KuppingerCole Report

LEADERSHIP COMPASS

By Richard Hill
April 26, 2022

Access Management 2022

This Leadership Compass provides up to date 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 / Executive Summary

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 traditional approach that puts a layer in front of web applications that takes over authentication and – usually coarse-grained – authorization management. Also, tools increasingly support 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). Although Identity Federation can be used in various configurations, most vendors today provide integrated solutions that support centralized access management based on federation protocols such as SAML v2, OAuth, and OIDC.

Over the years, vendors have made significant changes to their product architecture to make them cloud-ready while extending to on-premises applications. These methods include delivering a single sign-on (SSO) experience to 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.

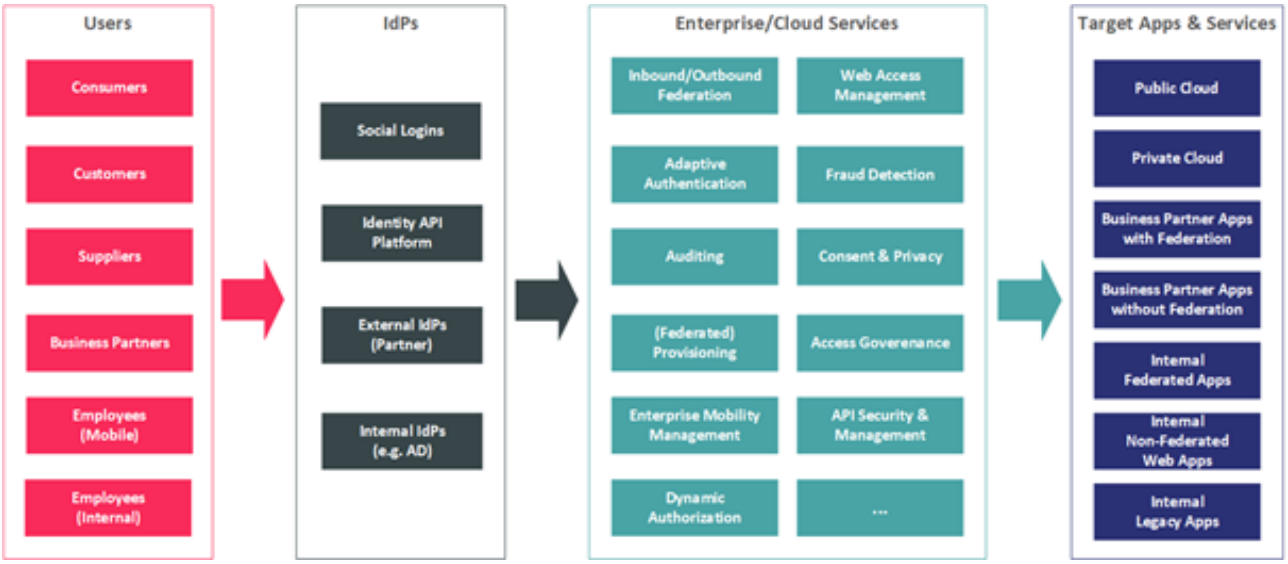


Figure 1: The enterprise requires access to systems, either on-premise or in the cloud, for all types of user populations

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

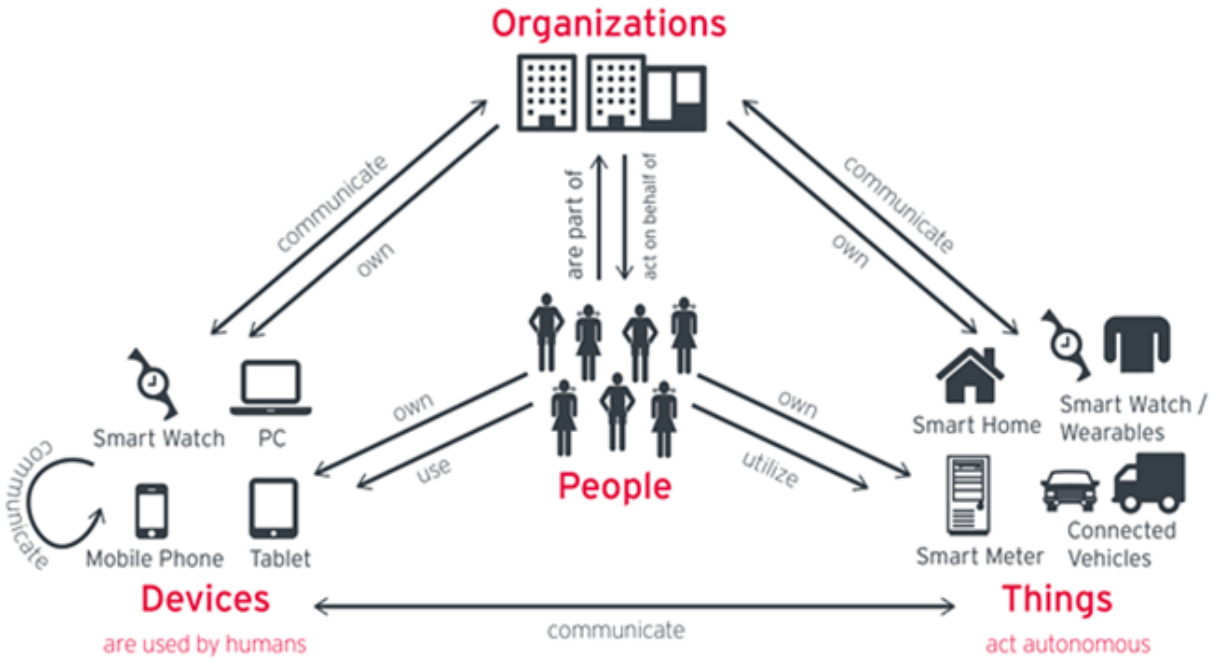


Figure 2: The increasingly connected enterprise ecosystem

The Access Management market provides a number of options to organizations. In the IDaaS market, with its ease of adoption and cloud-native integrations, is slowly overtaking the on-premises IAM market. At the same time, the IDaaS market continues to evolve. 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. There's a varying level of support available from Access Management vendors to manage CIAM functions that support requirements for managing and complying with data sharing and privacy regulations, such as consumer notification and consent management.

The support for open identity standards continues to shape the direction of Access Management implementations. Some of the most popular authentication and identity federation standards include support for LDAP, Kerberos, OpenID, OAuth, SAML, and RADIUS. Organizations with a need for dynamic authorization management might require support for XACML or UMA. User provisioning services commonly require support for SCIM. And having access to the Access Management solution's functionality via APIs or other programmable interfaces will go a long way in keeping your IAM flexible and sustainable. API-based platforms typically require a developer-ready solution, providing API toolkits such as widgets or SDKs that facilitate rapid development.

Access Management continues to evolve beyond the traditional capabilities seen in the past. Increasingly, we see Access Management solutions providing security for APIs becoming more readily available and driven by the need to meet emerging IT requirements that include hybrid environments that span across on-premises, the cloud, and even multi-cloud environments. And although Fraud Detection solutions, also referred to as Fraud Reduction Intelligence Platforms (FIPS), is often considered a different market with their separate offerings, there has been a noticeable up-tick in Access Management solutions providing

some level of Fraud Detection capabilities ranging from the detection of identity fraud through Identity Proofing to the detection of unauthorized account takeover, response mechanisms, or support for user and device profiling as some examples. More recently, there has been some indication and interest of Access Management support for Verifiable Credentials. This Leadership Compass evaluates and reports on the level of Fraud Detection, and Verifiable Credentials support for each vendor, giving the reader an indication of the extent of this trend in the Access Management market.

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

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)
  - Risk- and context-based authentication
  - Adaptive, step-up, and continuous authentication
  - Passwordless Authentication
  - Device Authentication (e.g., IoT)
  - Toolkits for adding additional authenticators
- Authorization and Policy Management
- Password Management

- Session Management (e.g., Single Sign-On, Secure Token Translation, etc.)
- Identity Federation
    - Support for inbound and outbound federation
    - Including broad support for federation standards and related standards
    - Support for non-federation-enabled applications
- Support for a broad range of deployment models, including on-premise deployments
- Integration to existing directory services
- Support for access protocols (OAuth, OIDC etc.) and open identity standards such as FIDO, etc.
- Support for user self service
- User onboarding and registration
- Centralized management of users, authorization policies, dashboards, reporting, etc.
- Some level of access to the solutions capabilities via APIs
- API Security
- Security Orchestration
- Support for audit, forensics, compliance, and reporting
- Solution architecture (e.g., how modern is the architectures and the technologies used)
- Support for Administrators and DevOps

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

Other capabilities that are highly valued and considered but not quite mandatory for this category of products. However, delivering a very comprehensive set of capabilities will influence our ratings:

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

- Access Governance
- Verifiable Credential support

Inclusion criteria:

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

Exclusion criteria:

- Point solutions that support only isolated capabilities such as 2FA or Enterprise SSO centric solutions, but little support the other expected features
- MSP solutions that are based on technology of other vendors, with the MSP not owning the IP on the technology
- Vendors without active deployments at customers (e.g., start-ups in stealth mode) will not be considered.
- Solutions that lack a comprehensive set of APIs will not be considered.

We'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

2.1 Overall Leadership

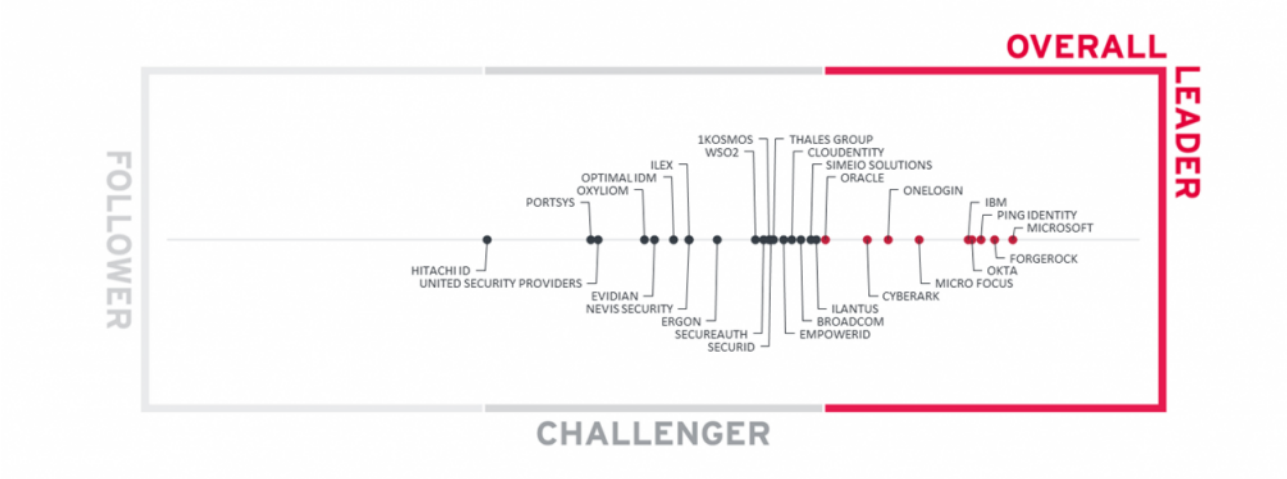


Figure 3: The Overall Leadership rating for the Access Management market segment

The Leader segment in the Overall Leadership rating depicts a mature market in which many vendors deliver feature-rich solutions. The market continues to be crowded, with 28 vendors we chose to represent in our Leadership Compass rating. Although the Access Management market is mature, it continues to

evolve to include other capabilities not previously considered part of it. As such, KuppingerCole has *raised the bar* on the level of features, market presence, and innovation to be included in the Overall Leadership section. Also, in the "vendors to watch" section, we listed a few other vendors that did not meet our essential evaluation criteria or declined participation in this year's edition.

In this year's Overall Leadership category, Microsoft holds the leadership position in the Access Management (AM) market, followed by ForgeRock, and Ping Identity. Next is IBM and Okta close together, followed by Micro Focus. Following is a group of vendors that includes One Login, CyberArk, and Oracle. 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 much 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 are Ilantus, Simeio Solutions, and Broadcom near the upper borderline, with Cloudentity, EmpowerID, Thales Group, 1Kosmos, SecurID, WSO2, SecureAuth, Ergon, Nevis Security, Ilex, Optimal IdM, Evidian, and Oxyliom, following in the upper part of the Challenger section. The Challenger section's lower portion consists of PortSys, United Security Providers, and Hitachi ID. 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.

In the Follower segment are a couple of vendors. This group of vendors is also a mix of established and emerging players, focusing on a few critical areas of Access Management or providing baseline capabilities that can be built upon to customize the solution so as to meet a customer's requirements. Also, vendors may be in the introductory position and intend to grow their capabilities over time. No vendors appear in the Follower segment.

Overall Leaders are (in alphabetical order):

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

2.2 Product Leadership

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

Figure 4: Product Leaders in the Access Management market segment

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and

completeness of services.

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 Ping Identity, followed by ForgeRock with Microsoft, Okta, and IBM following 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 are Micro Focus, OneLogin, Ilantus, and Simeio Solutions. A third grouping appears near the bottom border, which includes Broadcom, EmpowerID, 1Kosmos, CyberArk, Oracle, Cloudentity, and SecureAuth. All vendors in the Product Leadership deliver leading-edge capabilities across the depth and breadth of the Access Management capability spectrum evaluated for the purpose of scoring the vendors in this Leadership Compass. 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) Ergon, Evidian, Ilex, Nevis Security, Optimal IdM, Oxyliom, PortSys, SecurID, Thales Group, United Security Providers, 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.

Finally, one vendor appear in the Follower section which is Hitachi ID. These vendors provide baseline capabilities with the potential for continued feature growth in Access Management, as well as a starting point to build customer-specific customizations as needed.

Product Leaders (in alphabetical order):

- 1Kosmos
- Broadcom
- Cloudentity
- CyberArk
- EmpowerID
- ForgeRock
- IBM
- Ilantus
- Micro Focus

- Microsoft
- Okta
- OneLogin
- Oracle
- Ping Identity
- SecureAuth
- Simeio Solutions

2.3 Innovation Leadership

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

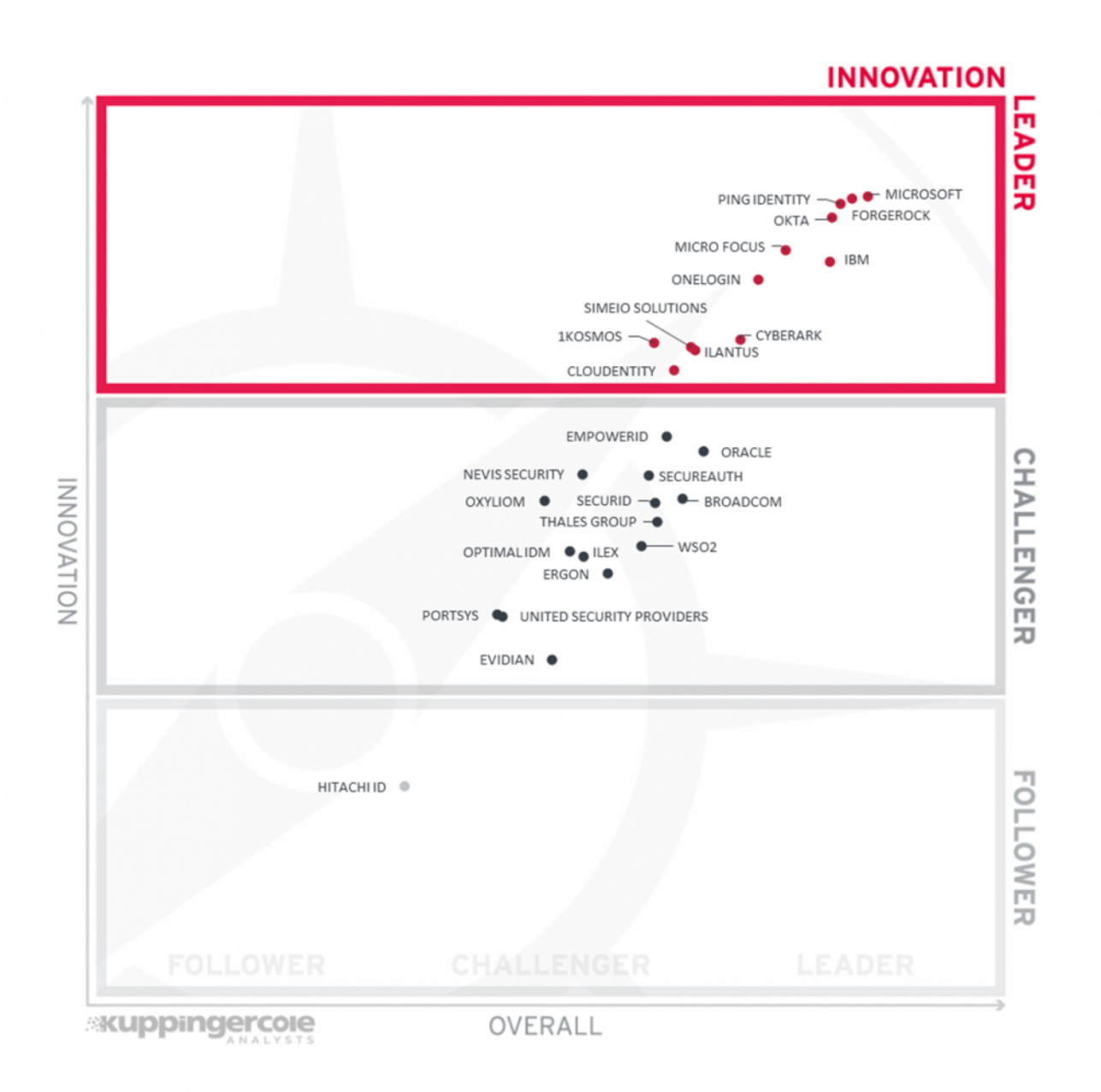


Figure 5: Innovation Leaders in the Access Management market segment

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 saw in the past was somewhat limited but has shown some growth areas of innovation over the last couple of years. Vendors continue to differentiate themselves by innovating in different areas, such as strong adaptive authentication capabilities, dynamic authorization, access intelligence, providing APIs and API security, fraud detection, automation, decentralized identity & verifiable credentials, 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.

Microsoft leads the Innovation Leadership evaluation, closely followed by ForgeRock, Ping Identity, and Okta. Another distinct grouping of vendors appears below them and includes Micro Focus, IBM, and OneLogin, completing the top half of the leadership section. The lower half of the Leadership segment shows CyberArk, 1Kosmos, Simeio Solutions, Ilantus, and Cloudentity that continue to change their AM product portfolio to align with other innovative vendors in the market. These vendors differ in many details regarding 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.

Over half of the Access Management Leadership Compass vendors made it into the Innovation Challenger segment. Close to this segment's top border, we see EmpowerID and Oracle with strong core AM functionality but less strength in innovative capabilities seen by the vendors in the Leadership section and Nevis Security, and SecureAuth following closely behind. Another distinct grouping is seen in the middle of the Challenger section is comprised of Broadcom, SecurID, Oxyliom, Thales Group, Optimal IdM, WSO2, Ilex, and Ergon. The remaining vendors in the lower third of this Challenger section are PortSys, United Security Providers, and Evidian. Vendor groupings often indicate similar levels of capabilities, and 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.

One vendor appears in the Follower segment: Hitachi ID. Although this vendor 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):

- 1Kosmos
- Cloudentity
- CyberArk
- ForgeRock
- IBM
- Ilantus
- Micro Focus

- Microsoft
- Okta
- OneLogin
- Ping Identity
- Simeio Solutions

2.4 Market Leadership

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

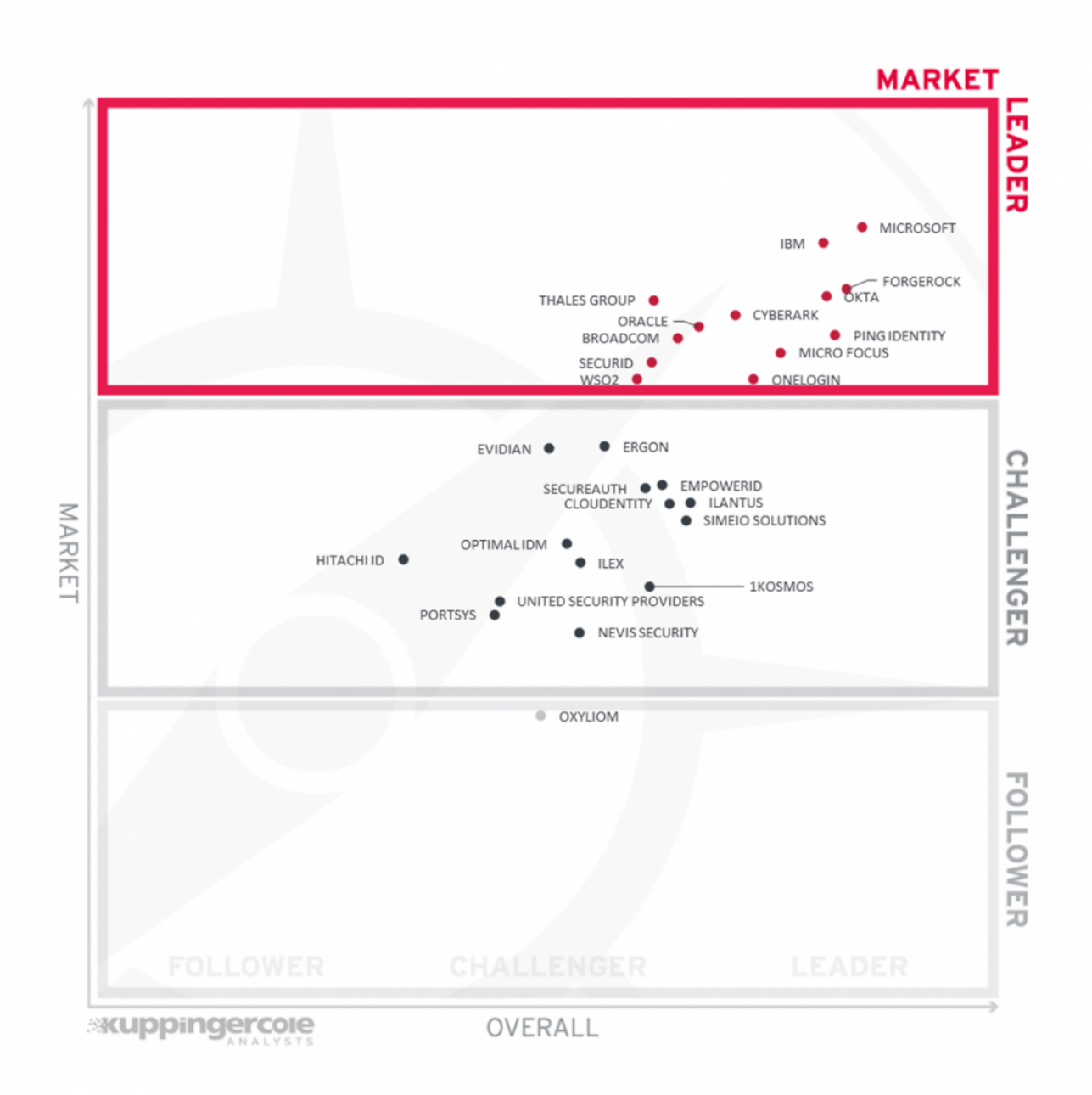


Figure 6: Market Leaders in the Access Management market segment

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, SecurID, Thales Group, and WSO2 – all of which have several deep-rooted complex Access Management deployments across multiple industries.

We find Ergon, and Evidian 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 good, but not strong technology

partner ecosystem for example. Following this group is (in alphabetical order) 1Kosmos, Cloudentity, EmpowerID, Hitachi ID, Ilantus, Ilex, Nevis Security, Optimal IdM, PortSys, SecureAuth, Simeio Solutions, and United Security Providers appear in the middle section of this Challenger segment.

In the Follower segment, we find Oxyliom - with considerable gaps in the specific areas we evaluate for Market Leadership of AM products, including the number of customers, the average size of deployments, effectiveness of their partner ecosystem, etc.

Market Leaders (in alphabetical order):

- Broadcom
- CyberArk
- ForgeRock
- IBM
- Micro Focus
- Microsoft
- Okta
- OneLogin
- Oracle
- Ping Identity
- SecurID
- Thales Group
- WSO2

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.

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

3.1 The Market/Product Matrix

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.

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

This comparison shows which vendors are better positioned in our Product Leadership analysis than their position in the Market Leadership analysis. Vendors above the line are somewhat “overperforming” in the

market. It comes as no surprise that these are often very large vendors, while vendors below the line may more often be innovative but focused on specific regions as an example.

In the upper right segment, we find “Market Champions”. Given that the Access Management (AM) market is mature but still evolving in areas, we see Microsoft and IBM as market champions positioned in the top right-hand box. Close to this group of long-established AM players in the same box are (in alphabetical order) Broadcom, CyberArk, ForgeRock, Micro Focus, Okta, OneLogin, Oracle, and Ping Identity. Being positioned closer to the axis, ForgeRock, Okta, Ping Identity, Micro Focus, and OneLogin represent a slightly better market versus product leadership balance.

The Thales Group, SecurID, and WSO2are 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 a number of vendors that deliver strong product capabilities for Access Management but are not yet considered Market Champions. EmpowerID, Ilantus, Cloudentity, Simeio Solutions, SecureAuth, and 1Kosmos have a strong potential to improve their market position due to the more robust product capabilities they are already delivering.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not market leaders. They also have moderate market success as compared to market champions. These vendors include (in alphabetical order) Ergon, Evidian, Ilex, Nevis Security, Optimal IdM, PortSys, and United Security Providers.

Hitachi ID appears in the left middlebox, indicating a better market presence than AM product capabilities. In the bottom middlebox is Oxyliom with moderate product features but lower in the AM market.

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.

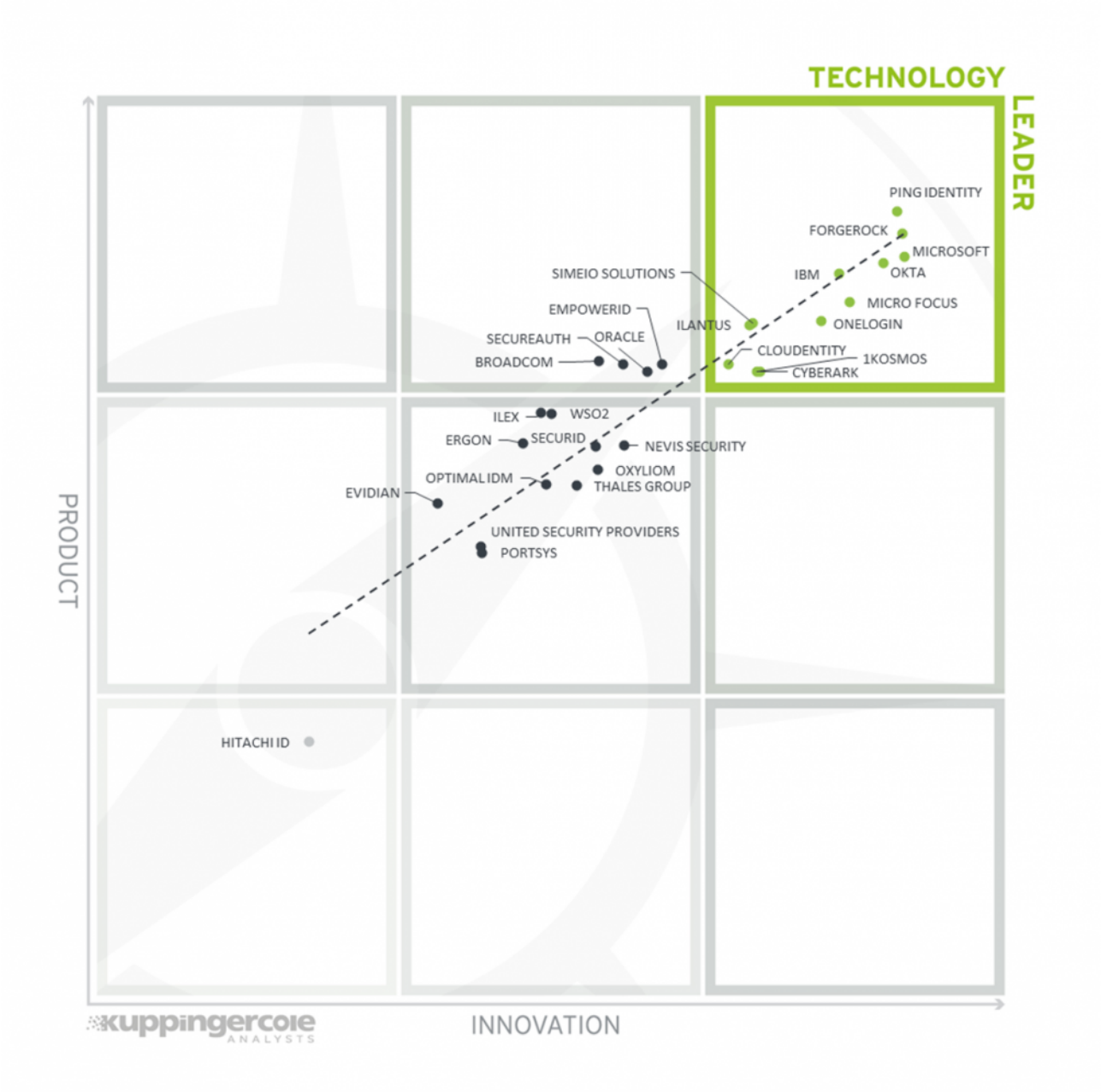


Figure 8: The Product/Innovation Matrix

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. Many vendors placed close to the dotted line, indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find most leading vendors scattered throughout the box in the upper right corner. The leading vendors are Ping Identity, followed by, ForgeRock, Microsoft, Okta, IBM, Micro Focus, OneLogin, , Simeio Solutions, and Ilantus. ForgeRock, IBM, and Ilantus are placed closest to the axis depicting a good balance of product features and innovation. 1Kosmos, CyberArk, and Cloudentity are

following found more towards the bottom of the box.

Four vendors appear in the top middlebox with good product but less innovation than the leaders, including Broadcom, EmpowerID, Oracle, and SecureAuth.

Over a third of the vendors appear in the middlebox, showing both innovation and product strength, which includes (in alphabetical order) Ergon, Evidian, Ilex, Nevis Security, Optimal IdM, Oxyliom PortSys, SecurID, Thales Group, United Security Providers, and WSO2.

One vendor, Hitachi ID, 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.

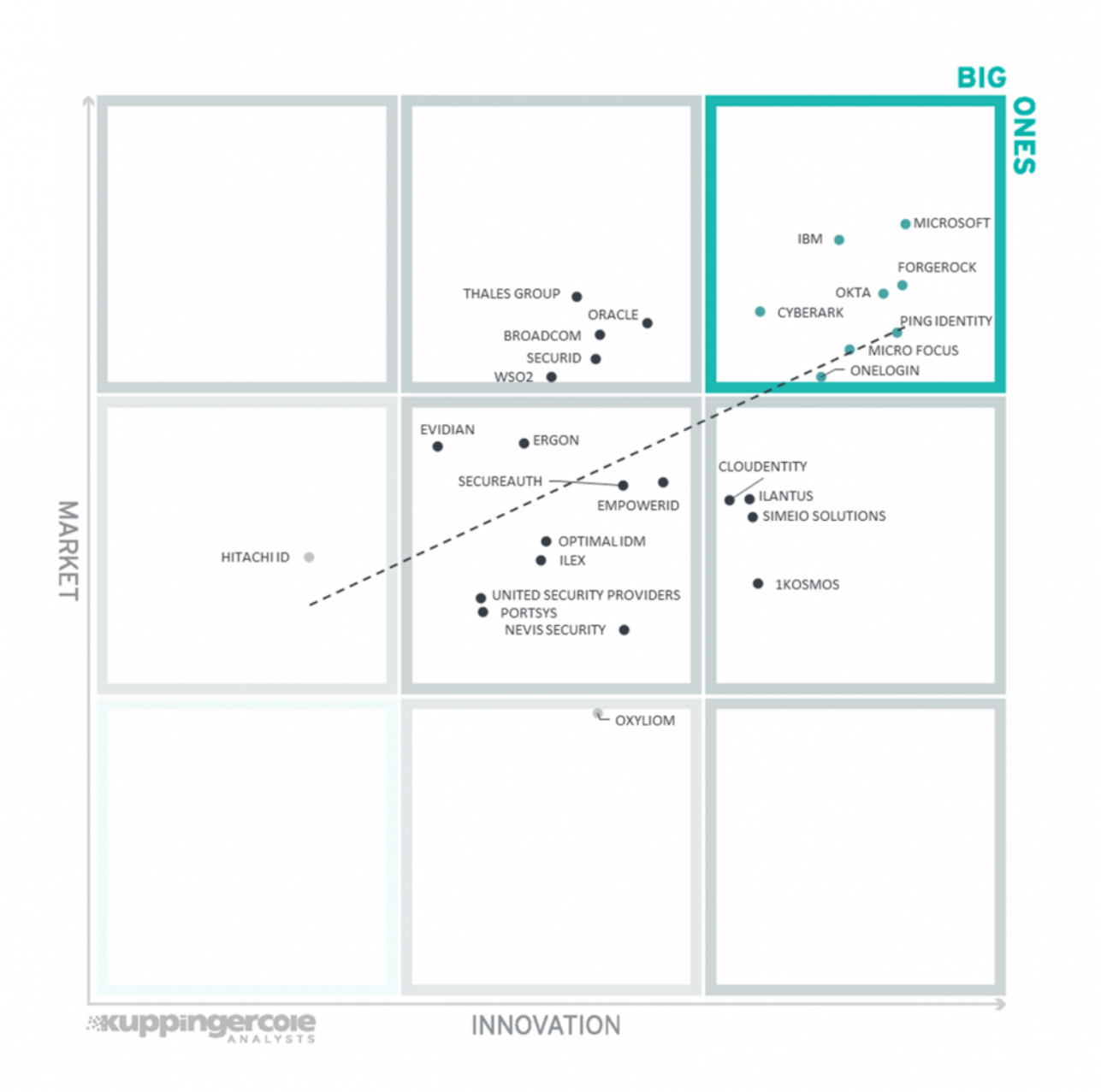


Figure 9: The Innovation/Market Matrix

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

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

In the upper right-hand corner box, we find the “Big Ones” in the Access Management market. We see 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) ForgeRock, Okta, CyberArk, Ping Identity, Micro Focus, and OneLogin, indicating that they haven't yet reached the same market position as the more established players.

Thales Group, Oracle, Broadcom, SecurID, and WSO2 are shown in the top middlebox with a stronger market, although less innovation than the leaders.

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

The segment in the middle of the chart contains a third of the vendors rated as challengers both for market and innovation, which includes (in alphabetical order) EmpowerID, Ergon, Evidian, Ilex, Nevis Security, Optimal IdM, PortSys, SecureAuth, and United Security Providers.

Only Hitachi ID appears in the middle left box, indicating market presence with lower innovation. Oxyliom is shown in the lower middle box with some innovation, although less in the market. 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 we have analyzed within this KuppingerCole Leadership Compass on Access Management Platforms. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

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

Product	Security	Functionality	Deployment	Interoperability	Usability
1Kosmos Block ID	●	●	●	●	●
Broadcom Symantec Access Management	●	●	●	●	●
Cloudentity Dynamic Authorization Fabric	●	●	●	●	●
CyberArk Identity	●	●	●	●	●
EmpowerID	●	●	●	●	●
Ergon Airlock Suite	●	●	●	●	●
Evidian Suite	●	●	●	●	●
ForgeRock Identity Platform	●	●	●	●	●
Hitachi ID Bravura Identity	●	●	●	●	●
IBM Security Verify	●	●	●	●	●
Ilantus Compact Identity	●	●	●	●	●
Ilex Sign&go Global SSO	●	●	●	●	●
Micro Focus NetIQ Access Management	●	●	●	●	●
Microsoft Azure Active Directory	●	●	●	●	●
NEVIS Security Identity Suite	●	●	●	●	●
Okta Identity Cloud	●	●	●	●	●
OneLogin Trusted Experience Platform	●	●	●	●	●
Optimal IdM OptimalCloud	●	●	●	●	●
Oracle OCI Identity and Access Management	●	●	●	●	●
Oxyliom Solutions GAÏA Trust Platform	●	●	●	●	●
Ping Identity PingOne Cloud	●	●	●	●	●
PortSys Total Access Control	●	●	●	●	●
SecureAuth Identity Platform & Identity Store	●	●	●	●	●
SecurID	●	●	●	●	●
Simeio Identity Orchestrator	●	●	●	●	●

Product	Security	Functionality	Deployment	Interoperability	Usability
Thales SafeNet Trusted Access	●	●	●	●	●
United Security Providers Secure Entry Server	●	●	●	●	●
WSO2 Identity Server	●	●	●	●	●
Legend		● critical	● weak	● neutral	● positive	● strong positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
1Kosmos	strong positive	neutral	positive	weak
Broadcom Inc.	positive	positive	strong positive	strong positive
Cloudentity	strong positive	positive	neutral	positive
CyberArk	strong positive	positive	positive	strong 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	strong positive
Hitachi ID Systems	weak	neutral	positive	neutral
IBM	strong positive	strong positive	strong positive	strong positive
Ilantus Technologies	strong positive	positive	critical	positive
ILEX International	neutral	neutral	strong positive	neutral
Micro Focus	strong positive	positive	strong positive	positive
Microsoft	strong positive	strong positive	strong positive	strong positive
NEVIS Security AG	positive	weak	positive	weak
Okta	strong positive	strong positive	strong positive	strong positive
OneLogin	strong positive	positive	positive	positive
Optimal IdM	positive	neutral	positive	neutral
Oracle	positive	strong positive	strong positive	positive
Oxyliom Solutions	neutral	critical	positive	weak
Ping Identity	strong positive	positive	strong positive	positive
PortSys	neutral	neutral	neutral	weak
SecureAuth	positive	positive	positive	positive
SecurID	positive	positive	strong positive	positive
Simeio Solutions	strong positive	positive	positive	neutral
Thales	positive	strong positive	strong positive	strong positive
United Security Providers	neutral	neutral	positive	weak
WSO2	positive	positive	positive	positive
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

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

Spider graphs

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

- **Federation, SSO, & Session Management:** The depth in which solution supports Identity Federation, Session Management & SSO is provided and its support of standards. Identity Federation ability to supply Service Provider (SP) and/or Identity Provider (IdP) functionality and federation provisioning to cloud services, for example. The solution's use of APIs/ SDKs to expose federation services, consume third-party identities, and social media integration are also considered. Session Mgmt & SSO looks at the depth to which the solution can handle user web sessions, session protection, ability to detect session attacks as examples. Also, the solution's ability to provide Web SSO, Enterprise SSO, and supported SSO mechanisms and secure token translation are evaluated as well.
- **Authentication:** The breadth of authentication support for multiple form factors and support for step-up authentication is measured, as well as the depth of contextual and risk-adaptive authentication. Also considered are various aspects of contextual attributes at each interaction channel and layer, for example.
- **Authorization & Policy Management:** This category looks at the solution's level of policy management and the ability to manage access using authorization features. Examples include the types of policies available using ABAC, RBAC, and/or CBAC principles for example, dynamic vs. coarse-grained policies, the capability to make rule-based decisions, and the ability to define and test policies using authoring/editing tools as examples.
- **API Security:** This section evaluates the level of API security such as protecting APIs against other attacks such as API authentication & authorization, validating API calls against API schema, scanning and/or filtering traffic, or API key management, to name a few API security features.

- **Analytics and Access Intelligence:** This looks at the level of analytics and access intelligence is used within the Access Management solutions.
- **Fraud Detection:** This category measures the solution’s level of fraud detection and mitigation abilities. Some capabilities include collecting and analyzing information for fraud prevention, User and Entity Behavior Analytics (UEBA), detect unauthorized account takeover, user and device profiling, orchestration of fraud signals, and identity proofing.
- **UI, Dashboards & Reports:** This section looks at the solution's overall user interface usability as well as its ability to provide a consolidated view and management of all access, regardless of where the solution is deployed. Centralized visibility often features a single pane view via a dashboard and provides visibility to users, threats, policy management, licenses, configuration, etc. Also elevated is the solution's ability to demonstrate compliance, support auditing, and forensic activities through capabilities such as logging a user's access to resources or administrators' changes to the system and running out-of-the-box, ad-hoc, or custom reports in various formats.
- **Admin & DevOps Support:** This category measures the ability to provide IT environmental assistance options for administrators and the operations team to support their tools, automation, and continuous integrations. Also evaluated is the vendor's ability to support developers using the solution's APIs through documentation, tutorials, tools, knowledge-base, and community support/platform for developers.

5.1 1Kosmos

1Kosmos was founded in 2018 and is headquartered in New Jersey. They address the consumer and workforce identity management markets with its blockchain ID solution aimed at returning secure identity control to the user, emphasizing reducing fraud. 1Kosmos is a decentralized identity (DID) and distributed identity attribute aggregator. Offered in this Leadership Compass is the BlockID platform that provides a suite of products for enterprise use (BlockID Workforce), private consumer use (BlockID Customer), and identity verification (BlockID Verify).

1Kosmos offers a single platform implemented as microservices in a product suite. Its authentication service supports a good range of OTPs, QR codes but a small set of popular authenticator apps. Good biometric authenticator options are given, including Android and iOS facial and fingerprint, as well as more advanced voice recognition and iris scan biometrics. 1Kosmos also provides its own authenticator, which is FIDO2 certified but also supports Yubico, Trust Key, Thales, OneSpan, Solo Keys, Kona. BlockID supports contextual and risk-adaptive authentication via user location and device and that they are using to logon. Contextual attributes can be used in access policies that can trigger step-up authentication such as a higher level of biometrics based on the sensitivity of the transaction. Access policies are managed through the administrative portal and stored centrally. User's access can be managed through RBAC, RAdAC, and user-group based policies. Delegated policy management is supported through the BlockID administration portal that utilizes the concept of communities within the platform. User browser sessions are managed through the server cache or browser cookies. Good detection of sessions attacks is also given. Support for SSO across multiple web applications as well as for non-web applications such as IT systems desktop apps, thick clients, etc. Identity federation includes SP and IdP functionality as well as user control and consent capabilities. A wide range of federation related standards are also supported.

BlockID recently updated its administrative portal to allow for user management, enrollment of user passwordless access and defining authentication for an organization. Dashboards are provided to monitor threats define authentication policies and policy enforcement. User self-service gives end-users visibility into their ID profile, apps, and devices, reducing the need for help desk intervention, and protecting against fraud. Also provided is a state machine-based graphical authentication and authorization flow editor to orchestrate and set up rules. Strong fraud detection capabilities are given through some native fraud detection capabilities and enhanced with third-party fraud detection and prevention tools such as Behaviosec, IDDataWeb, Imperva, and iovation. Detection of unauthorized account takeover uses a machine-learning behavioral profiling engine, global profiling, and device network reputation. Also, strong decentralized identity & verifiable credential support is given.

BlockID as SaaS supports public and private cloud and hybrid deployment models. The BlockID platform is delivered as container-based on Kubernetes, which is deployed to multiple cloud providers, such as AWS, GCP, Azure, and Oracle Cloud. Supported container-based platforms include Docker, Red Hat, and all Kubernetes distributions. A wide range of IaaS platforms is also supported. The solution is not offered as a managed service. However, it can be white-labeled by a managed service provider. There are no operational infrastructure requirements other than the broker component requires Linux and currently

requires Java JDK. The BlockID platform provides APIs for its proofing, authentication, and platform management. Supported API protocols include REST, JSON-RPC, gRPC, and Webhooks, as some examples. BlockID provides both web SDK for mobile applications such as Android and iOS and web SDK to enable passwordless access into applications. SDKs for Java, Python, and JavaScript programming languages are also supported. 1Kosmos has been independently certified to support compliance with the ISO/IEC 27001 standards, as well as certified by FIDO, NIST 800-63-3, and is currently undergoing SOC2 Type II certification.

The 1Kosmos BlockID platform provides good core access management with some interesting features, including strong fraud detection and support for verifiable credentials. 1Kosmos customers are primarily in North America with a growing presence in the APAC region supporting mid-market to enterprise organizations. 1Kosmos appears in both the product and innovation leadership categories which should be of interest to organizations in North America.

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

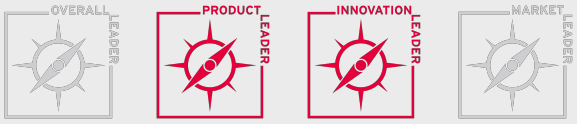
Strengths

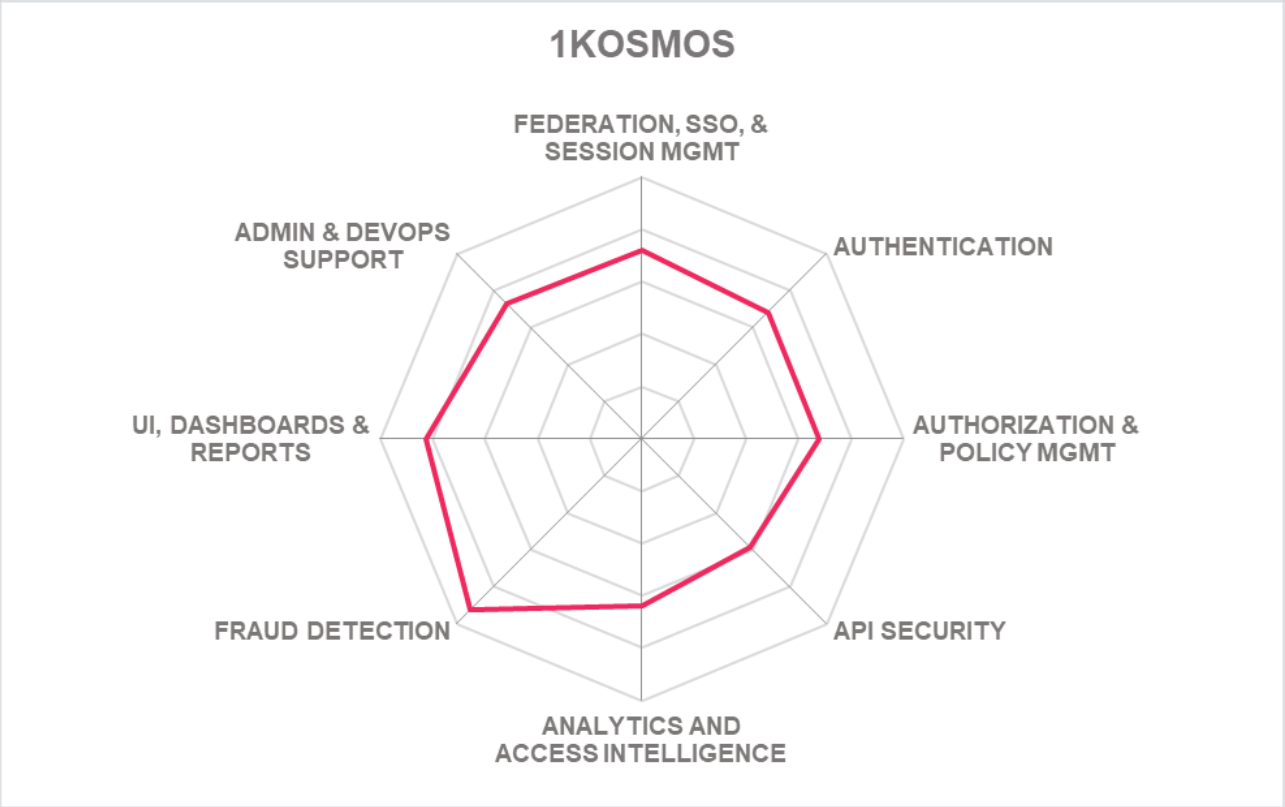
- Fraud detection
- Admin UI, dashboard capabilities
- OOB GDPR and operations reporting
- Identity federation
- SSO and session management
- Authorization and policy management
- Authentication
- Delegated policy management support
- Graphical flow editor
- Verifiable credential support

Challenges

- Little market visibility outside of North America and the APAC regions
- Small, but growing partner ecosystem
- Limited selection of popular authenticator apps and hardware tokens supported
- SCIM based provisioning to cloud services is not supported
- The company must still convert a critical mass of users and enterprises to establish its ecosystem.

Leader in




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

5.2 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 many customers worldwide but estimates that a small fraction of these customers uses products from the Symantec Identity Security portfolio, including 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 is implementing an IAM Fabric platform utilizing shared services built on a more modern architecture that integrates tighter with its other offering. Business services are layered on top of this architecture, such as VIP Authentication Hub that can be combined with Symantec SiteMinder giving context-aware authentication policies, password-less/MFA, and risk factors to make authorization decisions. 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 exists within SiteMinder and the Broadcom IAM Fabric although modeling of Resource Server permissions is from the API Gateway portion of the Broadcom offering.. A good breadth of authentication methods that includes basic password, OTP, QR Code, apps, biometric, FIDO, and hardware tokens 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, RAdAC, ReBAC or user-group based is available. The administrative UI provides a policy editing capability, although policy testing tools are not provided. Basic role management requires features of Symantec IGA, a separate, but complementary offering.

Broadcom SiteMinder offers logging of user authentication and access activity as well as audit trails of administrative activity. SiteMinder does not offer OOB reports. Instead, it directs its log information to a 3rd party reporting system. Identity authentication events are provided in a Grafana dashboard.. 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. Fraud detection and prevention delivered via the Authentication Hub extension is comprehensive for affecting authentication flows. Additionally, there is support for call outs to external intelligence sources via a service provider interface.. However, SiteMinder offers a continuous assessment of an end user's device via its Enhances Session Assurance with the DeviceDNA feature. Third-party verifiable credential providers can be used in Government use cases that include smart card issuers of the US DoD PIV cards & eID cards in Belgium.

Broadcom SiteMinder is primarily software-based that can be deployed to supported operating systems on-premises or in IaaS. Symantec VIP (MFA) is delivered via SaaS. An optional Virtual Appliance is provided for Symantec IGA. The Symantec IAM Fabric Security Services Platform is micro-service based, containerized, and supports K8s. SiteMinder can also be offered as a managed service by 3rd party service providers. SiteMinder provides SOAP, REST, LDAP, and RADIUS interfaces. SCIM support is provided by Symantec Directory and Symantec IGA, and VIP Authentication Hub uses webhooks to call out to integrated

services. Additional SiteMinder integration options include Perl scripting support and an SDK for custom authentication development. Support is also given for Swagger Codegen and opensource tools to simplify server code generation for 20+ languages and client SDKs in 40+ languages. Good support for 3-party services such as Threat Intelligence or EPP solution via API or SDKs is given.

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. However, Broadcom's IAM Security Fabric approach is moving in a positive direction. Broadcom has a global presence with customers focused primarily in North America but a relatively smaller number of specialized integration partners than other international IAM suite vendors.

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

BROADCOM

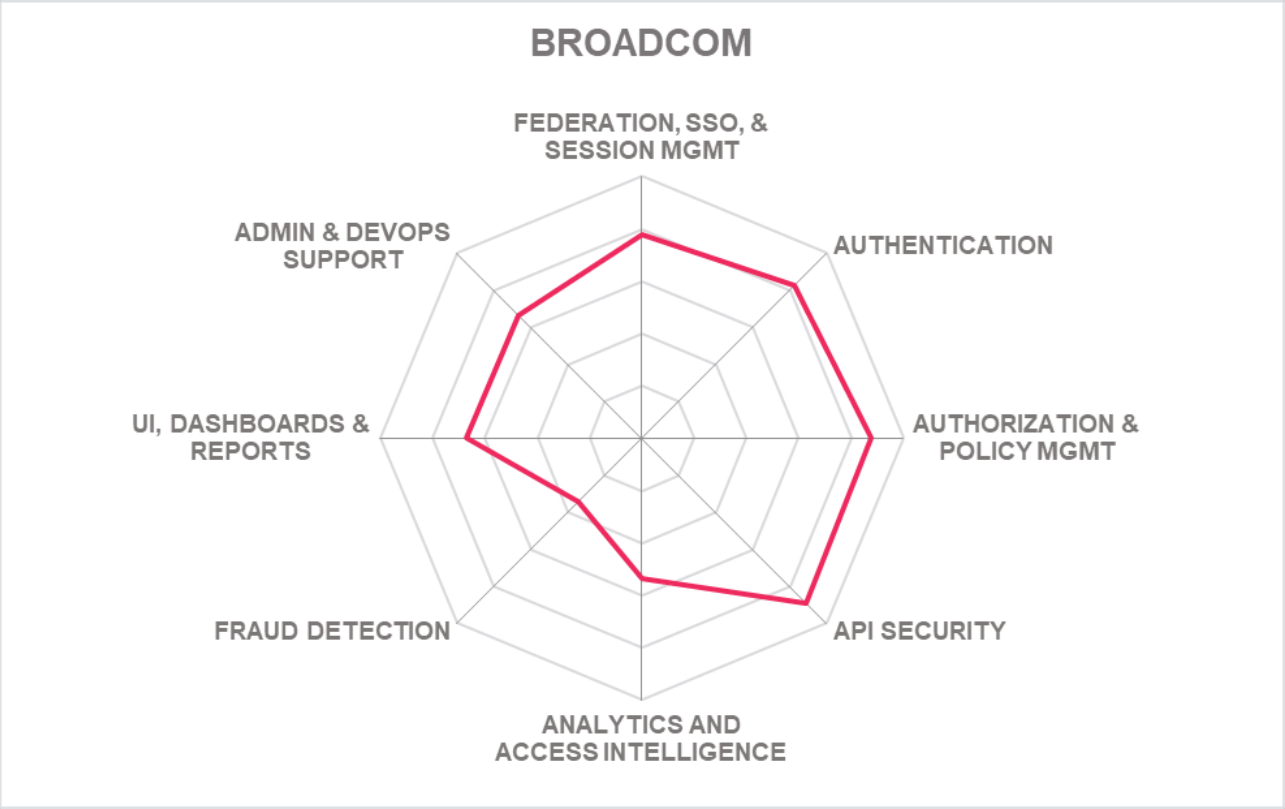
Strengths

- Good federation, SSO, & session management capabilities
- Breadth of authentication methods
- Contextual and risk-adaptive authentication
- Authorization and policy management
- API security
- Utilizes a modern IAM Security Fabric platform
- Third-party verifiable credential providers can be used in Government use cases
- 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, with strong customer support regardless of geographic location
- Analytics and other access intelligence rely on third party solutions
- SiteMinder lacks OOB reporting capabilities
- Weak fraud detection support
- Wide focus on other capabilities such as API Security Management. or PAM, although not delivered directly from SiteMinder

Leader in


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

5.3 Cloudentity

Cloudentity is a privately held identity and access management company headquartered in Seattle, WA. The company introduced its CIAM.next platform in 2018 as a cloud-native identity and authorization platform that separated authentication away from authorization 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 platform for traditional and API-driven Access Management solutions.

Cloudentity provides a public or private SaaS platform (which can optionally be deployed private by or for customers) that automates the discovery, identity context, 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 authorization-based orchestration with external APIs or microservices. Cloudentity features extend existing infrastructure through open standards to integrate identities beyond people, including workloads, applications, APIs, and IoT devices. Cloudentity provides centralized access control ranging from fine-grained authorization to fine-grained consent on individual data objects with distributed policy decisions to provide continuous and contextual authorization on a transactional basis. Cloudentity supports basic authentication methods such as username/password, OTPs, FIDO2 and support for popular authenticator apps. Mobile device biometric support for Android and iOS is available. Support for hardware token authenticators other than YubiKey. Good support for contextual and risk-adaptive authentication is given. Good federation support is available, and for most federation-related standards with exceptions like WS-Federation. Cloudentity's scale allows them to provide transactional authorization, where tokens are short-lived and minted for individual transactions. A variety of different session attacks, usage anomalies can be detected and dynamically protected against. SSO and API access control is achieved through reverse proxy sidecars, existing API Gateway(s), web server proxy for web-based applications, but SSO for non-web applications/ IT systems (Desktop apps, thick clients, etc.) require direct integrations unless they can be configured as OAuth clients or OIDC relying parties. However, password vaulting is available for applications that don't support proxy or web-server agent technology.

Cloudentity features strong API security features and protects against the OWASP API top 10 by providing plug-ins for popular API Gateways, Kubernetes, service meshes, and FAAS platforms. Cloudentity provides data lineage and tagging for sensitive information, IdP discovery for mapping to existing IAM infrastructure and distributed policy decision agents called Authorizers that provide API & service discovery, and distributed PDP authorization. For fraud detection, Cloudentity provides account takeover protection against session replay attacks (transactional sessions). Insecure OAuth Flows and transactional step-up authentications. External fraud scores can be pulled in and leveraged during policy evaluation via RESTful API callouts, and third-party fraud detection/prevention tools are used through integrations with Akamai, Imperva, Webroot, and Fastly. All report-related data is accessible via API queries. Support for verifiable credentials is on Cloudentity near-term roadmap, although integrations to third-party verifiable credential providers is possible today. Major compliance frameworks are available out-of-the-box, such as GDPR, NIST SP 800-53, -171, and PCI DSS. Cloudentity also offers full compliance with Open Banking UK, Open

Banking Brazil, CDR, and FDX with FAPI Advanced standards. In addition, IGA and/or AG related reports are available out-of-the-box.

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 , LGPD, CDR, and CCPA and has recently been certified for both SOC 2 Type 2 and ISO 27001 compliance.. 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, gRPC, GraphQL, SQL, LDAP, SCIM, and LDAP. SDKs are generated on the fly to provide SDKs for over 40 different programming languages and variants.

Cloudentity serves mid-market to enterprise organizations, with customers in North America, LATAM, EU, and APAC. Cloudentity's Dynamic Authorization Fabriccould be considered unorthodox from other traditional Access Management solutions, it provides a modern Zero-Trust approach to Access Management use cases for APIs and legacy Apps. Cloudentity provides some very innovative features to unify access controls to data across identity providers and applications with data governance in an easy to use and flexible way, which should be of interest to potential customers.

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

CLOUDENTITY

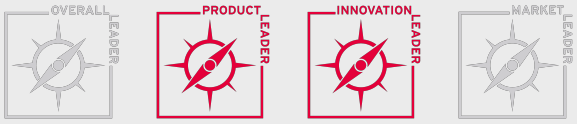
Strengths

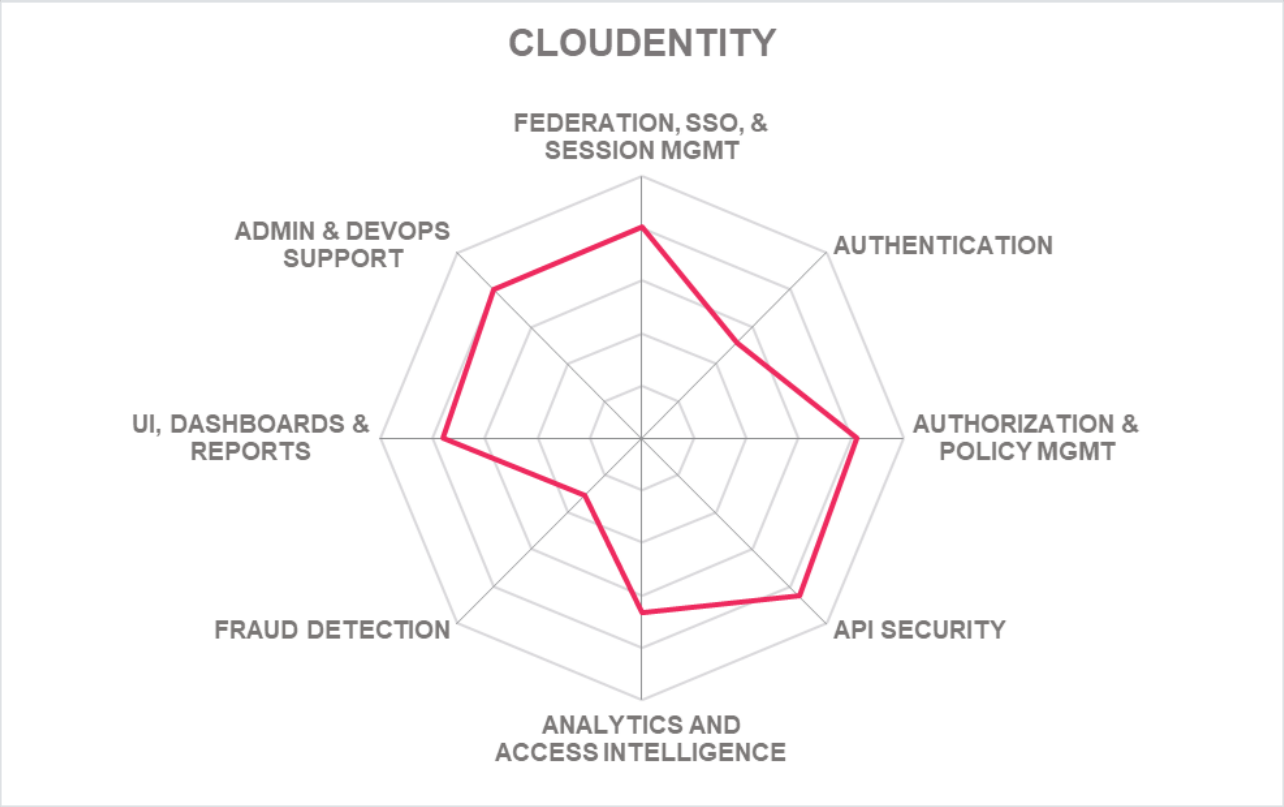
- Good federation, SSO, and session management support
- Authorization and Policy Management
- Strong API security
- Advanced OAuth (mTLS, FAPI 1&2) support
- Good Admin and DevOps support
- Reporting API & OOB compliance framework support
- Flexible drag and drop Data Linage UI
- Highly scalable TPS
- Data governance controls
- Good access control for both front end and back-end apps

Challenges

- Somewhat limited breadth in authenticator options (e.g., hardware tokens, QR Code)
- Limited fraud detection support
- Missing verifiable credential support, although on its near-term roadmap
- SSO for non-web-based applications not supported

Leader in




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

5.4 CyberArk

CyberArk, known for its Privileged Access Management (PAM) solution, acquired the Idaptive identity platform in mid-2020. In this Leadership Compass, CyberArk offers its CyberArk Identity product, which includes Workforce Identity and Customer Identity. Together with CyberArk Remote Access (formerly Alero), it provides the capabilities for Access Management.

CyberArk Identity offers a breadth of authentication methods, including OTP, QR Code, a variety of popular authenticator apps, mobile Android, and iOS biometric support, except for voice recognition or iris scan authentication technologies. Support for FIDO U2F and FIDO 2 is also given. Good support for hardware tokens is also available. Risk-based authentication is part of the adaptive SSO and MFA offering, which covers all contextual use cases evaluated in this report, with the exception of device-based contexts. CyberArk Idaptive stores all its access policies centrally in its cloud directory. CyberArk Identity provides a configurable rules-based GUI as well as a JavaScript-based policy scripting engine. Policy lifecycle is exposed via APIs. CyberArk Identity supports standard federation protocols such as SAML, OIDC, WS-Federation, OAuth 2.0, JWT, and SCIM, allowing the federation of identities to SaaS and on-premises applications. The solution provides good session protection and can detect multiple types of session attacks. The CyberArk Identity offers a modern UI that is easy to navigate and use. Its User Behavior Analytics provides built-in reports and dashboards with a flexible and customizable widget framework. Missing are reports for major compliance frameworks such as GDPR or SOX, for example, out-of-the-box, although CyberArk recently added the ability to see how customer MFA policies align to NIST Authenticator Assurance Levels. Good set user self-service capabilities are provided for user self-registration or user profile setting through its UI. Integrations with the ServiceNow ITSM solution is also possible.

CyberArk Identity provides good API security features such as rate-limiting, DoS protection, analyzing protocol-specific attacks through input sanitization and validation. Also, CyberArk Secrets Manager offers built-in API key management. CyberArk Identity also uses its proprietary real-time event and user behavior analytics for Online Fraud Detection. No third-party fraud detection or prevention tools are used. Integrations to Account Take Over (ATO) Detection & Prevention tools are not available OOB. Support for decentralized identity & verifiable credentials is missing, although integrations with third-party identity proofing providers is supported.

CyberArk Identity is a multi-tenant SaaS cloud solution that runs on the AWS platform. It supports public cloud and hybrid deployment models with its App Gateway, enabling VPN-less, Zero Trust access, SSO, and access management capabilities back to on-premises applications and services. The cloud service supports a Managed Service Provider mode, where MSPs can manage the entire lifecycle of customer tenants. CyberArk Identity services are 100% built upon RESTful APIs. 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, and Go programming languages.

CyberArk, established in 1999, has a strong offering for Access Management, with its CyberArk Identity offering serving primarily mid-market to enterprise organizations. CyberArk mainly focuses on the US as the

primary market with growth in the EMEA, APAC, and Latin America markets supported by a good partner ecosystem. CyberArk appears in all Leadership segments with a well-balanced set of features for Access Management.

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

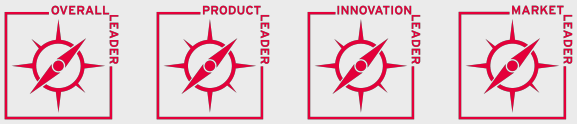
Strengths

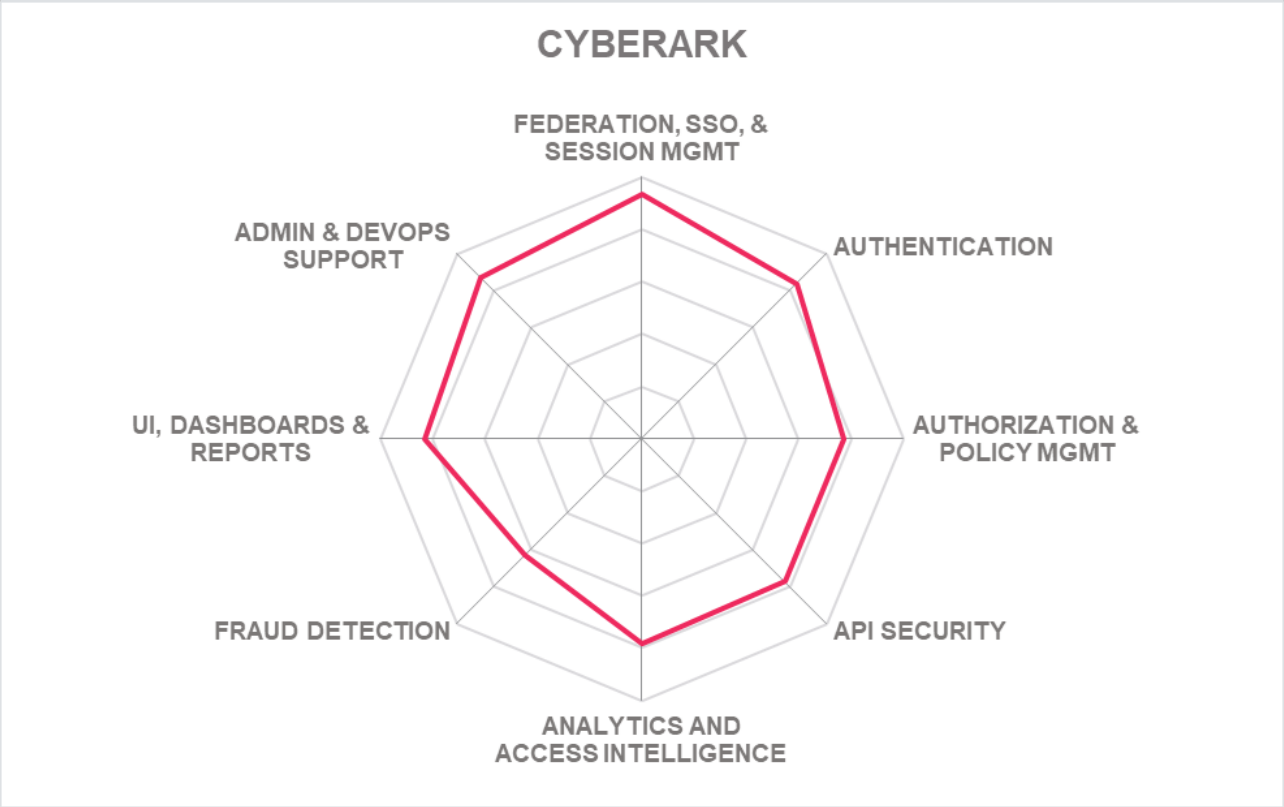
- Strong federation, SSO, & session management
- Breadth of authentication options
- Authorization & Policy Management.
- Good API security
- Fraud detection features
- Good use of analytics and access intelligence
- Good UI, dashboard and reporting
- Admin & DevOps support
- Partner ecosystem

Challenges

- Strong focus on the US as the primary market with growth in EMEA, APAC, and Latin America markets
- Missing decentralized identity & verifiable credentials support
- Limited third-party integrations to fraud detection & protection solutions OOB
- Good risk-based authentication with the exception of device-based contexts

Leader in




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

5.5 EmpowerID

Founded in 2005 and based in Ohio (US), EmpowerID offers multiple products in a suite which includes EmpowerID Password Management, Group Management, Dynamic Group Management, Lifecycle Management, Advanced Lifecycle Management, Single Sign-On, Multi-factor Authentication, Access Recertification, Risk Management (SoD), Advanced Risk Management (SoD), Policy-Based Access Control, and Privileged Access Management as components of its Access Management portfolio.

EmpowerID offers a range of authentication options, including OTPs, QR Code, some of the more popular authenticator apps (e.g., Duo, Google, LastPass, Microsoft), Android & iOS mobile biometrics, and FIDO 2, and a good set of hardware token options. Although a more advanced iris scan authenticator is available, voice recognition is not. Support for contextual and risk-adaptive authentication is part of the MFA service and focuses on the device, user location, and some network contexts. EmpowerID provides good session management capabilities and the ability to detect various types of session attacks. SSO can be achieved by either reverse proxy or web-server agents. Along with the solution's support for managing access of users based on ABAC, RBAC, CBAC, RAdAC, ReBAC, and user group-based controls, EmpowerID has implemented the full UMA 2.0 Specification within the product and extended its authorization engine with PBAC. This allows the registration of resources, OAuth UMA scopes, etc., via the EmpowerID UI or API. Management of roles is also given. Identity federation capabilities and standards are well supported, and provisioning to cloud services such as Azure, AWS, Salesforce, ServiceNow, SAP HANA, SAP Ariba is supported out-of-the-box. Also, a ServiceNow ITSM integration is possible.

EmpowerID offers a modern UI with a visual workflow editor. Also provided are many out-of-the-box reports, including many that support major compliance frameworks like GDPR, PDS2, HIPAA, SOX, etc. API security can be accomplished via an API Gateway, UMA, RBAC, ABAC, PBAC, and Scopes. Basic API protocol-specific attacks can be detected, and other features such as API key management, schema validation, rate liming, and content filtering. Fraud detection, as part of the EmpowerID Access Management, is limited. However, EmpowerID can trigger adaptive authentication workflows, which can force identity verification or proofing. Verifiable credential support is currently not supported but is on the roadmap. Integrations with third-party identity proofing providers such as RSA and Equifax options are available.

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, RedHat, SUSE and runs on Azure AKS, making it Kubernetes compatible. Microsoft SQL database server is required at deployment. Microsoft IIS and Azure application servers are also supported. EmpowerID provides a fully integrated directory, although standard LDAPs and Microsoft AD/AAD are supported. All EmpowerID functionality is exposed via REST API. SCIM support is given too. EmpowerID Workflow Studio IDE supports creating customer APIs - to be published and run on EmpowerID or Azure as App Services or Functions.

EmpowerID customers are primarily mid-market to enterprise-size companies located in North America and the EMEA region. EmpowerID provides Access Management functions and services that are largely

targeted at meeting the common access management requirements of mid-market to enterprise-size companies. 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 along with a useful visual workflow editor 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	●●●●●
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●●

empowerID

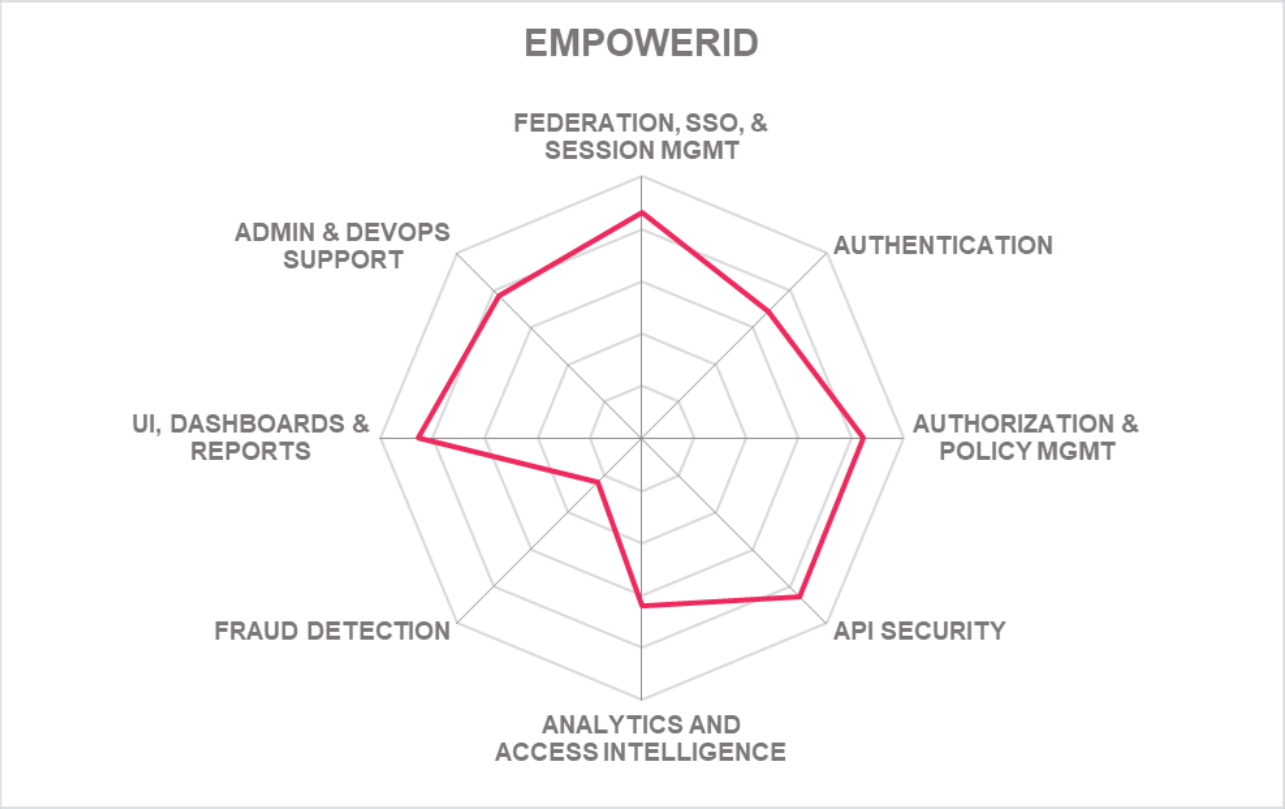
Strengths

- Good federation, SSO, & session management
- Strong authorization & policy management
- Range of authentication options
- API support and security
- UI, Dashboard & reporting
- Admin & DevOps support
- FIDO 2 support
- Full UMA 2.0 capabilities
- Good support services
- Certified compliant with multiple standards

Challenges

- Limited market presence outside of the NA and EMEA regions
- Runs on and remains focused on Microsoft technology
- Smaller but selective partner ecosystem mainly concentrated across Europe
- Limited fraud detection capabilities
- Missing verifiable credential support, although it's on the roadmap

Leader in


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

5.6 Ergon

Airlock is a single security product by Ergon with multiple services within the Secure Access Hub. The Secure Access Hub includes a WAF, API Gateway, and IAM that leverages the synergies from the close integration between components such as the Airlock WAF policy enforcement point for access decisions by Airlock IAM. Both the Airlock Gateway and Airlock IAM will be considered in this Access Management Leadership compass.

Airlock provides a good range of authentication options which includes SMS OTP, mTAN/eTAN, QR Code, Client-side certificates, Mobile push notifications, a few select authentication apps such as Google and OneSpan Mobile ES, RADIUS, Android and iOS mobile biometrics, and a number of popular hardware token options. Passwordless authentication is accomplished using FIDO2 and Airlock 2FA support. Risk-based and adaptive authentication is also available, supporting some device, user, and location-based contexts that can be used within access policies. Authentication flows can be defined using a system of tags and roles and a choice of authentication factors to be used. Authentication factors can be combined with social logins for step-up authentication scenarios, for example. Access policies are managed and stored centrally, along with policy authoring tools provided that support ABAC, RBAC, CBAC, PBAC, RAdAC, and user-group-based access management. Delegated policy management is not given. 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. The close integration of the WAF and cIAM offering allows for more advanced protection for session management and SSO. 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 available. Airlock includes a good administrative UI as well as a user-self-service that includes self-registration with access request/approval workflows support along with other capabilities such as password reset, account unlock. REST APIs are provided to access the built-in reporting solution as an option to the UI. Kibana-based dashboards are given and may be customized. All reporting is given via the dashboards, and reports for major compliance frameworks such as GDPR, SOX, etc., are not available OOB.

Strong API security is given derived from its long history in the WAF market, focusing on content security. A wide range of protocol-specific attacks can be detected. API DoS protection through rate-limiting and geolocation-based protection is provided. Good API key mechanisms are used. The Airlock WAF provides good blacklist content filtering that can be applied to JSON attributes as well. API statistics, monitoring, and reporting are available, as well as support for microservice architectures via a containerized Microgateway component. Fraud detection capabilities have some dependencies on integrations with IBM Trusteer Pinpoint Solution and/, or Webroot Threat Intelligence feeds. Unauthorized account takeover can be detected using built-in anomaly detection, as well as session hijacking can be detected too. Airlock IAM can both provide digitally signed credentials as well as receive and verify for verifiable credentials support. Third-party identity proofing providers can be integrated using extension points and providing custom plugins. SwissID by SwissSign is a third-party verifiable credential provider that can be used. Airlock also gives end-users informed consent and control over who has access to their identity data.

Ergon Airlock can support on-premises, full multi-tenancy for cloud, and hybrid deployment models. The Airlock Gateway is available as an appliance using an ISO file installed onto a Hypervisor. It includes a hardened OS and networking, REST-based APIs, configuration center UI, and reporting. The Microgateway version of the Airlock Gateway is delivered as a Docker container focused on security features such as deny rules, JWT validation and processing, OpenAPI specifications, and uses DSL for configuration. Airlock IAM is delivered as a software component, not an appliance. It can be deployed either as a self-contained application or as a Docker image that can be run on any container platform. The product is not available for IaaS installations, although a SaaS and managed service is provided through partner companies, but not directly by Ergon. The solution's functionality is primarily available via REST-based APIs, although LDAP, RADIUS, and Java are supported. Android and iOS SDKs are available for the 2FA solution, and a Java API is available for cIAM extensions and customizations. Customizing and styling of the Login application can be accomplished through Javascript and CSS.

Ergon is a Swiss-based company established in 1984 with customers primarily in the DACH EMEA region with some growth in APAC followed by the North American region targeting medium and mid-market organizations. However, Airlock is growing its enterprise presence. Their partner ecosystem is again focused on DACH. Airlock has well-established and mature set of Access Management products with a strong focus on WAF, API Gateway, cIAM, and strong authentication in one solution. Ergon Airlock Secure Access Hub continues to grow its feature set and remains an interesting alternative to other solutions within the DACH EMEA region.

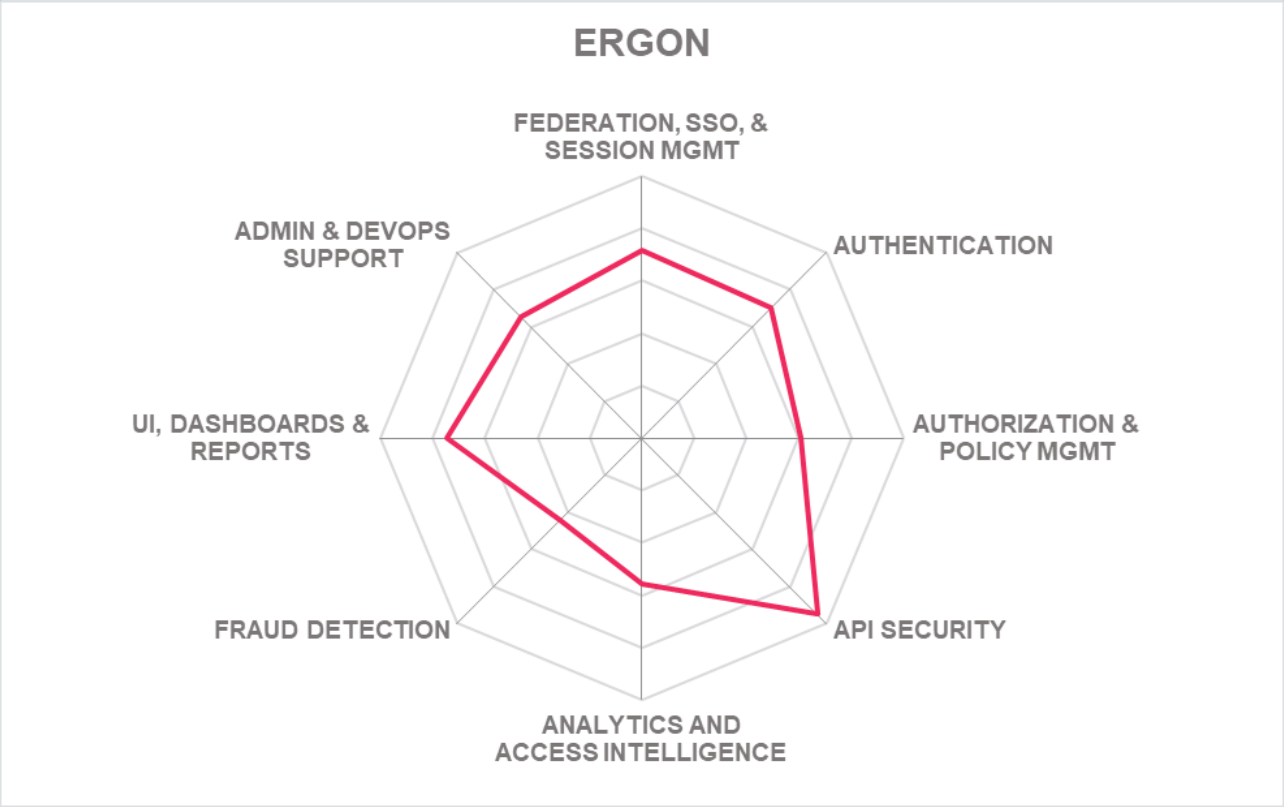
Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●○

Strengths

- Strong API security
- Federation support
- Strong SSO & session management
- Passwordless authentication options
- Adaptive Authentication
- OOB Airlock 2FA
- Verifiable credential support
- Good UI, dashboards, user self-service
- Modern product deployment & delivery options

Challenges

- Small partner ecosystem & limited global reach
- Somewhat limited fraud detection capabilities
- Limited API protocol support outside of REST
- Missing delegated policy management
- Missing OOB reports to major compliance frameworks such as GDPR, SOX, etc.


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

5.7 Evidian (was acquired by Atos)

One of the leading IT service providers in Europe, Evidian is a dedicated business branch of the Cybersecurity division of French group ATOS since 2015. The Evidian Suite includes multiple products such as Evidian Web Access Manager (WAM), and Evidian IDaaS as its Access Management portfolio evaluated in this Leadership Compass, although some capabilities are possible via integrations with Evidian Identity Governance and Administration (IGA), and Evidian Analytics and Intelligence (A&I).

Evidian provides a wide array of supported authentication methods, including OTP options, QR codes, client-side certificates, popular authenticator apps, Android & iOS mobile biometrics, with a wide range of supported hardware tokens. Push notification-based Authentication is also supported, via the “Evidian Authenticator” app. Evidian supports full FIDO compliance, and can be used with Yubico, Neowave, and Google (Titan) authenticators, for example. Adaptive authentication supports the device, network, and user-based contexts. For location-based contexts, the Evidian WAM engine can determine the geocode of a user’s IP. 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 but don't 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 requires the use of 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.

The UI is modern, with user-friendly layouts that are flexible and fully featured. User self-service registration is supported through HTML forms or social ID provider integrations. User self-service registration access/approval requests workflows require an Evidian IGA integration, although consent management workflows are integrated within the Evidian WAM & IDaaS offering. Good reporting capabilities are given as well as out-of-the-box reports for major compliance frameworks such as GDPR, HIPAA, PCS DSS, and SOX. Evidian WAM and Evidian IDaaS can act as an OAuth2.0 authorization server 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. Fraud detection is not supported, although Captcha can be used to prevent automated bot-based accounts creation. Support for verifiable credentials includes integrations with regional third-party verifiable credential providers such as FanceConnect, SwissID, Itsme, Belgium eID card, and ProSantéConnect.

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. The product is available for the most popular IaaS platform installations. All administration actions can be performed via REST, Webhooks, SCIM, LDAP, RADIUS 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 customers are mid-market to enterprise-level companies, localized mainly in the EMEA region followed by APAC and some growth in North America. With a regional but healthy partner ecosystem across Europe, ATOS acquisition helped Evidian gain access to large customers and enter new geographies, and its roadmap and vision will continue to move Evidian in a more positive direction.

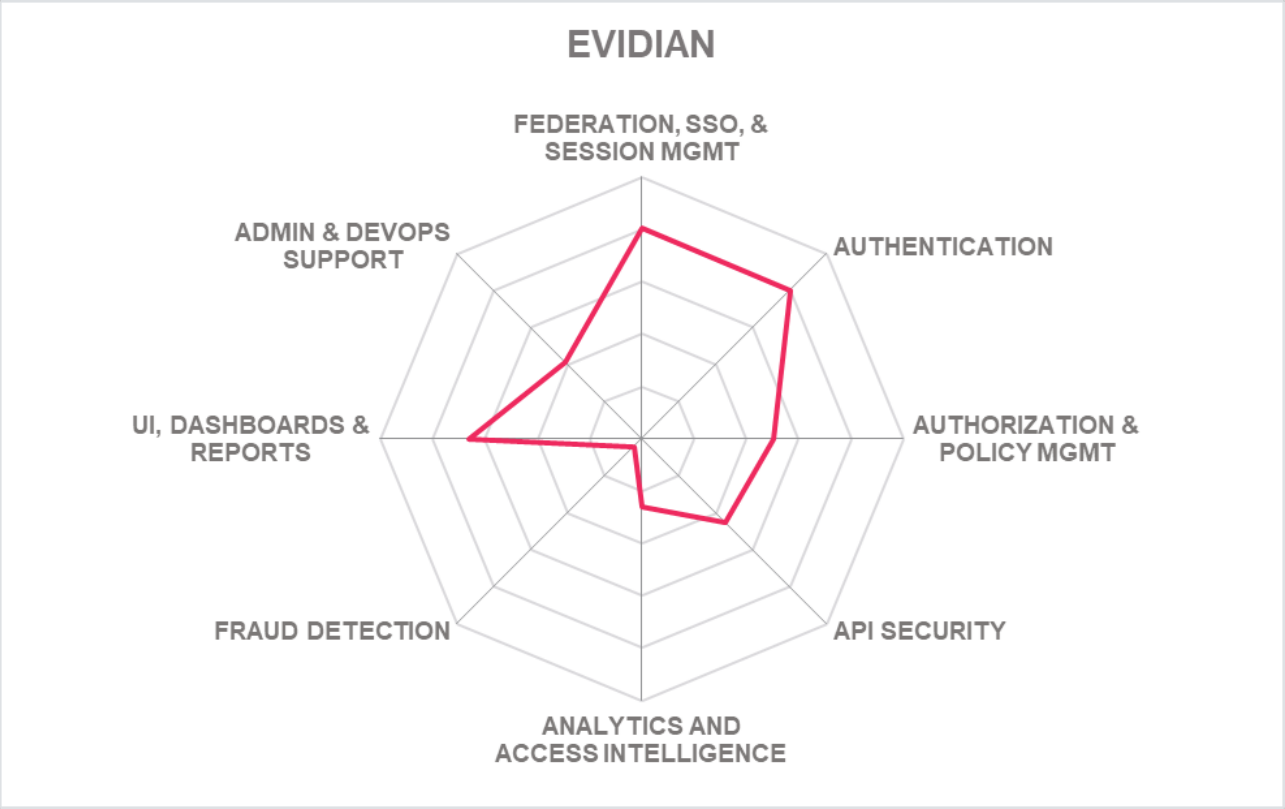
Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●○○
Usability	●●●●○

Strengths

- Mature Web Access Management
- Good breadth of supported authenticators
- Good federation support
- Session management & SSO
- Adaptive authentication
- Good UI, dashboards, and reporting
- Built-in consent management
- Integrates with regional third-party verifiable credential providers
- Tightly integrated suite of products

Challenges

- Limited presence and partner ecosystem outside Europe, and the APAC regions
- Moderate authorization & policy management
- Limited API security
- Limited admin & devops support
- Weak fraud detection options
- Weak analytics and access intelligence


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

5.8 ForgeRock

ForgeRock is a leader in the IAM space, providing a single integrated suite based on their Identity Platform. More recently, ForgeRock has become a publicly traded company. 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 advanced biometrics like iris scan, voice recognition, and full FIDO/FIDO2 support. All adaptive authentication contexts evaluated are supported, including device, network, user, and location context attributes that can be used within access policies. ForgeRock supports ABAC, RBAC, CBAC, PBAC, RAdAC, ReBAC, and user-group based policy principles, as well as delegated policy management. ForgeRock Access Management supports many standard federation related protocols, such as SAML, XACML, OAuth2, OIDC, and SCIM, as well as GOV.UK Verify Identity Assurance Hub Service SAML Profile, FICAM (U.S. Federal Identity, and Credential and Access Management SAML Profile. SSO is achieved by reverse proxy or web-server agents. SSO is supported across multiple web or non-web applications. Good support for session detection and protection is also given across a range of attack types. Good OOB integrations with UEM solutions such as Citrix, and Mobile Iron, or Endpoint Threat Protection Platforms like ThreatMetrix, ID Dataweb, and EnTrust are given.

The ForgeRock platform UI is modern with useful dashboards and good mobile device support. The centralized dashboard can be branded and themed but is currently not customizable, although it's on its roadmap to do so. The Intelligent Authentication Trees features allow customers to quickly build complex authentication policies leveraging authenticators and risk intelligence sources to address high security and high assurance use cases. The graphical workspace UI is straightforward to use, making it easy to see the entire flow graphically rather than paging through multiple configuration screens. The ForgeRock platform 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 third-party gateways. 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. Fraudulent account creation is detected through third-party detection solutions, proofing services, and bot protection. ForgeRock does not provide direct support for verifiable credentials, although support for identity proofing through built-in extensibility points in the ForgeRock Identity Platform with integration support available through its Trust Network of technology partners.

ForgeRock Identity Platform is a developer and administrator friendly product. ForgeRock solutions support on-premises deployments or deployments within IaaS providers such as AWS, GCP, and Azure. ForgeRock does not offer a managed service directly, although a good partner network offers the ForgeRock Identity

Platform as a managed service. 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 Docker containers as well as scripted installers. All of the ForgeRock platform functionality is exposed through SOAP, REST, gRPC, Webhooks, LDAP, and RADIUS APIs, with half of the functionality available through a CLI. Both APIs and CLI are documented on ForgeRock's developer portal. Available SDKs support Android, iOS, and JavaScript programming languages. ForgeRock Identity Platform components do have a dependency on Java technology requiring a Java runtime environment using either Oracle JDK11 or OpenJDK 11, although when delivered as a docker container OpenJDK 11 and Tomcat are provided. ForgeRock Identity Cloud requires no additional databases, directories, or application server.

Established in 2010, ForgeRock is now a publicly-traded company that targets large enterprise customers primarily in North America, followed by EMEA, with a growing presence in the APAC region. ForgeRock provides a well-balanced solution for Access Management and continues to invest in product development. This investment shows their rapidly improving capabilities, placing them in the Innovation Leadership category. Overall, ForgeRock is amongst the leading-edge vendors in the IAM space and should be considered in product evaluation.

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

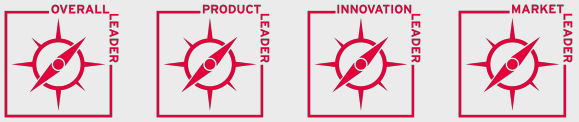
Strengths

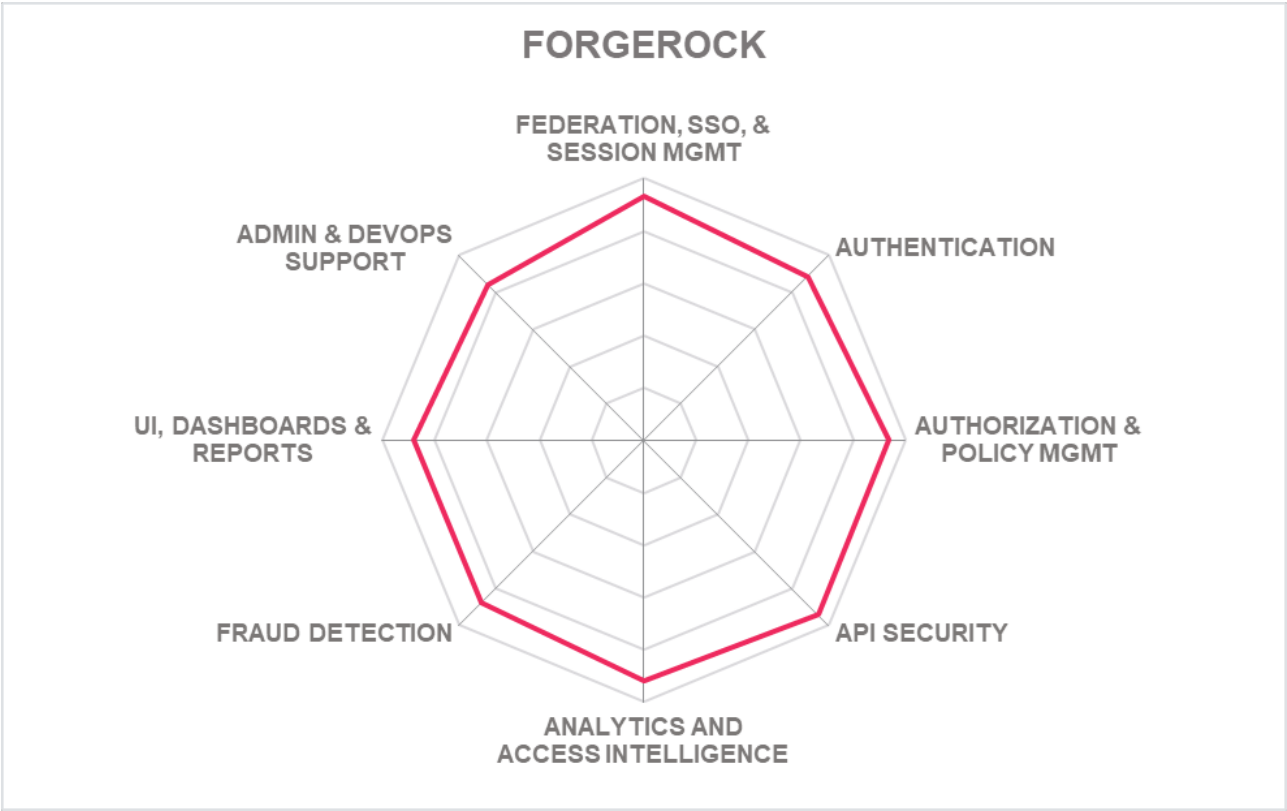
- Strong federation capabilities
- SSO, & session management
- Wide range of authentication options
- Strong Adaptive/Risk-based authentication
- Good analytics and access intelligence
- Intelligent configuration flow UI
- Good reporting capabilities
- Strong API security
- Fraud detection
- Good third-party integration options OOB
- Good DevOps support
- Broad partner ecosystem support

Challenges

- ForgeRock Identity Platform components have Java runtime dependencies, although the SaaS delivery option is fully turnkey
- Supported container-based platforms are limited to Docker
- Missing direct support for verifiable credentials, although third-party integration support available
- UI dashboard is not customizable beyond branding and theme, although its currently on its roadmap

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


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

5.9 Hitachi ID Systems

Hitachi ID Systems is well established in the Identity Management market and is headquartered in Calgary, Alberta, Canada. Its security product line is under its Bravura Security Fabric platform and offers other integrated IAM components. The common platform provides consistent UIs, database, connectors, API throughout the other components in the Hitachi ID security fabric. The Bravura Pass solution provides management of credentials across IT systems and applications, while the Bravura Identity supports identity lifecycle management automation, access governance, workflows, and analytics.

Hitachi ID's Access Management offering supports a limited set of authenticator options and includes some OTP, QR Codes, and a few popular authentication apps and hardware tokens. Missing are biometric options and FIDO support. The base authentication service supports contextual and adaptive authentication features. Contextual attributes include good user context, some device, and network, but missing location-based contexts. Contextual attributes can be used in the solutions policies, supporting ABAC, RBAC, CBAC, PBAC, ReBAC, and user groups. Both basic role management and role mining capabilities are also available. User browser session management is given using browser cookies, and various session timeout options are given, although the detection of session attacks is not. SSO is available across multiple web applications. Missing is SSO support for non-web applications and other IT systems (e.g., thick clients, desktop apps). The solutions support both SP and IdP federation functionality and support SAML 2 only at this time. Hitachi ID has OAuth2, OIDC, and SCIM on its current roadmap.

The solutions administrative UI are basic, with some tab-based navigation and dashboard graphics. A user self-service management does not support self-service registration or workflows, but managed registration and self-service password reset capabilities are given. A good set of ITSM integration options include ServiceNow, Remedy, Remedyforce, Cherwell, CA Service Desk, Footprints, and HP Service Manager. A good set of reporting capacities and has a high number of out-of-the-box (OOB) reports, including some support for major compliance frameworks like GDPR and SOX and IGA related reports. Advanced Access Management capabilities such as fraud detection verifiable credential support are unavailable, and only minimal API security features are given.

Hitachi ID Bravura Pass and Hitachi ID Bravura Identity can be deployed on-premises, public, private, multi-cloud, or as a managed service. Hybrid environments between on-premises and the cloud are possible. The solutions can be delivered as either SaaS or software installed on a server. When running the solution as-a-service, customers can optionally deploy its connector proxy on-premise to integrate with on-premise applications. Both Windows Server with IIS and Microsoft SQL Server are required components, and a Windows Server OS is required for the connector proxy installation. The product is available for IaaS installation and supports AWS, GCP, and Azure. The Hitachi ID SaaS service itself is hosted on AWS. Almost all of the solution's functionality is accessible via APIs such as SOAP and REST. A SCIM API is not available at this time but is on Hitachi ID's current roadmap. CLI access to capabilities is included, and SDK is available for the C/C++ and Python programming languages. The product has been independently certified to support compliance with the FIPS 197 advance encryption standards.

Hitachi ID security customers are mid-size to enterprise organizations with a partner ecosystem primarily in North America, and with a footprint in the EMEA region and some presence in other parts of the world. Overall, Hitachi ID Bravura Identity is stronger as an IGA solution with less capability in Access Management, and Bravura Pass solution adds credential management to the combined feature set. Hitachi ID Bravura Pass and Hitachi ID Bravura Identity should be of interest to Bravura Security Fabric platform customers.

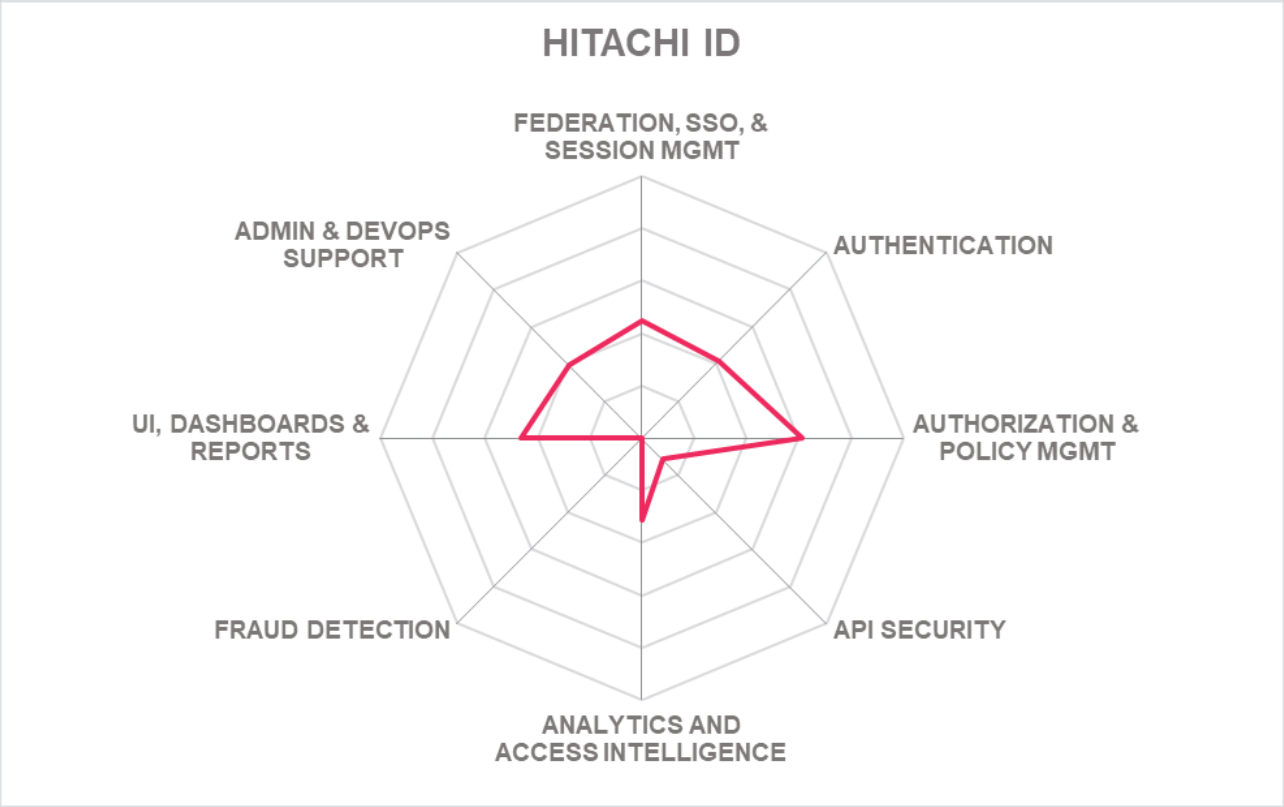
Security	●●●○○
Functionality	●●○○○
Deployment	●●●○○
Interoperability	●●○○○
Usability	●●●○○

Strengths

- Authorization and policy management
- Administrative UI and dashboards
- Basic, but well selected authenticator options
- Good set of OOB Reports
- Password management
- Basic device registration
- Good set of ITSM integration options
- Certified to support compliance with FIPS 197

Challenges

- Somewhat limited footprint and partner ecosystem outside of North America
- Required Microsoft technology only dependencies for on-premises deployments
- Missing SCIM support, although it's on the near-term roadmap.
- Missing FIDO and biometric authenticator options
- Missing fraud detection capabilities


HITACHI ID
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS AND ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS & REPORTS
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. In 2020, IBM 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 authentication apps 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. Passwordless authenticators are supported by FIDO2, QRadar, and third-party vendors such as BlokSec, or Keyless. Good contextual and risk-adaptive authentication functionality is with contextual support using user, device, network, location, and a range of available fraud factors. Support is also given for external risk engines such as QRadar UBA, Trusteer Pinpoint, and UEM. Access policies are managed and stored centrally with a policy authoring tool provided, although policy test tools are not. All user access principles such as ABAC, RBAC, CBAC, RAdAC, and user-group are possible and support external risk engines like QRADAR UBA, Trusteer Pinpoint, and UEM solutions. Delegated policy management is supported but limited to the selection of policies rather than the editing of policies. Good web session management is available, with a range of session attack detection. SSO is achieved through a reverse proxy and can be applied across multiple web applications. 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, SCIM, and WS-Trust federation-related standards.

IBM Verify provides a modern web UI with dashboards with various activity and usage widgets. User self-service is customizable or can be exposed via an API. Support for reporting is accessed through the SaaS native UI and QRadar on-premises. Missing is out-of-the-box reports for major compliance frameworks such as GDPR, PSD2, HIPAA, etc., although supported, can be given through QRadar. API security includes methods of DoS rate-limiting content filtering but not content-based routing. Also, a number of protocol-specific attacks can be analyzed, and there is some API firewall-like features that allow the identification of abuse. A WAF module that can detect a range of attack signatures is also available. In addition, the product includes a Security Token Service and some limited ability to use API key mechanisms to block anonymous traffic or control the number of calls made to an API. IBM Security Verify proprietary fraud detection uses fraud reduction intelligence sources and supports Online Fraud Detection (OFD). The solution uses in-network fraud reduction intelligence sources. The unauthorized account takeover detection is accomplished with a Trusteer integration on-premise or natively within the SaaS offering. IBM uses a range of technologies to detect fraudulent account creation. Generally available support for verifiable credentials is not given at this time, and missing support for out-of-the-box (OOB) integrations with third-party identity proofing providers are not available. However, the solution support integrations with third-party verifiable

credential providers such as Evernym, Trinsic, and others.

IBM Security Verify is a single platform built on a modern microservice-based architecture 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, container-based, or 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, GCP, IBM, and Oracle Cloud. Both Docker and Red Hat container-based platforms are supported. All of the IBM Security Verify functionality is available via APIs, in which SOAP, REST, WebSockets, SCIM, LDAP, and RADIUS protocols are supported. CLI support is given as well for on-premises solutions. SDKs for SSO, authentication & authorization APIs, configuration, DevOps, and mobile and web development include support for Android, iOS, Java, C/C++, Python, and JavaScript programming languages. ITSM support is given through IBM Security Resilient to remediate incidents in Verify by interacting with user profiles or ServiceNow through a ServiceDesk app.

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 stems from very mature products that have long existed in the market. IBM Security Verify provides both depth and breadth in feature support. It remains a leading product in this Access Management Leadership Compass and should be considered for enterprise product evaluation.

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

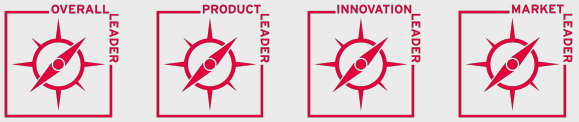
Strengths

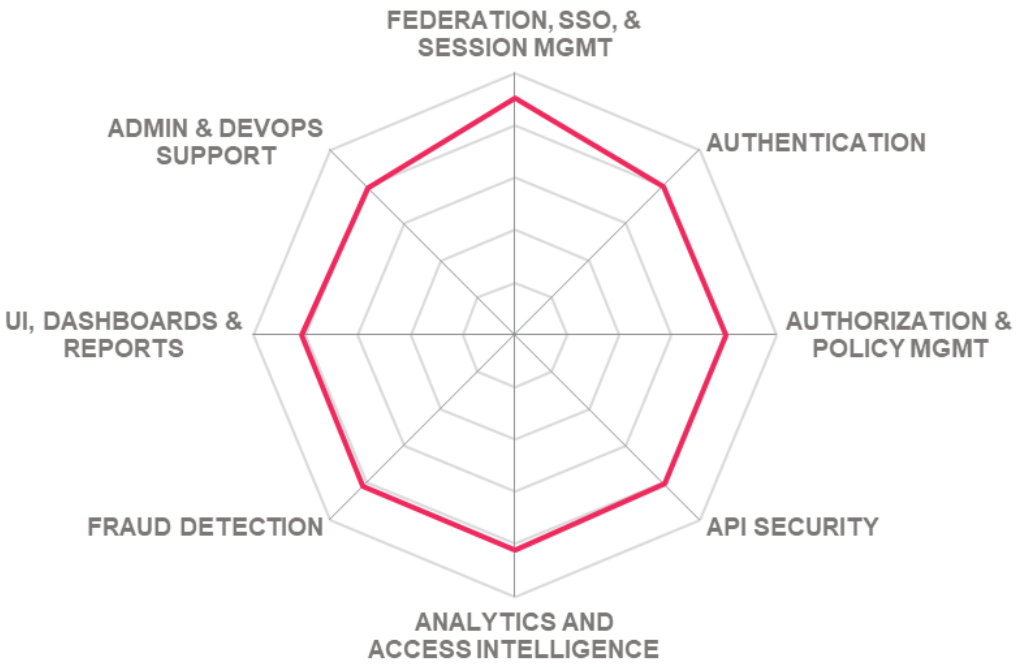
- Mature access management
- Strong and Adaptive authentication
- Session management and SSO
- Authorization and policy management
- API security
- Fraud detection
- Support for delegated policy management
- Admin & DevOps support
- Good compliance and certifications
- Strong partner ecosystem globally
- 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 OOB reports for major compliance frameworks, although supported through QRadar
- Limited verifiable credential support
- Limited third-party integration options to other solutions such as EDR, Analytics, AI/ML, ATO, fraud reduction intelligence sources, etc.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


IBM
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS AND ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS & REPORTS
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 implemented in a microservices architecture on a single platform with multiple services. The product services include 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 & U2F, FIDO2 are also supported. Risk-adaptive authentication is available with some support for the device, user, and network contexts, and Compact Identity requires extensions 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, RAdAC, ReBAC, and user-group access principles with basic role management support. Device management capabilities such as device registration and associated management is missing. Password management supports password syncing across multiple identity repositories and a range of password recovery options. Compact Identity also supports passwordless authentication on the Web and Desktop access. Session management includes web browser management using cookies and 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 both administrative and user self-service UIs that are functional with intuitive color-coded indicators, although the dashboard graphics are somewhat basic. Good reporting capabilities are given, including IGA related reports and support for some major compliance frameworks available out-of-the-box. The solution also supports Online Fraud Detection and third-party fraud detection prevention tools from Akamai, Arkose, Behaviosec, ThreatMetrix, and Webroot Threat Intelligence. The solution uses fraud reduction intelligence sources in-network or sources that are manually configured with coding and API calls to Securonix, Gurukul, and TransmitSecurity. For API security, Compact Identity protects all APIs via the OAuth framework. It provides a means to protect against DoS attacks and uses a WAF to identify other API abuses such as protocol-specific attacks. Mechanisms for API keys can block anonymous traffic, revoke access tokens upon threat detection, or filter logs by API key identifier.

Ilantus supports on-premises, cloud, and hybrid deployment models, delivered as SaaS or software deployed to a server or 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. A container-based delivery option supports Docker, Red Hat, and SUSE container-based platforms. For IaaS installations, Ilantus Compact supports most cloud platforms such as AWS, GCP, Azure, etc. A majority of features and capabilities are available via REST APIs. Other API protocols such as SOAP, WebHooks, SCIM, JSON-RPC, and XML-RPC are supported, although gRPC is

not. CLIs arguments are available for all bulk import operations, and SDK support for a wide range of programming languages is available but is limited to Identity and provisioning capabilities.

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 with IGA and Access Governance capabilities. Ilantus Compact Identity appears in both the Product and Innovation Leadership categories.

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

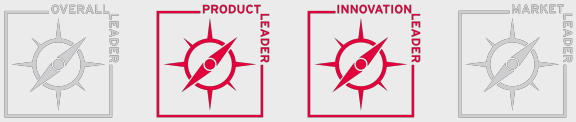
Strengths

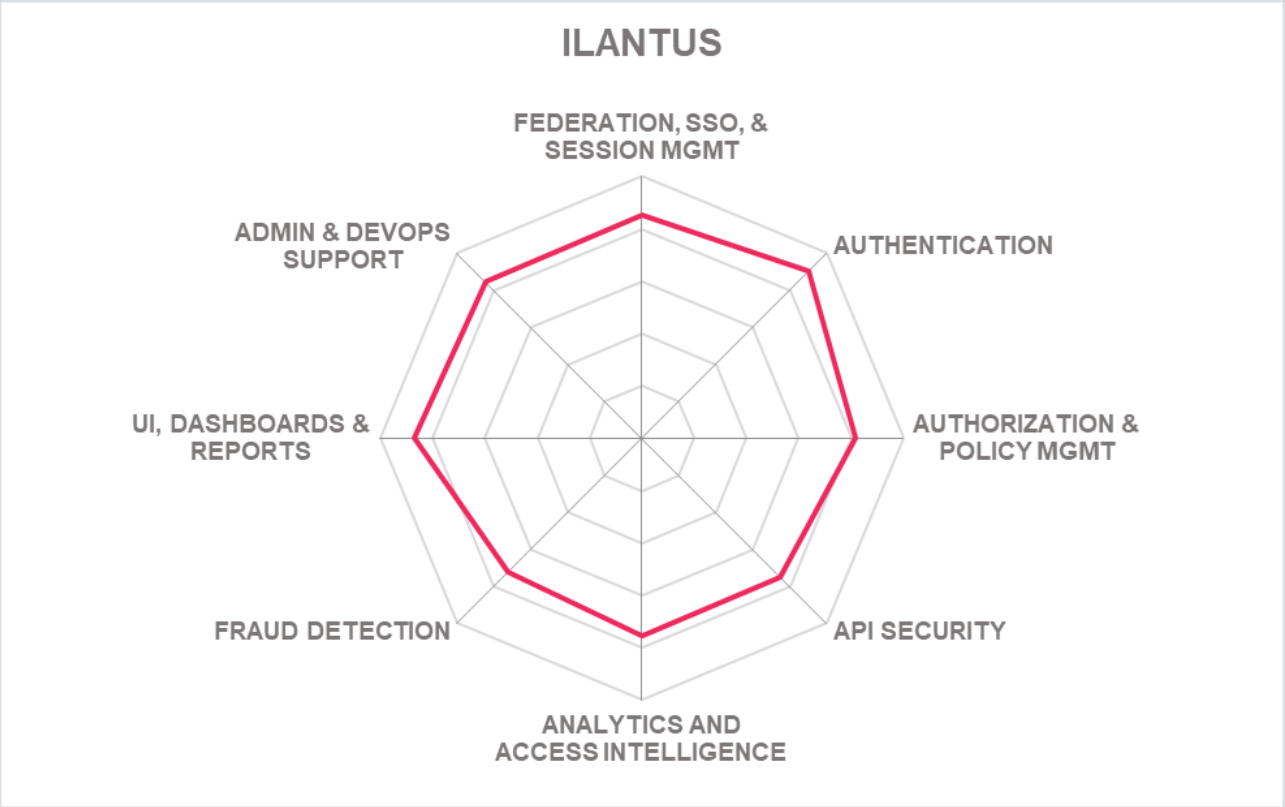
- Good authenticator options
- Authorization & policy management
- Identity Federation support
- Session management & SSO
- FIDO 2 authentication options
- Authorization & policy management
- Good reporting capabilities
- Modern UI and dashboards
- Verifiable credential support
- Admin & DevOps support

Challenges

- Customer presence is still primarily focused on the US and some APAC countries
- Moderate partner ecosystem focused in NA and APAC regions
- Focused on the mid-market
- Weak financial strength
- Limited capabilities available via SDKs
- Missing device management support

Leader in




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

5.12 ILEX International

For Access Management, Ilex provides “Sign&go Global SSO,” a unified SSO solution that includes multifactor and adaptive authentication, web access management, identity federation, and enterprise and mobile SSO capabilities. ILEX also offers Sign&go Authenticator for MFA and Sign&go CMS, allowing for the lifecycle management of authentication tokens.

Ilex Sign&go provides a single platform with modular services. A review of authentication shows strong support for most authenticators evaluated, including OTPs, QR Codes, popular authenticator apps, hardware tokens, and full FIDO support. Most biometric authenticators include Android and iOS facial and touch biometrics, voice recognition, vein technology with Idemia or Hitachi, and multibiometric with United Biometrics. Contextual and risk-adaptive authentication is also given that supports device, network, user, and location-based context-aware. Access policies are managed and stored centrally. Access of users can be based on ABAC, RBAC, CBAC, PBAC, RAdAC, ORBAC, and user group principles. Advances rules can be managed by its IDSPhere module, which is natively integrated into the Sign&go SaaS offering. User browser sessions are managed through browser cookies, and other session management controls for timeouts are given. The detection of session attacks is somewhat limited to session ID anomaly detection, although session ID lifecycle monitoring is available. Strong SSO can be used across multiple web applications, and SSO support is given to non-web applications such as desktop apps and thick clients, for example. With the exception of UMA, good identity federation and related standards are supported, such as SAML, OAuth, OIDC, WS-Federation, JWT, and SCIM. OOB third-party integrations include ServiceNow for ITSM, Proofpoint for threat intelligence, and Lexis Nexis for analytics and intelligence information.

Ilex Sign&go provides a basic but modern user and administration set of UIs with intuitive action icons and some graphical dashboard of the scope of access review. User self-service management includes registration workflows. A good set of out-of-the-box (OOB) reports are available, including IGA related reports. Missing are OOB reports for major compliance frameworks such as GDPR, HIPPA, or SOX, for example. Ilex's online fraud detection capabilities rely on a third-party integration with ThreatMetrix solution (LexisNexis), as well as some Inetum group solutions, like KDPrevent. ReCaptcha, Email Validation, Scan of a national identity card or passport via partners are techniques used to detect fraudulent account creation. Verifiable credential support is not provided natively, but integrations with third-party solutions like LexisNexis are possible.

Ilex Sign&go supports on-premises, public, private, and government cloud, as well as hybrid deployment models that can be delivered as SaaS, virtual appliance, container-based, software deployed to a server, or managed service. The container-based option supports both Docker and Red Hat platforms. For software deployed to a server, a wide range of operating systems are supported, including Windows, Linux, and Unix, as well as a number of popular application servers, directories, and databases, are supported. Running the solution as a service on-premises, only an eSSO agent is required to deploy the enterprise SSO module of Sign&go Global SSO. The SaaS option is hosted with a French cloud provider with both data and support services in France. APIs to the solution’s feature set are available via SOAP, REST, JSON-RPC, XML-RPC, and SCIM is supported. CLI access to functionality is supported, as well as SDK support that includes

Android, iOS, Java, and JavaScript programming language. Sign&go has been independently certified to support compliance with France cybersecurity, OpenID Foundation, UAF (used by the French Army) standards.

Ilex has a good mid-market to enterprise customer base with a moderate partner ecosystem, primarily within the EMEA region with some growth in the APAC region. However, with the Inetum acquisition of Ilex in late 2021, we expect an expansion in market presence. Ilex Sign&go provides strong core access management capabilities and the potential to grow into the more advanced areas of Access Management solutions seen in the market today. It will also be interesting to see how the recent acquisition by Inetum will impact its product development. Sign&go's unified SSO solution provides a good Access Management alternative solution set to consider in their primary geographic region.

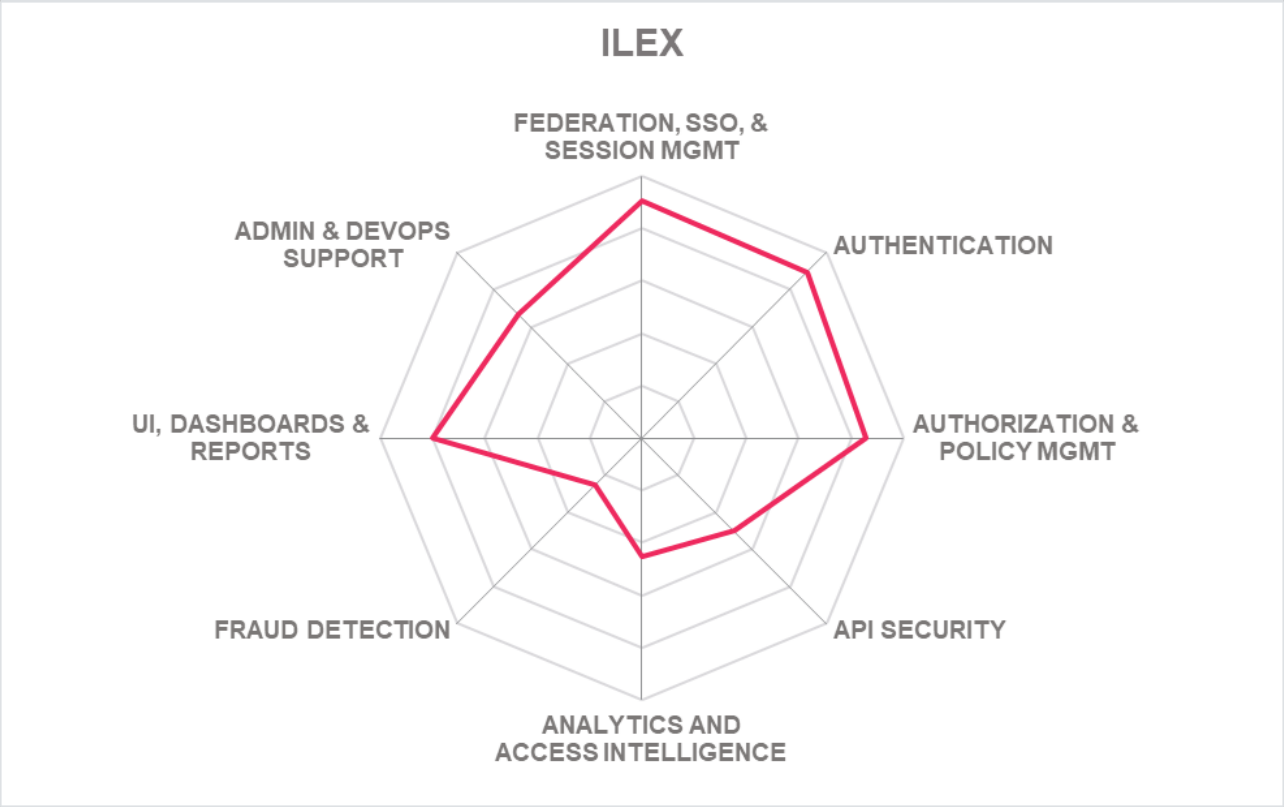
Security	●●●●●
Functionality	●●●●●
Deployment	●●●●○
Interoperability	●●●●●
Usability	●●●●○

Strengths

- Good identity federation
- Strong SSO support
- Session management
- Good authentication options
- Full FIDO support
- Good set of biometric authenticator options
- Authorization and policy management
- Comprehensive administration UI
- User self-service supports
- Good OOB reporting available

Challenges

- Customer and partner base are primarily limited to the EMEA region
- Weak fraud detection support
- Limited analytics and access intelligence, although third party integrations are possible
- Limited API security
- Missing verifiable credential support


ILEX
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS AND ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS & REPORTS
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 the spin-merger with HPE, and more recently, Interset to provide AI/ML capabilities into its security product line. Access Management is part of NetIQ within the Micro Focus CyberRes portfolio.

Core Access Management capabilities include good authentication method options with biometrics options for Android, iOS, and voice recognition. Some popular authentication apps and hardware token options are given, and FIDO UAF, FIDO U2F and FIDO2 are also supported. Risk-adaptive authentication is given with support for network, device, user, or location contexts, in which context attributes can be utilized with access policies. NetIQ Access Manager also provides a REST interface to interact with any external context parameters. Access policies are managed and stored centrally, and integration with external policy management tools through API integrations is also possible. It provides a flexible policy definition UI, and extension capabilities can support a combination of ABAC, RBAC, CBAC, RAdAC, and user-group factors that can be used for access policies. SSO is achieved through a reverse proxy. Good session attack detection, if provided, and protection from replay attacks, session renewal prevention, and device fingerprinting are given. Access Manager also offers a built-in Secure Token Service that supports secure token translation across applications and protocols. Good identity federation support is given for SP, IdP, as well as brokering capabilities. Also, coverage of federation-related protocols is supported. The Access Management platform supports major open standards and is independently certified to support compliance with Common Criteria EAL 3+, FIPS 140-2, and compatible with HSDP-12, PCI-DSS, and ISO 27002.

Micro Focus provides an impressive and modern administrative UI with useful dashboards. In addition, there is extensive out-of-the-box reporting that also support a wide range of major compliance framework. Good user self-service options with customizable UI look and feel and registration flow. 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, content filtering, rate-limiting, and detection of protocol-specific attacks. The API firewall type of features is 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. Online Fraud Detection is part of Micro Focus access management capabilities. The Micro Focus platform supports additional capabilities, which offer pre-built machine learning algorithms to detect financial fraud, compromised accounts, and privilege escalation attacks. Fraud reduction intelligence sources can come from in-network or third-party sources available with OOB connectors. OOB third-party fraud detection and prevention tool options include Behaviosec, Imperva, ThreatMetrix, and Webroot Threat Intelligence as some examples. Integrations to Account Take Over Detection & Prevention tools available OOB include Radware. NetIQ Access Manager supports verifiable credentials through integration APIs and workflows for validation of identities with external systems and Government digital identity services, for example. Third-party identity proofing providers such as Jumio and VerifyMe, among

others.

Micro Focus NetIQ Access Manager can support both on-premises and cloud deployment use cases. The hybrid model has some components that can be deployed on-premise and in a cloud service. Delivery options include virtual appliances, containers, and multi-platform software installations. The product is implemented as a microservices architecture with all components in the SaaS offering as microservices and cloud software offerings are a mix of microservice and traditional architectures. Support is also given for a range of container-based platforms such as Docker, Red Hat, SUSE, Amazon Kubernetes Services, Azure Kubernetes Services, and RHEL OpenShift. Access Management is also available via a managed service provided by Micro Focus partners. All 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. SCIM, LDAP, and Java APIs are also available. CLI is supported for administrative functions, updates, automation tasks, etc. SDKs are available for a wide range of programming languages. Out-of-the-box (OOB) third-party ITSM solution integrations include ServiceNow and Remedy, as well as their own Micro Focus SMAX. Other third-party integrations include threat intelligence, EPP, and EDR solutions. Microsoft Azure UEM and Micro Focus ZENworks integrations are also available OOB.

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, NetIQ Access Manager is one of the leading products in the Access Management market segment. They remain in the leadership categories for the product, market, and innovation segments, as well as in the overall leadership category. Micro Focus NetIQ Access Management is recommended for consideration for mid to enterprise organizations.

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

MICRO FOCUS®

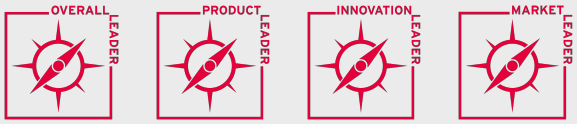
Strengths

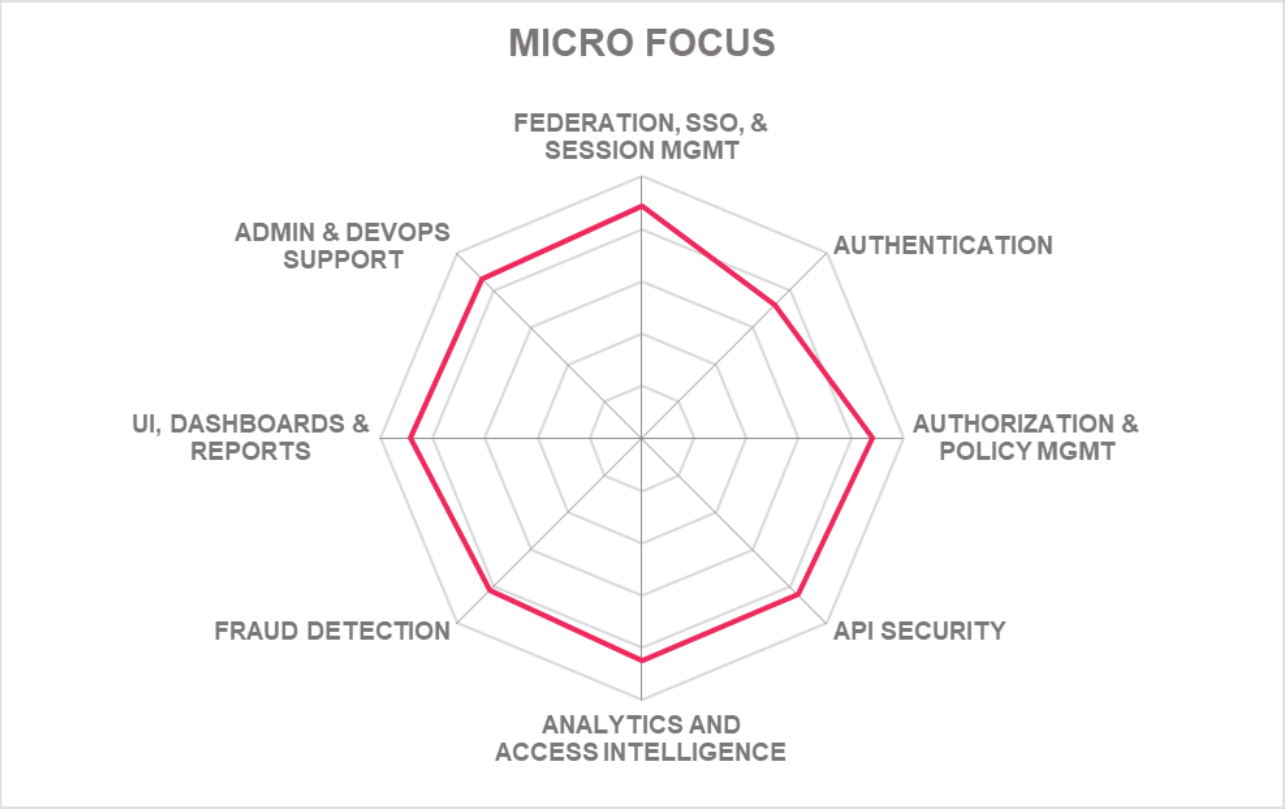
- Identity federation
- Session management & SSO
- Authentication support
- Authorization and policy management
- API security
- Fraud detection
- Good use of analytics and access intelligence
- Strong UI, Dashboards & Reporting
- Third-party integration options
- Verifiable credential support

Challenges

- Limited presence and partner ecosystem outside North America and the EMEA regions
- Enterprise-level product solution may exceed small-to-medium company requirements
- Cloud delivery does not support full multi-tenancy for all components, although on its near-term roadmap

Leader in




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

5.14 Microsoft

Microsoft Azure Active Directory (Azure AD) is an IDaaS that operates on a massive scale globally and runs notable first-party systems such as the Microsoft Office Suite and the Azure platform. Microsoft offers Azure AD as its primary IDaaS Access Management platform. Microsoft Azure Active Directory (Azure AD) provides Directory Services, Identity Federation, and Access Management from the cloud in a single integrated solution with extensive integrations as well as the ability to address traditional IAM (B2E), B2B, and B2C use cases.

Microsoft Azure AD gives strong support for Access Management capabilities. Most of the authenticators evaluated are supported with a few exceptions, such as the Google Titan hardware token, although Microsoft support's FIDO 2 complaint keys. 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, ABAC, PBAC, RAdAC, and ReBAC principles are supported, and Azure AD roles can be assigned to users, groups, and service principals. Role management is given. Conditional Access can target users who are members of dynamically-generated groups. Supervised machine learning detects a wide range of session anomalies and attacks. SSO is available for application supporting standard protocols like SAML 2, OAuth 2, OIDC, and WS-Federation both natively and also 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. Conditional Access insight report provides a view of policies with monitoring tools to see what is covered by a given policy. An analysis of a customer tenant environment for specific regulatory compliance is available through its Microsoft Defender for Cloud. Also, the Identity Secure Score provides recommendations to guide customers on the best practice for the Azure AD service.

One of Microsoft's Azure AD's more significant capabilities evaluated in this report is its fraud detection. Microsoft's fraud detection capabilities are proprietary and powered by its own machine learning system. Online fraud detection (OFD) occurs across the entire IAM stack. Azure AD Identity Protection uses machine learning and heuristic systems to detect compromise in real-time and offline risk detection. Third-party fraud detection and prevention tools include Akamai, Telesign, and RSA NetWitness. Integrations to Account Take Over (ATO) solutions can use Arkose Labs. Azure AD Verifiable Credentials, which is currently in preview, allows customers to issue and verify Verifiable Credentials. Integrations with third-party identity proofing providers include Acuant, Au10tix, Jumio, Idemia, LexisNexis, Onfido, Socure, Vu, CLEAR , Experian and IDology as well. using an extensible model based on DIF standards. Azure AD uses OAuth 2.0 / OIDC tokens issued by Microsoft to protect its APIs. Both content filtering and content-based routing are given protection against a wide range of API-related attacks.

Microsoft SaaS offering includes Azure Azure AD, Azure AD B2C, Azure AD Domain Services, and on-premises software products, which have 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 integrating 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 and 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 Azure Active Directory functionality is available via REST, JSON-RPC, XML-RPCSCIM, LDAP, RADIUS, Java, AMQP, and UDP Socket API.

Microsoft Azure Active Directory (AD) is a leader in the product, market, innovation, and overall segment of this Access Management Leadership Compass. Microsoft continues to move Azure AD in a positive direction with innovative capabilities. Azure AD should be considered for cloud-based Access Management and extending on-premises AD infrastructures to the Cloud.

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

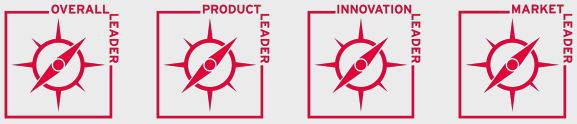
Strengths

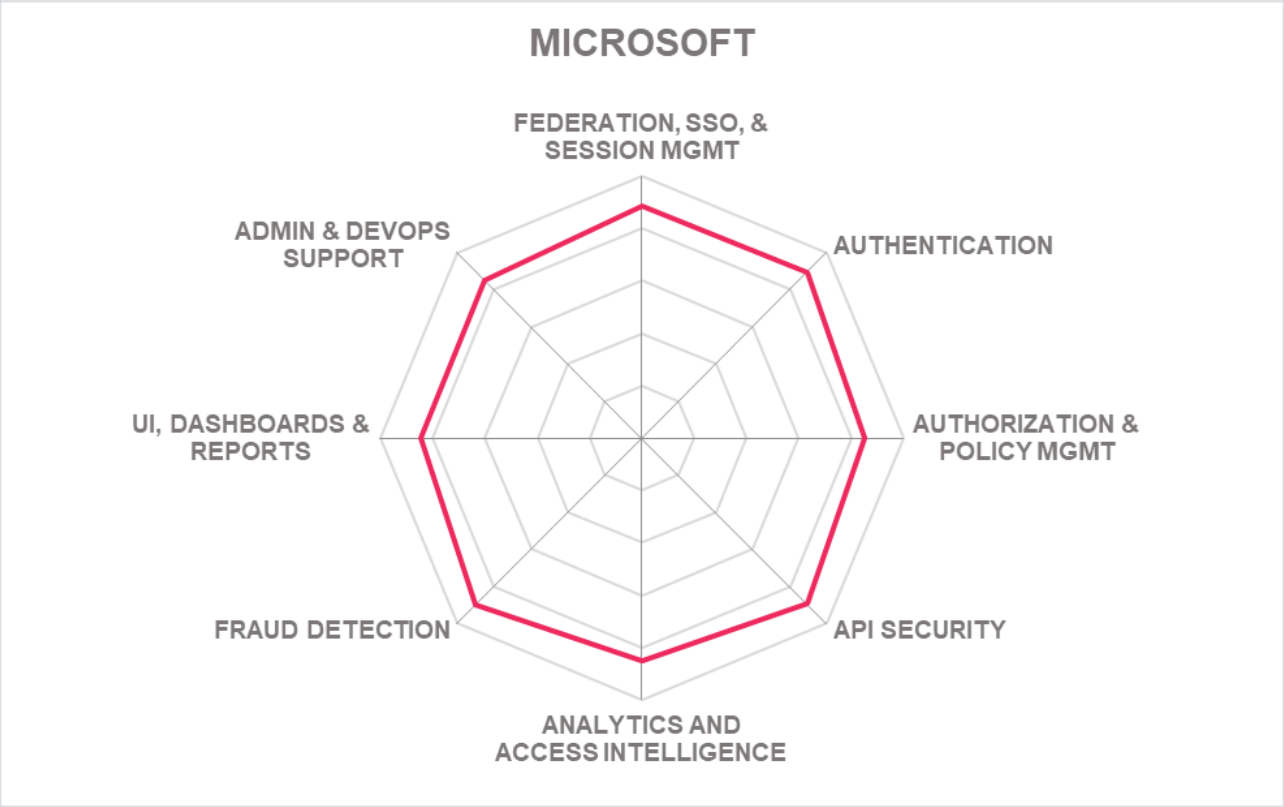
- Identity federation
- SSO & session management
- Good authorization and policy management
- Fraud detection
- Good overall authentication support
- FIDO2 and app-based passwordless MFA options
- API security
- Innovative insights and recommendations
- Resilient against cyber attacks
- Capable of scaling to extremely high workloads
- Broad standards support
- Extensive partner ecosystem

Challenges

- Primary customer presence inside the North America and the EMEA regions, with growth in the APAC and Latin America
- Hybrid scenarios primarily support using Microsoft technologies
- Efficient administration often requires relatively complex Microsoft PowerShell scripting, while most other features are available via the web UI and APIs

Leader in




MICROSOFT
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS AND ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS & REPORTS
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 Authentication-as-a-Service since 2020, and a full IDaaS offering in 2021. Nevis Identity Suite, Nevis Identity Cloud, and Nevis Authentication Cloud is given as its Access Management solution for consideration in this Leadership Compass.

The NEVIS Security Cloud suite is its SaaS based CIAM solution. The NEVIS Security Authentication Cloud is a passwordless authentication solution that extends existing IAM solutions.

NEVIS Security Access Management core capabilities include some good authenticator options, including OTPs, QR Code, mTAN/eTAN, and client-side certificates. Some popular authenticator apps options are given, as well as some mobile biometrics for iOS and Android, although more advanced iris scan and voice recognition capabilities. FIDO support includes FIDO for platform-native authenticators with FIDO WebAuthn on their near-term roadmap. Supported hardware tokens include OneSpan Digipass and RSA SecurID. Adaptive authentication is available, starting with the advanced package. Risk-based, continuous authentication is available with the premium package and includes the OEM components of Behaviosec and Arxan. Centralized access policies are configurable in the nevisAdmin 4 configuration tool, and more complex policies require programming with the Lua programming language on the nevisProxy reverse proxy. Access policies support ABAC, RBAC, CBAC, RAdAC, and user-group principles. The Session Management Engine is configurable and supports headers, cookies, and TLS based sessions. Session brute force and session ID guessing attacks can be detected, although session anomaly detection 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.

Good user self-service registration via UI or APIs is given as well as an integration with its partner Pixel vision to provide identity verification during user onboarding. Their nevisAdmin 4 GUI has a GitOps architecture providing an IDE for Nevis. It provides both the configuration as well as the deployment to on-premises VM-based installations and Kubernetes and monitoring of deployments. Limited out-of-the-box reports are available, although a GDPR compliance report is given, and ad-hoc reports can be created via REST or SOAP APIs. Protocol-specific attacks against APIs can be analyzed based on core and custom rulesets which can be configured via ModSecurity. WS-Trust Security Token Service is part of the product. API content filtering is available based on input queries. API key mechanisms can be used to block anonymous traffic or control the number of calls made to your API. NEVIS Security can support Online Fraud Detection and account takeover detection using the nevisDetect component to implement 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. The solution does not support verifiable credentials. Third-party identity proofing providers such as SwissID and Verimi can be used. Third-party

Threat Intelligence solutions are available, although other integrations with EPP, EDR, UEM, or other Endpoint Threat Protection platforms are not.

The NEVIS Identity suite supports on-premises which 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 NEVIS's hardened CentOS-based Linux distribution is available on the nevisAppliance. All Nevis components are provided as self-contained microservice with their own embedded application servers. Supported container-based platforms include Docker, OpenShift from RedHat, Rancher Labs, Pivotal, and the SuSE CaaS platform. Nevis's software can be deployed on IaaS platforms like Azure, AWS, GCP on Kubernetes services. The NEVIS Identity Cloud suite functionality is offered as a SaaS service. NEVIS Identity Cloud suite is available on the Microsoft Azure platform. A managed service be delivered through partners like AdNovum, WIB, FSP, trans4mation, etc. Most of the solution's functionality is available via APIs and supports SOAP API only for nevisIDM and nevisAuth, REST APIs for all new functionality, and JMS / AMQP for identity lifecycle events. nevisProxy supports ICAP to integrate custom threat analysis, and Webhooks can be used with its nevisDataPorter module for data provisioning. All microservices are provided a CLI. Supported SDKs include Java and Groovy for nevisAuth and Lua scripting for extending nevisProxy WAF functionality. 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 Germany and Hungary, with customers focused on mid-market to enterprise-sized companies. Nevis Security Suite is well established with some interesting features. Their product provides core Access Management capabilities with strengths in Identity Federation, SSO, and session management. NEVIS Security continues to improve its set of Access Management capabilities and should be of interest to organizations within the EMEA region.

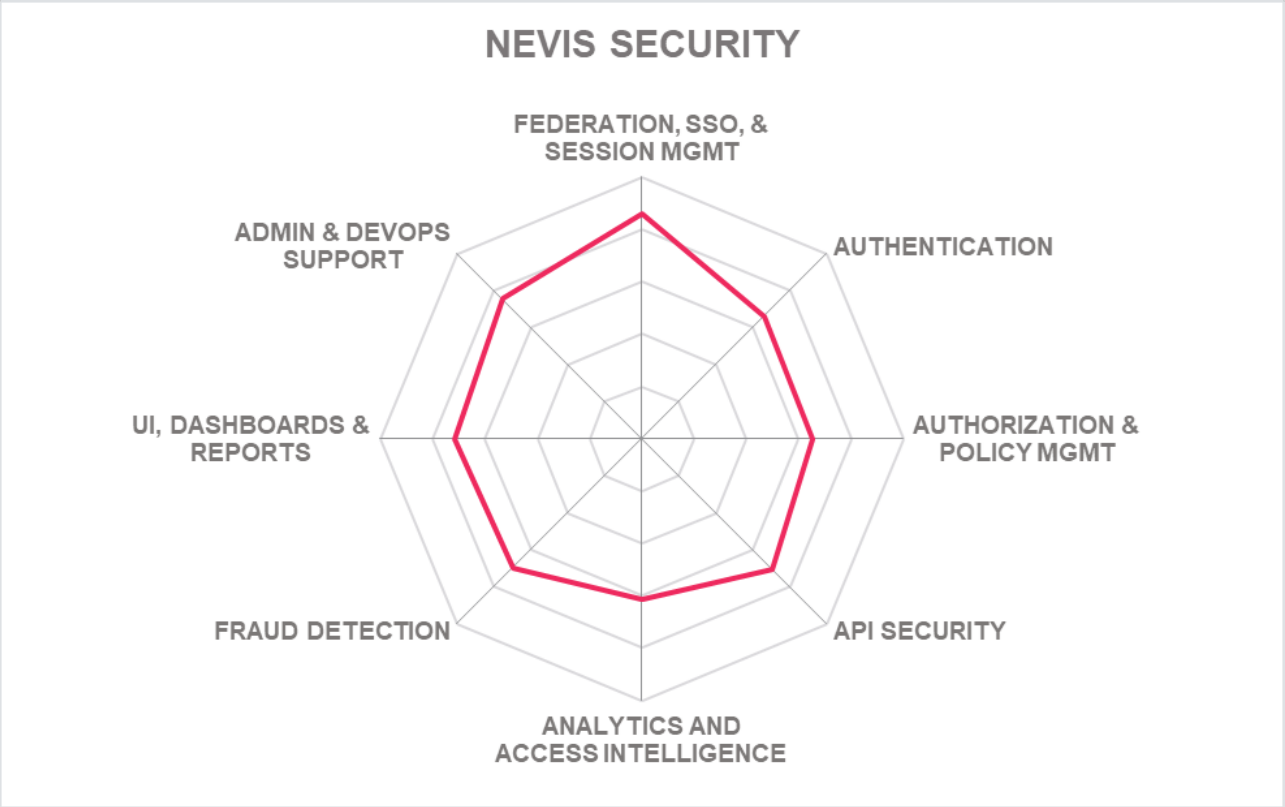
Security	●●●●●
Functionality	●●●●○
Deployment	●●●●●
Interoperability	●●●○○
Usability	●●●●○

Strengths

- Good federation, SSO, & session mgmt
- Some good authenticator options
- Authorization and policy management
- Fraud detection
- API security
- Identity proofing integrations available
- Good admin and devops support
- GDPR reports OOB

Challenges

- Limited market reach outside the EU, with a relatively small partner ecosystem
- Limited FIDO support, although FIDO WebAuthn on their near-term roadmap
- Some limitations on third-party integration options
- More complex access policies require some programming by developers
- Missing support for verifiable credentials


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

5.16 Okta

Based in San Francisco, California (US), Okta's cloud identity platform is targeted at the workforce and customer identity management. Okta's acquisitions of Auth0 (CIAM, developers) and at Spoke (IGA) broadened Okta's portfolio in 2021. Today the complete Okta portfolio is sold via one integrated sales team. Okta's workforce identity solution addresses organizations' access and identity management requirements with 7,000+ pre-built integrations to application and infrastructure, a universal directory service, SSO, MFA, behavior detection for adaptive MFA, identity lifecycle management, identity governance, API access management, and identity orchestration using Okta Workflows. The Okta Identity Cloud is used by customers, developers and businesses to address complex identity problems as a result of its authentication, policy management, authorization, and extensibility capabilities. With the recent launch of Identity Governance, Okta now offers a converged IAM and Governance solution to improve customers' security posture targeted at helping enterprises mitigate modern security risks and improve efficiencies.

Okta provides good support options for authentication methods, including OTPs, popular authenticator apps, mobile biometrics for iOS, Android, full FIDO support, and a wide range of hardware tokens. Missing are more advanced biometric options such as iris scan or voice recognition , although Okta can integrate with iris, voice and face recognition software FastPass is Okta's passwordless authentication that can register the device to its universal directory using its Verify App without recording your face ID or touch ID biometric. FastPass allows touch ID, face ID or visual hello to authenticate the device giving access to the user's applications. The Okta Identity Cloud provides SSO using industry standards like SAML, OIDC, WS-Fed, and adaptive MFA capabilities using behavior detection insight from millions of users, devices, and authentications, providing SSO to on-premises applications using Okta's Access Gateway (leveraging integration patterns, such as Kerberos, certificates, and header-based authentication). Its adaptive MFA allows organizations to implement passwordless authentication. 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, RAdAC, and user-group access policy management are given with delegated policy management and policy testing tools. However, integration with other policy management tools is not possible. Basic role management is available, but role discovery/mining is not. Okta uses HTTP session cookies to manage a user's browser session across applications. Detection of session attacks is given and uses its ThreatInsight to aggregate data across the Okta customer base and uses this data to detect malicious IP addresses. For on-premises applications, SSO is achieved through a reverse proxy using its Access Gateway solution, which supports integration patterns, such as Kerberos, certificates, header-based authentication, and complex on-prem apps such as Oracle E-Business Suite, SharePoint, and others. Okta provides strong support for identity federation use cases and offers support for a wide range of federation related standards. Okta's platform also has been independently certified to support FedRAMP ATO and compliance with a range of standards such as ISO/IEC 15408 (Common Criteria), ISO/IEC 27001, PCI-DSS v 3.2, ISAE 18 SOC 2, and HIPAA/HITRUST.

Okta provides a good set of web UIs for administration and user self-service. Insights, real-time behavior graphics, and easy-to-use drag and drop no code/low code workflow capabilities are given. Okta gives a

moderate number of out-of-the-box reports but good support for a wide range of reports for major compliance frameworks such as GDPR, HIPPA, and SOX, to name a few. Okta's API security is accomplished through its API Access Management authentication and authorization layers for APIs via OAuth 2.0 interfaces. Okta Provides DoS/DDoS protection for the Okta API Authorization Server endpoints as part of its core capabilities, although API firewall-like capabilities or content filter features are not given. Okta does provide basic Security Token Service capabilities for exchanging end-user tokens to OAuth/OIDC tokens and scopes/claims. Okta's ThreatInsight feature protects the registration endpoint and can stop bot-driven fraudulent account creation for fraud detection. Third-party fraud detection and prevention tools integrations include Akamai, Imperva, iovation, Preempt security, and Telesign, as well as PerimeterX, Signal Sciences (Fastly), F5/Shape Security, and Human Security. Limited support is given for Verifiable Credentials and supports integrations with identity proofing partners.

As a result of its recent acquisitions, today, Okta offers a multi-tenant cloud service for private (Auth0) and public cloud (Okta or Auth0 on AWS) with SaaS, IaaS, and IDaaS deployment options. On-premise integration is available through the Okta Access Gateway (OAG), an on-prem virtual appliance deployed on-prem or by using public IaaS services. Additionally, customers can use DevOps tools to automate the deployment and configuration of Okta. Okta 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. On-premises appliances, containers, or software delivery options are not available. Okta is also not available for IaaS installations. Okta’s APIs provide access to its functionality via REST, SCIM, , and LDAP allowing WebHooks to extend the Okta platform. Okta customers can use the extensibility platform to leverage workflows, actions, rules, and hooks to build a no-code/low-code or pro-code extension. Using custom code or Okta's no-code solution Okta Workflows, allows IT Administrators to quickly create custom logic using a visual solution in a no-code environment. 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. CLI capabilities are available with its Advanced Server Access service. The solution is also capable of integrating with third-party such as ITSM, EPP, EDR, and threat intelligence solutions.

Founded in 2009, Okta headquarters are split between San Francisco and San Jose in the heart of Silicon Valley. Okta historically focused on the North American market but is expanding rapidly into the APAC and EMEA marketsawhile still growing the APAC regions. Okta’s recent acquisitions helped broaden its CIAM and IGA (for workforce) capabilities geographical footprint. 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. Okta appears in all leadership segments of this Leadership Compass. Organizations contemplating a move to the cloud for their Access Management services might consider Okta.

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

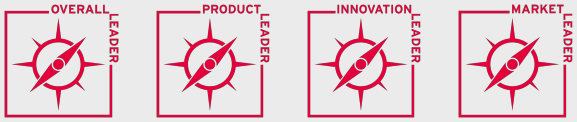
Strengths

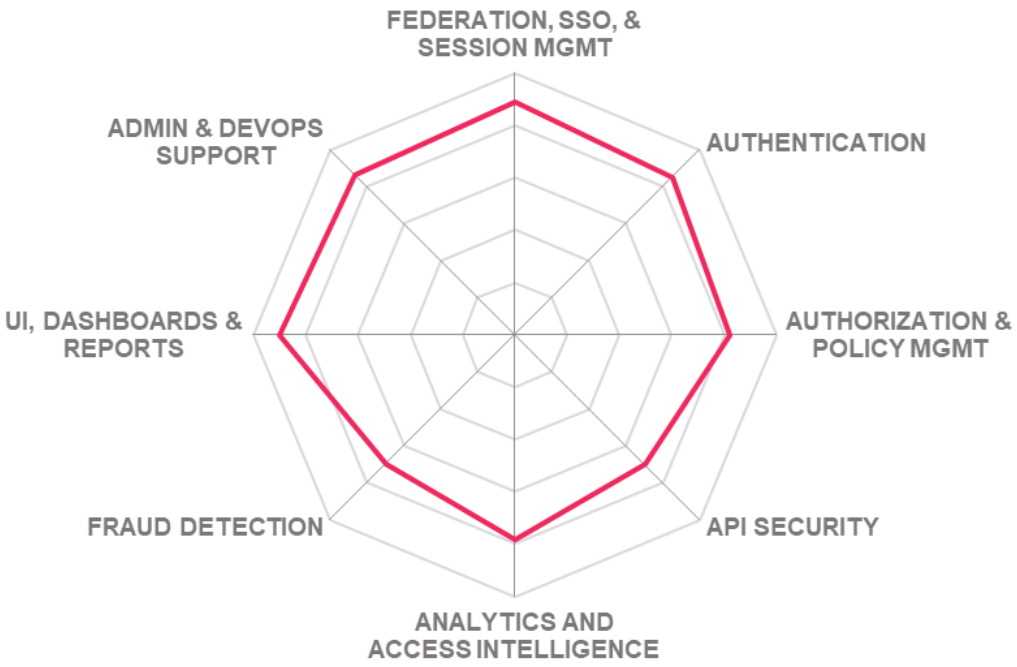
- Strong identity federation
- Session management and SSO
- Good authentication options
- Passwordless support
- Authorization and policy management
- Analytics and access intelligence
- No code/low code workflow editor
- Good admin and DevOps support
- API Security
- Fraud detection
- Wide range of compliance certifications
- Range of third-party integration options

Challenges

- Primarily focused in the North American market with a growing presence in EMEA & APAC
- Limited, but effective API protocol options
- Purely cloud based SaaS with agent for on-premises.
- Need to integrate with on-premises appliances, containers or software delivery options from partners or third parties.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


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

5.17 OneLogin

OneLogin, by One Identity, was founded in 2009 as one of the first vendors to enter the IDaaS market. It was acquired by One Identity in late 2021 as a core part of its vision to help customers shift from a fragmented to a holistic approach to identity security. Today, One Identity's Unified Identity Security Platform brings together Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM), and Active Directory Management and Security (ADMS) capabilities. OneLogin Trusted Experience Platform is offered as its Workforce and Customer Access Management solution with real-time actionable intelligence and automated configurations. 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 soft MFA authenticators and most hardware tokens. Also included are biometric authenticators for Android, iOS, voice recognition, and iris scan. Missing is a QR Code authenticator option. 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. OneLogin's Smart Factor Authentication is an add-on package that provides support for risk-based authentication that includes features such as compromised credential check, and its Smart Flows capability. OneLogin certificate-based device trust can also be used as part of its add-on SmartFactor Authentication. OneLogin Vigilance AI is fully integrated into its authentication flow. All OneLogin policies reside in the OneLogin Admin console and support ABAC, RBAC, CBAC, RAdAC, ReBAC, and both user and policy groups access policy models. OneLogin's Smart Hooks allows for customizable features to assign policies dynamically based on the user's context, browser, time, last login, location, for example. Good session management is provided, and 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. OneLogin's federation-related capabilities include support for SAML 2.0, OAuth 2, OIDC, WS-Federation, WS-Trust, JWT, and SCIM.

The OneLogin Trusted Experience Platform provides a modern, easy-to-navigate administrative UI and user self-service. Good graphics dashboards and reporting options are given with some out-of-the-box (OOB) support for some significant compliance frameworks like GDPR, PDS2, and PCS DSS. Also, provided OOB is a good set of IGA related reports. Vigilance.AI is OneLogin's fraud detection service that creates behavioral profiling of users by consuming a combination of contextual user and device information and ingesting threat intelligence from third-party services. Integrations to other third-party fraud detection and prevention tools are limited to Signal Science. OneLogin uses in-network fraud reduction intelligence sources and OOB connectors to Tor Network, Project Honeypot, AlientVault Open Threat Exchange, Have I Been Pwned, and Enzoic. 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 by default and some protection from DoS

attacks of its APIs. Still, capabilities such as API content filtering, content-based routing, schema validation, or protection from API protocol-specific attacks are not available. OneLogin uses its OIDC integration to bridge with verifiable credentials providers to be able to issue and verify verifiable credentials and partners with third-party identity verification services such as Onfido and Jumio.

OneLogin supports a public cloud deployment model with a microservices architecture using Hydra Cloud Infrastructure. The Trusted Experience Platform can be delivered as SaaS, with an on-premises reverse proxy available as a Docker container. Smart Hooks leverage a serverless platform and require no customer hosting. On-premises components of the platform are IaaS agnostic, supporting a wide range of IaaS platforms. It provides a fully integrated database, and the Universal Connector supports a number of DBs such as MSQL, Oracle, IBM DB2, MSQL, and PostgreSQL, to name a few. OneLogin, as a managed service, is possible through partner MSSP & MSPs. Most of OneLogin's functionality is available via REST APIs and WebHooks. APIs are provided for most admin functionality, including a Terraform Provider and much of the authentication capabilities. An AWS CLI offers advanced authentication support, including MFA and role-based access. SDKs are available for a wide range of programming languages, with the exception of Groovy. OneLogin has been independently certified to support compliance standards such as SOC1,2,3 and ISO 27001, ISO 2017 & ISO 2018, to name a few.

OneLogin focuses on SMB organizations with growth in mid-market to enterprise presence. OneLogin customers are primarily in North America, with growth in the APAC and EMEA regions. OneLogin also supports a good partner ecosystem.
OneLogin appears in all leadership categories in this Leadership Compass for Access Management and should be considered by organizations in North America.

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

onelogin

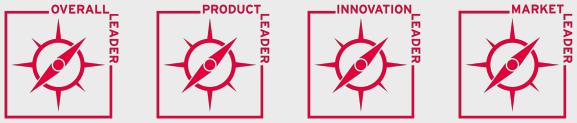
Strengths

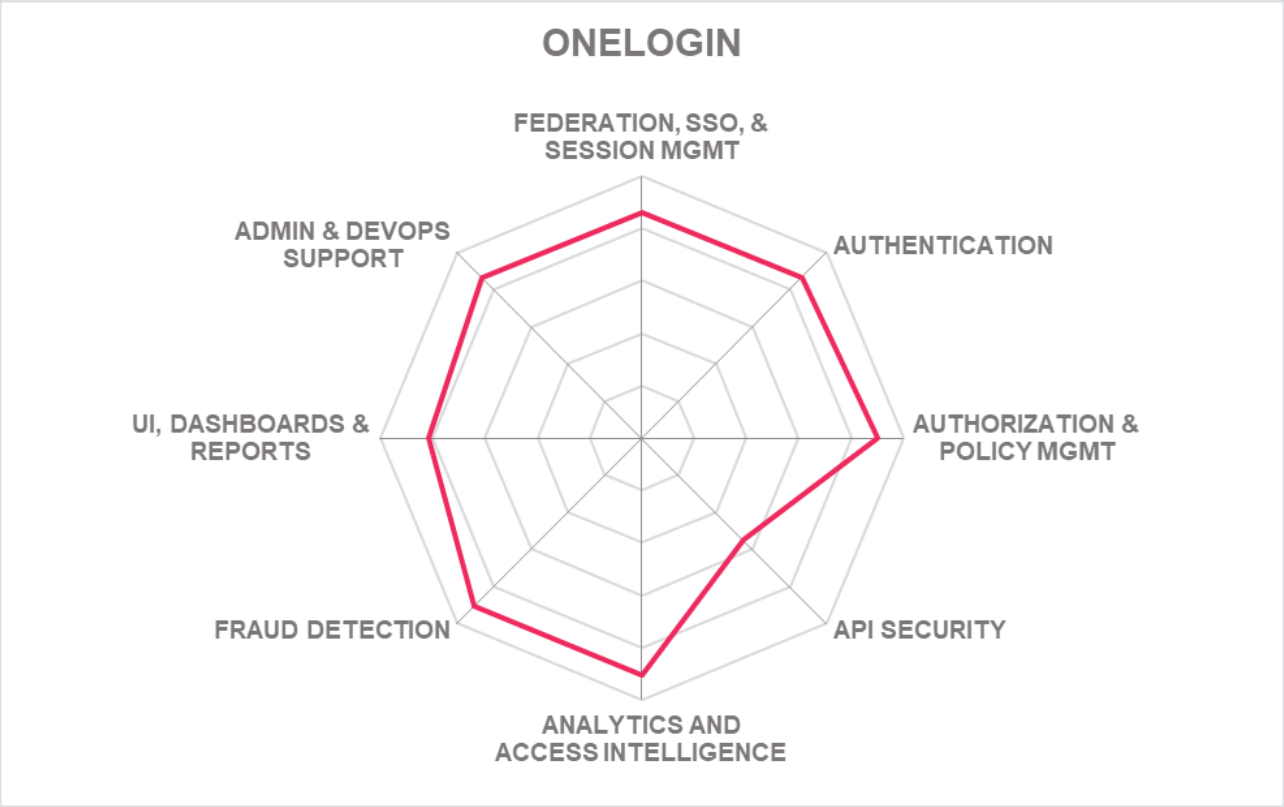
- Strong authorization and policy management
- Good authentication options
- Fraud detection
- Good use of analytics and access intelligence
- Identity federation
- SSO and session management
- Modern admin and user self-service UI
- Strong use of analytics and access intelligence
- Good partner ecosystem

Challenges

- Primary customer focus in North America, with growing presence in the APAC and EMEA regions
- Deep integration with legacy on-prem systems can be a challenge
- Adaptive risk-based authentication requires an add-on service
- Limited API security

Leader in




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

5.18 Optimal IdM

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

Optimal IdM OptimalCloud gives moderate support for authentication methods and a few popular authenticator apps and hardware tokens. Optimal IdM offers its own device-based authenticator, the Optimal Authenticator. Support for Android and iOS biometric authenticators for core Access Management capabilities is also given. FIDO support includes FIDO U2F and FIDO 2, for compliant authenticators, and FIDO UAF. Risk-adaptive authentication provides some device, user, network, and location contexts to be used in access policies. The OptimalCloud central policy management offers a user interface for the administrator or delegated administrator to view, edit, and test all access policies supporting ABAC, RBAC, CBAC, RAdAC, ReBAC, 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. Third-party integration options include ITSM, EPP, EDR, Threat Intelligence, and Analytics or Intelligence (AI/ML) solutions.

The OptimalCloud administrative UI provides tab-based navigation with some good color-based action indicators making it simple and easy to use. The dashboard gives widgets that can display a variety of stats and basic graphics. A good set of out-of-the-box reports are offered, including IGA, performance metrics, and a wide range of reports for major compliance frameworks. Fraud detection support includes a number of third-party integrations to fraud detection, and prevention tools are available. Fraud reduction intelligence sources can be in-network or use connectors to third-party providers. 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, are not provided. Support for verifiable credentials is not given, although integration to third-party identity proofing and other verifiable credential providers using the OptimalCloud plug-in framework.

Optimal IdM OptimalCloud is delivered a SaaS and offers a Virtual Identity Server to support on-premises, as well as a managed service. Container-based delivery options are not available. Optimal IdM

OptimalCloud is a dedicated multi-tenant cloud offering built on .NET and hosted on Windows servers. IaaS platform support includes Amazon AWS, GCP, Azure, and Oracle Cloud. 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. SCIM and Webhooks are also supported. Native CLI capabilities are not supported, although most other CLI frameworks can invoke OptimalCloud APIs. Popular programming languages support a wide range of SDKs. It is based on standard protocols and offers many downloadable code samples for programming languages such as C#, VB.NET, Java, JavaScript, and Swift. OptimalCloud is independently certified to comply with the FIPS 197, FIPS 140-2, ISO/IEC 15408 (Common Criteria), ISO/IEC 27001, ISAE 18 SOC 2 standards.

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 such as identity federation, SSO, and a particular strength with authorization & policy management support.

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

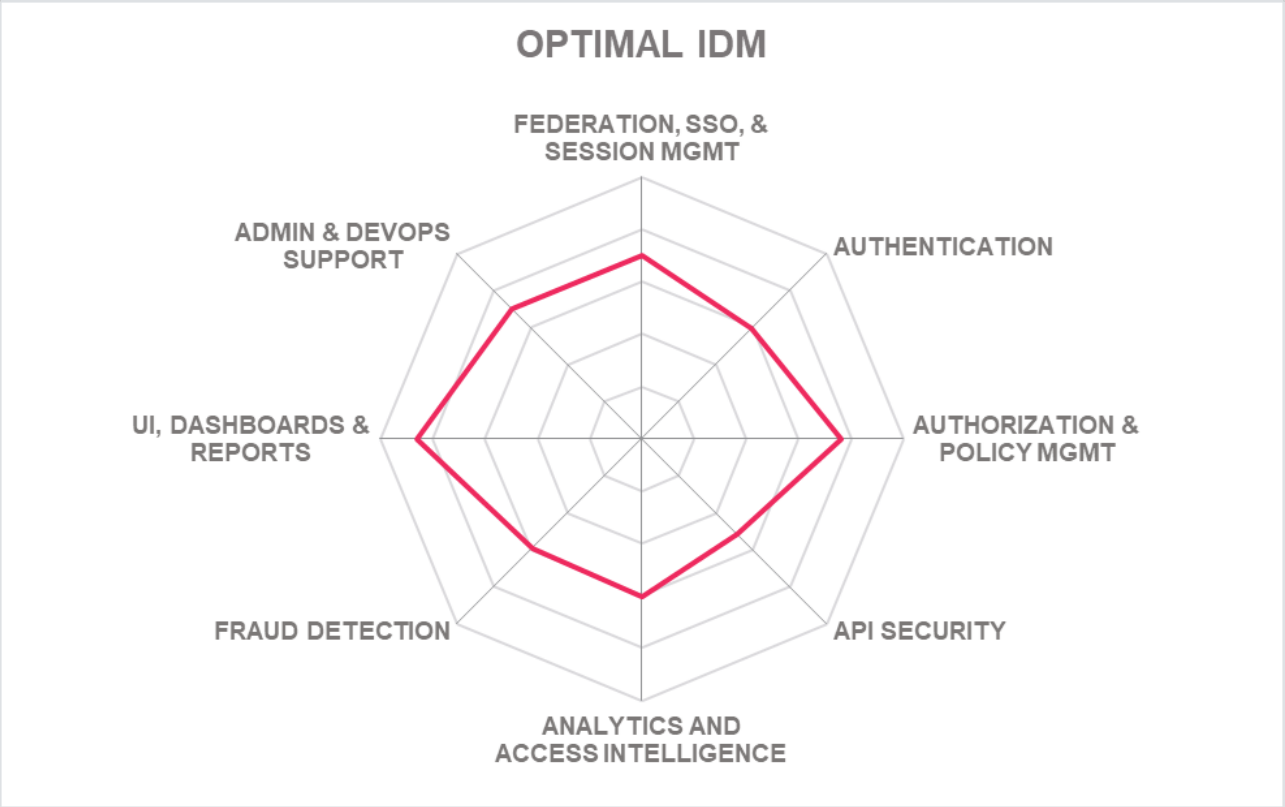
OPTIMAL IdM
Identity & Access Management

Strengths

- Authorization and policy management
- Identity federation
- Session management
- Single Sign On
- Some API security capabilities
- Admin and DevOps support
- Good set of reports OOB
- Independently certified to be in compliance with a number of standards
- Good third-party integration options

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 some third-party integrations are available
- Moderate API security capabilities
- Moderate authenticator options
- SSO for non-web applications or IT systems are not supported


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

5.19 Oracle

Based in Texas, Oracle, the leading provider of Cloud infrastructure, database management and enterprise resource planning software. Since 2016, Oracle Identity Cloud Services (IDCS) is its IDaaS service, delivers Identity Administration and Access management capabilities from the cloud. More recently, OCI Identity and Access Management (OCI IAM) 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.

OCI Identity and Access Management (OCI IAM) Access Management capabilities offer moderate authentication support such as OTPs, certificate-based, RADIUS, Kerberos, and some popular authentication apps, but good FIDO support for UAF, U2F, and FIDO 2 is given. Both Android and iOS biometrics authenticators like fingerprint and facial recognition are available Also, limited hardware token support is given that includes YubiKey. Good support risk-adaptive authentication features can analyze user, network, location, and some device health state contexts that can be used in access policies. OCI IAM provides an API for policy authoring supporting ABAC, RBAC, CBAC, RAdAC, and user groups for managing user access. OCI IAM 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, although role mining is not. Entitlement discovery is supported via integrations with Oracle OIG and components from Kapstone and Aquera. OCI IAM 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. OCI IAM SSO can be accomplished using its reverse proxy, web-server agents, and support header-based authentication for SSO across multiple web applications. OCI IAM has a good application catalog of applications that supports SAML, which are pre-integrated and configured for OCI IAM as a service provider. OCI IAM can also act as an IDP for various applications. Supported federation-related standards include SAML, OAuth, OIDC, WS-Federation, JWT, and SCIM.

Oracle OCI IAM 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. OCI IAM supports API rate limiting, a means of DoS protection, content filtering, content-based routing, schema validations, detection of protocol-specific attacks, and providing an include a Security Token Service. Good API key management is also given. OCI IAM can integrate with Oracle Cloud Services for fraud detection 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. OCI IAM can integrate with fraud reduction intelligence sources that support SCIM integration and other standards. Oracle also offers a separate product Cloud Guard as an Account Take Over (ATO) detection and prevention tool integrated with IDCS. OCI IAM supports identity verification or proofing via partner solutions such as Singular Key, 1Kosmos, and TruU.

OCI IAM (formerly IDCS) is implemented in a microservices architecture and provides a fully integrated standalone SaaS solution that offers all the core identity and access management capabilities through a

multi-tenant cloud platform. OCI IAM runs on the Oracle Cloud Infrastructure (OCI), and installations on other IaaS platforms are not possible. OCI IAM cannot be delivered as software or via containers, although Oracle offers software- and container- based AM solutions via OAM. A managed service option is also available. IDCS uses and depends on Oracle database technologies. IDCS supports REST APIs for all available features with support for standard SCIM core schemas as well as Oracle schema extensions. Access to IDCS functionality via CLI options is given. SDKs support the Java, C/C++, Python, .Net, Ruby, JavaScript, Groovy, iOS, and Android programming languages. IDCS has been independently certified to support compliance for a wide range of standards. Also, IDCS can support integrations with third-party services such as ITSM, EPP, EDR, Threat Intelligence, and UEM solutions.

Oracle OCI IAM provides a strong offering in the Access Management market and provides a solution that will be attractive to existing Oracle customers. It is tightly integrated with other Oracle business products as well as other Oracle security products. Organizations considering a cloud-based Access Management can consider OCI IAM for a product evaluation.

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

ORACLE

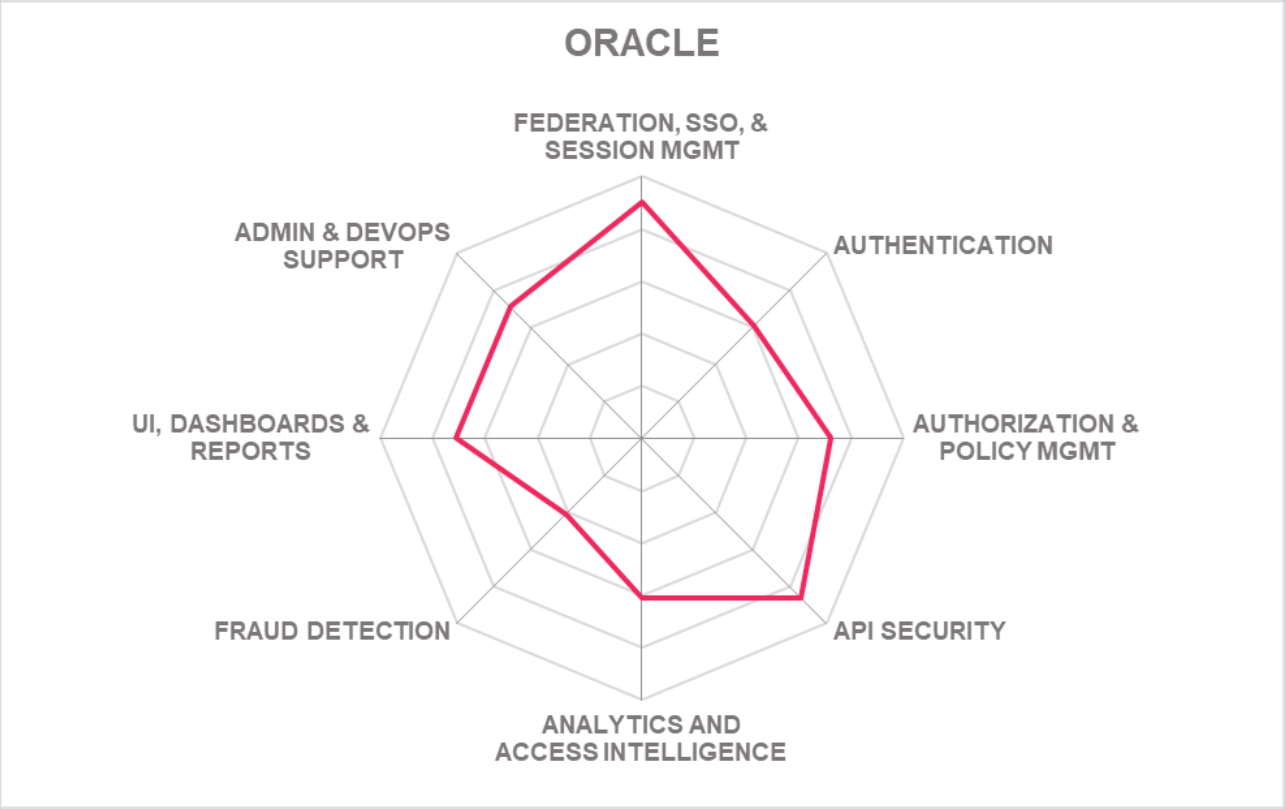
Strengths

- Identity federation
- Session management and SSO
- Good API security
- UI, dashboards and reporting
- Admin and DevOps support
- Adaptive authentication
- Full FIDO support
- Good third-party integration options

Challenges

- Only REST APIs are support for all capabilities
- Moderate range of authenticators offered
- Only the Oracle Cloud IaaS is supported
- Limited fraud detection
- Limited reporting OOB

Leader in


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

5.20 Oxyliom Solutions

Oxyliom Solutions is a publicly listed company headquartered in Morocco with offices in Luxembourg and Dubai. Oxyliom Solutions started as a system integrator in 2012. Since then, the company developed the GAÏA Trust Platform, which provides two solutions: GAÏA Advanced Identity Management and GAÏA Trust Services Management for securing electronic transactions. The GAÏA Trust Platform has a modular architecture for delivering various services related to Advanced Identity Management and Trust Services Management (TSM).

The Oxyliom Solution provides a single platform with multiple services that are implemented in a microservice architecture. A good set of authentication methods include OTPs, QR Code, and some popular authentication apps and hardware tokens. Authenticators such as Android and iOS fingerprint and facial recognition biometrics are supported, but more advanced voice recognition and iris scan biometric options are not. Good FIDO support is given. Contextual and risk-adaptive authentication is supported as part of the base authentication service. The solution's access policies are managed and stored centrally, capable of managing user access based on the ABAC, RBAC, CBAC, and user-group-based principles. Although role mining or discovery capabilities are not, basic role management is available. Also, delegated policy management is supported. Device management includes the registration of both mobile and IoT devices. Session management is provided with abilities to detect sessions attacks. SSO is achieved via a reverse proxy to support multiple web applications, although SSO support is not given for non-web applications or IT systems (e.g., thick clients). Federation includes SP and IdP functionality, and support for SAML, OAuth, OIDC, WS-Federation, JWT, SCIM, and UMA federation related standards.

The administration user interface is simple and effective, with customizable dashboards. The user profile settings can control the user's self-service screen content. Some OOB reporting is given, including some reports for major compliance frameworks such as GDPR, PDS2, HIPAA, SOX as examples, and some IGA related reporting. A good level of fraud detection is given. It limits the access to applications to approved or trusted customers based on their IP, authentication, time of day, and other information that constitutes a context. In addition to these features, they also provide connectors to the Arxan and Broadcom anti-fraud platforms. Some good API security features are also provided, including DoS protection, rate limiting, content filtering, schema validation, and analysis of protocol-specific attacks. Support for verifiable credentials is accomplished through a third-party verifier.

Oxyliom Solution's GAÏA Trust Platform can support on-premises, private cloud, and hybrid deployment models. Its delivery models include SaaS, container-based, and a managed service. The GAÏA Trust Platform SaaS delivery option is hosted in its facilities with full multi-tenancy. Both Docker and Red Hat container-based platforms are supported. Many Linux-based and Windows operating system options are available, and an application server and database are fully integrated. Supported IaaS platforms include Alibaba, AWS, and Azure. The majority of the platform's functionality is available via REST, Webhooks, and SCIM APIs. Access to its capabilities via CLI is not given. SDKs for Android, iOS, and JavaScript are available, although only a small percentage of the solution's capabilities are accessible. A standard connector to Symantec EDR and ATP platforms is also given.

Oxyliom Solution's customer base is focused on the mid-market in the EMEA region. GAÏA Trust Platform runs both the Advanced Identity Management and the Trust Services Management solutions and provides a good set of integrated components for identity and trust use cases. Oxyliom Solutions provides some core Access Management capabilities with particular strength in delivering API security capabilities. Oxyliom Solutions GAÏA Trust Platform should be of interest to mid-market organizations in the EMEA region.

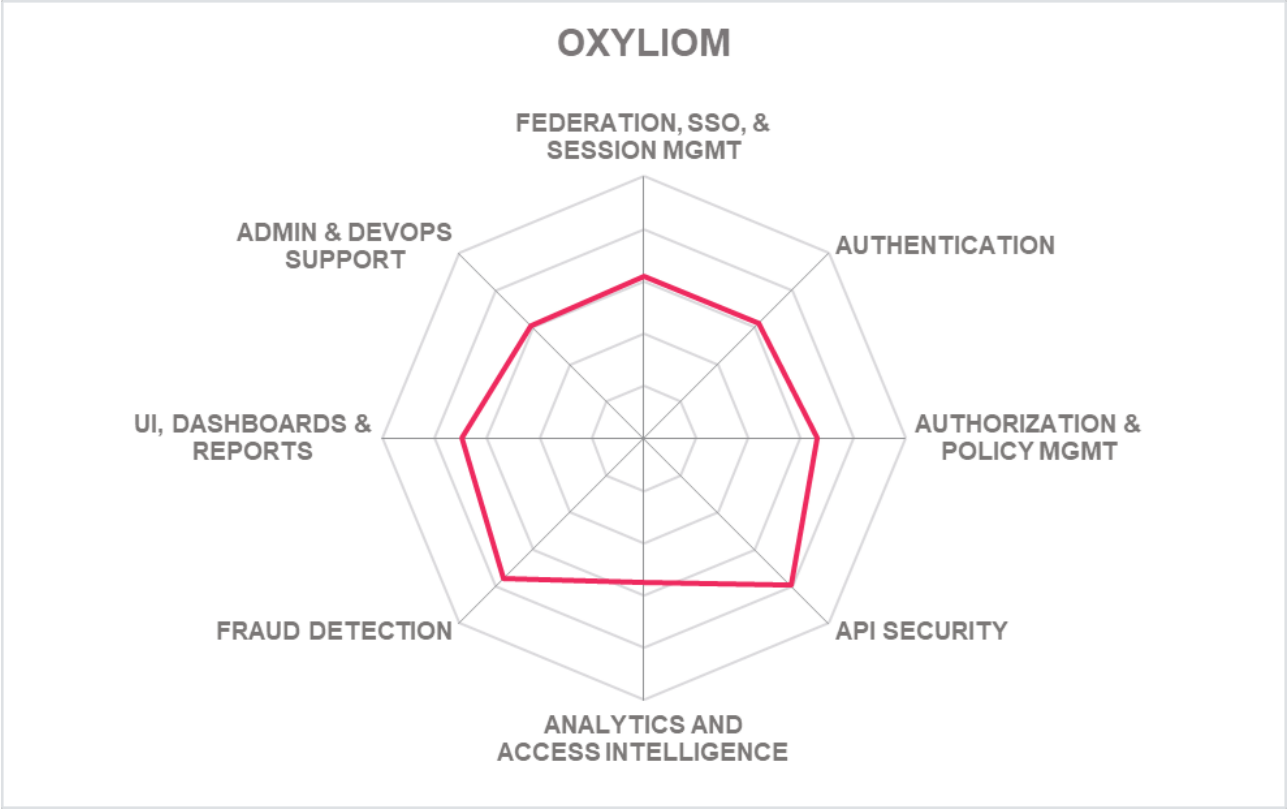
Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●●○
Usability	●●●●○

Strengths

- API security capabilities
- UI, dashboards and reporting
- Authorization and policy management
- Authentication options
- Fraud detection
- Delegated policy management
- Device management supports both mobile and IoT registration
- UMA support
- Admin and devops support

Challenges

- Customer base solely in in the EMEA
- Limited partner ecosystem outside of the EMEA regionModerate analytics and access intelligence
- Limited SDK and CLI support


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

5.21 Ping Identity

Ping Identity was founded in 2002 and is 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 and accelerated innovative features by acquiring Symphonic Software for policy-driven authorization in 2020, and more recently SecuredTouch to add anti-fraud capabilities and Singular Key for user experience orchestration across their platform in 2021. These acquisitions augment the other areas of their identity portfolio, which is made up of mostly cloud services, and software products if needed. The PingOne Cloud Platform offers a complete portfolio of access management functions for B2B, B2E, and B2C scenarios.

PingOne Cloud Platform Access Management capabilities offer strong authentication methods, including hard and soft authenticators, good biometrics authenticator support and FIDO U2F, and FIDO 2 certified authenticators. However, FIDO UAF capabilities are not offered. Contextual and risk-adaptive authentication are well supported as part of its base authentication service. Access policies are capable of utilizing user, network, device, and contextual location 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 users' access based on ABAC, RBAC, CBAC, RAdAC, ReBAC, and user-group principles. Its PBAC offers a graphical policy administration for fine-grained P/ABAC to address Web, API, and Data use cases. Basic user and admin role management are supported across all Ping solutions, although role mining/discovery capabilities are not supported. Session management features support web session management through session HTTP header and browser cookies and various 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 can use 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.

The PingOne Cloud Platform gives good visibility into all Ping Identity environments via the PingOne unified administration console, which provides a number of dashboard widgets and administrator SSO into all Ping Identity products. PingOne DaVinci is a no-code visual design tool that will allow organizations to design their own user experiences through automated workflows. Good reporting capacities include support for a wide range of major compliance frameworks such as GDPR, PDS2, HIPAA, and a number of NIST and FIPS, to name a few. Ping's proprietary fraud detection includes UEBA/OFD behavior pattern capabilities based on access to devices, browsers, operating systems, and geo-locations are available within its MFA and Risk solutions. PingOne Fraud addresses the convergence between IAM and Online Fraud Detection in the future to detect account takeover, credential stuffing, human/bot detection, session risk analysis as examples. PingOne API Intelligence gives risk governance for APIs that can track API activity in a single view and provide insights using AI capabilities to identify API misconduct and breaches. 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. PingOne API Intelligence leverages its AI capability to learn traffic behaviors to detect and block abuse of a customer's APIs automatically. PingOne API Intelligence can use API keys to detect anomalies based on client behavior and usage patterns. PingOne Verify gives ID verification to allow for self-service customer onboarding using a live facial and government ID verification. PingOne Verify helps to prevent fraudulent activity and comply with KYC regulations.

The PingOne Cloud Platform is a multi-tenant IDaaS platform. For enterprises that require advanced capabilities and data isolation, it also deliver a dedicated tenant option, PingOne Advanced Services, managed and hosted by Ping or its MSP partners.. Cloud-ready Docker images are also offered with support for a wide range of container-based platforms. The software can be deployed to a server with many operating systems, application servers, and databases supported for on-premises, although an appliance option is not available. The solution's functionality is available via APIs and supports SOAP, REST, JSON-RPC, WebHooks, SCIM, LDAP, and Radius. All platform functionality is also available via CLIs. SDKs are provided for a wide range of popular programming languages. Also, the ShoCard app is a distributed identity wallet for consumers via a mobile SDK and PingOne for Individuals for businesses using the PingOne for Individuals SDK. Third-party integrations are well supported, which includes integration to popular ITSM, threat intelligence, EPP, EDR, and UEM solutions.

Ping Identity has a strong presence in North America and good representation in EMEA and APAC regions with a suitable partner ecosystem. They appear in all leadership categories in this Leadership Compass and continue to innovate in a positive direction. As such, Ping Identity’s platform should be included in any shortlist for Access Management platform solutions to consider.

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

Ping Identity

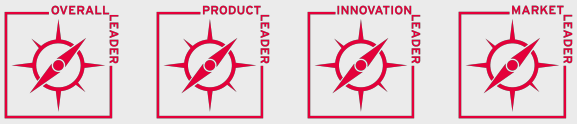
Strengths

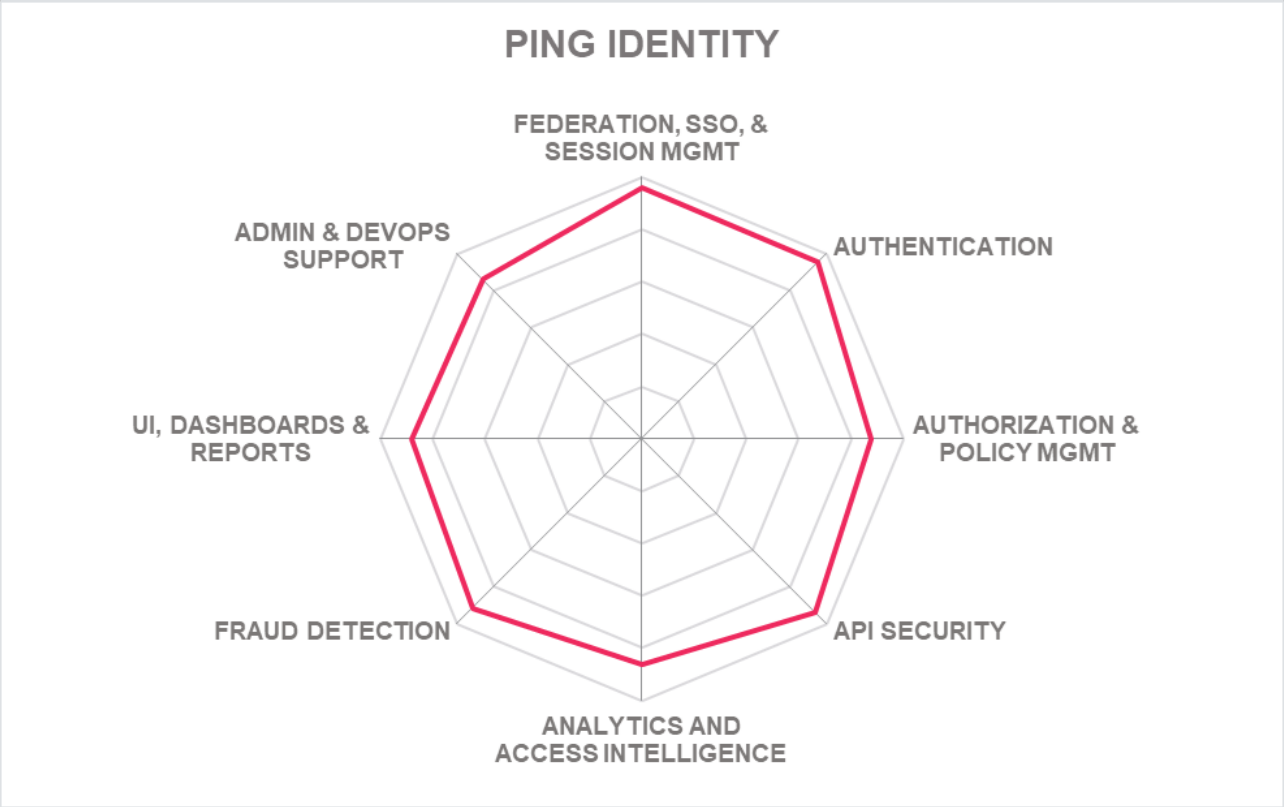
- Strong Federation, SSO, & session management
- Strong authentication support
- Good API security
- Authorization and policy management
- Good use of analytics & access intelligence
- Strong fraud detection
- Identity verification capabilities
- UI, dashboards and reporting
- Admin and DevOps support
- Delegated administration support

Challenges

- Primary customers are focused in North America, with growth in EMEA and APAC
- Some Access Management use cases require on-prem PingFederate component
- FIDO UAF capabilities are not offered
- Some fraud detection capabilities require an integration with PingIntelligence for APIs solution

Leader in




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

5.22 PortSys

PortSys is a privately funded company founded in 2008 and based in Marlborough, Massachusetts. PortSys began building security appliances with Microsoft and HP and has evolved to provide Zero Trust Access Controls to various commercial organizations and government agencies in North America and the EMEA regions. PortSys' solution utilizes reverse proxy-based access controls with authentication, authorization policy management, identity federation, and SSO capabilities.

PortSys Total Access Control (TAC) is a single product with multiple technologies fully integrated together. TAC offers a wide range of authenticator types such as OTPs, QR Codes, popular authenticator apps, and hardware tokens, as well as Android and iOS facial and fingerprint biometrics. Also given are FIDO U2F and FIDO 2 support. Risk-adaptive and contextual authentication is offered as part of the base authentication service. Contextual attributes can be added to the TAC centralized management. Policy testing tools are provided. Supported policy principles include ABAC, RBAC, CBAC, PBAC, and user groups. Both basic role management and mining are available and support for delegated policy management. Browser sessions can be managed using session HTTP headers or browser cookies, and good support for session attack detection is given. Federation support includes SP functionality, and, IdP functionality is on its short term roadmap to be released in May 2022. SAML 2, OAuth, OIDC, WS-Federation, JWT identity federation standards are also supported.

User self-service doesn't support self-service registration, workflow capabilities, or access via APIs, although managed registration is supported and users can make self-service password resets. Basic reporting is given, and some out-of-the-box (OOB) reports support for IGA and operations-related reports are available. OOB reports for major compliance frameworks such as GDPR or SOX are not available. Fraud detection can detect unauthorized account takeover through the use of MFA, Geo IP, and Device detection, and customers can use SIEM and other data analysis tools to query log information. OOB integrations to Account Take Over (ATO) Detection & Prevention tools are missing. API security includes a unique API Access Key generation and validation, a means of DoS protection such as response caching, content filtering, and routing, as well as some protocol-specific attacks that can be analyzed. TAC does not provide or manage verifiable credentials, although TAC can consume and verify credentials from other sources. The solution also supports integrations with third-party identity proofing providers.

PortSys TAC can be deployed on-premises, in a public, private, government, multi-cloud, or in hybrid environment. The TAC reverse proxy is built on virtual appliances and delivered as a hardened hardware or software appliance. TAC requires a Windows Server 2019 operating system. The product is also available for IaaS installation, in which AWS, Azure, and Dell Nutanix are supported. A SaaS delivery option is not available. Only a very limited amount of TAC capabilities is available via a REST API or CLI. SDKs are not available. Integrations with third-party ITSM solutions are not given, although third-party integrations with EDR, EPP, or analytics solutions are possible.

PortSys’s customers are primarily mid-market organizations in the North American and EMEA regions, with some growth in APAC. PortSys Total Access Control provides good core Access Management capabilities

with the potential to grow more advanced features seen in the market today. Potential mid-market organizations in the North American and EMEA regions may be interested in evaluating PortSys Total Access Control.

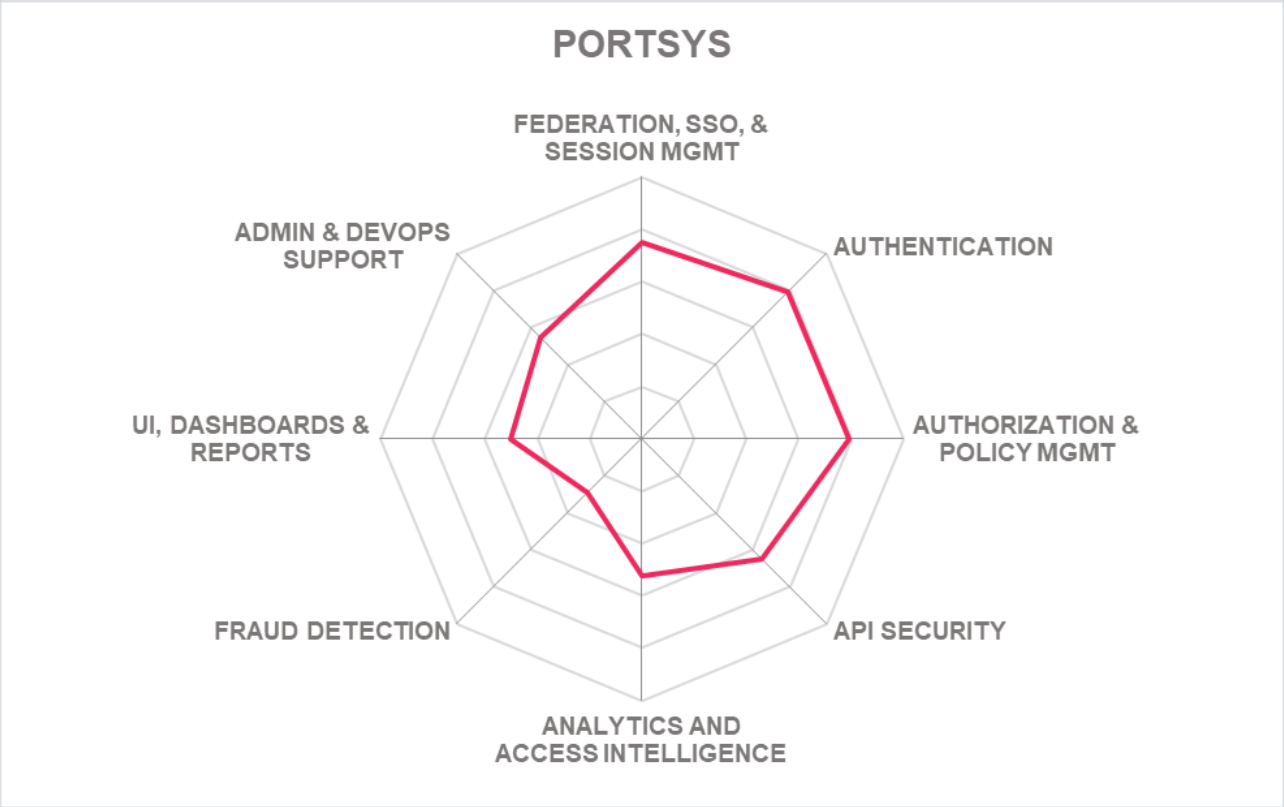
Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●○○
Usability	●●●○○

Strengths

- Authorization and access policy management
- Authentication options
- Identity federation
- SSO and session management
- API security
- Role management and mining
- Can consume and verify credentials from other sources
- third-party identity proofing integration support

Challenges

- Limited market visibility outside of NA and EMEA regions
- Limited partner ecosystem
- Limited fraud detection capabilities
- Limited OOB reporting
- Limited API access to product functionality
- Missing SDKs
- Limited user self-service capabilities


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

5.23 SecureAuth

SecureAuth has been in the market since 2005 and is headquartered in Irvine, CA. More recently, SecureAuth's acquisition of Acceptto in late 2021 added contextual behavior threat intelligence to its list of capabilities. SecureAuth brings telemetry of access management, network, vulnerability, and endpoint together with the identity context. The SecureAuth Access Management solution gives MFA, Risk-based Adaptive Authentication, SSO, Authorization and Policy Management, and User Self-Service capabilities.

SecureAuth, Access Management capabilities include good authentication supports for OTPs, many popular authenticator apps, and hard tokens with support for Android and iOS biometric authenticator options. Also supported are fingerprint sensors for Windows Hello and macOS Touch ID. However, advanced voice recognition and iris scan biometrics are not supported. Interestingly, QR code authentication is also not supported. Full FIDO support includes UAF, U2F and FIDO 2 / WebAuthn authenticators, which 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. SecureAuth only supports RBAC 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 given. SSO is delivered via a reverse proxy, as well as cookie-based options and Web browser via SAML, OIDC, WS-Federation, or LTPA, as examples. Sessions management is achieved via web browser cookies. Session timeouts are configurable per realm. Brute force, credential stuffing, session ID anomaly detection, and password spraying session attacks can also be detected. SecureAuth includes SP & IdP functionality supporting SAML, OAuth, OIDC, WS-Federation, SCIM and JWT federation-related standards.

SecureAuth's acquisition of Acceptto with its eGuardian risk engine has accelerated its zero-trust posture by extending intelligent MFA, passwordless, continuous, FIDO, and device trust & telemetry enhancements to its capabilities. Also given is a broader set of analytics and visualization tools. SecureAuth provides some threat and fraud detection capabilities as part of the overall solution by ingesting third-party identity fraud information such as Telesign, Telephony fraud detection from Nexmo, and 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 is available through its built-in KrakenD implementation. The product includes a Security Token Service. Also, API key mechanisms are used to ensure that only known applications are able to connect to the SecureAuth platform. Missing is direct support for verifiable credentials, although the solution does support integrations with third-party identity proofing providers.

SecureAuth's solution is implemented in a microservice architecture that can support on-premises, cloud, and hybrid deployment models as well as air-gapped environments. The product can be delivered SaaS, software deployed to a server, virtual appliance, or Docker container. A managed service option is not available. Software deployments require a Windows 2019 or Windows 2016 operating system, although a

hardened version of Windows 2019 is currently included with the SecureAuth Virtual Appliance option. Installations of on-premise agents support CentOS and RHEL. Also, a wide range of application servers and database servers are supported. Its SaaS offering supports fully multi-tenancy and is hosted by SecureAuth on AWS. Almost all of SecureAuth's functionality is available via REST APIs, although Webhooks, SCIM, LDAP, and RADIUS are also available. CLI support is not given. SDKs are given that support Java, .NET, Python, Go, Ruby, and JavaScript programming languages and SDKs for Android and iOS platforms. The product has been independently certified to support compliance with FIPS 140-2, ISO/IEC 27001, and SSAE 18 SOC 2 standards. Third-party integrations are possible for ITSM, threat intelligence, EPP, EDR, analytics, and AI/ML solutions.

SecureAuth, as a privately held company, has a large customer base in medium to enterprise organizations, predominantly in North America, with some growth in the EMEA and APAC regions. SecureAuth continues to move in a positive direction and appears in both the product and innovation leadership categories of this Leadership Compass and shows particular strength in API security, identity federation, and authentication, making it an appealing Access Management for an organization in North America, focusing on these capabilities.

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

SECUREAUTH

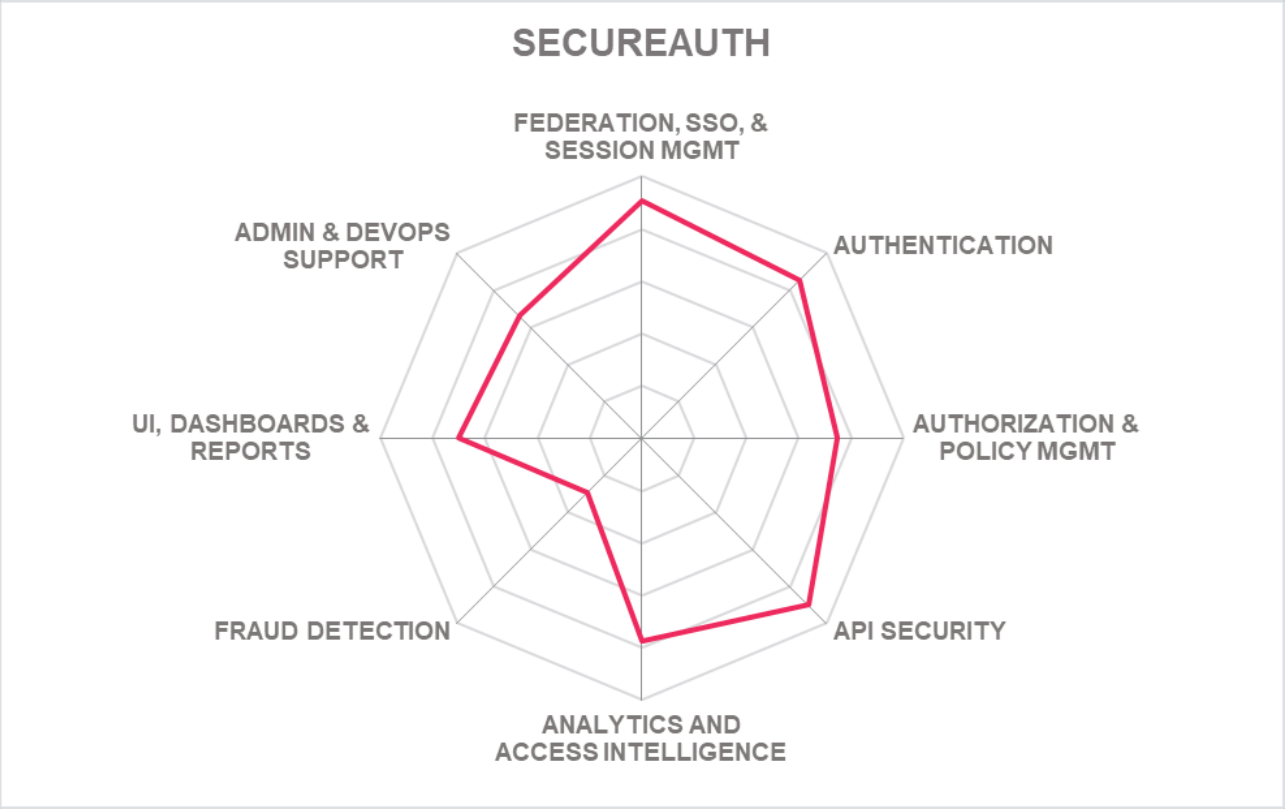
Strengths

- API security
- Identity federation
- SSO and session management
- Good authentication support
- Full FIDO support
- Contextual & risk-based authentication
- Analytics and access intelligence
- Delegated policy management
- Third-party identity proofing support
- Good ecosystem of IAM partners

Challenges

- Heavily concentrated in the North American market
- Only RBAC and user-group-based access policy principles are supported
- Missing OOB reports for major compliance frameworks.
- Limited fraud detection
- A managed service option is missing

Leader in


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

5.24 SecurID

SecurID, an RSA business, provides authentication, access & SSO, and governance and lifecycle security solutions. RSA, formerly part of Dell Technologies, had been acquired by the Symphony Technology Group in 2020 and is now a privately owned and independent company. RSA is a leading security solution provider. SecurID Identity Platform provides Authentication, Access & SSO and Identity Governance and Lifecycle Management (IGL). Primarily targeted at organizations' B2B and B2E access management requirements, 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.

SecurID core Access Management capabilities give good support for basic authentication methods as well as strong support for hardware authenticators. Both iOS and Android biometric authenticators are offered, such as Android and iOS face and fingerprint biometrics. However, some more advanced biometrics are missing, such as iris scan and voice recognition. SecurID is FIDO2 certified with broad support for USB, BLE, and NFC security keys. SecurID, however, does not support the older FIDO UAF protocol.. Also supported are FIDO2 security keys, Windows Hello, and Android phones. The level of contextual and risk-adaptive authentication depends on the customer's license level. A Base Edition license allows administrators to construct policies based on the user's IP Address. An Enterprise Edition 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. A Premium license includes all attributes and adds Threat Aware Authentication and Identity Confidence capabilities. 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, CBAC, PBAC, and RAdAC, 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. SecurID can act as both a SAML IDP and SAML SP. Support for federation-related standards includes SAML2, OIDC, WS-Federation, and JWT. SSO for traditional web applications is supported through an optional reverse proxy component. SSO for non-web applications and IT systems is also possible when using a browser-based authentication flow or when SecurID leverages HTTP-Federation, which uses password vaulting and form POST behind the scenes on a user's behalf. SCIM is not supported.

SecurID provides a straightforward and efficient administration UI with tab-based navigation. Dashboards can display different widgets containing charts and graphs of security information such as authentication attempts or user behavior over time. Also, good support for reporting, including IGA related reports and support for major compliance frameworks reports OOB. The SecurID platform provides limited fraud detection support through behavior and context analysis, although Outseer, formerly RSA Fraud & Risk Intelligence, has a platform to help organizations with fraud detection. Optionally, third-party solutions can notify SecurID thru a REST API regarding high-risk users and either forces them to step up the next time or even lock them out. SecurID API security supports content filtering 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. Verifiable credentials are not supported, although SecurID is developing a verifiable credentials verification service.

All of the SecurID solutions are cloud-based SaaS solutions implemented in a microservices architecture and hosted on Microsoft Azure leveraging its global datacenters. SecurID supports on-premises OTP Tokens, with the SecurID Identity Planform in the cloud. SecurID allows for a hybrid model with authentication and governance & Lifecycle capacities. The hybrid model requires the SecurID Identity Router (IDR) virtual appliance that acts as a secure proxy between the cloud and the on-prem environment. The on-premises version of the SecurID solution is deployed as a hardware or virtual appliance that includes all the necessary for the operation that consists of a hardened SuSE operating system, PostgreSQL database, and WebLogic application server. No external components are required. Also, a managed service is offered through SecurID partners. Almost all SecurID Access solution functionality is primarily available via REST APIs. CLIs allow admins to perform bulk operations, view logs and manage services. SDKs support various programming languages and provide an OpenAPI interface definition source file containing details on the SecurID Authentication API REST endpoints and JSON objects. The solution has been independently certified to support compliance with standards such as SOC2 Type 2, FIPS 140-2, FedRAMP, and ISO9001:2015, to name a few.

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

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

RSA SecurID®

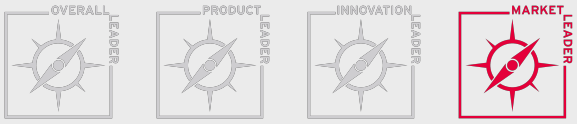
Strengths

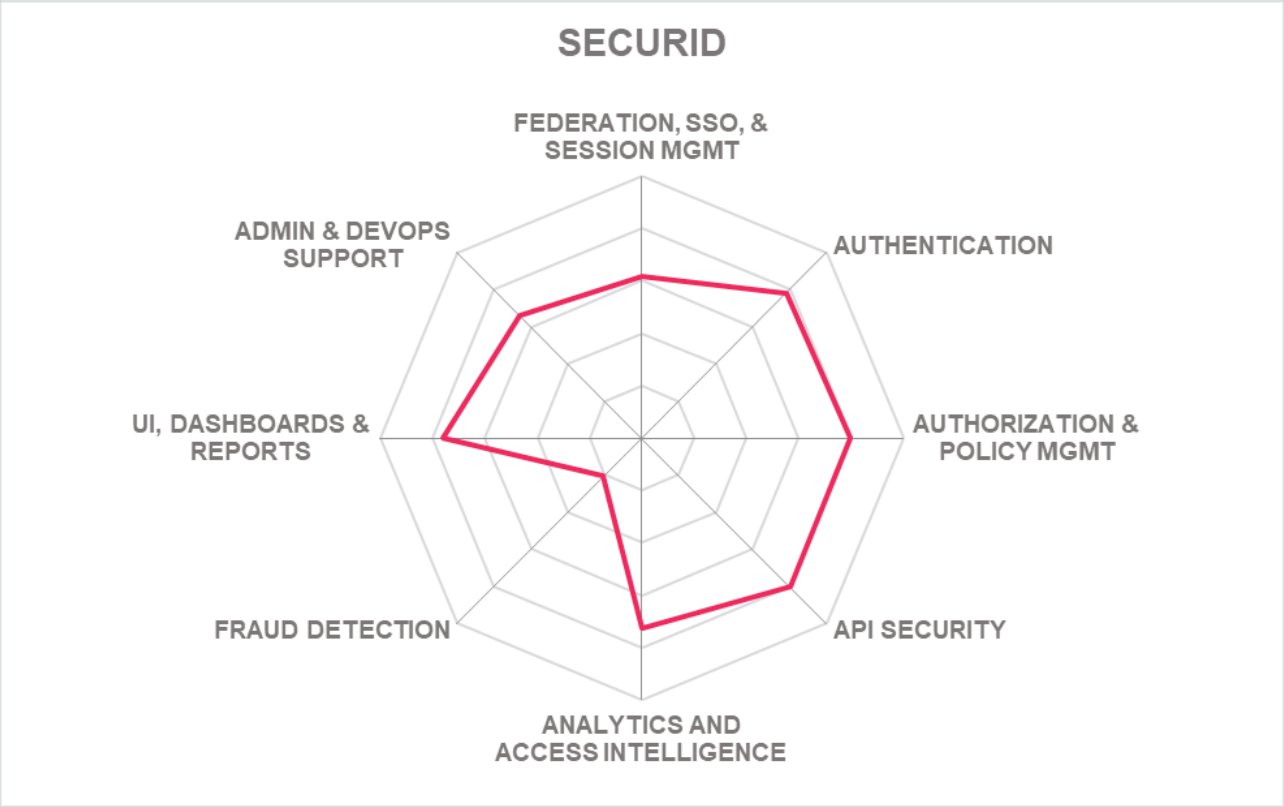
- Hardware authenticator support
- Adaptive authentication
- Authorization and policy management
- API security
- Good UI, dashboards and reporting
- Admin and DevOps support
- Good support for standards compliance
- Support for non-web based & legacy applications
- Professional service and partner ecosystem

Challenges

- Moderate identity federation capabilities
- Limited fraud detection
- Missing support for many popular authenticator apps.
- Missing verifiable credentials support
- Some API security features rely on Microsoft Azure

Leader in




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

5.25 Simeio Solutions

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

Simeio's gives good support to most authentication methods, including OTPs, some popular authenticator apps, full support for FIDO UAF, U2F, and FIDO 2 for Microsoft Windows Hello and YubiKeys. Support for Android and iOS biometric authenticators is available, although support for more advanced voice recognition or iris scan biometrics is unavailable. Also, less support is given for hardware tokens, supporting only 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. Imports and exports via XACML are also possible. User access management supports ABAC, RBAC, CBAC, PBAC, and RAdAC, and user-group base principles. Role management is given with role mining and discovery capabilities available. Sessions can be managed in server cache or external storage. User web sessions can be controlled via Session HTTP Headers and browser cookies and the configuration of various session time-out capabilities. Good detection of session attacks and protection are 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 UMA.

Simeio has worked towards a unified UI for all IAM Services. Simeio provides a modern UI framework with dashboard widgets displaying various customizable security metrics and graphs, although the look and feel are basic. User self-service registration is given with a code-based (not graphical) workflow that can be tied into an identity proofing service. Good reporting capabilities are available, including IGA and AG-related reports and strong support for reports based on major compliance frameworks out-of-the-box. Online Fraud Detection (OFD) is a part of the access management solution, in which third-party fraud detection and prevention tools can be used such as Arxan Threat Analytics, Behaviosec, IDDataWeb, Imperva, iovation, Preempt security, Telesign, and ThreatMetrix. In-network fraud reduction intelligence sources can also be used. Bot detection of unauthorized account takeover is available via an integration with Signal Sciences. Simeio also provides its own Identity Proofing application. API security utilizes the AWS API Gateway to protect APIs exposed to the internet or customer-facing APIs. 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. Its API gateway mechanism provides attack analysis, schema validation, and API key management. Verifiable credential support is not provided, although it's on their long-term roadmap.

Simeio Identity Orchestrator is implemented in a microservices architecture and supports primarily the cloud with an on-premises option and a hybrid deployment model. Its SaaS offering is fully multi-tenant, providing isolation at the network layer, not the application layer, and is hosted on AWS, Azure, and Oracle cloud platforms. Both virtual appliance and container-based delivery options are provided. Supported container-based platforms include Docker, Rancher Labs, and Pivotal. Simeio also provides support options for IaaS installations, which include 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 on-premises when delivered as software deployed to a server. All Access Management functionality is available via the UI via REST APIs, and LDAP, SCIM, and Webhook APIs can be enabled upon customer request. Only some access is available via CLI. Only SDKs for Java and .NET are available. Integrations to third-party services include ITSM, Threat Intelligence, EPP, EDR, and UEM solutions. The product has also been independently certified to support compliance with FIPS 140-2, NIST 800-57, ISO/IEC 27001, and AICPA SOC 2 standards.

Simeio is a leader in the product and innovation categories of this Leadership Compass, offering good Access Management capabilities as part of the Simeio Identity Orchestrator solution. Simeio supports enterprise 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 give a viable alternative to several established vendors. Organizations that lack IAM knowledge and expertise internally will require detailed guidance and support for transitioning existing on-prem Access Management to the cloud. Simeio should be considered by organizations primarily in the North American and EMEA regions.

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

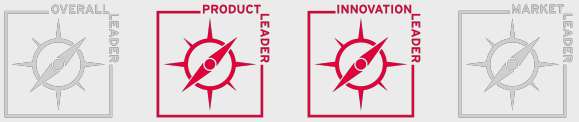
Strengths

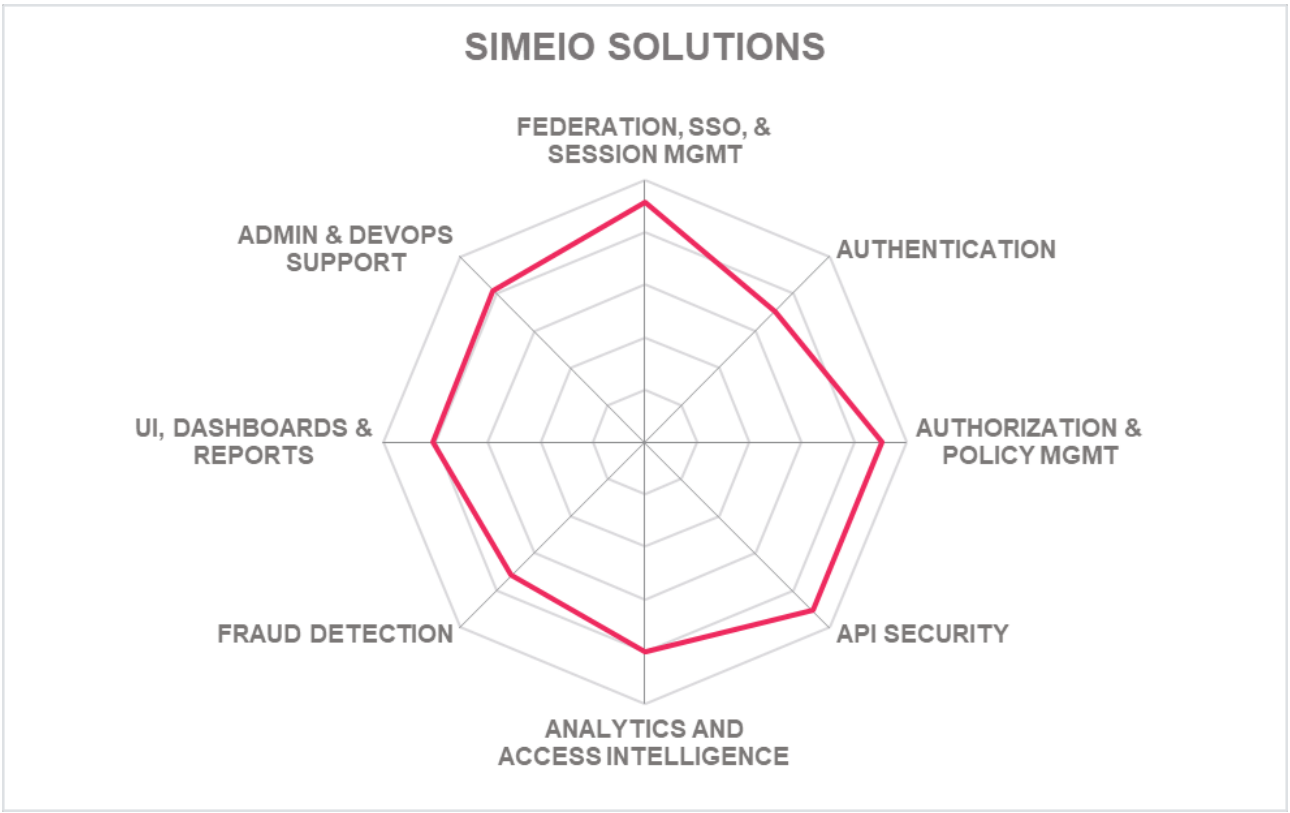
- Identity federation
- Session management and SSO
- Authorization and policy management
- API security
- Good use of analytics and access intelligence
- Full FIDO support
- Good reporting support
- Admin and DevOps support
- Fraud detection capabilities
- Analytics and access intelligence
- Good third-party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

Challenges

- SDK support to functionality is limited, although REST APIs are available
- Good ability to execute in North America, but limited system integrator partner network on a global scale
- Lack of focus on the SMB market
- Missing verifiable credential support
- A wide-spread reputation of being a global SI vendor than an IDaaS vendor, although its IDaaS reputation is becoming well established

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


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

5.26 Thales

The Thales Group, based in France, acquired Gemalto in 2019, which brought SafeNet Trusted Access to its portfolio as its primary access management product. SafeNet Trusted Access offers a single product with multiple services in a suite that includes directory, SSO, MFA, policy and authorization, reporting, anomaly detection, and targets B2B, B2E, B2C, and G2C market segments.

SafeNet Trusted Access core Access Management capabilities include good support for some 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. Also missing is support for QR Code authenticators, although interestingly a QR Code can be used to setup the SafeNet MobilePASS+ mobile app. FIDO UAF is not supported, although FIDO U2F and FIDO 2 support is given for a range of FIDO SafeNet IDPrime, eToken, and IDCore models. Good contextual and risk-adaptive authentication is given supporting location, user, network, and device contexts and 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, RAdAC, ReBAC, and group-based principles. Basic role management and entitlements discovery is possible, although role mining is not. Also, support for delegated policy management is available. Web session management is basic and lacks capabilities for session attack detection and session protection other than protection given through a digitally signed browser cookie and a protection mechanism against session hijacking. SSO is supported across OIDC and SAML web applications. Secure token translation for SSO across multiple applications supports Kerberos to SAML or OIDC only. Identity federation supports IdP and SafeNet Trusted Access supports redirection to external IDPs which allows it to serve as the service provider. Support for federation-related standards includes SAML 2, OIDC, and WS-Federation.

The SafeNet Trusted Access administration UI provides multiple customizable dashboard widgets and views of security-related information. A user self-service registration is given with a simplified workflow. A good set of reporting capabilities includes some IGA related reports and support for major compliance frameworks that are available out-of-the-box. Fraud detection capabilities are available via the Thales Gemalto IdCloud platform. Integrations to third-party fraud detection and prevention is limited to Behaviosec when used in the context of the Gemalto IdCloud platform. 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. Verifiable credentials support is offered through the Thales MobileID to connect to national identity schemes for identity validation and verifying credentials. The Thales Digital ID Wallet also offers in-person verification.

SafeNet Trusted Access supports a public cloud deployment that is fully multi-tenant SaaS implemented in a microservice architecture. Support for IaaS installation is not available. Depending on the product component, on-premises and private cloud components are delivered as software deployed to a server or a Docker container. Some on-premises deployment installed on Windows, and some agents are available for

CentOS, RHEL, AIX, and Solaris. A managed white-labeled cloud service is also offered. More than half of the solution's functionality is accessible via SOAP, REST, and SCIM APIs. CLI access to SafeNet Trusted Access capabilities is not given, although professional services can provide API-based PowerShell scripts when requested. SDKs provide Access to nearly product functionality and are available for the Android, iOS, Java, C/C++, .NET, and Python programming languages. The product has been independently certified to support compliance with a wide range of standards, including FIPS, NIST, ISO, and eIDAS, to name a few.

The Thales Group was established in 2000 with a primary customer focus on mid to large organizations and governments in the EMEA and North American markets, with some growth in the APAC and other regions. Thales Group centers on ground transportation, aerospace, space, defense, and digital security. The Thales Group SafeNet Trusted Access has a particular strength in authentication capabilities. Organizations with strong multi-factor and API security Access Management requirements with a useful UI, dashboards, and reporting capabilities should consider SafeNet Trusted Access.

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

THALES

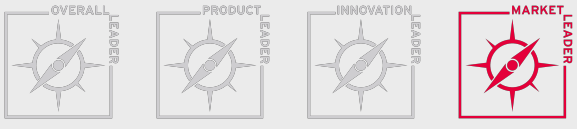
Strengths

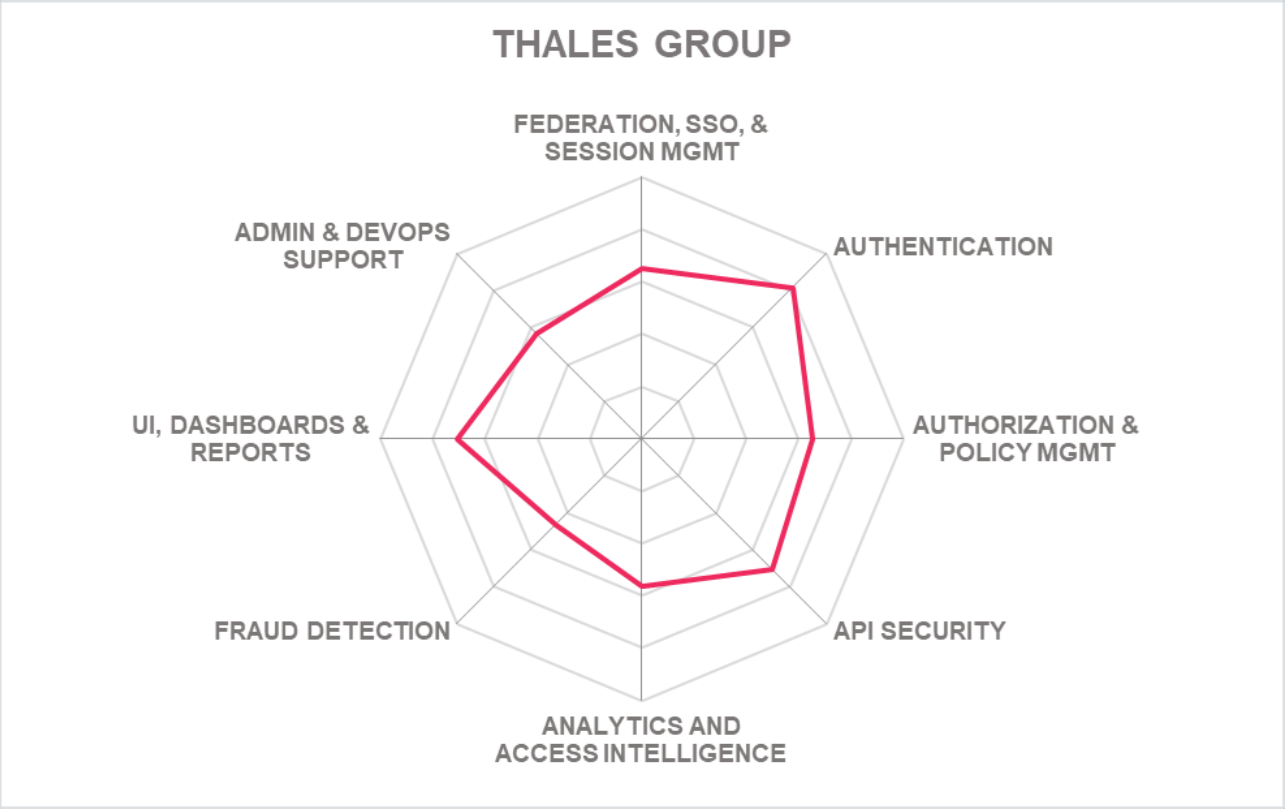
- Good authentication support
- API security
- Modern UIs and dashboards
- Authorization and policy management
- Delegated policy management support
- FIDO support
- Good contextual & risk-adaptive authentication
- Good reporting capabilities
- Strong partner ecosystem

Challenges

- Moderate identity federation support
- Basic session management and SSO
- Fraud detection relies on the Thales Gemalto IdCloud platform
- Limited on-premise deployment options
- Moderate admin and DevOps support
- Some limitation to functionality via APIs

Leader in




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

5.27 United Security Providers

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. USP provides both products and services that include USP Connect for cybersecurity services, consulting services, USP Network Authentication system, and its USP Secure Entry Server for Web Access Management which is evaluated in this Leadership Compass. 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.

United Security Provider has designed SES to provide an Access Management and Identity Federation solution to meet its customer's business requirements regarding agility, performance, user experience, and security. SES provides good authenticator options, including OTPs, many popular authenticator apps, and Android & iOS facial and fingerprint biometric options. More advanced biometrics such as voice recognition or iris scan options are unavailable. Good FIDO support is provided as well as the strong support of many popular hardware tokens. Contextual and risk-adaptive authentication includes the utilization of device, network, user, and location-based information, in which these contextual attributes can be used in the SES access policies. Its centralized policy management supports ABAC, RBAC, CBAC, PBAC, RAdAC, and user group policy principles. Basic role management is provided, although role mining or discovery is not. Also, delegated policy management is supported. Device management such as device registration and tracking are not given, although device fingerprinting is available. Further, an integration option to the third-party MobileIron is possible. Strong session management capabilities are available in which user browser sessions can be managed via browser cookies or session HTTP headers. Also, good session attack detection mechanisms can be used. Good SSO is also available across web applications, and the integration of legacy web applications unable to support federation standards can be supported via a reverse proxy integration with authentication enforcement and security context/user identity propagation within the reverse proxy. SES provides strong identity federation capabilities and supports a wide range of federation standards.

A good administration UI is provided some good security dashboard views. User self-service allows for self-registration is available through SES's login portal and provides good workflows. The user self-service registration is also exposed as a REST API. The reports are generated from the dashboards showing real-time data, and dashboards can be ad hoc and custom-defined. The SES WAF component turns the product suite into a full web security platform by protecting applications and managed data from common threats. For API security, a broad set of filters and validators within the product itself protects API endpoints such as content filtering, rate limiting, and detection of protocol-specific attacks. API keys can be used to block anonymous traffic and filter logs by API key. SES supports integrations with the third-party verifiable credential provider SwissID. Missing are fraud detection capabilities.

USP SES supports on-premises, public, private, and multi-cloud deployment models. Both hybrid and air-gapped deployment models are also supported. A managed service is offered as well. Hardware and virtual appliance delivery options are given, as well as container-based options and software installed on a

customer's server. Docker, Red Hat OpenShift, Google Anthos, and Exoscale SKS container-based platforms are supported. When SES software is installed on a customer's server, CentOS, RHEL, and SUSE operating systems are supported as well, as a good set of application server options are given. A SaaS option is not available, although IaaS support options include AWS, Exoscale, and Azure. A small percent of SES functionary is available via REST APIs. CLI access to SES capabilities is not available, although SDKs are provided for the Java and Groovy programming languages. The solution can also integrate with a third-party Threat Intelligence solution. SES has been independently certified to support compliance with TÜV Germany standards.

United Security Provider's initial and primary target market is the DACH region of Germany, Switzerland, and Austria, with some growth in southern Europe. It has a greater global reach for its professional service. United Security Providers Secure Entry Server's offering provides good core access management capabilities that will be of interest to potential customers in their primary target DACH region.

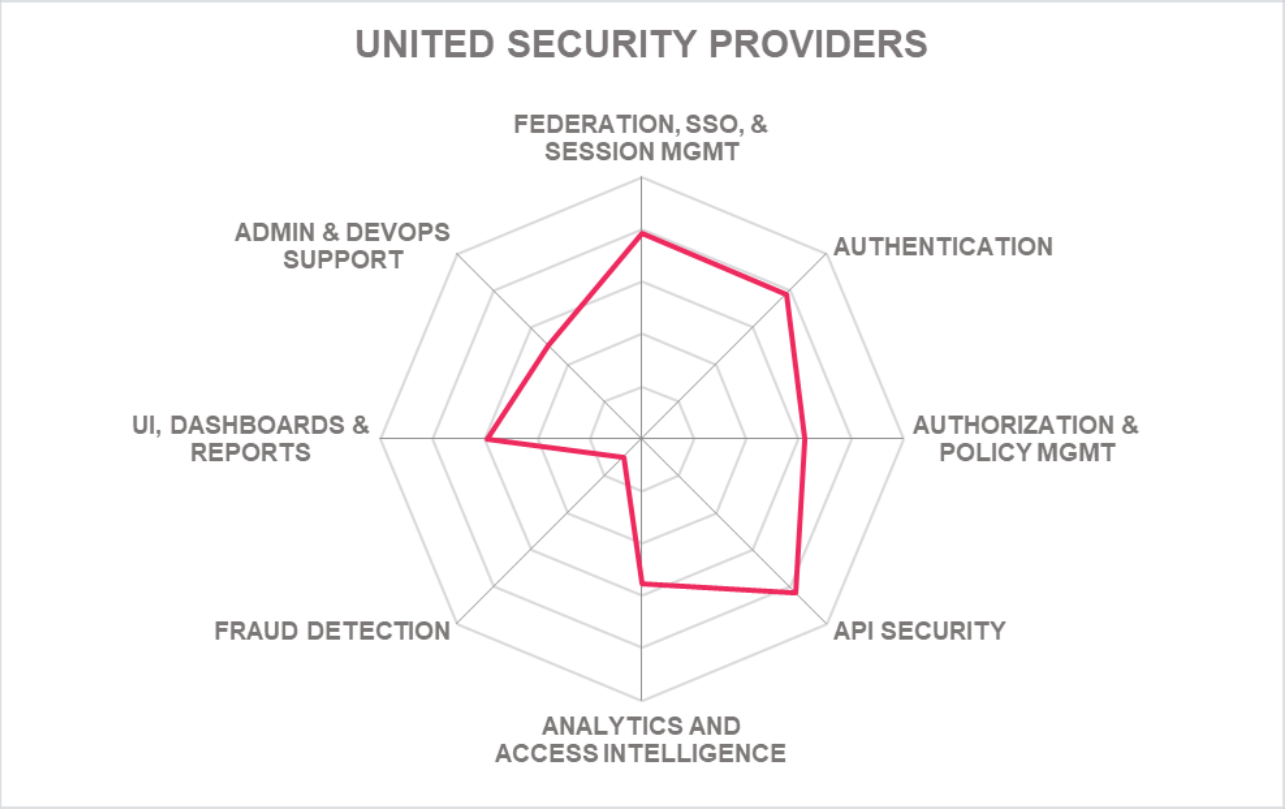
Security	●●●●●
Functionality	●●●●○
Deployment	●●●●○
Interoperability	●●●○○
Usability	●●●○○

Strengths

- API security
- Identity federation
- SSO and session management
- Wide range of authenticator options
- Good set of security dashboards
- UI, dashboards and reporting options
- User self-service with good workflow support
- Authorization and policy management
- Good container-based platform support
- Global professional services

Challenges

- Limited market presence outside of the DACH region.
- Weak fraud detection capabilities
- Limited device management
- Limited access to product functionality via APIs, CLI and SDKs
- Missing integration with third-party ITSM products


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

5.28 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, the WSO2 Identity Server focuses on Access Management capabilities.

WSO2 Identity Server core Access Management capabilities include support for OTPs, QR Codes, RADIUS, Kerberos, client-side certificates, and popular mobile authenticator app, as well as good support for hardware tokens. Support for biometric authentication is missing, although support third-party biometric authentication integrations with VeridiumID and Aware Biometrics are available. FIDO U2F support is given as well as passwordless authentication with FIDO 2, although FIDO UAF is not. 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 authoring and editing of XACML 3 policies, although the XACML templates work with raw XML, requiring some technical knowledge. Within policies, ABAC, RBAC, CBAC, PBAC, RAdAC, and user-group-based principles can be used in combination as well. Basic role management is given, but role discovery of mining capabilities is 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, based on the browser cookie. Good sessions attack detection and protection are available, including detecting abnormal logins and abnormally long sessions. The Identity Server session operations can be published to the WSO2 Identity Analytics Server. WSO2 supports SAML as a first-class authentication protocol in the product and provides an agent library for application developers to implement SAML in their client applications.. Secure token translation between standards and 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.

WSO2 Identity Server console provides a good administrative UI allowing the management of users, groups, roles, and approvals, amongst other functionality that can easily be enabled or disabled using a toggle-based control used throughout the console. The user self-service registration is available through the login portal via the REST API. Reports are generated from the WSO2 Identity Analytics Server as well as a number of defined dashboards out-of-the-box. Missing are out-of-the-box reports for major compliance frameworks and governance. Fraud detection capabilities are not supported out-of-the-box, although integrations with the Identity Server using adaptive authentication scripts such as Integration with a third-party fraud reduction intelligence source. Fraudulent account creation detection is available through email and SMS verification at self-registration, reCaptcha, or workflows for approving account creations.

Additionally, Identity Server APIs, as well as external APIs, can be accessed via WSO2 API Manager's API gateway for additional API protection capabilities and managed security. Any third-party API gateway solutions can also be used, while the 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, supports 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 AWS, GCP, and Azure. WSO2 recently introduced its Asgardeo IDaaS. The Asgardeo IDaaS replaces the older generation WSO2 Identity Cloud as its developer-focused IDaaS platform. Asgardeo is built on top of the WSO2 Identity Server inheriting its features and functionalities. Asgardeo also integrates with Choreo, WSO2's iPaaS, providing a low-code environment to build, test and deploy microservices in Kubernetes, manage APIs and orchestrate integrations. On-premises and legacy applications can be connected to the IDaaS using Asgardeo Connect. One of the widest ranges of API protocols evaluated is supported, including SOAP, REST, RPC, MQTT, AMQP, OData, WebHooks, and WebSockets. Access to the Identity Server functionality via CLIs is not given, although SDK support for Android, Java, .NET, JavaScript, React, and Angular programming languages are given, and additional supported languages are on the roadmap. 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 facilitate integrations into CI/CD pipelines or with DevOps/Admin tools for automation. Integrations with third-party ITSM solutions are also available, and its partner MDM solution, Entgra.

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, as well as a promising set of upcoming features on WSO2's roadmap. 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 strong product and market challenger in this Access Management Leadership Compass.

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

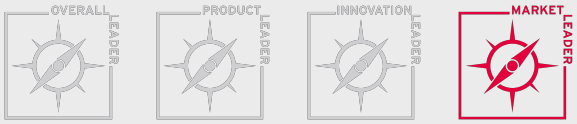
Strengths

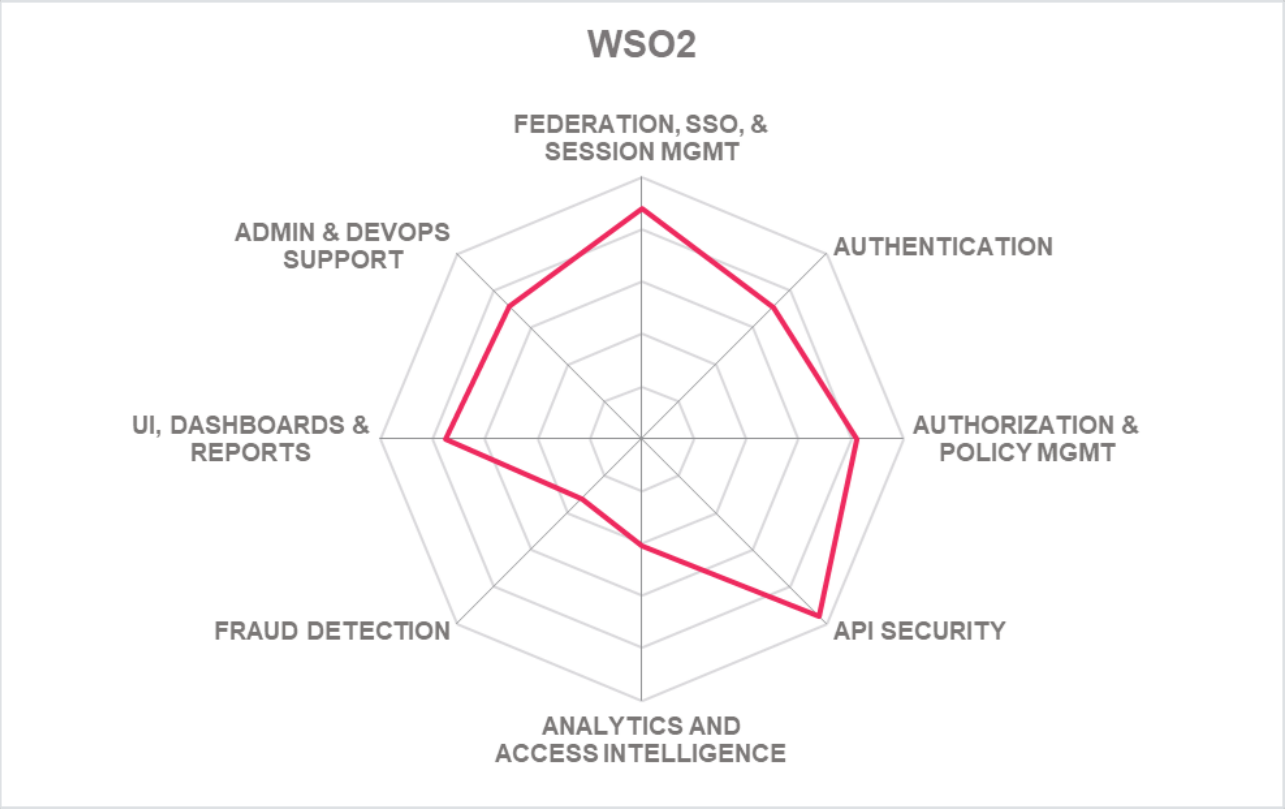
- Strong Identity federation
- SSO and session management
- Good authorization and policy management
- Session management and SSO
- Adaptive authentication
- API security via WSO2 API Manager
- Admin UI and dashboards
- Admin and DevOps support

Challenges

- XACML templates work with raw XML requiring some technical knowledge
- Limited fraud detection
- Missing biometric authenticators, although third party integration options are available
- Threat analytics and ML capabilities require third-party solutions
- Basic role management is given, but role discovery or mining capabilities are not

Leader in




WSO2
FEDERATION, SSO, & SESSION MGMT
AUTHENTICATION
AUTHORIZATION & POLICY MGMT
API SECURITY
ANALYTICS AND ACCESS INTELLIGENCE
FRAUD DETECTION
UI, DASHBOARDS & REPORTS
ADMIN & DEVOPS SUPPORT

6 Vendors to Watch

6.1 Authlete

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

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

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

6.2 AvocoSecure

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

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

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

6.3 F5 Networks

Established in 1996, F5 Networks has a strong presence with large companies in North America with a

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

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

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

6.4 Identity Automation

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

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

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

6.5 Indeed Identity

Indeed Identity was founded in 2010 as a privately-owned cybersecurity company. Indeed Identity maintains

key areas of expertise in multi-factor authentication, privileged access management, and PKI management, providing a single platform with multiple services in a suite with partial functionality provided through third-party products and services.

Indeed Identity focuses on the EMEA and APAC regions supporting medium to enterprise organizations. The Indeed Access Manager provides identity federation, SSO, and authentication, with strength in API security, and may be of interest to organizations in the EMEA and APAC regions with these core requirements.

Why worth watching: Watch for Indeed Identity's continued advancement in its capabilities through planned Access Management features on its roadmap.

6.6 Ory

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

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

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

6.7 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. Pirean provides Strong Authentication, Consumer, and Workforce IDaaS platform called Access: One.

Pirean's 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 to orchestrate the platform's capabilities.

Why worth watching: Watch Pirean continued growth backed by Exostar.

6.8 Radiant Logic

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

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

6.9 SecZetta

SecZetta is a private company headquartered in Newport, Rhode Island, United States. It offers its Third Party Identity Risk Solution, which gives the ability to manage non-employee identity lifecycles from onboarding through to offboarding and manage the needs of those third parties while in the care of the organizations securely and at the same time, providing greater efficiency.

SecZetta Third Party Identity Platform allows for API-controlled integrations with existing applications, including PAM, IAM, SSO, HRIS, and VMS tools, which can make it easier to integrate into many existing security and identity management portfolios. Its management tools can provide a good balance between maintaining strict control of third-party identities but also provide flexibility. The risk assessment and scoring capabilities are given along with an extra layer of security when allowing third-party access to infrastructure.

Why worth watching: Look for SecZetta to provide third-party identity management capabilities that work well with existing IAM, PAM, other risk management tools, and HR tools.

6.10 Signicat

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

Security, eID, and Dokobit in 2021. Signicat offers its Signicat Authentication and User Management as an Access Management offering.

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

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

6.11 Silverfort

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

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

6.12 SSO Easy

SSO Easy is a privately owned US-based company headquartered in Quincy, Massachusetts, with offices in New York and Australia. EasyConnect is SSO Easy's core enterprise SAML solution that supports both SAML 1.1 and 2.0 standards. EasyConnect can act as either an Identity Provider (IdP) or Service Provider (SP) and offers multi-factor SSO options. EasyConnect doesn't require any coding or customization but rather offers pre-configured drop-in templates that can support Google Apps or Salesforce SAML connections, as some examples. Easy SSO can be implemented on-premises or in the cloud. For cloud deployments, Easy SSO provides Amazon EC2 support. EasyConnect also includes a set of built-in REST APIs to facilitate integrations with any client environment. Out-of-the-box support is given for AD and LDAP,

Kerberos/IWA/NTLM, popular applications, web servers, and form-based authentication support.

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

6.13 TrustBuilder

TrustBuilder was founded in 2017 with offices in Belgium, and New York, NY, USA., and shortly after debuted its TrustBuilder Identity Hub for the financial services market. In recent years, TrustBuilder has added IdPs and applications to its TrustBuilder.io Service Catalog, moved its offering to the cloud, and added HR services for Retail Banks and Financial Services. Today, TrustBuilder has joined the inWebo Group, an independent vendor of MFA solutions.

Why worth watching: Look for TrustBuilder to continue to build out its end-to-end C/IAM solution.

7 Related Research

Executive View: 1Kosmos BlockID - 79064
Executive View: Cloudentity Authorization Control Plane - 80539
Executive View: CyberArk Privilege Cloud - 80122
Executive View: EmpowerID - 70297
Executive View: Ergon Airlock Suite - 72509
Executive View: Evidian Identity & Access Management - 70872
Executive View: ForgeRock Access Management - 80319
Executive View: Hitachi ID Bravura Privilege - 80447
Executive View: IBM Cloud Identity - 79065
Executive View: Ilantus Compact Identity - 80177
Executive View: Micro Focus Access Manager - 80311
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: Oxyliom Solutions GAÏA Advanced Identity Management - 80175
Executive View: Ping Identity's PingFederate - 80330
Executive View: PortSys Total Access Control - 80556
Executive View: RSA SecurID® Access - 70323
Executive View: SecureAuth IdP - 71327
Executive View: Simeio Identity Orchestrator - 80549
Executive View: Symantec Privileged Access Manager - 80331
Executive View: Thales SafeNet Trusted Access Platform - 80547
Executive View: United Security Providers Secure Entry Server - 79040
Executive View: WSO2 Asgardeo - 80553
Executive View: WSO2 Identity Server - 80060
Leadership Compass: Access Governance & Intelligence - 80098
Leadership Compass: API Management and Security - 80477
Leadership Compass: Cloud-based MFA Solutions - 70967
Leadership Compass: Enterprise Authentication Solutions - 80062
Leadership Compass: IDaaS Access Management - 79016
Leadership Compass: Identity API Platforms - 79012
Market Compass Providers of Verified Identity - 80521

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 within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

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

Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack 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 they become Overall Leaders by being above average in all areas.

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

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

- **Security
- Functionality
- Deployment
- Interoperability
- Usability**

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

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

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

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

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

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

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

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

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position

- Financial strength
- Ecosystem

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

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

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

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

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

Rating scale for products and vendors

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

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

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral

Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.

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

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

Inclusion and exclusion of vendors

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

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

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