MICRO FOCUS
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.14 Microsoft

Microsoft offers Azure Active Directory (Azure AD) as its primary IDaaS Access Management platform. Azure AD Connect helps connecting on-premises Active Directory (AD) to the cloud and provides real-time data synchronization across on-premises and cloud directories, enabling the use of a single identity across Office 365, Azure, and other SaaS applications. Azure AD Connect provisions users, groups, and other AD objects ensuring data synchronization between on-premises and cloud identity infrastructures.

Microsoft Azure Active Directory gives strong support for Access Management capabilities. Most of the authenticators evaluated are supported with a few exceptions, such as mTAN/eTAN or Google Titan hardware token. Both Android and iOS biometric authenticators are supported, although more advanced voice recognition and iris scan biometrics are not. With the exception of FIDO UAF, good FIDO U2F and FIDO 2 is capabilities are available. Access control policies are centrally stored and managed in Azure AD, in which policies are validated before they are persisted. CBAC, RBAC, and ABAC principles are supported, and Azure AD roles can be assigned to users, groups, and service principals. Basic role management is given. However, role mining is not. User browser sessions are managed through web browser cookies and session timeout mechanisms. Supervised machine learning detects a wide range of session anomalies and attacks. Session protection includes protection against token replay for Windows10 registered devices. SSO is available for application supporting standard protocols like SAML 2, OAuth 2, OIDC, and WS-Federation either through a reverse proxy or web server agents. Full SP & IdP federation functionality is given with support for a wide range of federation related standards. Good administration UI, dashboards, and reporting are given except limited reports for major compliance frameworks OOB.

One of Microsoft's Azure Active Directory's most significant capabilities evaluated in this report is its fraud detection. Online fraud detection (OFD) occurs across the entire IAM stack, and Azure AD Identity Protection uses machine learning and heuristic systems to detect compromise in real-time and offline risk detection. Identity Protection is provided, and Microsoft Cloud App Security can detect unusual behavior across cloud applications to identify ransomware, compromised users, or rogue applications as examples. Azure AD B2B services give transparency and fraud detection on invitation links/emails. Azure AD B2C integrates with Arkose labs to enable its customers to implement their OFD for their customer identity solutions. Other integration includes Telesign and RSA NetWitness. Azure AD uses OAuth2.0 tokens issued by Microsoft eSTS service to protect its APIs. Multiple API rate limiting options are available, as well as using Microsoft Graph as an API gateway to implement DoS protection. Both content filtering and content-based routing are given and protection against a wide range of API related attacks.

Microsoft SaaS offering includes Azure Active Directory (Azure AD), Azure AD B2C, Azure AD Domain Services, and its on-premises software products has Windows Server Active Directory (AD), Active Directory Federation Services (AD FS), and Microsoft Identity Manager (MIM). Although Azure Active Directory primarily supports its cloud service, it also allows for the integration of on-premises identities with its cloud services and applications, which includes identity management across all categories of their Azure cloud, such as SaaS, PaaS, and IaaS. In the other direction, integration with on-premises web-based applications is also given. Azure AD provides many other identity integration options for on-premises such as the

federation and synchronization of identities as well as self-service password resets. Managed services offerings include official Microsoft offerings hosted by its Microsoft Consulting Services organization, the Managed Service Expert Provider program, and Azure Lighthouse. Most of Azure Active Directory functionality is available via REST, OData, and WebHooks APIs, with PowerShell as its CLI based tool and a wide range of supported SDKs.

Microsoft Azure Active Directory is a leading offering in the market segment of Access Management with cutting edge capabilities making it a logical choice for cloud and extending on-premise Active Directory infrastructures to the Cloud.

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

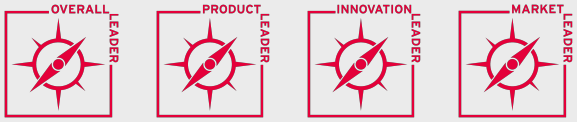
Strengths

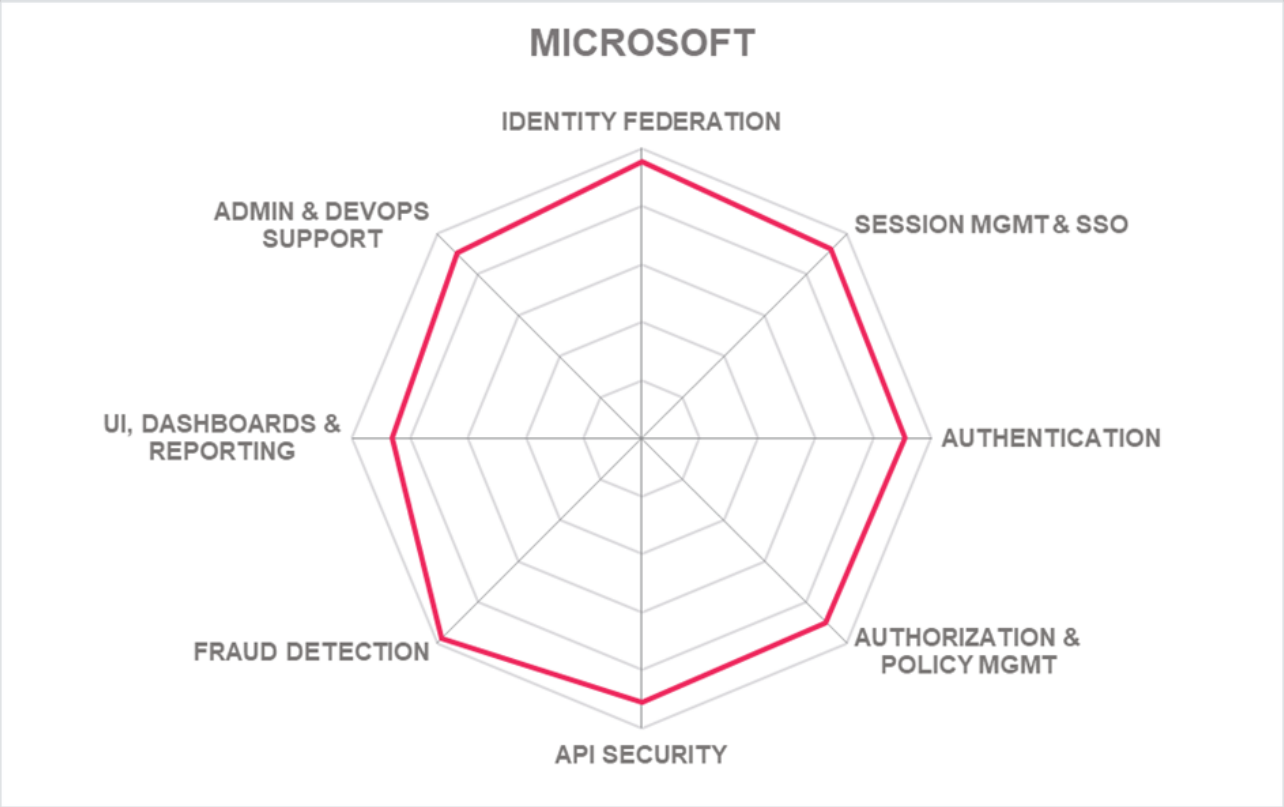
- Identity federation
- Fraud detection
- Good overall authentication support
- FIDO2 and app-based passwordless MFA options
- Good authorization and policy management
- API security
- Resilient against cyber attacks
- Capable of scaling to extremely high workloads
- Broad standards support

Challenges

- Hybrid scenarios primarily support using Microsoft technologies, however Microsoft products can also run on iOS, MacOS and Android providing customers selection and choice
- Efficient administration often requires relatively complex Microsoft PowerShell scripting, while most other features are available via the web UI and APIs
- Limited reports for major compliance frameworks OOB

Leader in




MICROSOFT
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.15 NEVIS Security AG

NEVIS Security provides Identity and Access Management (IAM) security solutions protecting 80% of Switzerland's e-banking transactions. Nevis has over 20 years of IAM experience leveraged from AdNovum Informatik, offering end-to-end Customer IAM. NEVIS Identity Suite is given as its Access Management solution for consideration in this Leadership Compass.

NEVIS Security Access Management core capabilities include moderate support for authentication methods with Android and iOS biometric with FIDO UAF fingerprint, Face recognition and PIN. FIDO U2F is not supported, and FIDO 2 is on the near-term roadmap. Adaptive authentication supports some user, network, device, and location contexts that can be used in access policies. Centralized access policies are configurable in nevisAdmin 4, with more sophisticated policies require programming, but can be stored in a central git repository managed by nevisAdmin 4. Access policies support ABAC, RBAC, CBAC, and user-group principles. Roles and attributes from the nevisIDM user repository can be used as decision parameters to authenticate a user with nevisAuth or to authorize a user with nevisProxy at runtime. Sessions are managed using browser cookies, although the customer can further configure a custom based Session Management Filter. Session brute force attacks can be detected, although session protection such as session ID lifecycle monitoring or binding the session ID to a user's property is not available. SSO is achieved through a nevisProxy reverse proxy that supports SSO across multiple web applications. SSO for non-web applications is provided through Kerberos. Supported federation related standard include SAML 2, OAuth 2, OIDC, WS-Federation, and JWT. SCIM support is not given. Identity Federation is supported primarily through OIDC, and SAML 2 for both SP and IdP use cases.

NEVIS Security can support online fraud detection using the nevisDetect component to implements continuous, risk-based user authentication through the correlation of the output of multiple anomaly detection technologies. NEVIS Security fully embeds third-party fraud detection tools from Behaviosec and Arxan Threat Analytics, which are integrated into the NEVIS offering. NEVIS API security allows for the authorization of APIs supports OAuth2 and SAML2 as well as integrations with 3rd party API gateways through APIs like Token Introspection endpoints. API responses can be filtered based on input queries, and WS-Trust Security Token Service is part of the product.

The NEVIS Identity suite supports primarily on-premises with some cloud and hybrid deployments and can be delivered as a virtual appliance, container-based deployed on Kubernetes, or software deployed to a server. Supported operating systems are limited to RHEL and SUSE Linux, although a hardened CentOS-based Linux distribution by NEVIS is available on the nevisAppliance. A subset of the NEVIS Identity suite functionality is currently offered as a SaaS service, which includes WAM and passwordless authentication via mobile push authentication as a second factor. An IDaaS offering is planned on its near-term roadmap. NEVIS Identity suite is available for IaaS installation on the Microsoft Azure platform. Most of the solution's functionality is available via APIs and supports SOAP API only for nevisIDM and nevisAuth, REST APIs for nevisIDM, and JMS / AMQP for identity lifecycle events. The solution's functionality is not available via CLI. Supported SDKs include Java for nevisAuth, Groovy for nevisAdmin and nevisAuth, and Lua for nevisProxy. SDKs for Android and iOS are also available.

NEVIS Security was founded in 2020 as a spin-off of AdNovum Informatik. NEVIS Security has a strong DACH regional presence with headquarters in Zurich, Switzerland, and offices in both Germany and Hungary. Nevis Security Suite is well established and offers some interesting features. Their product provides core Access Management capabilities with strengths in Identity Federation, SSO, and session management. It has a well-defined architecture that integrates well with other services in the backend. Still, one of NEVIS Security's greatest challenges remains to be their limited reach, which is primarily focused on the Swiss market with little presence outside of the EMEA region and their relatively small partner ecosystem.

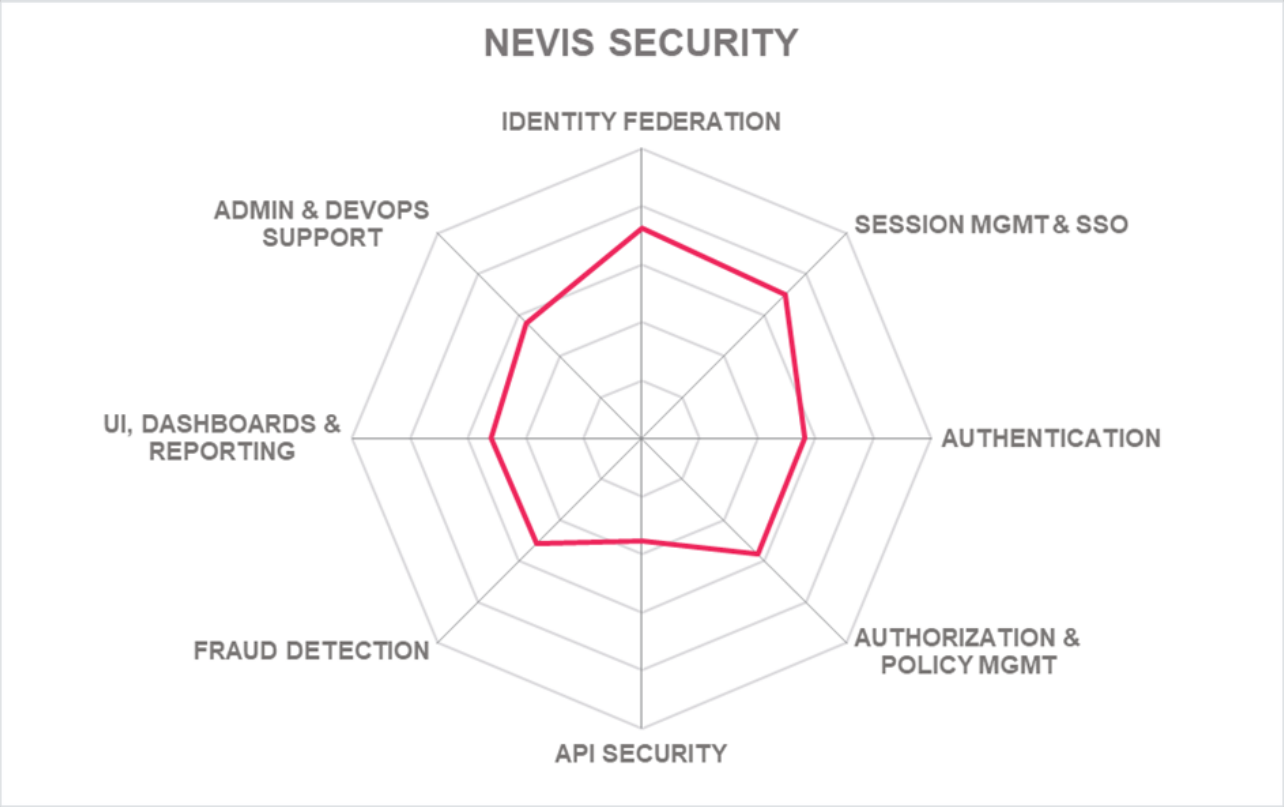
Security	●●●●●
Functionality	●●●○○
Interoperability	●●●○○
Usability	●●●●●
Deployment	●●●●○

Strengths

- Identity federation
- Session management
- Single Sign On
- Authentication
- Authorization and policy management
- Fraud detection

Challenges

- Limited market reach outside the EU, with a relatively small partner ecosystem
- Third-party tools are used for fraud detection capabilities
- Limited API security
- Limited FIDO support


NEVIS SECURITY
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.16 Okta

Based in San Francisco, California (US), Okta offers a cloud identity platform targeted at the workforce and customer identity management. Okta's workforce identity solution caters to organizations' access management requirements, including a universal directory service, SSO, MFA, identity lifecycle management, and API access management. Okta offers its Identity Cloud solution as a single platform for Access Management with its authentication, policy management, and authorization capabilities.

Okta provides good support option for authentication methods. The Okta Identity Cloud provides SSO and adaptive MFA capabilities, as well as leveraging HTTP header-based authentication. Its adaptive MFA allows organizations to implement passwordless authentication. FIDO U2F supports Yubico U2F keys and FIDO 2 support, although FIDO UAF is not supported. Also, any custom OTP token or authenticator that supports SAML is possible as well. 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 and user-group access policy management are given with delegated policy management and policy testing tools, although integration with other policy management tools is not possible. Basic role management is available, but role discovery/mining is not. Okta offers SSO or Adaptive SSO for base Access Management functionality for workforce identity use cases. More recently, Okta SSO and Adaptive SSO were expanded to allow Okta Insights (HealthInsight, UserInsight, ThreatInsights), agentless desktop SSO, integrations with VPNs, RDP, and ADFS, new Identity Providers as well as the addition of IdP discovery and routing rules. Okta provides strong support for identity federation use case and federation related standards.

Okta’s API Access Management allows for the extension of security policies to an organization’s APIs through OAuth 2. Also supported are access token introspection, refresh, revocation, and is OpenID Connect certified. Integrations with third-party API Gateways are also possible and include APIgee, MuleSoft, AWS APIGateway, Azure API Management, Kong, and SoftwareAG. Fraud detection capabilities include detecting unauthorized account takeover via various authentication techniques, but not the detection of fraudulent account creation, for example. However, Okta does allow integrations with strategic partners such as Experian for ID proofing, PerimeterX for bot detection, and ArcSight for security analytics as some examples.

Okta is a fully multi-tenant cloud SaaS service in which most of Okta’s services run within the cloud environment with identity bridge agents for on-premises. Okta is available for Amazon AWS IaaS installation. Okta’s APIs provide access to its functionality via REST and allow WebHooks to extend the Okta platform using custom code. CLI capabilities are available. SDKs for a wide range of programming languages are offered. Okta’s Advanced Server Access gives identity and access management for cloud infrastructures to provide Linux and Windows servers passwordless authentication, replaces static credentials such as SSH keys with ephemeral certificates.

Founded in 2009, Okta headquarters are split between San Francisco and San Jose in the heart of Silicon Valley. Okta’s primarily focuses on the North American market but is expanding to the EMEA and APAC

regions. Okta provides a comprehensive and mostly cloud-based solution with strong federation, SSO, authentication, and policy management for both CIAM and workforce use cases with good DevOps support.

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

okta

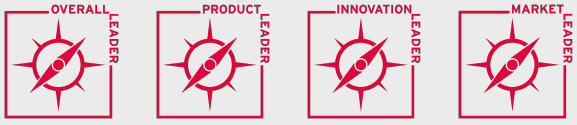
Strengths

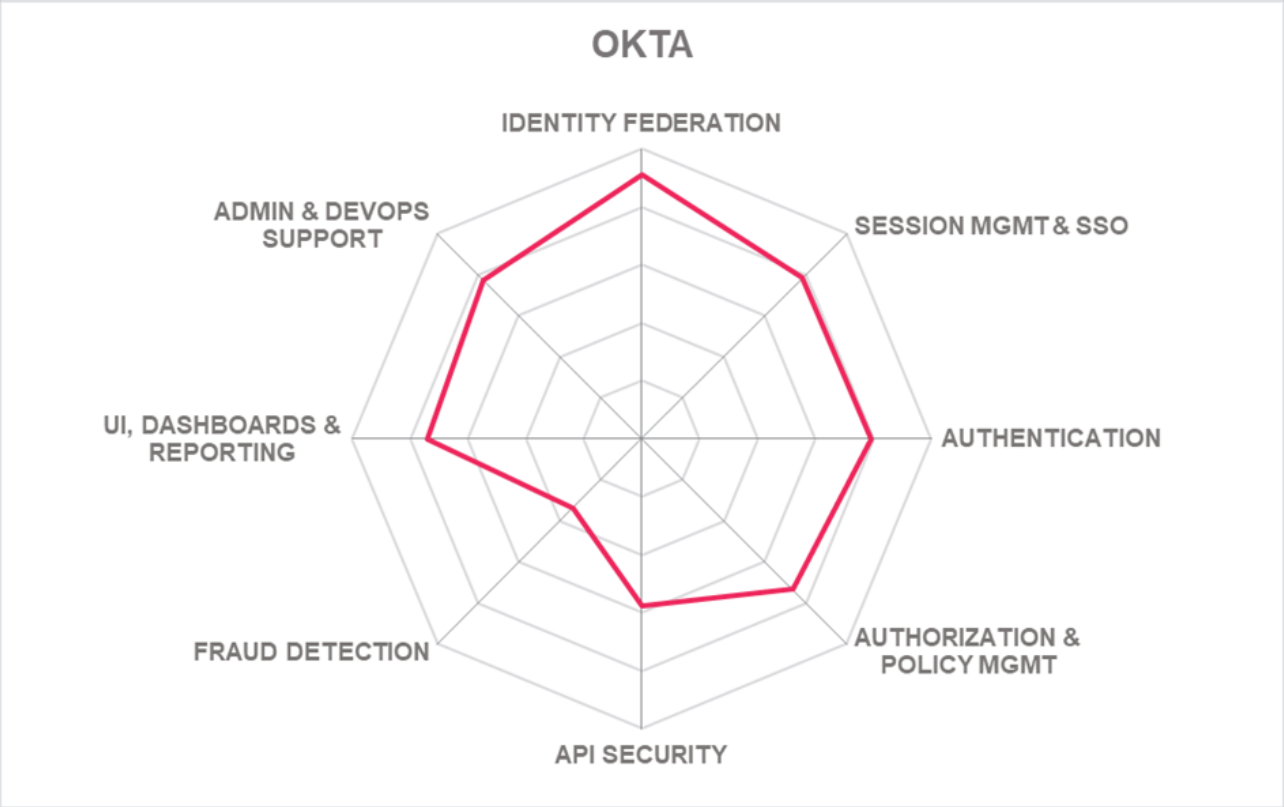
- Strong identity federation
- Session management and SSO
- Good authentication options
- FIDO U2F and FIDO 2 support
- Risk-adaptive authentication
- Authorization & policy management
- Good admin and DevOps support
- API Security

Challenges

- Primarily focused in the North American market with recent presence in EMEA & APAC
- Limited fraud detection abilities
- Deep integration with legacy on-prem systems is still a challenge
- Lacks risk-based analytics and dashboarding capabilities, but has integration to SIEM tools

Leader in




OKTA
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.17 OneLogin

OneLogin was founded in 2009 and is headquartered in the San Francisco Bay Area, and were one of the first vendors to enter the IDaaS market. OneLogin Trusted Experience Platform is offered as its Access Management solution. OneLogin supports a large number of pre-configured cloud services that can be easily connected and provide services for access management, single sign-on, user provisioning, mobile identity, compliance, and both multi-factor and adaptive authentication.

OneLogin Trusted Experience Platform's core Access Management capabilities include strong authentication support for a wide range of hard and soft MFA authenticators, including biometric authenticators for Android, iOS, voice recognition, and iris scan. OneLogin also supports WebAuthn out-of-the-box allowing biometric sensors supporting FIDO 2/WebAuthn to be used. FIDO U2F support is given, although FIDO UAF is not. Support for both LDAP and RADIUS authentication protocols are also given. Adaptive authentication requires the add-on service OneLogin SmartFactor Authentication, which supports user, device, network, and location-based contexts that can be used within access policies. OneLogin certificate-based device trust can also be used as part of its add-on SmartFactor Authentication. All OneLogin policies reside in the OneLogin Admin console, and support ABAC, RBAC, CBAC, and both user and policy groups access policy models. Its rules engine comes with a built-in testing framework. Integrate with other policy management tools can be accomplished via its APIs. SSO for on-premises applications is achieved either through a Dockerized reverse proxy managed from the OneLogin cloud or through agents embedded within web or application servers, while for cloud or SaaS based applications standard protocols such as SAML 2.0 and OpenID Connect are used. For applications that don't support proxy or web-server agent technologies, a browser extension available for Chrome, IE, Edge, Firefox, and Safari enables password vaulting and playback of credentials for login forms. OneLogin's federation related capabilities include support for SAML 2.0, WS-Federation, WS-Trust, SCIM, and OIDC via Authorization Code Grant, PKCE, Implicit Grant, Client Credential Grant, and Resource Owner Password Grant.

Vigilance.AI is OneLogin's fraud detection service that is configurable as part of a user login policy or as a standalone API. Vigilance.AI risk scoring models and other algorithms are used to provide its anomaly detection service. Fraud detection is provided through third-party integrations by default with no additional configuration required. Third-party fraud reduction intelligence sources can be used via OOTB connections to services such as Tor Network, Project Honeypot, and AlientVault Open threat exchange. Vigilance.AI APIs can be used to blacklist known ranges of IPv4/IPv6 IPs as well as geo-block countries. Have I Been Pwned, and Enzoicare is used for compromised credential checking. OneLogin API security uses a combination of OIDC for user authentication and an ability to return customized JWT access & refresh tokens for downstream API use. Rate limiting is available for OneLogin authentication, and administration APIs and some protection from DoS attacks of its own APIs, but capabilities such as API content filtering, content-based routing, schema validation, or protection from API protocol-specific attacks are not available.

OneLogin supports primarily a cloud deployment model with a microservices architecture allowing the ability to auto-scale services independently. OneLogin Access and Directory connectors can be used to support hybrid deployment model on-prem or private cloud requirements. OneLogin Access extends the OneLogin

Trusted Experience Platform to on-premises applications as well as in public or private clouds. OneLogin Access is Dockerized as on-premises enforcement points and managed and monitored in the cloud. OneLogin, as a managed service, is possible through partner MSSP & MSPs. Most of OneLogin's functionality is available via REST APIs and WebHooks. CLI based tools are limited to generating AWS temporary session credentials or importing OneLogin state into Terraform configuration files. SDKs are available for a wide range of programming languages, with the exception of C/C++.

OneLogin has a focus on SMB organizations with growth in mid-market to enterprise presence. OneLogin customers are primarily in North America, followed by the EMEA region, with growth in APAC. OneLogin also support a good partner ecosystem. OneLogin appears as an Overall Leader in this Leadership Compass for Access Management and should consideration for cloud focused organizations in North America.

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

onelogin

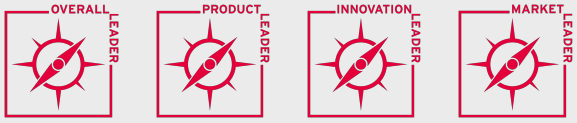
Strengths

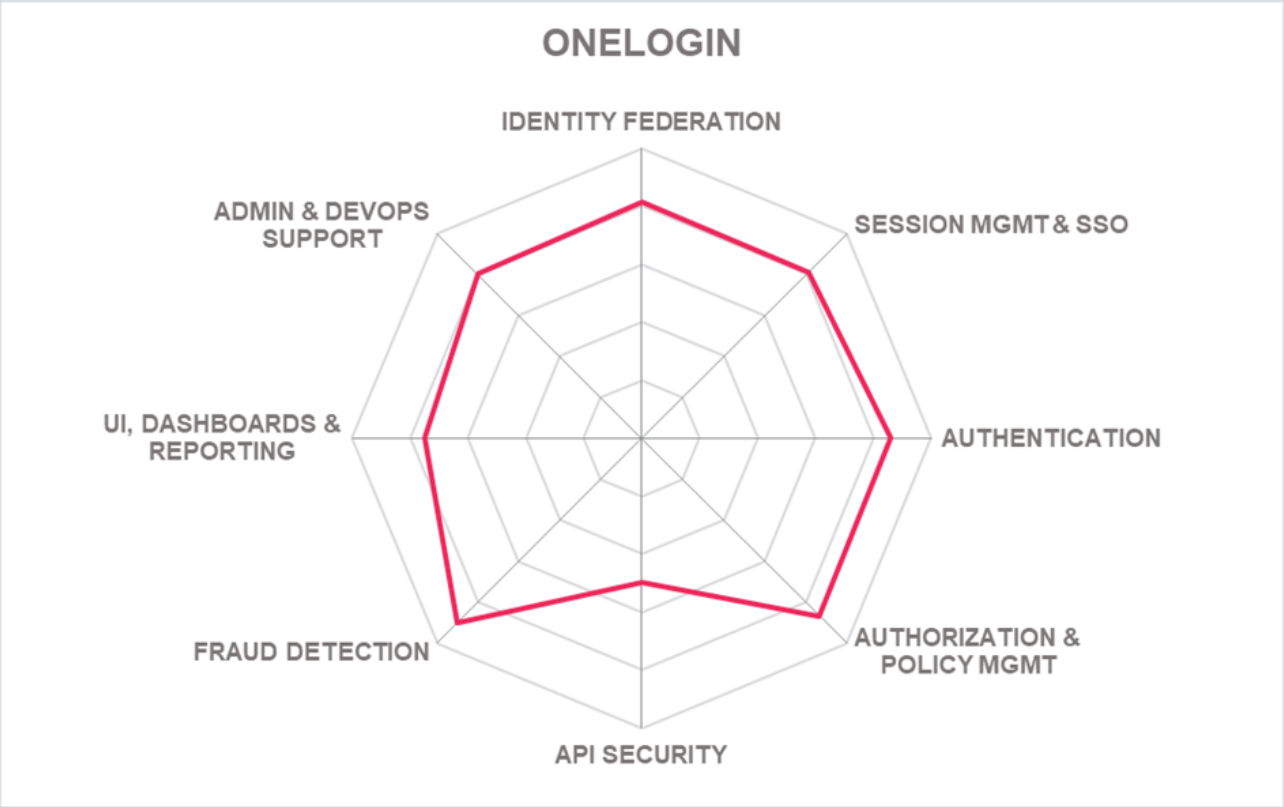
- Strong authentication support
- Authorization and policy management
- Fraud detection
- Identity federation
- Session management
- Single Sign On
- Good partner ecosystem

Challenges

- Deep integration with legacy on-prem systems can be a challenge
- Adaptive authentication requires an add-on service
- Limited API security

Leader in




ONELOGIN
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.18 Optimal IdM

Established in 2005, Optimal IdM is an SMB company headquartered in Lutz, Florida, in the U.S, with other regional offices in the U.S. and Melbourne, Australia. Optimal IDM offers OptimalCloud as its Access Management service providing Single Sign-On, MFA, Federation capabilities for Federation IAM, CIAM, and IDaaS use cases. OptimalCloud also provides APIs for WAM solutions.

Optimal IdM OptimalCloud gives moderate support for authentication methods with support for Android and iOS biometric authenticators for core Access Management capabilities. FIDO support only includes FIDO U2F for compliant authenticators. 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, and user-group access principles. The OptimalCloud is built on the Optimal IdM Virtual Directory (VIS), allowing the integration of information about users from different sources that can be combined and be used in authorization policies. Base role management is given, although role mining/discovery capabilities are not. SSO can be accomplished using a reverse proxy for non-federated web applications, although SSO for non-web applications or IT systems (Desktop apps, thick clients, etc.) are not supported. User browser sessions are managed via browser cookies, and session timeout capabilities are limited, although session attack detection and protection capabilities are given. The OptimalCloud supports most Identity federation use cases using federation-related standards such as SAML 2, OpenID Connect, OAuth2, WS-Trust, JWT, and SCIM. User-related information, including additional data, can be propagated in SAML, JWT, or HTTP headers.

The OptimalCloud API security provides Authentication and Authorization APIs for API Gateways, and all communication is over TLS secured protocols. The solution support API rate limiting, a means of DoS protection, schema validation, and protocol-specific analysis for an attack such as XSS, SQL injection, and shell injections is given. Support for content filtering, content-based routing, or API key mechanisms to block anonymous, identify API usage patterns, or filter logs by API key, as examples, is not provided. Out-of-the-box fraud detection capabilities are somewhat limited. Fraudulent email and domain checks are conducted during a user's self-service registration process as well as other IP network validations. Optimal IdM does have additional fraud detection capabilities planned on its short-term roadmap.

Optimal IdM OptimalCloud supported on-premises, cloud, and hybrid deployment models and delivered as SaaS, software deployed to a server, or managed service. Optimal IdM OptimalCloud is a dedicated multi-tenant cloud offering built on .NET and hosted on Windows servers. Its SaaS solution supports hosting on AWS and Azure platforms. Optimal IdM also offers an on-premise Federation product called Optimal Federation & Identity Services (OFIS) that allows access to applications in the cloud and/or on-premise. Almost all of the OptimalCloud functionality is available via SOAP and REST APIs. 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 is an SMB company with customers in enterprise-level organizations that are primarily focused in North America with a presence in the EMEA and APAC regions with a smaller partner ecosystem in its respective locations. Although Optimal IdM appears as a Challenger in this Leadership Compass, it does show some core strength in Access Management capabilities, particularly with identity federation support.

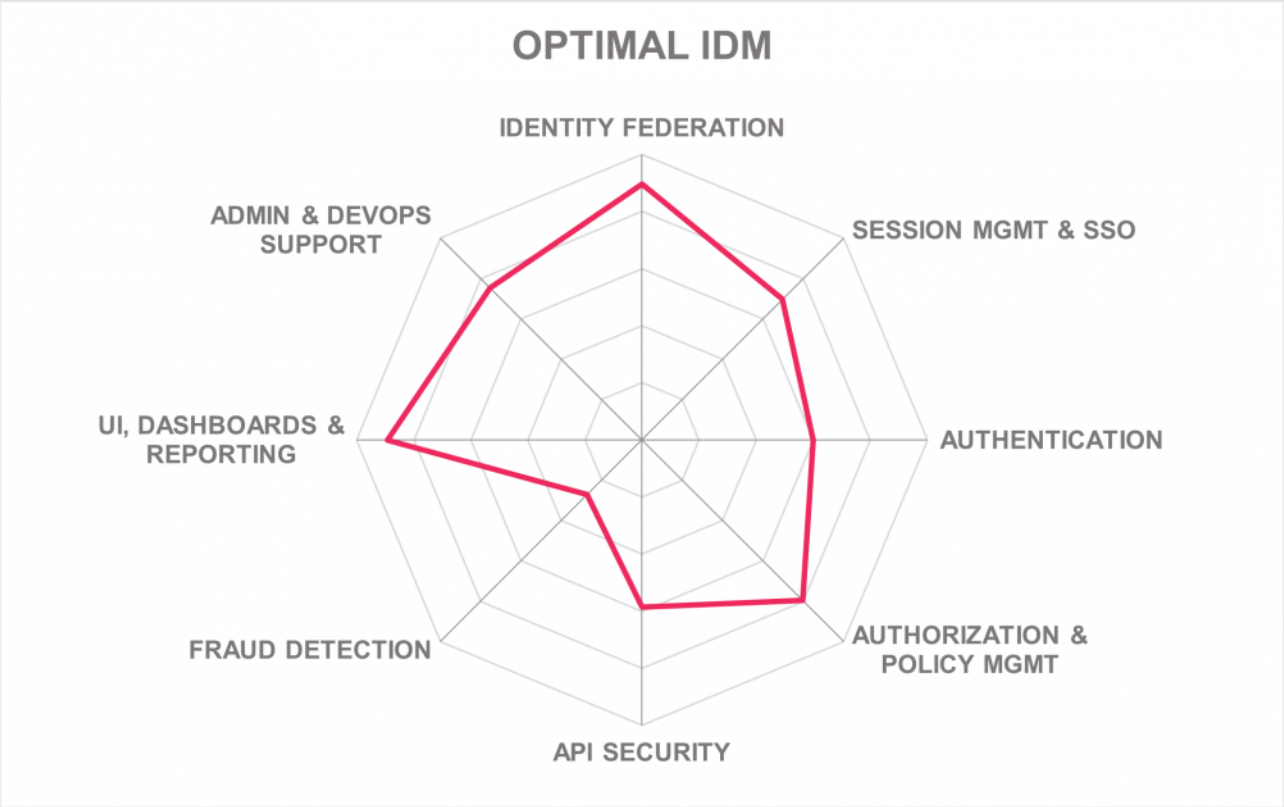
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●●
Deployment	●●●●○

Strengths

- Identity federation
- Authorization and policy management
- Session management
- Single Sign On
- Some API security capabilities
- Admin and DevOps support

Challenges

- Primarily focused in North America with a growing presence the EMEA and APAC regions
- A small but well-selected partner ecosystem
- Limited fraud detection capabilities, although more capabilities are on the road map


OPTIMAL IDM
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.19 Oracle

Based in Texas, Oracle, the leading provider of Cloud infrastructure, database management and enterprise resource planning software, and since 2016, Oracle Identity Cloud Services (IDCS) as its IDaaS service that can deliver necessary identity administration and access management capabilities from the cloud. Oracle Identity Cloud Service (IDCS) is intended to meet organizations' needs in a range of typical use-case scenarios. It is offered as its Access Management solution for this Leadership Compass.

Oracle Identity Cloud Service Access Management capabilities offer moderate authentication support, but good FIDO support for UAF, U2F, and FIDO 2, as well as its own Oracle Mobile Authenticator. Good support risk-adaptive authentication features can analyze user, network, location, and some device health state contexts that can be used in access policies. IDCS provides an API for policy authoring supporting ABAC, RBAC, and CBAC for managing user access. IDCS supports coarse-grained group-based authorization for SaaS applications and fine-grained resource-based authorization for web applications and programmatic API flows. Basic role management of application while provisioning a user is provided, and role mining capabilities are given out-of-the-box with an OIG integration. IDCS session management supports session configurations such as timeouts, user logouts, or admin session revocations and provides an admin session API for session search and filters. Good session detection and protection capabilities are also given. IDCS SSO can be accomplished using its reverse proxy, web-server agents, and support header-based authentication for SSO across multiple web applications. IDCS has a good application catalog of applications that supports SAML, which are pre-integrated and configured for IDCS as a service provider. IDCS can also act as an IDP for various applications. Supported federation related standards include SAML, OAuth, OIDC, WS-Federation, JWT, and SCIM. Excellent support for major compliance frameworks is available out-of-the-box reports are given.

For fraud detection, IDCS can integrate with Oracle Cloud Services like Security and Monitoring Cloud Service and Oracle Cloud Access Security Broker (CASB), and Cloud Guard. IDCS also allows customers to export data into a third-party solution like Splunk. IDCS can integrate with fraud reduction intelligence sources that support SCIM integration for example, as well as other standards. IDCS can detect unauthorized account takeovers and fraudulent account creation through integrations with Oracle Cloud Guard, CASB, and third-party tools. IDCS uses an OAuth/OIDC service, authorization policy engine, and an Application Gateway that can function as a policy enforcement point to protect APIs and web resources. IDCS supports API rate limiting, a means of DoS protection, content filtering, and content-based routing, schema validations, detection of protocol-specific attacks, as well as providing an include a Security Token Service. Good API key management is also given.

Oracle Identity Cloud Service provides a fully integrated standalone SaaS solution that offers all the core identity and access management capabilities through a multi-tenant cloud platform. IDCS runs on the Oracle Cloud Infrastructure (OCI), and installations on other IaaS platforms are not possible. For on-premises deployments, an Oracle cloud at customer sites is delivered as a hardware appliance. IDCS uses and depends on Oracle database technologies. IDCS only supports REST API for all features with support for standard SCIM core schemas as well as Oracle schema extensions. Access to IDCS functionality via CLI

options are not given. OAuth SDKs support the Java, PHP, Python, .Net, Ruby, iOS, and Android programming languages. IDCS also has a set of APIs to support integrations with UEM tools.

Oracle Identity Cloud Service provides a solution that will be very attractive to existing Oracle customers. It is tightly integrated with other Oracle business products as well as Oracle security products. Although the suite of services' complexity should not be underestimated, Oracle Identity Cloud Service provides a strong offering in the Access Management market. It should be considered for a product evaluation shortlist.

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

ORACLE®

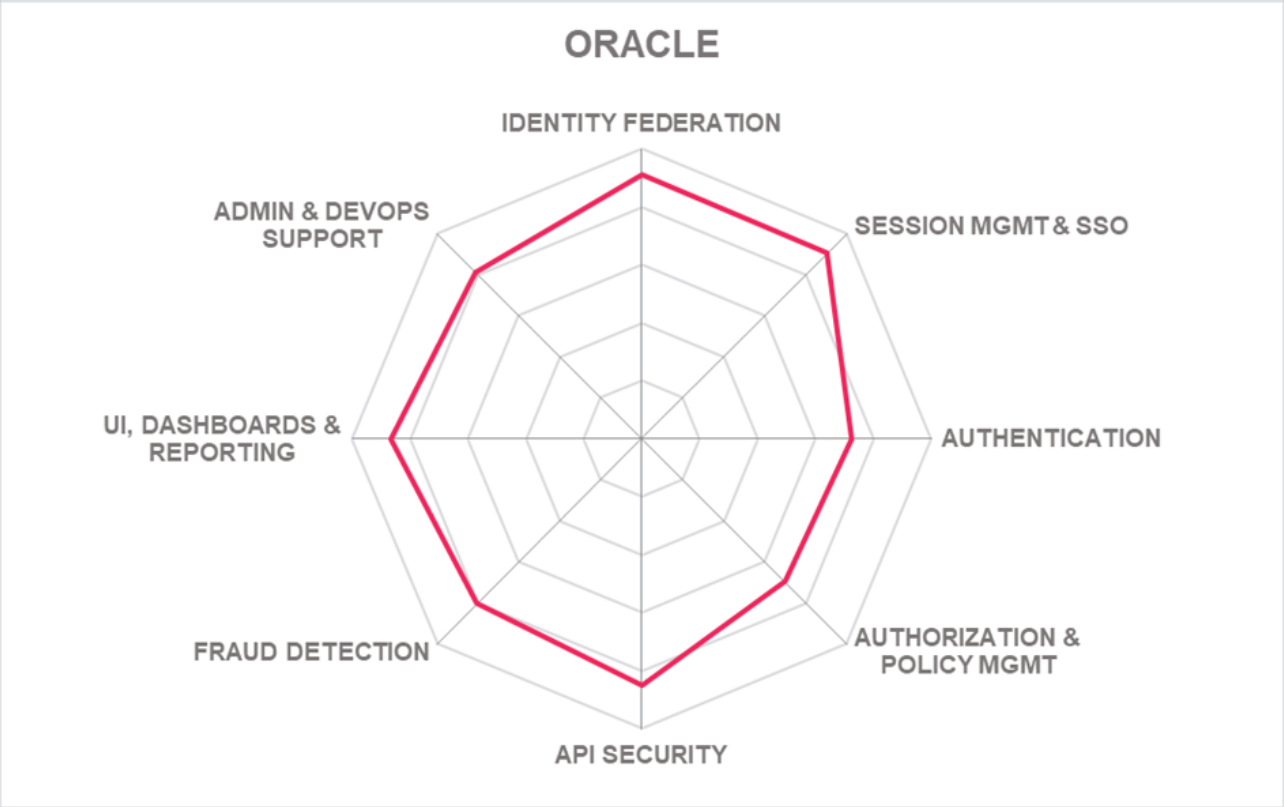
Strengths

- Identity federation
- Session management and SSO
- API security
- Fraud detection
- UI, dashboards and reporting
- Admin and DevOps support
- Adaptive authentication
- Full FIDO support

Challenges

- Only REST APIs are support
- Limited biometric authenticators offered

Leader in


ORACLE
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.20 Ping Identity

Ping Identity was founded in 2002 and based in Denver, Colorado (US). Ping Identity started with a primary focus in the area of Identity Federation. Since then, Ping Identity has steadily grown to add innovative features to fill out other areas of their Identity Platform, which is made up of several software products and cloud services. Ping Intelligent Identity Platform offers a complete portfolio of access management functions for B2B, B2E, and B2C scenarios.

Ping Identity Platform Access Management capabilities offer strong authentication methods that include hard and soft authenticators, good biometrics authenticator support and FIDO U2F, and FIDO 2 certified authenticators. However, FIDO UAF capabilities are not offered. Contextual and risk-adaptive authentication are supported as part of its base authentication service. Access policies are capable of utilizing user, network, device, and location contextual information as well as any metadata available from a request or response, made available by the user agent, or the protected application. The solution supports managing access of users based on ABAC, RBAC, CBAC, and user-group principles. Enforcement points request policy decisions based on a subset of the XACML-JSON standard. Basic user and admin role management are supported across all Ping solutions, although role mining/discovery capabilities are not supported. Session management features to support the management of web sessions through session HTTP header and browser cookies and a variety of session timeout configuration options. Detection of common session attacks and protection support is given, which includes session ID guessing, brute force attacks, and session ID anomalies that can all be detected using the machine learning model. SSO is supported across multiple web applications using reverse proxy and web-server agents. Non-web applications can be backed by PingAccess intergeneration via HTTP Headers to the application, or PingAccess use of PingFederate Secure Token Server functions to create tokens and embed them in the request to the backend server as some examples. Identity federation is well supported and gives good support for the most used federation related standards such as SAML, OAuth, OIDC, JWT, and SCIM. Also, strong support for reports for major compliance frameworks is available out-of-the-box.

Ping's proprietary fraud detection includes UEBA/OFD behavior pattern capabilities based on access to devices, browsers, operating systems, and geo-locations. Detection of unauthorized account takeover or fraudulent account creation requires the PingIntelligence for APIs solution. On the roadmap, PingOne Risk Management service will provide attack specific detection such as account takeover, credential stuffing, human/bot detection, session risk analysis as examples. API security support includes API rate limiting and other DoS capabilities. Also, given is support for content filtering, content-based routing, and other "API firewall" like features. PingIntelligence for APIs leverages its AI capability to learn traffic behaviors to detect and block abuse of a customer's APIs automatically. PingIntelligence for APIs can use API keys to detect anomalies based on client behavior and usage patterns.

The Ping Identity Platform supports on-premises, cloud, and hybrid deployment models. It can be delivered as SaaS hosted on AWS, software deployed to a server, containerized Docker images and Kubernetes orchestrations, or a managed service. PingCloud provides authentication, authorization, and user directory capabilities as a managed service and allows Ping Identity MSP partners to offer all Ping capabilities as a

managed service as well. For software deployed to a server delivery option, both Linux and Windows operating systems are supported, as well as a wide range of application servers and JDBC compliant database databases. However, a Java runtime environment is required. All Ping Identity Platform functionality is available via APIs and supports SOAP, REST, WebHooks, and WebSockets. All platform functionality is also available via CLIs. SDKs are provided for a wide range of popular programming languages.

Ping Identity has a strong presence in North America and good representation in EMEA and APAC regions with a suitable partner ecosystem. They are established as a leader overall as well as leaders in the product, market, and innovation ratings. As such, the Ping Identity Platform should be included in any shortlist for Access Management platform solutions to consider.

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

Ping Identity

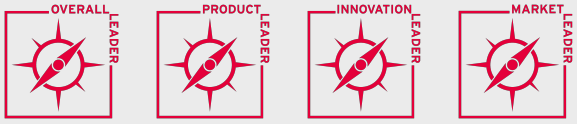
Strengths

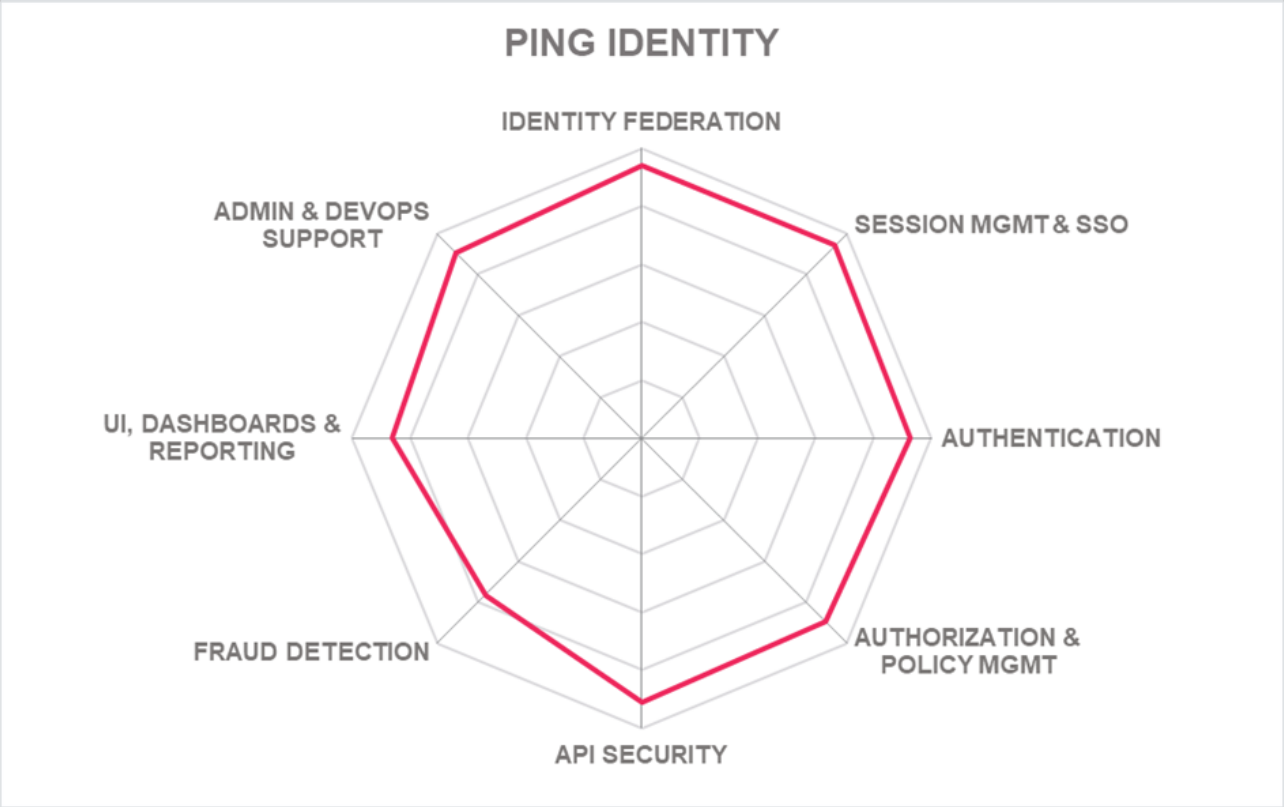
- Identity federation
- Single Sign On
- Session management
- Strong authentication support
- Authorization and policy management
- API security
- UI, dashboards and reporting
- Admin and DevOps support

Challenges

- Some Access Management use cases require on-prem PingFederate component
- PingFederate requires a Java runtime and JDBC compliant database for on-premise, although single-tenant SaaS is also available
- Some fraud detection capabilities require an integration with PingIntelligence for APIs solution

Leader in




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

5.21 RSA Security

RSA, formerly part of Dell Technologies, has been recently acquired by the Symphony Technology Group and is now an independent company. RSA is a leading security solution provider. It offers RSA SecurID Suite that combines RSA SecurID Access and RSA Identity Governance and Lifecycle Management (IGL). Primarily targeted at B2B and B2E access management requirements of organizations, RSA SecurID Access offers one of the most widely deployed multi-factor authentication (MFA) solutions with risk-aware contexts and access policies for timely and convenient access to applications.

RSA core Access Management capabilities give good support for basic authentication methods and strong support for hardware authenticators and biometric authenticators, including Android and iOS face and fingerprint biometrics and iris scan. With the exception of FIDO UAF, support for USB, BLE, or NFC security keys that are FIDO U2F compliant, such as the YubiKey for RSA SecurID Access, is available. Also supported are FIDO2 security keys, wearables, Windows Hello, and Android phones. The level of contextual and risk-adaptive authentication depends on the customer's license level. A base license allows administrators to construct policies based on the user's IP Address. An enterprise license allows for additional, conditional attributes such as Authentication Type, Authentication Source, Country, Known Browser, Trusted Location, Trusted Network, and User-Agent to be used. The premium license includes all contextual attributes and adds Threat Aware Authentication for High-Risk users and Identity Confidence that adapts based on patterns of user behavior. Centralized access policy management is given with a cloud-based administrative interface to configure policies. However, policy testing tools are not available. Support for ABAC, RBAC, and CBAC or a combination of attributes, roles, groups, and context can be used within access policies as rule sets.

Web browser sessions are managed using browser cookies. Session ID anomaly attack detection and the binding of session ID to user properties for protection is given. SSO is achieved via a reverse proxy for SSO across multiple web applications. RSA SecurID Access SSO Agent is configured with a max and idle session timeout. SSO support for non-web applications IT systems is possible when using a browser-based authentication flow or when RSA SecurID Access leverages HTTP-Federation, which uses password vaulting and form POST behind the scenes, on a user's behalf. For federation support, the RSA SecurID Access Cloud Authentication Service and SSO Agent can act as both a SAML IdP and SAML SP. Support for federation related standards includes SAML 2, OIDC, WS-Federation, and JWT. SCIM is not supported. Also, good support for reporting, including major compliance frameworks, reports OOB.

The RSA SecurID Access risk engine was originally built on the RSA Fraud and Risk Intelligence Adaptive Authentication technology and Threat-Aware Authentication (High-Risk Users) API allows 3rd-party SIEM solutions to notify RSA SecurID Access about accounts with suspicious activity. RSA SecurID Access support for content filtering is available for API security, but support for content-based routing is not. Protocol-specific attacks on JSON or XML objects can be analyzed. API rate limiting is achieved through the support of API keys. DoS protection is accomplished using Azure's native WAF capabilities in combination with API key protection mechanisms.

The RSA SecurID Access Cloud Authentication Service is a multi-tenant SaaS cloud environment with RSA SecurID Access supporting on-premises or a hybrid cloud architecture deployment model. The RSA SecurID Access on-premises components are delivered as a hardware or virtual appliance that includes a SuSE-based operating system with an internal database and application server. The on-premises components can also be deployed as virtual machines hosted on AWS or Azure platforms. Also, a managed service is offered through RSA partners. Almost all of the RSA SecurID Access solution functionality is available via APIs & SDKs, including authentication, policy evaluation, and critical administrative tasks. CLIs are available to allow admins to perform bulk operations, view logs, and manage services. CLI utilities are also available for testing authentication and managing node secrets on platforms. SDKs support a wide range of programming languages and provide an OpenAPI interface definition source file containing details on the RSA SecurID Authentication API REST endpoints and JSON objects.

RSA customers include medium to enterprise organizations with a strong presence in the North American, EMEA, and APJ regions. RSA has focused on enabling these customers' migration to the cloud, supported by a click-and-shift approach from the former on-premises tools. RSA SecurID Access makes a good Access Management platform choice for organizations with either existing deployments of RSA products or requirements to onboard an intelligent authentication and access management service.

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

RSA

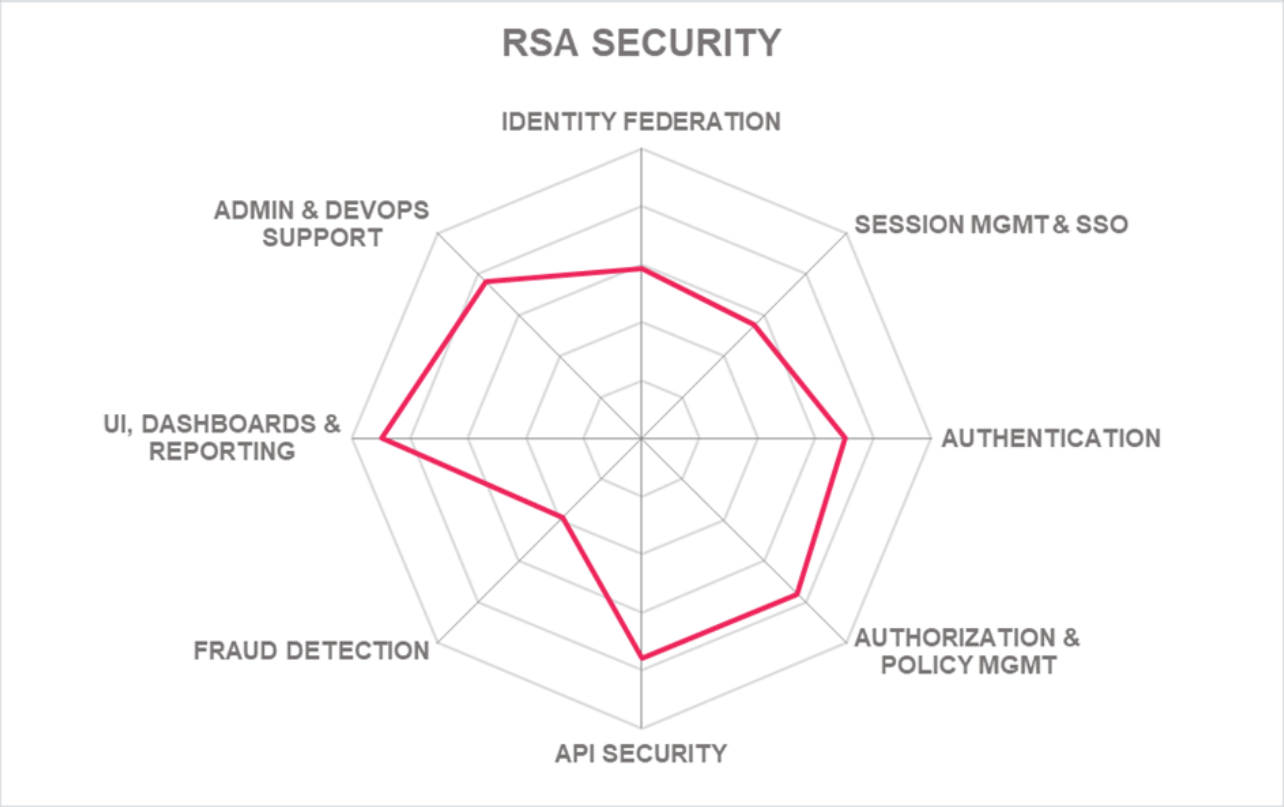
Strengths

- Hardware authenticator support
- Adaptive authentication
- Authorization and policy management
- API security
- Good UI, dashboards and reporting
- Admin and DevOps support
- Professional service and partner ecosystem

Challenges

- Moderate identity federation capabilities
- Limited session management
- Limited fraud detection
- Recent acquisition impacts are yet to be determined

Leader in


RSA SECURITY
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.22 SecureAuth

SecureAuth has been in the market since 2005 and is headquartered in Irvine, CA. The company aims to enable responses by bringing the telemetry of access management, network, vulnerability, and endpoint together with the identity context. The SecureAuth Access Management solution giving MFA, Risk-based Adaptive Authentication, SSO, Authorization and Policy Management, and User Self-Service capabilities.

SecureAuth, Access Management capabilities, include good authentication supports for basic, MFA, and hard tokens with support for Android and iOS biometric authenticator options. However, advanced voice recognition and iris scan biometrics are not supported. Interestingly, QR code authentication is also not supported. FIDO UAF and U2F authentication is not given, although support for FIDO 2 / WebAuthn authenticators includes Windows Hello, Mac OS, Android OS, YubiKey, Google Titan Key, as examples. SecureAuth's contextual and risk-adaptive authentication is part of the base product offering for Protect and Prevent subscription customers, including user, device, network, and contextual location support, which can be used within access policies to create and enable policies for specific users/groups and resources. SecureAuth includes a centralized access policy management as part of the base solution and stores all configuration information on the appliance or in a single-tenant cloud database. Policy testing tools are not given. Although SecureAuth supports ABAC, RBAC, CBAC, and user-group-based access policy principles, role-based access policies are used to determine the level of administrative rights. Also, delegated policy management capabilities are not given. SSO is accomplished through web browsers via SAML, OIDC, WS-Federation, LTPA, and customizations across multiple web applications. Sessions management is achieved via web browser cookies and .NET ViewState. Session timeouts are configurable per realm. Brute force, credential stuffing, and password spraying session attacks can be detected. SecureAuth includes SP & IdP functionality supporting SAML, OAuth, OIDC, WS-Federation, and JWT federation related standards.

SecureAuth provides some threat and fraud detection capabilities, as part of the overall solution by ingesting third party identity fraud information, as well as information from other sources, as part of its threat service without the need for customer interaction. API security includes both password and MFA throttling for its means of DoS protection. API content filtering and content-based routing are not given. The solution performs IP checks against real-time threat intelligence feeds and uses Machine Learning to continually understand user behavior and detect anomalies and protect against XSS attacks. The product also includes a Security Token Service. API key mechanisms are used to ensure that only known applications are able to connect to the SecureAuth platform.

SecureAuth supports not only on-premises, cloud, and hybrid deployment models but also air-gapped deployments as well. Its SaaS offering is fully hosted and managed by SecureAuth on AWS. SecureAuth also allows any IaaS provider to import standard OVA virtual appliances to be used. For on-premises, both virtual appliances and software deployed to server delivery options are available. When deploying software to a server, the Windows operating system is supported. The virtual software appliance offers a hardened OS. Standard integrations across Microsoft and non-Microsoft web application servers are given with any ODBC compliant DB server. Almost all of SecureAuth’s functionality is available via REST APIs only. CLI support is not given. SDKs are limited to Java, .NET, Python, Go, and JavaScript programming languages.

Some HTML5/CSS/JS coding skillsets are required for GUI customizations and branding.

SecureAuth, as a privately held company, has a large customer base in mid to enterprise organizations, predominantly in North America, with some growth in the EMEA and APAC regions. SecureAuth shows particular strength in identity federation and authentication, making it an appealing Access Management for an organization in North America, focusing on these capabilities.

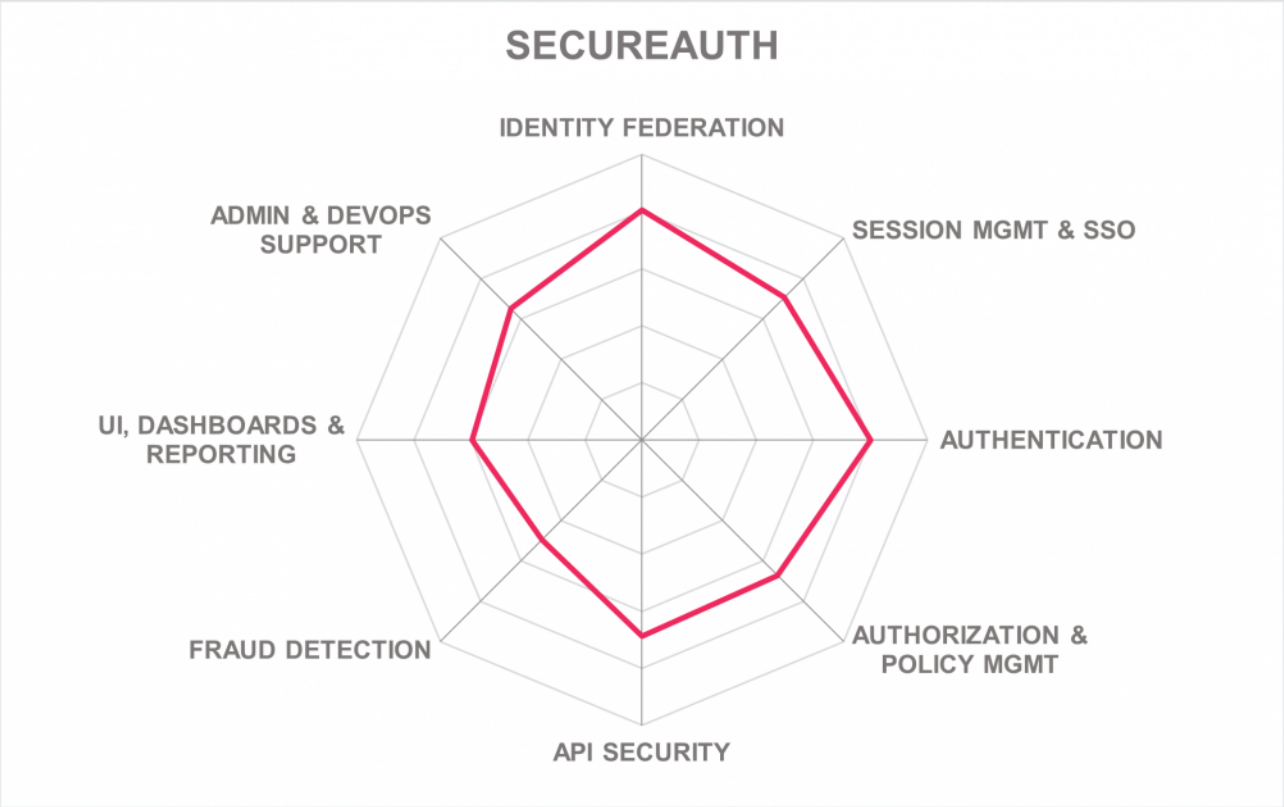
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●○○
Deployment	●●●●○

Strengths

- Identity federation
- Authentication support
- Adaptive authentication
- API security
- Single Sign-On capability
- Authorization and policy management
- Fraud and threat detection
- Good ecosystem of IAM partners

Challenges

- Heavily focused in the North American market
- Focused on Microsoft technologies
- SaaS based on AWS centers only
- Limited reporting capabilities


SECUREAUTH
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.23 Simeio Solutions

Based in Atlanta, Georgia (US), Simeio Solutions witnessed significant growth when shifting from its IAM system integration business into a full-fledged IDaaS service provider over the past years. Previously offering dedicated hosted services underpinned by other IAM vendor's products, Simeio enters mainstream IAM business with Simeio Identity Orchestrator. Simeio Access Management Service is its primary service, comprising of authentication, authorization, SSO, and identity federation for a hybrid IT environment. Also, Simeio Identity Orchestrator comes with strong IGA capabilities. For this Leadership Compass, Simeio offers the Access Management component of its Simeio Identity Orchestrator.

Simeio's gives good support to most authentication methods, including full support for FIDO UAF, U2F, and FIDO 2 for Microsoft Windows Hello, and YubiKeys. Support for Android and iOS biometric authenticators are available, although support for more advanced voice recognition or iris scan biometrics is not. Also, moderate support for hardware tokens is given, supporting only RSA SecurID, Symantec VIP, and YubiKeys. Risk-adaptive authentication supports the device, location, time-of-day, and network-range contexts. Access policies are managed and stored centrally within a directory, which can be import and export via XACML. User access management supports ABAC, RBAC, CBAC, and user-group base principles. Role management is given with role mining capabilities available. Sessions can be managed in server cache or external storage, and user web sessions can be controlled via Session HTTP Headers and browser cookies as well as the configuration of various session time out capabilities. Good detection of session attacks and protection is given. SSO can be achieved via reverse proxy and web-server agents, as well as identity federation protocols and Kerberos. Secure token translation for SSO across multiple applications is also given. Support for non-web applications and IT systems is accomplished via Kerberos and OAuth. Simeio uses an OIDC adapter that is header based for legacy applications. Simeio provides IdP and SP functionality with SP onboarding capabilities. Good support for all identity federation related protocols is given with the exception of Simple Web Token (SWT). Good reporting capabilities are available included 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 your access management solution, in which third-party fraud reduction intelligence sources detection tools such as ThreatMetrix, Akamai, and Imperva are used. In-network fraud reduction intelligence sources can also be used. Bot detection of unauthorized account takeover is available, as well as some support for fraudulent account creation detection. API security utilizes the AWS API Gateway to ensure APIs that are exposed either as the internet or customer-facing APIs are protected. DoS protection is provided through integration into a WAF linked to the API Gateway with throttling controls. Content filtering is accomplished via LAMBDA functionality in the AWS API gateway. Attack analysis, schema validation, and API key management are provided through its API gateway mechanism.

Simeio Identity Orchestrator supports cloud, on-premises, and hybrid deployment models. Its SaaS offering is fully multi-tenant, providing isolation at the network layer, not the application layer, and is hosted on AWS, Azure, and Oracle cloud platforms. Simeio also provides support options for IaaS installations, which

includes AWS, GCP, Azure, OCI, and CenturyLink. 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 for on-premises deployments. Standard deployments do require Apache Tomcat application servers and a MySQL database. On-premise deployments are optional but not required to use its Access Management component. All of the Access Management functionality is available via the UI is available via REST APIs, although some of the solution's components support SOAP APIs as well as CLI access. Only SDKs for Java and .NET are available.

Simeio supports organizations primarily in North America with a growing footprint in the EMEA and APAC regions. Simeio combines its IAM development experience and systems integration expertise to present a viable alternative to several established vendors, particularly for organizations that lack IAM knowledge and expertise internally and will require detailed guidance and support for transitioning existing on-prem Access Management to the cloud. Overall, Simeio offers good Access Management capabilities as part of the Simeio Identity Orchestrator solution and should be considered by organizations primarily in the North American and EMEA regions.

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

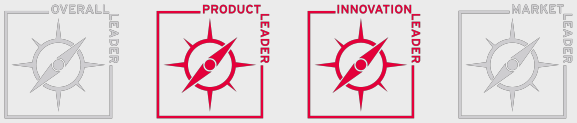
Strengths

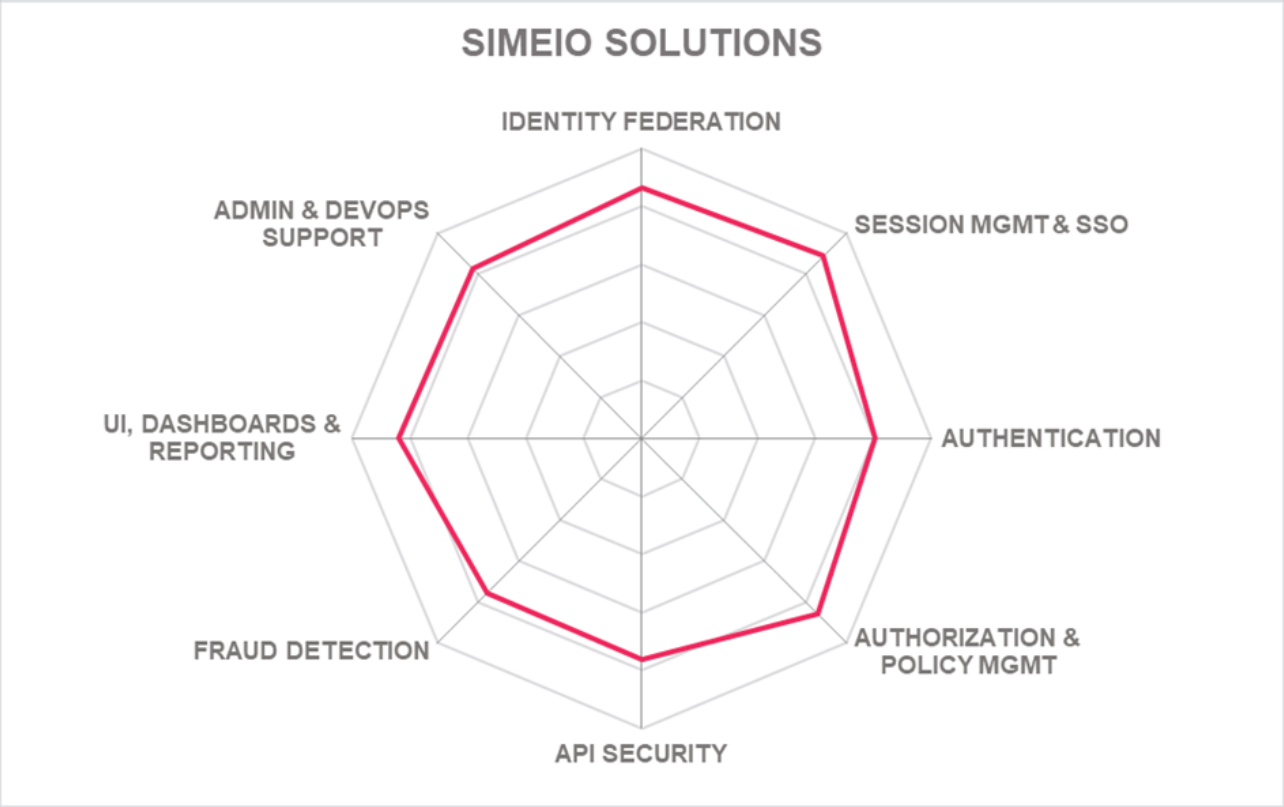
- Identity federation
- Session management and SSO
- Full FIDO support
- Good reporting support
- Admin and DevOps support
- Authorization and policy management
- Fraud detection capabilities
- API security

Challenges

- The wide-spread reputation of primarily being a global SI vendor than an IDaaS vendor
- SDK support to functionality is limited, although REST APIs are available
- Functionality partially provided through 3rd party products or services
- Good ability to execute in North America, but limited system integrator partner network on a global scale

Leader in




SIMEIO SOLUTIONS
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.24 Soffid

Based in Spain and established in 2013, Soffid IAM provides an open-source Identity and Access Management (IAM) and Single Sign-On (SSO) solution. Soffid offers a subscription service to an enterprise edition of the software product and technical support service. Consulting and deployment services are also available through Soffid services.

Soffid IAM is a single product with simple SSO solutions to complex web access and identity governance functionality. For Access Management, Soffid supports good basic authorization method support with some Android and iOS biometric authenticators. Hardware token support covers RSA SecurID and YubiKeys. FIDO UAF for fingerprint sensor built into a laptop, phone, or tablet, and U2F USB with fingerprint or NFC. FIDO 2 support is given for Android. Support for contextual and risk-adaptive authentication is part of the base authentication service. Contexts for adaptive authentication includes support for the user, network, location, and some device attributes. Access policies are managed and stored centrally and support ABAC, RBAC, CBAC, and user-group based access principles. Delegated policy management is not supported, although both role management and role discovery capabilities are included. Sessions can be managed using browser cookies with max and idle session timeouts. Session ID anomaly detection is available to detect session attacks. Session protection techniques include binding of session ID to user properties and session ID lifecycle monitoring. SSO is achieved through a reverse proxy for SSO across multiple web applications. SSO for applications that don't support proxy technology can be accomplished through password vaulting and forwarding. Identity federation support for both IdP and SP functionality is given with support for SAML, OAuth 2, OIDC, SWT, JWT, and SCIM federation related standards. Good reporting options are available, which includes IGA and AG related reports that are available out-of-the-box.

Both fraud detection and API security are not offered as part of the Soffid IAM solution.

Soffid IAM can support not only on-premises but also public & private cloud and hybrid deployment models. Hybrid solutions can be accomplished by mixing Kubernetes and software-based components. The solution can be delivered as a hardware appliance, container-based, and as a managed service, although a virtual appliance option is not available. Soffid IAM supports a wide range of operating systems, gives a fully integrated version of the TomEE derivative of Tomcat, and requires an external database such as MariaDB, MySQL, PostgreSQL, Oracle, or MS SQL Server. The SaaS delivery can be hosted on AWS, GCP, Azure, and OCI platforms. Soffid states that 100% of the solution's functionality is exposed via SOAP and REST APIs, as well as CLI. WebHooks and WebSockets can also be used. SDKs are not available. Product customization requires Java programming skills.

Soffid IAM primarily serves medium to mid-market organizations with some inroads to enterprise-level organizations. Customers are focused in the EMEA region, with some expansion into APAC and Latin America. Soffid’s partner ecosystem is relatively small and located in the customer’s geographic locations. Soffid offers some base Access Management capabilities, specifically in identity federation, policy management, and SSO. However, the product provides an alternative open source solution to mid-market organizations.

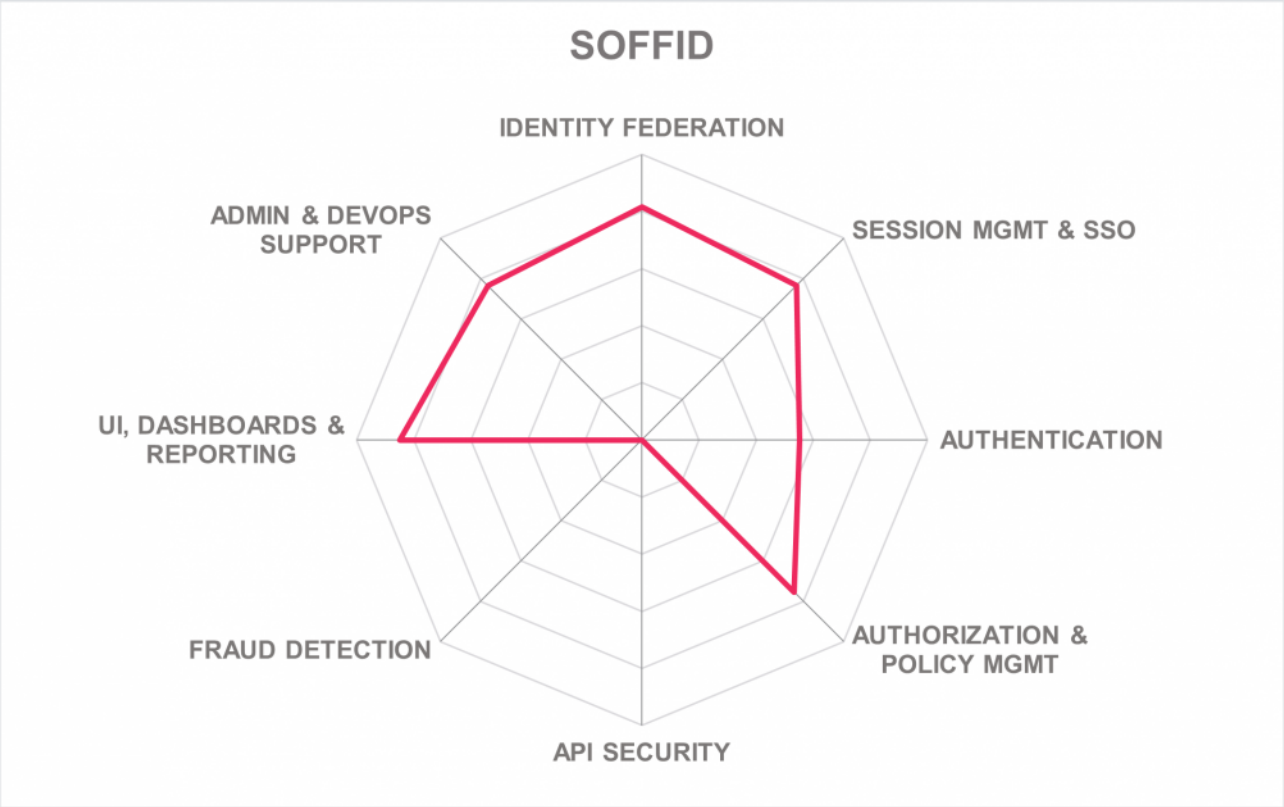
Security	●●●●○
Functionality	●●●○○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●●

Strengths

- Identity federation
- Single Sign On
- Session management
- Authorization and policy management
- Good reporting capabilities
- Admin and DevOps support
- Fully open source

Challenges

- Limited market presence outside Europe with a relatively small partner ecosystem
- Rudimentary, but functional UI, although improvements on the roadmap
- Limited authentication support
- Missing fraud detection
- Missing API security


SOFFID
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.25 Thales

The Thales Group, based in France, recently completed the acquisition of Gemalto, which brought SafeNet Trusted Access to its portfolio as its primary access management product. SafeNet Trusted Access offers a single product with a wide range of authentication factors combined with broad support for contextual attributes to deliver risk adaptive authentication along with some access management functions targeted at B2B, B2E, B2C, and G2C market segments.

SafeNet Trusted Access core Access Management capabilities include good support for basic hardware tokens and popular mobile app authentication methods with support for Android platform native - fingerprint, face recognition, PIN, and iOS Face and Touch ID biometric authenticators. More advanced voice recognition and iris scan types of biometric authenticator options are not given. FIDO UAF is not supported, but FIDO U2F and FIDO 2 support is given for SafeNet IDPrime FIDO and eToken FIDO. Contextual and risk-adaptive authentication is given supporting location, user, network, and device contexts, as well as screen, unlock events for adaptive Windows Log-on, in which access policies can be created for different contextual conditions. Centralized policy management with policy authoring tools is available. Authorization controls allow for the use of ABAC, RBAC, CBAC, and group-based principles. Basic role management and entitlements discovery possible, although role mining is not. Also, support for delegated policy management is not available. Web session management is basic and lacks capabilities for session attack detection and session protection other than protection given through the use of a digitally signed browser cookie. Identity federation is the primary SSO mechanism, although web-server agents are available for Microsoft IIS, Outlook Web Access, and Epic Hyperspace. SSO support for the application that doesn't support proxy or web agent requires integration through technology partners. Secure token translation for SSO across multiple applications supports Kerberos to SAML or OIDC only. Identity federation supports IdP, but not SP use cases. Support for federation related standards only includes SAML 2 and OIDC. Good reporting capabilities are given with reports for major compliance frameworks that are available out-of-the-box.

Fraud detection capabilities are somewhat limited and include identity proofing of new users at registration time and endpoint device profiling, although additional capabilities are on the product roadmap. For API security, the REST API is secured using an API Gateway, combined with rule-based application firewalls, log monitoring, and rate-limiting. API protocol-specific attacks such as XSS, SQL Injection, or Shell Injection can be analyzed. API key mechanisms can be used to control APIs such as traffic usage patterns, limiting the number of calls to an API, or filtering based on service account assigned to the API key.

SafeNet Trusted Access supports public cloud and a limited hybrid deployment model delivered as a fully multi-tenant SaaS hosted on AWS. Support for IaaS installation is not available, although it is on the Thales Group roadmap. Slightly more than half of the solution’s functionality is accessible via SOAP and REST APIs. CLI access to SafeNet Trusted Access capabilities is not given, although professional services can provide API-based PowerShell scripts on demand. SDKs provide Access to nearly product functionality and are available for the Android, iOS, Java, C/C++, .NET, and Python programming languages.

The Thales Group was established in 2000 with a primary customer focus on mid to large organizations and

governments in both the EMEA and North American markets with growth in the APAC and other regions. Thales Group centers on ground transportation, aerospace, space, defense, and digital security industry sectors. Organizations with authentication and authorization Access Management requirements with a useful UI, dashboards, and reporting capabilities should consider SafeNet Trusted Access.

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

THALES

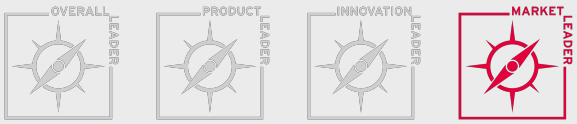
Strengths

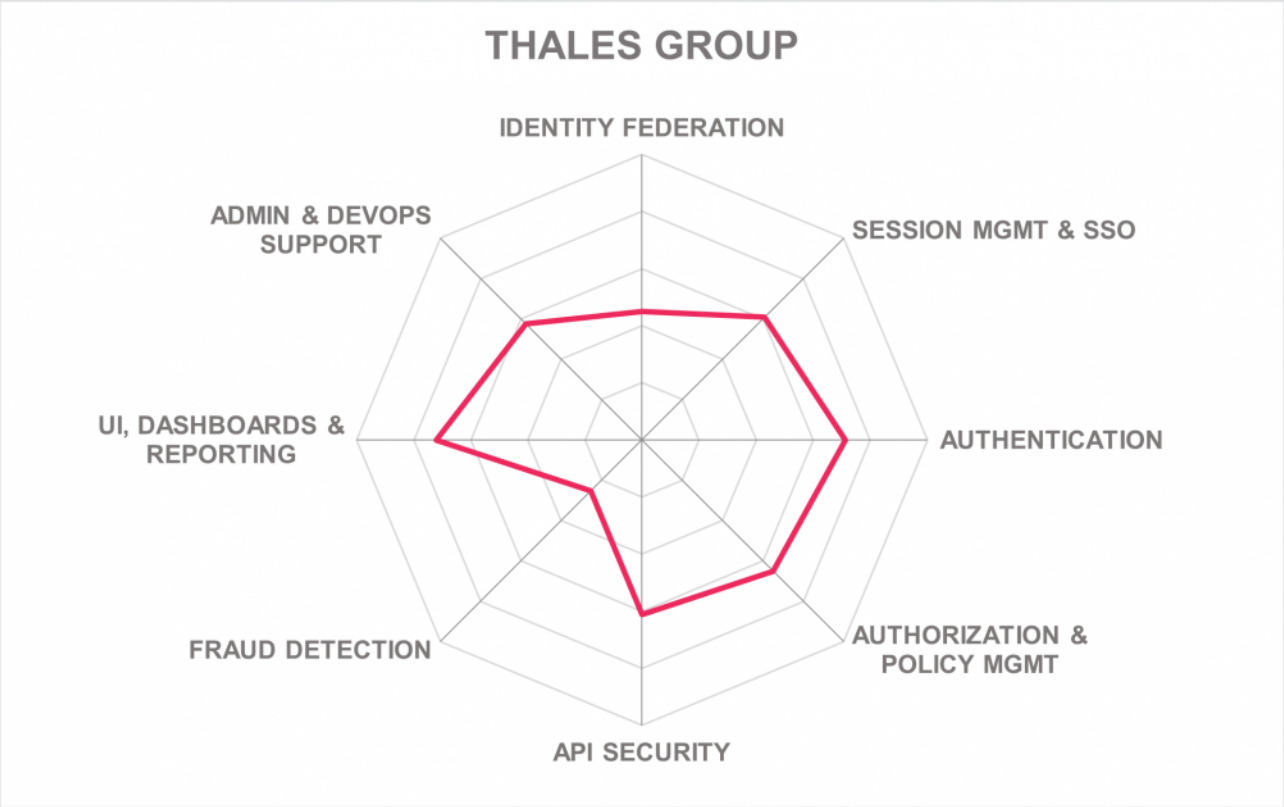
- Authentication support
- Authorization and policy management
- Good reporting capabilities
- Modern UIs and dashboards
- Moderate API security

Challenges

- Limited identity federation support
- Basic session management and SSO
- Limited fraud detection
- Limited on-premise deployment options

Leader in




THALES GROUP
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.26 Ubisecure

Ubisecure is a Finland based company established in 2002 with a customer base primarily in the Nordic region. Their Identity Platform is delivered as a single product with multiple IAM services integrated within a suite focusing on CIAM use cases. Ubisecure Identity Platform is offered as its Access Management offering for this Leadership Compass report.

Ubisecure Identity Platform Access Management supports core capabilities. For identity federation, IdP and SP features are given. Also support for most major federation related standards such as SAML 2, OAuth 2, OIDC, and JWT as well as regional Mobilivarmenne/ETSI MSS 102 204, Swedish BankID, Mobile Connect, Finnish Trust Network (FTN) standards. Basic support for authentication methods is given, although both Android and iOS biometric authenticators are available, as well as integration with Hitachi VeinID. Hardware tokens and FIDO authentication support is missing. Risk-adaptive authentication gives limited contextual support through IP restrictions. Policy management with authoring tools and centralized storage is available and supports ABAC, RBAC, and user-group based, but not CBAC user access principles. The platform provides delegated administrations features for organizations to manage their access policies and related configuration. Session management can be accomplished through browser cookies and a variety of session timeout configurations. Missing is the ability to protect or detect sessions attacks. SSO across multiple web applications can be achieved through OpenID Connect & SAML integrations, and support for SSO secure token translation across multiple applications is given. SSO is not supported for non-web or applications that don't support proxy or web-server agent technology. Also, a modern UI with good dashboards are provided.

Fraud detection is limited to user verification through BankID, Finnish Trust Network identity proofing in the Nordics & Onfido ID/passport verification integration. API security is limited to XML schema validation, although system integrators can enable additional features within the customer environments that will enable additional security features.

Ubisecure Identity Platform supports on-premises, cloud, and hybrid deployment models, and it can be delivered as SaaS, software deployed to a server, or as a managed service. SaaS can be hosted on AWS, and its managed service can be provided through Ubisecure or its partners. Container-Based and Microservices related installations are on the Ubisecure roadmap. For software deployed to a server, Windows, CentOS, and RHEL Linux operating systems are supported as well as Tomcat, WildFly, PostgreSQL, LDAP (OpenLDAP/ADLDS). Java is required to run Ubisecure applications. Most of the solution's functionality is available via REST APIs only. Access to product functionality via CLIs and SDKs is not available.

Ubisecure has a relatively small presence outside the Nordic region and a limited partner ecosystem. However, they provide some interesting CI/CD and Robot Framework features. Ubisecure Identity Platform shows some strengths with identity federation, session management, SSO, and authorization and policy management. However, they lack some modern authentication capabilities. Ubisecure appears as a Challenger in the Market Leader segment.

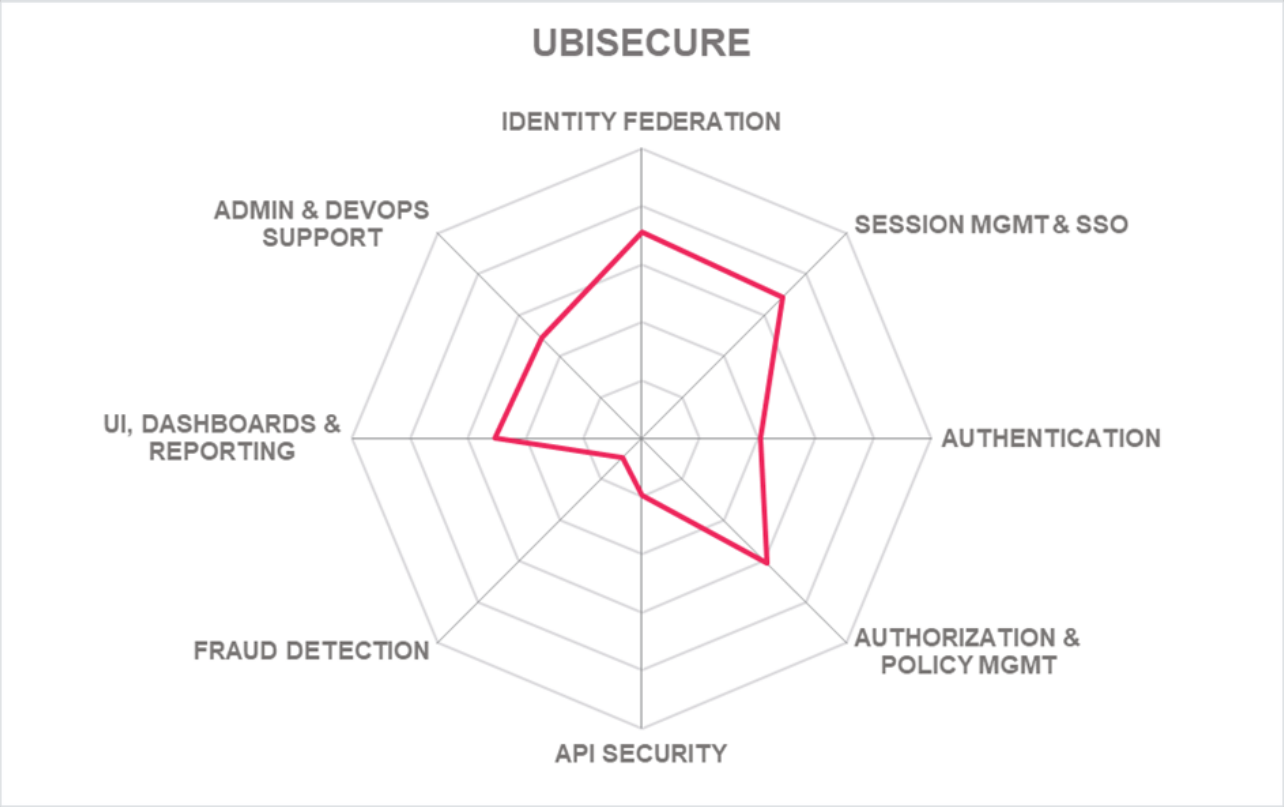
Security	●●●●○
Functionality	●●●○○
Interoperability	●●●○○
Usability	●●●○○
Deployment	●●●○○

Strengths

- Identity federation
- Single Sign On
- Session management
- Authorization and policy management
- Modern UI and dashboards
- DevOps CI/CD and robot framework features

Challenges

- Small partner ecosystem & limited global reach
- Missing FIDO and hardware token support
- Limited fraud detection
- Limited API security


UBISECURE
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

5.27 WSO2

WSO2 Identity Server is based on open source and provides a single solution that contains IAM capabilities including SSO, Identity federation, strong and adaptive authentication, and API & Microservices security. For this Leadership Compass evaluation, WSO2 Identity Server focuses on Access Management capabilities.

WSO2 Identity Server core Access Management capabilities include support for basic and popular mobile app push authenticators, as well as good support for hardware tokens. Support for biometric authentication is given with VeridiumID, as well as passwordless authentication with FIDO 2.. WSO2 adaptive authentication supports contexts for the user, device, network, location, as well as utilizing user behavior, level of assurance of the access request, risk analysis statistics, and machine learning algorithms. Context attributes can be passed down to the access policy for evaluation. Management of policies uses centralized storage connected to a WSO2 Identity Server and the ability to test policies before publishing to a Policy Decision Point (PDP) as well as testing for the collective effect of the policies active in the PDP. An editor tool allows for authoring and editing XACML 3 policies, although the XACML templates work with raw XML, requiring some technical knowledge. Within policies, ABAC, RBAC, CBAC, and user-group based principles can be used in combination as well. Basic role management is given, but role mining capabilities are not. Session management tracks user web sessions based on browser cookies. The product supports a “Remember Me” option where the product stores the user session up to a configured time period, based on the browser cookie. Good sessions attack detection and protection is available. For SSO, a SAML-based SSO agent is provided or used to put a reverse proxy solution to handle the SSO protocol. Secure token translation between standard as well some proprietary protocols for SSO across multiple applications is also given. WSO2 Identity Server can be integrated with WAF solutions such as Imperva, Akamai, and AWS WAF for additional capabilities. Comprehensive support for identity federation IdP and SP are included as well as addressing other required capabilities such as role and claim mappings. Strong support for all federation related standards evaluated is offered. Although WSO2 provides a useful administration UI and dashboards and basic reporting capabilities are given without report generation from the WSO2 Identity Analytics Server, missing are out-of-the-box reports for major compliance frameworks and governance.

Fraud detection is limited to fraudulent account creation detection through email and SMS verification at self-registration, reCaptcha, or workflows for approving account creations and integrations using adaptive authentication scripts third-party services such as the Evident identity verification services. Additionally, Identity Server APIs, as well as external APIs, can be accessed via WSO2 API Manager's API gateway for additional capabilities and managed security. Any third-party API gateway solutions can also be used, while WSO2 Identity Server acts as the authorization server. A wide range of protocol-specific attacks (XML, JSON, etc.) can be analyzed. API key mechanisms can be used, and the WSO2 API Manager component can support the use of a self-contained JSON Web Token (JWT) as the API key.

WSO2 Identity Server supports on-premises, cloud, and hybrid deployment models and can be delivered as software deployed to a server, hardware or virtual appliances, Docker containers for Kubernetes, SaaS, or as a managed service where product installation, maintenance, and infrastructure handling is done solely by

WSO2 or working with the customer. A wide range of Linux and Windows operating systems and databases are supported for software deployed to a server. WSO2 Identity Server has a fully integrated application server built on Apache Tomcat. Installation requirements include a Java runtime environment and database. The WSO2 Identity Server SaaS is hosted on AWS, and support for IaaS covers Alibaba, AWS, GCP, Azure, OCI, and Digital Ocean. One of the widest ranges of API protocols evaluated is supported, which includes SOAP, REST, RPC, MQTT, AMQP, OData, WebHooks, and WebSockets as examples. Access to the Identity Server functionality via CLIs is not given, although SDK support for Android, Java, .NET, and JavaScript programming languages is given. The REST APIs are based on OpenAPI v2/v3 specifications, and the API definitions can be used to generate SDKs via standard OpenAPI SDK generators. WSO2 Identity Server RESTful APIs facilitates integrations into CI/CD pipelines or with DevOps/Admin tools for automation.

Founded in 2005, WSO2 customers are focused in the EMEA and North America regions with some presence in the APAC supporting mid-market to enterprise company sizes, with a good partner ecosystem. WSO2 Identity Server provides some strengths in Identity Federation, API security, Authorization, and policy management. Still, it may not be the choice for those looking for Access Management with fraud detection capabilities. Overall, WS02 continues to improve in a positive direction and appears as a Challenger in this Access Management Leadership Compass.

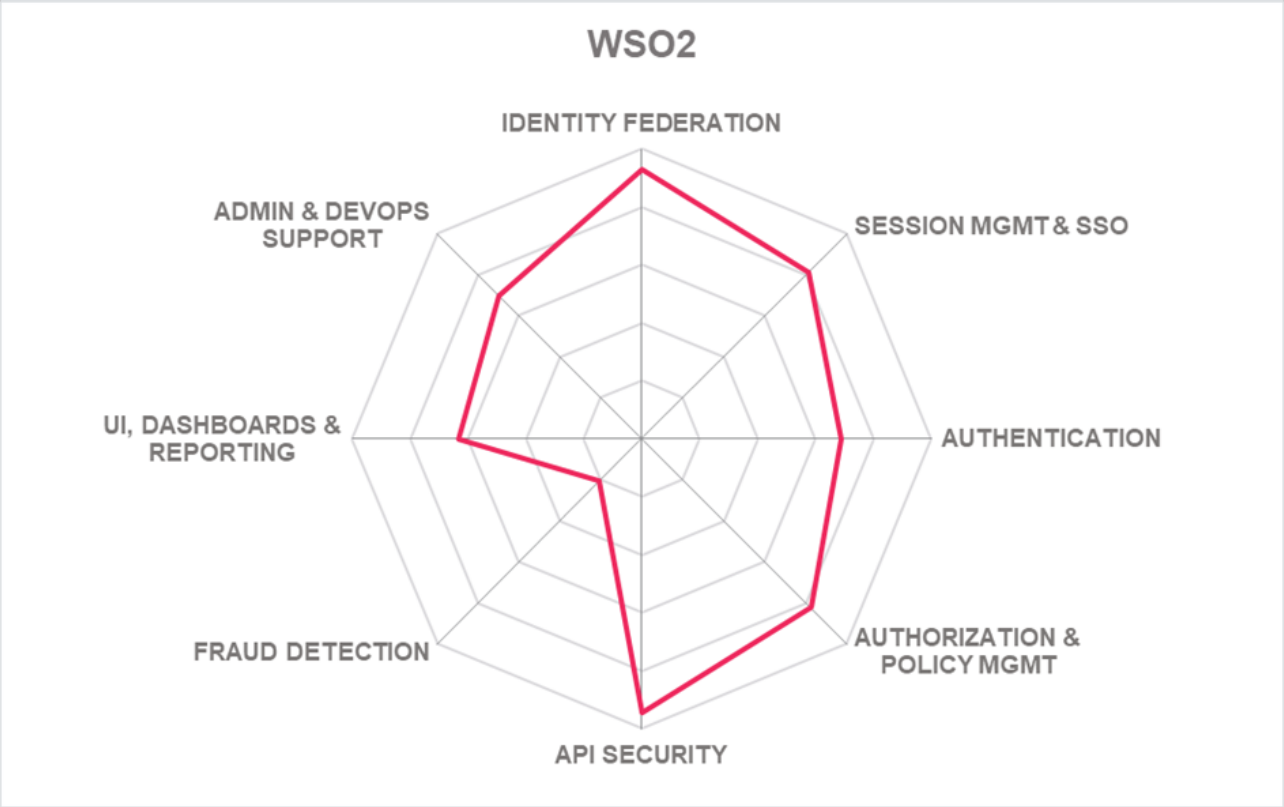
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●●

Strengths

- Identity federation
- API security
- Authorization and policy management
- Session management and SSO
- Strong authentication support
- Adaptive authentication
- Admin UI and dashboards
- Admin and DevOps support

Challenges

- XACML templates work with raw XML requiring some technical knowledge
- Limited fraud detection
- Missing biometric authenticator options
- Threat analytics and ML capabilities require third-party solutions


WSO2
IDENTITY FEDERATION
SESSION MGMT & SSO
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
FRAUD DETECTION
UI, DASHBOARDS & REPORTING
ADMIN & DEVOPS SUPPORT

6 Vendors and Market Segments to watch

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

6.1 1Kosmos

1Kosmos was founded in 2018 and is headquartered in New Jersey. The company is small but self-funded and profitable. They address the consumer and workforce identity management markets with blockchain ID solutions. BlockID Customer is their CIAM offering, and BlockID Verify handles identity vetting and KYC. Beyond providing consumer authentication, 1Kosmos is a decentralized identity (DID) and distributed identity attribute aggregator. 1Kosmos' solutions are hosted as SaaS in AWS and GCP, distributed across APAC, EU, and NA regions.

As a relatively new cloud-based startup, 1Kosmos has many interesting features. 1Kosmos is suitable for organizations that need these kinds of features and are comfortable with early-stage startups. Watch for 1Kosmos to push CIAM frontiers of Access Management.

6.2 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 for 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, which is good 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.

6.3 Avoco Secure

AvocoSecure is a privately-owned UK company offering Cloud and CIAM services. The Avoco Trust Platform API is a toolkit providing extended ecosystem functionality to deliver multiple components, including IDPs, hubs, brokers, verification, and blockchain. The solution is blockchain-agnostic and privacy enhanced. Trust Platform is not derived from traditional IAM but rather was built to UK government security standards for high assurance verification of consumer identities. AvocoSecure partners offer customer profile storage in cloud or hybrid installations. Any of the components generated using the Avoco Trust Platform API are available either as a cloud-based service or can be directly integrated into customer's on-premise environments. It has many second factors available OOTB and integrates to third-party credential management services that offer biometrics. Risk-based authentication is managed using dynamic rules. It accepts federated login via SAML, OIDC, and OAuth. Avoco also now supports OpenID CIBA.

Using REST APIs, the Avoco Identity platform can feed data to SIEM/RTSI systems and Splunk. Avoco Secure also provides privacy consent management functionality, although the Trust Platform does support UMA. Family management capabilities are available via a delegated administration model.

The AvocoSecure Trust Platform is an interesting offering considering its consent management and identity verification service provider integration. Since identity proofing is a key component to fraud reduction, watch AvocoSecure Trust-T Hub for its API driven orchestration and identity attribute verification that can be used to modernize an organization's customer on-boarding, KYC, and AML activities.

6.4 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.

For on-premises and private cloud deployments, F5 BIG-IP APM offers context-based remote access to private applications, centralized SSO / federation, with desktop and mobile platform security posture capabilities. Also given are authentication and authorization such as Kerberos, Header-based, RADIUS, NTLM, OAuth/OIDC, MFA, and step-up authentication, as well as 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 the ingestion of 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
Watch F5 BIG-IP APM continue moving in a positive direction to meet the evolving use case of Access Management.

6.5 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, Access Governance, Multi-Factor Authentication, and Single Sign-On. Integrated Privileged Access Management (PAM) capabilities that restrict and control privileged users' access is also available.

For the Access Management segment, the RapidIdentity platform focuses on SSO, MFA, and PAM. Their Single Sign-On (SSO) is standards-compliant, allowing integration with on-premises and cloud-based applications using SAML 2.0, OAuth, OpenID Connect, WS-Federation. SSO mobile access support to cloud applications for iOS and Android devices. A variety of authentication options includes remote access and VPN logins, MFA for Windows logins, adaptive MFA, and strong authentication for shared workstations. RapidIdentity offers a baseline PAM feature-set with shared account password management, application to application password management and basic auditing, and privileged activities logging. Support for SSH keys is included.

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

6.6 Pirean

Pirean was founded in 2002 with offices in London and Sydney. In 2018, Pirean was acquired by Exostar, an IAM and collaboration solutions provider for highly regulated industries such as Aerospace & Defense and Life Sciences. In July 2020, Exostar was acquired by Thoma Bravo. Pirean provides a Consumer and Workforce IDaaS platform called Access: One.

Pirean's strong feature set is dictated by its history in heavily regulated industries that require strict security. Pirean's Access: One provides a diverse set of capabilities that offers a fully-featured end-to-end IAM solution. Access: One supports both IAM and CIAM use cases on-premises and in the cloud. Pirean also goes beyond the traditional IAM feature set to securely connect mobile users and provide flexible integration and workflow options that allow for the orchestration of the platform's capabilities.

Given Pirean's growth and backing, watch for Pirean to increase its market share.

6.7 PortSys

PortSys is a privately funded company that was founded in 2008 and based in Marlborough, Massachusetts. PortSys started out building security appliances with Microsoft and HP and has evolved to provide Zero Trust Access Controls to organizations in North America and the EMEA regions. PortSys gives reverse proxy-based access controls that can be deployed on-premises, cloud, or hybrid environments. Unlike pure IDaaS and CASB solutions, they provide solutions for client-server and legacy apps. Other capabilities include MFA for devices, security posture, etc. PortSys can support LDAP, SAML, OAuth, SQL support. They can consume Identity information via API integration with Okta.

Watch PortSys as an alternate solution suited for SMBs, state, local, and even federal government agencies who need to integrate IAM with legacy apps as well as the cloud.

6.8 Signicat

Founded in 2006, Signicat has offices in the Netherlands covering Belgium and Luxemburg as well in the UK. Signicat customers are based in the EMEA region, such as the Nordics, Benelux, DACH/GSA, and Southern Europe. The Norwegian company, Signicat, offers a comprehensive set of solutions that support customers in creating seamless processes for Digital Assurance and Authentication, in tight integration with their existing IT infrastructure. Signicat recently acquired the Dutch company Connectis in 2020, which is known for its digital identity solutions. Signicat offers a Digital Identity Platform and Identity Broker for Access Management.

One of the Signicat Identity Platform 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 some other proprietary interfaces used primarily by governmental schemes and banks are also given. SSO is an integrated Signicat Identity Broker capability. Signicat Identity Platform is offered as a fully multi-tenancy cloud service that can support a multi-cloud strategy. SaaS is the only Signicat delivery option that can be hosted in a customer's facilities or on the AWS or Azure public cloud platforms. Almost all of the Signicat Identity Platform functionality is accessible via SOAP, REST, and SCIM APIs. SDKs for the Android, iOS, .NET, PHP programming languages are supported. The majority of the Signicat Identity Platform does not require custom coding except for the custom triggering of authentication & authorization flows or modifying optional aspects of APIs. All generic and relevant customization options are available through its GUIs.

The Signicat Identity Platform might be of particular interest to organizations in the EMEA region that require Access Management capabilities that can be customized and tightly integrate with their existing IT

infrastructure. Watch for Signicat's expansion into other European countries as it continues to extend its Access Management capabilities.

6.9 SSO Easy

SSO Easy 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 API's to facilitate integrations with any client environment. Out-of-the-box support is given for AD and LDAP, Kerberos/IWA/NTLM, popular application and web servers, as well as form-based authentication support.

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.

6.10 United Security Providers (USP)

Founded in 1994, United Security Providers (USP) is a Swiss software vendor and service provider with offices in Bern (headquarters), Zurich, London, and Minsk. USP has more than 100 security professionals and operates its own 24/7 Security Operations Center. While their initial and primary target market is Switzerland, they sustain a growing market reach beyond their domestic market, primarily in Germany, Austria, and the UK. The USP Secure Entry Server® (SES) offers a comprehensive modular suite that includes Web Access Management, Identity Federation, Single Sign-on, and Web Application Firewall capabilities.

USP has designed SES to provide an Access Management and Identity Federation solution for real-life business requirements regarding agility, performance, user experience, and security. The SES WAF component turns the suite into a robust web security platform by protecting applications and the managed data from common threats.

Watch for United Security Providers Secure Entry Server to provide a strong, unified, and interoperable access management solution offering customers located in their primary target regions of D/A/CH and the UK.

7 Related Research

Executive View: AdNovum NEVIS Security Suite - 80066
Executive View: Curity Identity Server - 80159
Executive View: EmpowerID - 70297
Executive View: Evidian Identity & Access Management - 70872
Executive View: ForgeRock Access Management - 80319
Executive View: Forum Systems Sentry and Identity Federation - 72511
Executive View: IBM Security Access Manager (ISAM) - 79066
Executive View: IBM Cloud Identity - 79065
Executive View: Ilantus Compact Identity - 80177
Executive View: Microsoft Azure Active Directory - 80401
Executive View: Okta Cloud IAM Platform - 70887
Executive View: Optimal IdM - Optimal Cloud - 80162
Executive View: Oracle Identity Cloud Service - 80156
Executive View: SecureAuth IdP - 71327
Executive View: Signicat - 72537
Executive View: Simeio IAM for SMB - 79071
Executive View: Symantec Privileged Access Manager - 80331
Executive View: Thales Vormetric Application Crypto Suite - 79069
Executive View: Ubisecure Identity Platform - 79072
Executive View: WSO2 Identity Server - 80060
Leadership Compass: Access Governance & Intelligence - 80098
Leadership Compass: Access Management & Federation - 71147
Leadership Compass: API Management and Security - 70311
Leadership Compass: Cloud-based MFA Solutions - 70967
Leadership Compass: Consumer Authentication - 80061
Leadership Compass: IDaaS Access Management - 79016
Leadership Compass: Identity API Platforms - 79012
Market Compass: Web Application Firewalls - 70324
Whitepaper: ForgeRock Identity Platform capabilities for Authentication under PSD2 - 79080
Whitepaper: Ping Identity solutions for Customer Identity and Access Management - 70289
Whitepaper: Preparing for PSD2 technical requirements using RSA solutions - 79062

Methodology

About KuppingerCole's Leadership Compass

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

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

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

Types of Leadership

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

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

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

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

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

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

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

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

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

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

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

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

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

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

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

Vendor rating

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

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

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

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

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

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

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

Rating scale for products and vendors

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

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

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

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

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

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

Inclusion and exclusion of vendors

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

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

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

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

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

Content of Figures

Copyright

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

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

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