KuppingerCole Report

LEADERSHIP COMPASS

by Richard Hill & Martin Kuppinger | February 2019

Access Management and Federation

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

by **Richard Hill**
rh@kuppingercole.com
February 2019

by **Martin Kuppinger**
mk@kuppingercole.com
February 2019

Leadership Compass
Access Management and Federation
By KuppingerCole

Content

Content of Tables

Content of Figures

Related Research

Advisory Note: The new ABC for IT: Agile Businesses, Connected - 70998

Advisory Note: Connected Enterprise Step-by-step - 70999

Advisory Note: IAM Predictions and Recommendations 2014-2018 - 71120

Executive View: AdNovum Nevis Security Suite - 71094

Executive View: CA SiteMinder® - 71022

Executive View: EmpowerID - 70894

Executive View: Ergon Airlock Suite - 72509

Executive View: Evidian Identity & Access Manager - 70872

Executive View: ForgeRock Identity Platform - 70296

Executive View: IBM ISAM - 79066

Executive View: Oracle Identity and Access Management Suite Plus 11g R2 - 70917

Executive View: Ping Identity PingOne® - 70288

Executive View: Ubisecure Identity Server - 70838

Executive View: WSO2 Identity Server - 71129

Leadership Compass: Adaptive Authentication - 79011

Leadership Compass: Identity Provisioning - 71139

Leadership Compass: Privilege Management - 72330

Leadership Compass: Identity as a Service: Cloud-based Provisioning, Access Governance, and Federation (IDaaS B2E) - 70319

Leadership Compass: Secure Information Sharing - 72014

Leadership Compass: Access Control / Governance for SAP environments - 71104

Leadership Compass: API Security Management - 70958

Leadership Compass: Infrastructure as a Service - 70959

Leadership Compass: IAM/IAG Suites - 71105

Leadership Compass: Access Governance - 70948

Leadership Compass: Cloud User and Access Management - 70969

Leadership Compass: Cloud IAM/IAG - 71121

1 Introduction

With the growing demand of business for tighter communication and collaboration with external parties such as business partners and customers, IT has to provide the technical foundation for such integration. Web Access Management and Identity Federation are critical technologies for that evolution. They enable organizations to manage access both from and to external systems, including cloud services, in a consistent way. Organizations have to move forward towards strategic approaches to enabling that integration, in support of the Connected and Intelligent Enterprise.

While Web Access Management technologies are well established, and Identity Federation has also been around for years; we have observed tremendous growth in interest and adoption of these technologies over the past years. Customers – and specifically their business departments – are requesting solutions for emerging business requirements such as the onboarding of business partners, customer access to services, access to cloud services, and many more. IT has to react and create a standard infrastructure for dealing with all the different requirements of communication and collaboration in the Extended and Connected Enterprise. In consequence, Access Management and Federation are moving from tactical IT challenges towards strategic infrastructure elements that enable business agility.

There are many vendors in that market segment. Most of them provide solutions for both Web Access Management and Identity Federation. The major players in that market segment are covered within this KuppingerCole Leadership Compass.

This Leadership Compass provides an overview and analysis of the Web Access Management and Identity Federation market segment, sometimes referred to as Access Management/Federation. The sole focus is on solutions that are available on premises, even while we consider the fact that several of these solutions also are offered as cloud services. This can be valuable to customers if they want to start on-premises and gradually move to the cloud.

Technologies typically support both Web Access Management as a gateway approach, sitting in front of standard applications and doing authentication and authorization for backend applications, and Identity Federation. Identity Federation is strategically the more important concept; however, support of existing applications frequently favors the use of traditional Web Access Management. In addition, some Access Management solutions add features such as self-registration of users. Others also add Reverse Proxy capabilities and, based on this, Web Application Firewall functionality, which we consider as an important and valuable add-on to the core features in-scope of this document.

Overall, the breadth of functionality is increasing. Support for social logins such as Facebook or Google+, standard support for established Cloud Service Providers, and the support for new federation and related standards such as OAuth 2.0, OpenID Connect or UMA are just some of the examples for features increasingly common for this type of product.

The entire market segment is relatively mature but still evolving, and we expect to see more changes within the next few years. However, given the surging demand of businesses, organizations now have to start with implementing a standard infrastructure for (Web) Access Management and Federation. This KuppingerCole Leadership Compass provides an overview of the leading vendors in that market segment.

Besides the established vendors providing complete IAM (Identity and Access Management) product portfolios, there are some smaller vendors with interesting offerings and also specialists that purely focus on that part of the overall IAM (Identity and Access Management) market.

Picking solutions always require a thorough analysis of customer requirements and a comparison with product features. Leadership does not always mean that a product is the best fit for a particular customer and their requirements. However, this Leadership Compass will help with identifying those vendors that customers should look at more closely.

1.1 Market Segment

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

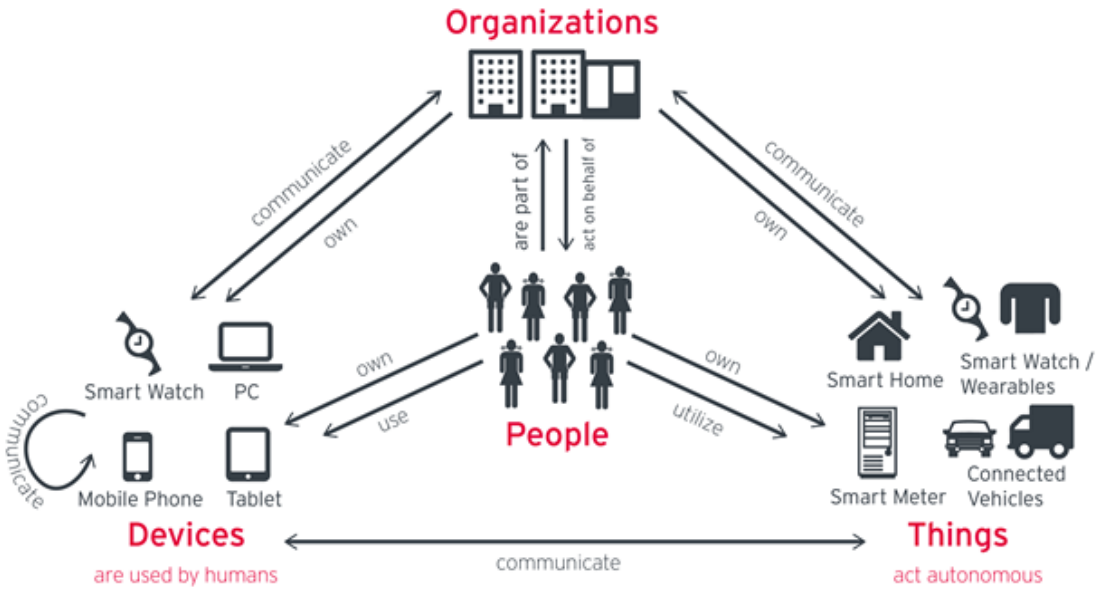


Figure 1: The Computing Troika pushes organizations to create an IT Infrastructure that goes beyond the perimeter of the organization.

Various drivers have led to this situation. At the core is the need for agility in a complex competitive landscape. Business models have to adapt more rapidly than ever before. Supply chains include more suppliers and become increasingly more complex, with reduced vertical integration in manufacturing. Organizations also need to react more rapidly to new attack vectors that are continually changing. Customers today expect vendor's systems to provide the intelligent access capabilities needed to combat these new threats than ever before. The changing workforce is also changing the idea that access to an organization's resources can only be performed on-premises breaking down the traditional perimeter model. While organizations always had challenges of their changing IT environments, the density and pace of change has increased as well as the need for IT support of a more Connected and Intelligent Enterprise.

All of these trends affect today's IT - the Computing Troika of Cloud, Mobile, Social and Intelligent Computing- stand for a shift towards an open, integrated enterprise that extend beyond the perimeter of the organization itself. Whether you tend to name this the Connected Enterprise or opt for Intelligent Enterprise does not matter. It is about the need for connecting and intelligently adapting today's on-premise IT with the outer world in various ways.

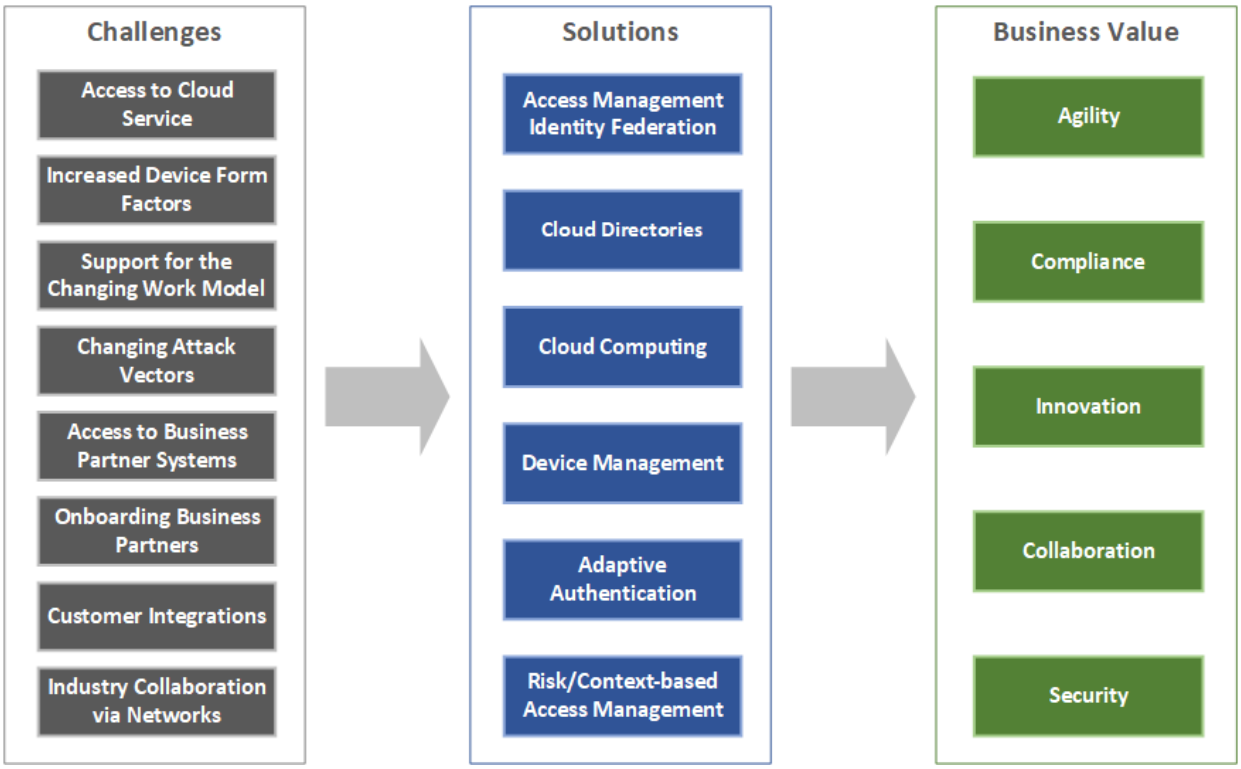


Figure 2: Supporting the Connected and Intelligent Enterprise helps organizations addressing major business challenges.

Various technologies support all the different requirements customers are facing today. The requirements are:

- Use Cloud Services: Enabling an organization to flexibly use cloud services, with maximum control of the internal and external identities using this service and the access rights they have.
- Device Form Factors: Support for the increasing number of different device form factors used in the enterprise, including desktops, tablets, mobile phones, and IoT devices
- Access Business Partner Systems: Enable your employees to have controlled access to business partner systems with flexible onboarding and full compliance; ensure that you meet the liability agreements etc. that you have with your business partners.
- Collaborate in Industry Networks: Participate in industry networks such as healthcare professional networks, allowing the re-use of identities on such networks and the controlled access by your employees to the network as well as by network members to your systems.
- Support new Working Models: Support new working models with freelancers, mobile workers, and other forms of collaboration that allow them to work from anywhere using any device
- Changing Attack Vectors: Provide IT security solutions that can quickly adapt and react to new forms of attacks using intelligent access controls.
- Onboarding of Business Partners: Allow your business partners to flexibly access your systems in a controlled, compliant way.
- Customer Interaction: Integrate your customers, support different types of identities such as social logins and self-registered identities, and extend your business processes to the customer.

Enabling this shift in IT from the traditional, internal-facing approach towards an open IT infrastructure supporting the Connected and Intelligent Enterprise requires various new technologies. Amongst these technologies are new types of cloud-based directory services, various other types of Cloud services including Cloud Identity Services, and improved technologies for authentication and authorization, such as risk- and context-based Access Management, also sometimes called “adaptive” authentication and authorization. However, the foundation is Access Management and Identity Federation which allows managing access to applications.

(Web) Access Management is a rather traditional approach that puts a layer in front of web applications that takes over authentication and – usually coarse-grained – authorization management. That type of application also can provide services such as HTTP header injection to add authorization information to the HTTP header that is then used by the backend application. Tools are increasingly supporting APIs for authorization calls to the system.

Identity Federation, on the other hand, allows splitting authentication and authorization between an IdP (Identity Provider) and a Service Provider (SP) or Relying Party (RP). The communication is based on protocols. Backends need to be enabled for Identity Federation in one way or another, sometimes by using the Web Access Management tool as the interface. Identity Federation can be used in various configurations, including federating from internal directories and authentication services to Cloud Service Providers or between different organizations.

Thus, these services are the foundation for enabling the various customer requirements mentioned above – enabling the Connected and Intelligent Enterprise without support for Access Management/Federation will not work.

In other words: 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 collaboration & communication.

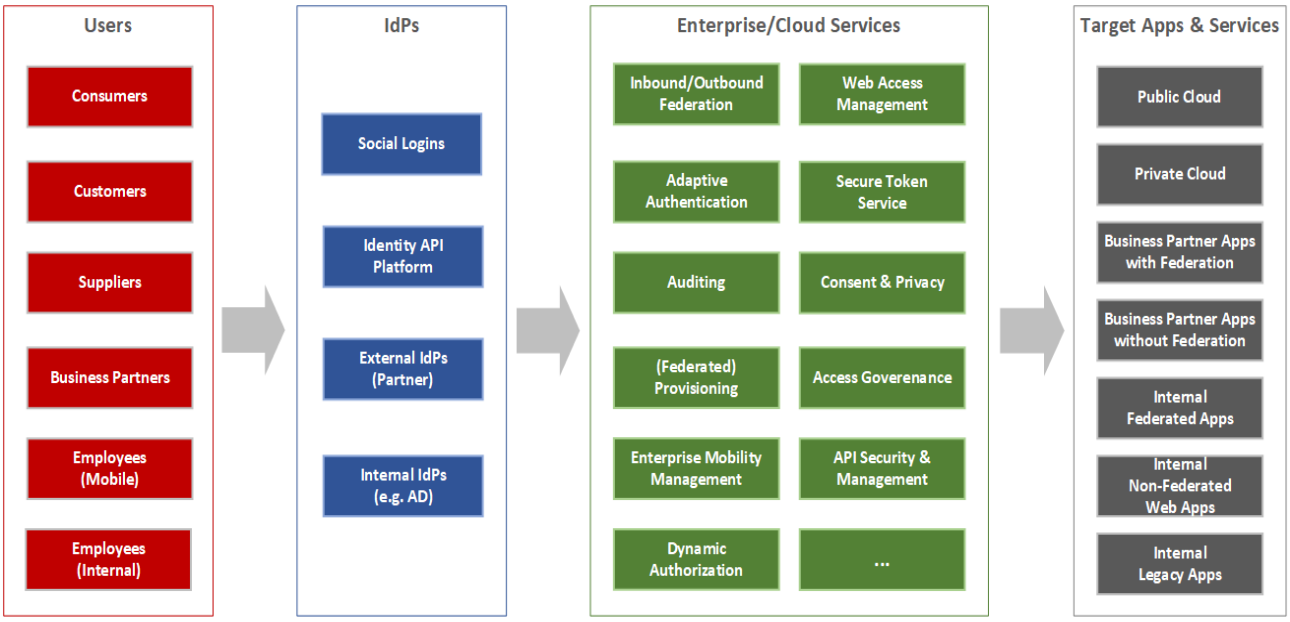


Figure 3: Dealing with all types of user populations will require adaptive authentication and federation/SSO.

The Connected Enterprise means that organizations have to deal with more and larger user populations than ever before. Beyond the employees and some externals that have been so far managed in internal systems, more business partners, customers, and even potential customers are being added. They require

access to systems, either on-premise or in the cloud. While some of the digital identities representing these persons are managed in the organization's internal directories, others will be federated in from external Identity Providers or managed by employing Cloud Directories.

Thus, especially Identity Federation is a technology that is essential for any organization. It allows the enterprise to deal with the external identities and all the different user populations.

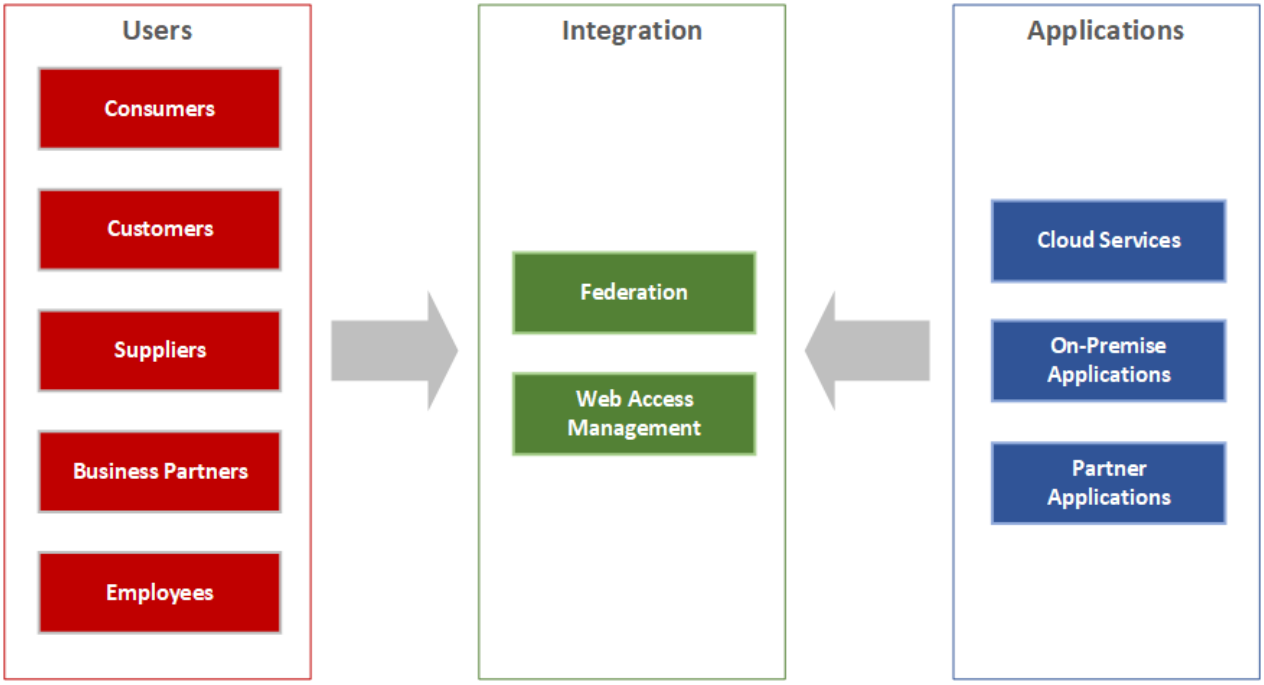


Figure 4: Federation and Web Access Management are essential technologies to connect all types of users to all types of applications

Web Access Management, on the other hand, comes into play when managing access to on-premise applications that do not support Identity Federation. While some vendors support lightweight integration to Identity Federation for such applications, in many cases customers will still rely on an upstream layer for authentication and authorization provided by a Web Access Management solution.

Based on our view on the market and the current demand, we opted for looking at both traditional Web Access Management and Identity Federation features in this Leadership Compass document. This view is underpinned by the fact that a number of vendors already have integrated their formerly separate offerings into a single product or at least a tightly integrated suite. Some few vendors either only support Identity Federation or still deliver two separate products. In the latter case, we have combined the separate products in our rating.

1.2 Delivery models

The focus is on on-premise solutions for this Leadership Compass. We also see a growing number of cloud services provided in particular Identity Federation capabilities, but also traditional Web Access Management features. However, many customers still focus on on-premise products for this area. Notably, most of the providers covered in this Leadership Compass also have cloud-based offerings, either based on the product covered in the Leadership Compass or as a separate product. This Leadership Compass only rates available cloud/SaaS (Software as a Service) versions as a positive feature, enabling customers to gradually switch to a SaaS approach.

Purely cloud-based offerings are covered in other KuppingerCole Leadership Compass documents, in particular, the Leadership Compass on Cloud User and Access Management, which includes companies such as Okta, OneLogin, Microsoft with their Azure Active Directory, and many more.

1.3 Required Capabilities

When evaluating the products, besides looking at the aspects of

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- platform support

we also considered several specific features. These include:

Federation Inbound	Inbound federation that allow organizations to accept credentials from third party services like partner organizations or social networking services. Clearly one of the most important criteria is the support for federation standards and related protocols such as SAML 2.0, OAuth 2.0.
Federation Outbound	Outbound federation that allow organizations to access external services such as SaaS applications, cloud providers and partner services. Support for single sign-on as well as federation standards and their related protocols such as SAML 2.0, OAuth 2.0 is also needed.
Backend integration	Besides supporting federation-enabled backends, there is a need for supporting existing applications. Integration with such applications, be it through APIs, HTTP header injection, or other technologies, is an important criterion for this analysis.
Adaptive Authentication	Adaptive authentication is increasingly becoming an expected capability. Support for WAM integration and interoperability via SSO is important, as well as support for multiple authenticators, ability to perform real-time risk analysis of behavioral and environmental factors, as well as the degree in which it integrates with security intelligence and forensic systems.
Registration	Registration has become more important than before which includes user self-registration, self-maintenance of attributes, and bulk provisioning.
User Stores/Directories	Here we are looking at the breadth and flexibility of support for user stores such as directory services that can be used by the Web Access Management and IdP capabilities of the products. We also look for support of virtual directory services, allowing for flexibly combining various user stores. It also includes capabilities for supporting strong and flexible (versatile) authentication of users.
Security models	Both the internal security model of the tools and the ability for fine-grain, secure management of access policies of users are important features for products in this category.

Deployment models	In today's IT environments, flexibility in deployment models is of high importance. We looked at support for soft appliance, hard appliance, and Cloud/MSP deployment models.
Customization	The less you need to code and the more you can configure, the better – that's the simple equation we took into account around customization. However, we also looked for features like a transport system to segregate development, test, and production environments. Notably, copying configuration files does not count for a transport system.
Multi-tenancy	Given the increasing number of SaaS deployments, but also specific requirements in multi-national and large organizations, support for multi-tenancy is highly recommended.

The support for these functions is added to our evaluation of the products. We've also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other offerings available in the market.

2 Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

Figure 5: The Overall Leadership rating for the Access Management and Federation market segment

The Overall Leadership rating is a combined view of the three Leadership categories, i.e., Product Leadership, Innovation Leadership, and Market Leadership. This consolidated view provides an overall impression of our rating of the vendor's offerings in the particular market segment. Notably, some vendors benefit, e.g. from a strong market presence will slightly drop in other areas such as innovation, while others show their strength, e.g. in the Product Leadership and Innovation Leadership, while having a relatively low market share or lacking a global presence. Therefore, we strongly recommend looking at all Leadership categories, the individual analysis of the vendors, and their products to gain a comprehensive understanding of the players in that market segment.

In the Overall Leadership rating chart, we see a typical mature market that remains crowded and is represented by the 15 vendors we chose to represent in our Leadership Compass rating.

In the market for Web Access Management and Federation, there are five companies in the Overall Leaders segment. These include CA Technologies, IBM, and Micro Focus as established players with strong offerings and customer base, complemented by two younger companies, ForgeRock, and Ping Identity, which have continued to hold its market share over the past few years and remains in the Leaders segment.

The remainder of the vendors fall into the Challenger segment making it considerably crowded, although there are distinct groupings. In the top group are more well-established vendors such as Oracle, Evidian, AdNovum, Ergon, and WSO2. EmpowerID clearly stands out between the first and second grouping. The second distinct grouping includes F5 Networks, One Identity, and Rohde & Schwarz Cybersecurity. Ubisecure trails in the overall rating.

None of the companies evaluated placed in the Followers section.

Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping to the product features by the company's products will be necessary.

Overall Leaders are (in alphabetical order):

- CA Technologies
- ForgeRock
- IBM
- Micro Focus
- Ping Identity

2.2 Product Leadership

The first of the three specific Leadership ratings is about Product Leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

Figure 6: Product Leaders in the Access Management and Federation market segment

Product Leadership is the view in which we focus on the functional strength and completeness of the Web Access Management and Identity Federation product. Since the Web Access Management and Identity Federation market is fairly mature, we find no followers, some challengers, and a greater number of vendors qualifying for the Leaders segment. As vendors offer a wide variety of Web Access Management and Identity Federation capabilities and differ in how well they support these capabilities, it is important for organizations to perform a thorough analysis of their Web Access Management and Identity Federation requirements to align their priorities while evaluating a Web Access Management and Identity Federation solution.

In the Product Leadership, IBM is at the top followed by ForgeRock, and Ping Identity. Other vendors in this segment include CA Technologies, Micro Focus, Oracle, Adnovum, with Evidian, Ergon, and WSO2 near the bottom border.

A third of vendors are in the upper section of the Challenger section where we find a range of good products which didn't quite make it into the Leaders sections because of maturity or missing some of the features found amongst the leaders.

Product Leaders (in alphabetical order):

- Adnovum
- CA Technologies
- Ergon
- Evidian
- ForgeRock
- IBM
- Micro Focus
- Oracle
- Ping Identity
- WSO2

2.3 Innovation Leadership

Another angle we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what customers require for keeping up with the constant evolution and emerging customer requirements they are facing. Innovation is not limited to delivering a constant flow of new releases, but focuses on a customer-oriented upgrade approach, ensuring compatibility with earlier versions especially at the API level and on supporting leading-edge new features which deliver emerging customer requirements.

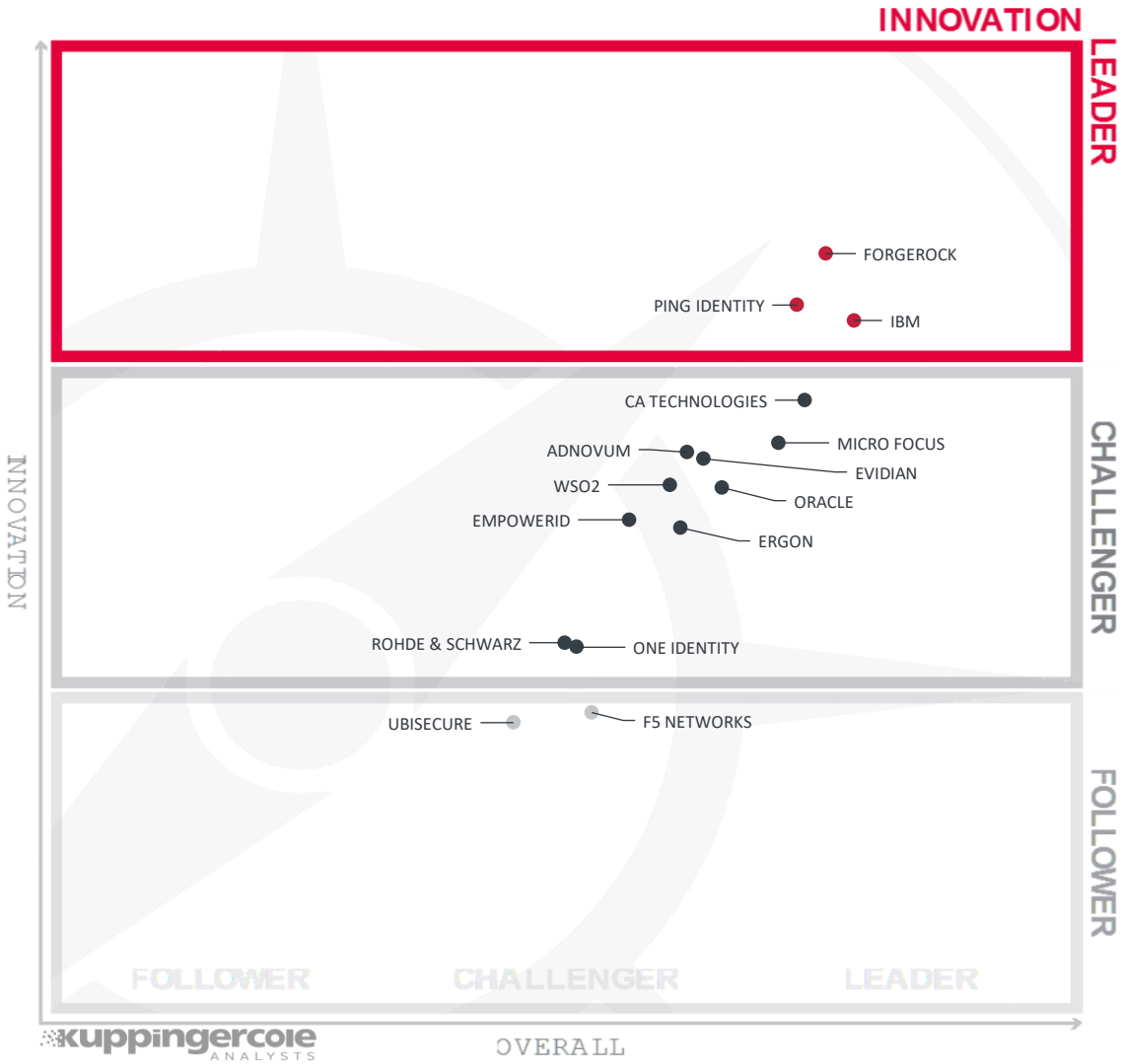


Figure 7: Innovation Leaders in the Access Management and Federation market segment

We have rated only a few vendors as Innovation Leaders in the Web Access Management and Identity Federation market, which has have driven this market forward through the innovation of their products. The leaders are ForgeRock, Ping Identity, and IBM.

The graphics need 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. Therefore, while some vendors are closer to the upper right edge, others being a little more left score slightly higher regarding their innovativeness.

In the Challenger section of Innovation Leadership evaluation, we find the majority of vendors. Given the maturity of Web Access Management and Identity Federation solutions, the amount of innovation we see is limited. The vendors, however, still continue to differentiate by innovating in niche areas.

Only two vendors are included in the Follower section, F5 Networks, and Ubisecure. Both present good products but fall behind in innovative features when compared to the other vendors.

Innovation Leaders (in alphabetical order):

- ForgeRock
- IBM
- Ping Identity

2.4 Market Leadership

Here we look at Market Leadership qualities based on certain market criteria including but not limited to the number of customers, the partner ecosystem, the global reach, and the nature of response to factors affecting the market outlook. Market Leadership, from our point of view, requires global reach as well as consistent sales and service support with successful execution of marketing strategy.

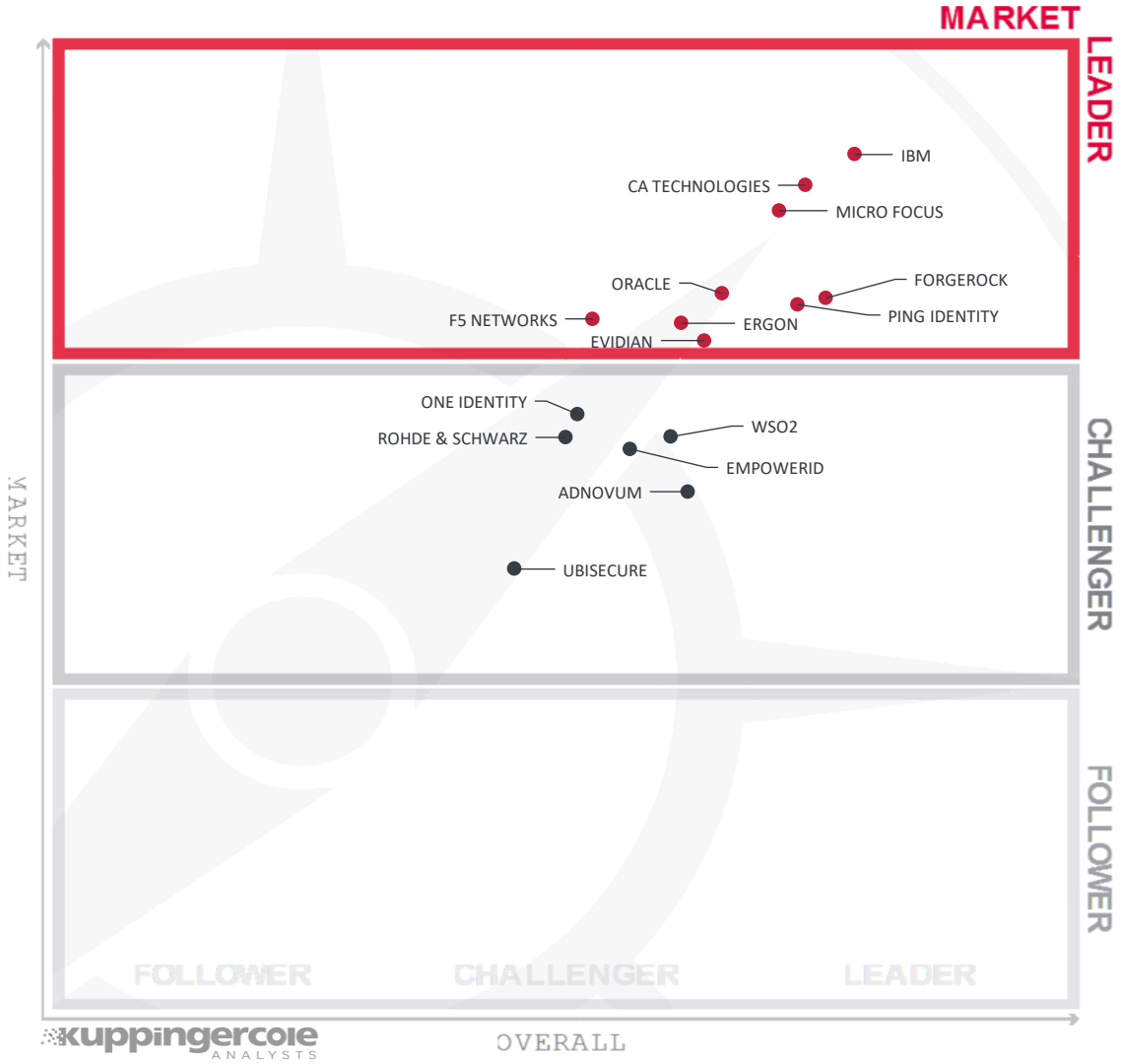


Figure 8: Market Leaders in the Access Management and Federation market segment

The Market Leadership evaluation, the top three are IBM, CA Technologies and Micro Focus primarily for their large global customer base, partner and support network. The bottom section of market leadership is comprised of ForgeRock, Ping Identity, and Oracle, followed by Evidian, Ergon and F5 Networks.

In the Challenger section, we find the remainder of the vendors have good products but may be lacking in one or more areas of their customer base, partner or support network compared to the market leaders.

Market Leaders (in alphabetical order):

- CA Technologies
- Ergon
- Evidian
- F5 Networks
- ForgeRock
- IBM
- Micro Focus
- Oracle
- Ping Identity

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for, say, 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 deliver additional analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

The first of these correlated views looks at Product Leadership and Market Leadership.

Figure 9: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

In this comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of "overperforming" in the market. It comes as no surprise that these are mainly the very large vendors, while vendors below the line are often innovative but focused on specific regions.

In the upper right segment, we find the "Market Champions", which are leading in both the product and market ratings. This segment contains IBM at the top followed by CA Technologies and Micro Focus. Others include ForgeRock, Oracle, Ping Identity, Ergon and Evidian.

F5 Networks is the only vendor to appear in the top middle box, which indicates strong market presence, although lacks the comparable feature set of the Market Champions.

In the middle right-hand box, we see the vendors that deliver strong product capabilities for Web Access Management and Identity Federation but are not yet considered Market Champions. All these vendors have a strong potential for improving their market position due to the stronger product capabilities that they are already delivering. These vendors are, from top to bottom, WSO2 and AdNovum.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not Market Leaders as of yet. They also have average market success as compared to market champions. These vendors include One Identity, Rohde & Schwarz Cybersecurity, EmpowerID, and Ubisecure.

3.2 The Product/Innovation Matrix

The second 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 few exceptions. This distribution and correlation are typical for most markets with a significant number of established vendors plus some smaller vendors.

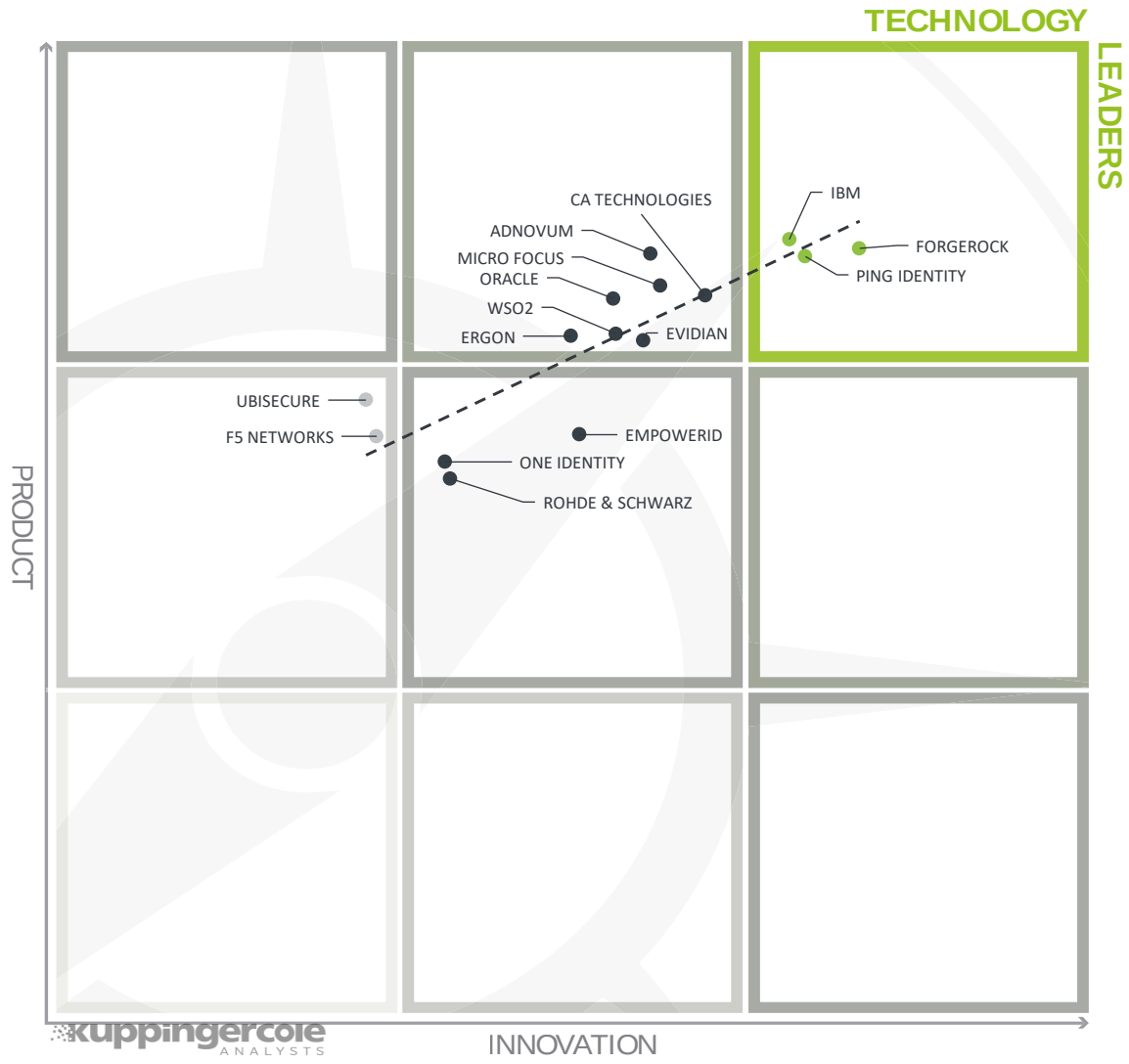


Figure 10: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we see a good correlation between the product and innovation rating, with most vendors being placed close to the dotted line indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find most of the leading vendors in the x corner, scattered throughout the box. The top-notch vendors are IBM, Ping Identity and ForgeRock with vendors placing closer to the axis depicting a better balance of product features and innovation.

The top middle box indicates vendors that provide good product features while behind the Technology Leaders in innovation. Here we find (in alphabetical order), AdNovum, Ergon, Evidian, Micro Focus, Oracle, and WSO2.

In the center of the chart, we see EmpowerID having slightly more product features and more innovation than One Identity and Rohde & Schwarz which appear further to the left of the center box.

Both Ubisecure and F5 Networks show up in the middle left box pointing to less innovation while maintaining good product features.

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 to their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors that are highly innovative have a good chance of improving on their market position but often face risks of failure, especially in the case of vendors with a confused marketing strategy.

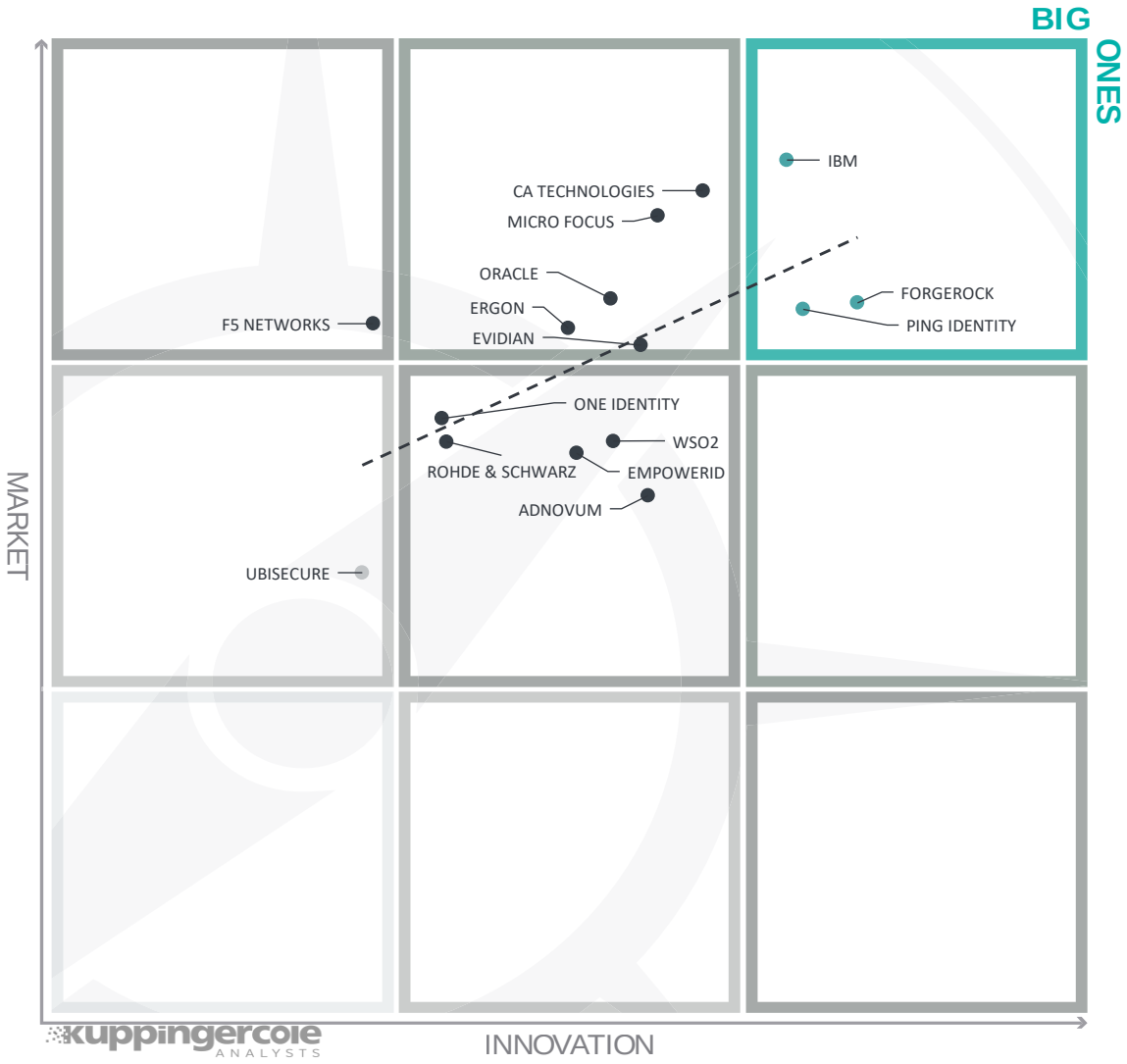


Figure 11: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relatively weak position in the Innovation Leadership rating, while vendors below the line show, based on their ability to innovate, the biggest potential for improving their market position.

In the upper right-hand corner box, we find the “Big Ones” in Web Access and Identity Federation market which are IBM ForgeRock and Ping Identity.

At the top and to the left of the Big Ones, in order of highest to lowest market, are CA Technologies, Micro Focus, Oracle, Ergon, and Evidian.

Further left at the top we find F5 Networks indicating better market than innovation position.

The segment in the middle of the chart contains the vendors rated as Challengers both for Market and Innovation Leadership, with (in alphabetical order), AdNovum, EmpowerID, One Identity, Rohde & Schwarz Cybersecurity, and WSO2.

Finally, although Ubisecure operates favorably in their own smaller geographic market, Ubisecure appears in the middle left box in this segment.

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 Web Access Management and Identity Federation. 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.

4.1 Ratings at a glance

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

Product	Security	Functionality	Integration	Interoperability	Usability
ADNOVUM	strong positive	strong positive	positive	strong positive	strong positive
CA TECHNOLOGIES	strong positive	strong positive	positive	positive	strong positive
EMPOWERID	positive	positive	positive	neutral	positive
ERGON	strong positive	positive	positive	positive	strong positive
EVIDIAN	strong positive	strong positive	positive	positive	strong positive
F5 NETWORKS	positive	positive	positive	positive	strong positive
FORGEROCK	strong positive	strong positive	positive	strong positive	strong positive
IBM	strong positive	strong positive	strong positive	positive	strong positive
MICRO FOCUS	strong positive	strong positive	positive	positive	strong positive
ONE IDENTITY	positive	positive	neutral	neutral	positive
ORACLE	strong positive	positive	positive	positive	strong positive
PING IDENTITY	strong positive	strong positive	positive	strong positive	strong positive
ROHDE & SCHWARZ	positive	neutral	positive	positive	positive
UBISECURE	positive	positive	positive	positive	positive
WSO2	positive	positive	positive	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
ADNOVUM	neutral	neutral	strong positive	neutral
CA TECHNOLOGIES	positive	strong positive	strong positive	strong positive
EMPOWERID	positive	positive	strong positive	positive
ERGON	neutral	positive	strong positive	positive
EVIDIAN	positive	positive	strong positive	positive
F5 NETWORKS	neutral	positive	strong positive	positive
FORGEROCK	strong positive	positive	positive	positive
IBM	positive	strong positive	strong positive	strong positive
MICRO FOCUS	positive	strong positive	strong positive	strong positive
ONE IDENTITY	positive	positive	positive	positive
ORACLE	positive	strong positive	strong positive	strong positive
PING IDENTITY	positive	positive	strong positive	positive
ROHDE & SCHWARZ	neutral	positive	neutral	positive
UBISECURE	neutral	neutral	neutral	neutral
WSO2	neutral	neutral	positive	positive

Table 2: Comparative overview of the ratings for vendors

Table 2 requires some additional explanation regarding the “critical” rating.

In Innovativeness, this rating is applied if vendors provide none or very few of the more advanced features we have been looking for in that analysis, like support for multi-tenancy, shopping cart approaches for requesting access, and others.

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

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

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

5 Product/service evaluation

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

5.1 AdNovum – Nevis Security Suite

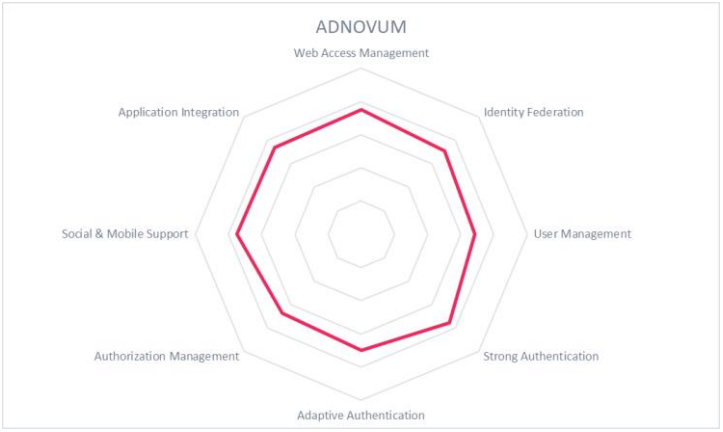
AdNovum is a Swiss-based company founded in 1988. Their Nevis Security Suite consists of various components that support Web Access Management and Federation, an entry gateway and Web Application Firewall (WAF), strong and adaptive authentication, social and mobile support, as well as user management with self-registration for the user and their devices. Although the suite components are tightly integrated, it integrates reasonably well with other backend applications and services.

Strengths	Challenges
• Wide range of authentication mechanisms, as well as some advanced methods • Social and mobile device support • FIDO UAF authentication capability • Deployments in major industry sectors with primarily large business size	• Limited market reach outside the EU • Small partner ecosystem • Limited federation provisioning to major cloud services

Table 3: AdNovum major strengths and challenges

The AdNovum Nevis Security Suite has a long history and experience in the market providing the key features for Web Access Management for both external users and internal applications. Course-grained authorization and support for websites that do not support federation protocols are given, as well as good session management and security. AdNovum Identity Federation provides both Service Provider (SP) and Identity Provider (IdP) functionality, giving flexibility with the SP identity mapping feature, and directory integrations for the IdP, both supporting the majority of federation standards. Although federation provisioning to major cloud services is not supported, the NEVIS provisioning module (nevisDataPorter) allows for customizable connectors to service using REST or SOAP APIs. AdNovum shows their strength through their support of a broad range of authentication mechanisms including some advanced behavioral and biometric authenticators such as BioID for facial recognition, Future's AI-assisted 2FA, and BehavioSec is also supported. In addition, some regional and national credentials like SuisseID, SwissID, and ePA are supported as well.

AdNovum continues to execute well on their roadmap by adding new features, such as the introduction of their FIDO UAF 1.1 support for their authentication server and mobile SDK for iOS and Android. Other improvements include deployment support with Ansible and Docker.



Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 4: AdNovum rating

AdNovum is a privately-owned company with a strong DACH regional presence. The AdNovum Nevis Security Suite is well established and offers some interesting and advanced features. Their product has a well-defined architecture that integrates well with other services in the backend. AdNovum's continued development to added new features and fill in missing gaps helps them to advance as a product leader. AdNovum's greatest challenge remains to be their limited reach, which is primarily focused on the Swiss with little presence in the APAC region and their relatively small partner ecosystem.

5.2 CA Technologies, A Broadcom Company – CA Single Sign-On

CA Technologies, recently acquired by Broadcom Inc., Single Sign-On is a very mature product in the market and is part of the CA Identity Suite. Although the CA Single Sign-On (formerly known as CA SiteMinder) provides very mature capabilities for Web Access Management and Identity Federation, it does require integration with both CA Strong Authentication and CA Risk Authentication products to fully meet the criteria outlined in this Access Management and Identity Federation Leadership Compass. It is the combination of these products that will be evaluated here. The CA Single Sign-On product itself has a vast customer base, is well established in the market and delivers solid platform support.

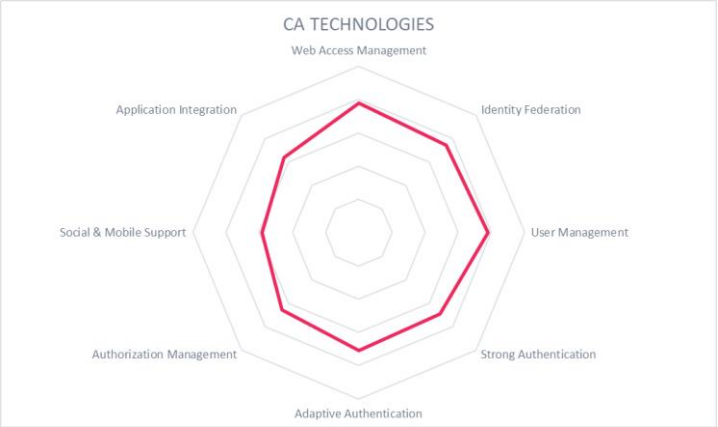
Strengths	Challenges
• Well established product with a very large install base • Strong User Management capabilities • Dynamic Access Management • Excellent platform support	• Some capabilities, such as strong & risk-based authentication, are delivered by other CA Technology products • Lacks mobile device management capabilities • Limited multi-tenancy

Table 5: CA Technologies major strengths and challenges

CA Single Sign-On provides many integration options into existing IT infrastructure and supporting applications and has a large number of customer deployment. They give multiple options that support application server infrastructures, operating systems, and an extensive set of APIs to integrate with existing systems.

The Single Sign-On product has very broad and mature Web Access Management capabilities. CA SSO gives flexible access control to web applications and services through fine-grained access control policies. Their Access Management further provides a REST-based authorization API, and the policy server can be extended to include risk evaluation by integrating with the CA Risk Authentication. Two-factor authentication capabilities can also be added using CA Strong Authentication system.

CA SSO supports both established and more modern federation protocols that include SAML, OIDC, OAuth2, WS-Federation & Trust, as well as JWT, although support for UMA is missing. Federation provisioning to major cloud services is supported out-of-the-box as well as support the SCIM standard. User self-service registration, request/approval, and support workflows are also available.



Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 6: CA Technologies rating

CA Single Sign-On is well-established in the Overall Leadership category and amongst the leading products in the Access Management and Federation market, being mature and widely deployed. CA Technologies has a good partner base for the Single Sign-On product and delivers leading-edge support.

5.3 EmpowerID – SSO Manager

EmpowerID SSO Manager is delivered as part of their base single integrated IAM suite and provides their Access Management and Federation capabilities.

Strengths	Challenges
• Effective adaptive authentication • Strong user management and reporting • Flexible customization workflows • Strong Identity Federation standard support • Good support for Identity Federation provisioning	• Primarily supports the Microsoft platform, except for their reverse proxy which uses a cross-platform NGINX • Relatively small partner ecosystem • Limited mobile device management support

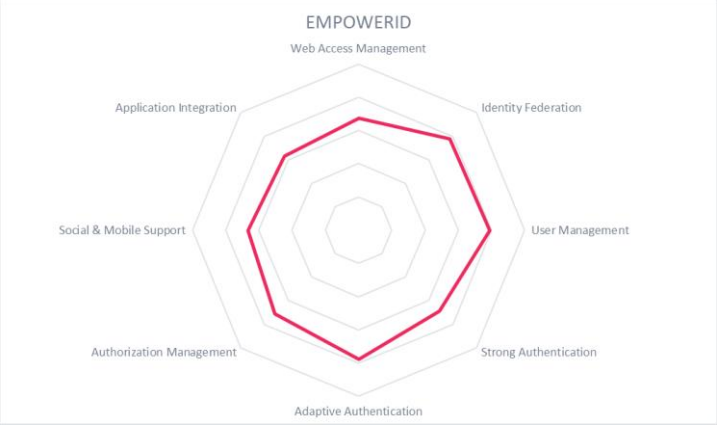
Table 7: EmpowerID major strengths and challenges

SSO Manager is strong in its user management and reporting capabilities. User self-service registration is supported using their Workflow Studio giving flexibility in customization. Reports can be designed and managed as source control items in Workflow Studio as well, and EmpowerID provides the highest number of out-of-the-box reports of the vendors evaluated.

Major social logins are supported as well as logins for with all standard compliant OpenID Connect or SAML based Identity Providers. SSO Manager also meets all adaptive authentication criteria evaluated demonstrating its strength in this category. Mobile Device Management (Lite) is a recently added capability that registers and monitors their mobile authenticator application.

EmpowerID's Web Access Management provides standard session management capabilities but can improve on some abilities to detect session attacks. SSO Manager supports the different forms of user access controls as well as supporting their polyarchical RBAC to control access by hierarchical business roles. RESTful APIs are also available to support application integration.

Identity federation is another capable area for EmpowerID through its support of related standard and provisioning to cloud services out-of-the-box. Workflow Studio can again be used for custom connectors to additional services.



Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	positive

Table 8: EmpowerID rating

Founded in 2005, and formerly known as The Dot Net Factory, EmpowerID supports medium to large companies primarily in the U.S. and northern Europe. SSO Manager provides ample support for Identity Federation and provisioning to cloud services. Their partner ecosystem is relatively small with a DACH focus. EmpowerID is worthy of consideration particularly for customers that build on Microsoft Windows Server infrastructures.

5.4 Ergon – Airlock Suite

Ergon Airlock is an integrated suite that combines Web Access Management and Identity Federation (Airlock IAM) with a Web Application Firewall (Airlock WAF), in which the WAF is used as policy enforcement point for access decisions by Airlock IAM.

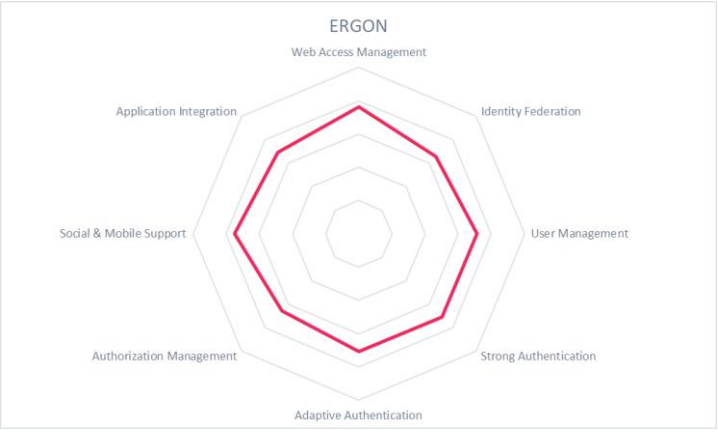
Strengths	Challenges
• Mature Web Access Management • Good strong authentication • Adaptive Authentication capabilities • Good social login and mobile support	• Small partner ecosystem & limited global reach • Federation provisioning to cloud service is somewhat limited without additional configuration

Table 9: Ergon major strengths and challenges

Ergon Airlock has a very mature and capable Web Access Management that integrates well with the Airlock WAF for additional support. Their Identity federation capabilities supports most major federation standards with a few exceptions and out-of-the-box federation provisioning to cloud service is somewhat limited without additional configuration, although comprehensive REST APIs give the ability to integrate other solutions.

Airlock provides good support for most strong authentication methods but is lacking in more advanced authentication methods using biometrics, although support for FIDO UAF and mobile SDKs is given. Their adaptive authentication also provides the majority of the features in that category, although we would like to see more in the way support context-based authenticating factors.

Airlock gives good social login support and is configurable to interact with other social logins using Oauth 2/OICD or SAML 2.0. Good mobile device capabilities are also supported but have 3rd party dependencies in some cases.



Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 10: Ergon rating

Ergon is a Swiss-based company established in 1984 with customers primarily in DACH and is also growing across EMEA and the APAC regions. Their partner ecosystem is again focused in DACH but remains small in the other areas. Airlock has well established and mature Web Access Management features and provides good support for both strong and adaptive authentication, as well as mobile and social login support. Ergon Airlock Suite continues to be an interesting alternative to other solutions as shown by their presence in both the product and market leadership categories.

5.5 Evidian

Based in France, Evidian was acquired by ATOS group and is now a dedicated business branch in their Cybersecurity division since 2015. Evidian provides Web Access Management and Identity Federation capabilities, as well as strong authentication, social login, adaptive authentication as part of their integrated IAM suite.

Strengths	Challenges
• Modular architecture with strong integration between components • Strong Web Access Management capabilities • Supports dynamic authorization • Strong user management support	• Limited presence and partner ecosystem outside Europe • Limited support for outside application servers, databases and directory services • Limited multi-tenancy

Table 11: Evidian major strengths and challenges

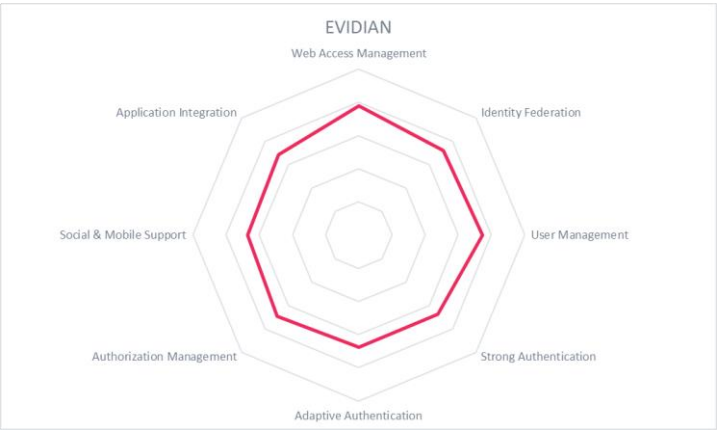
Evidian delivers a fully integrated suite at all technical layers of the product and each component of the suite can be implemented separately. All backend components such as application server and database are delivered with the product; however, integration with other application servers and databases are limited. All LDAP based directories are natively supported. Although Evidian's current on-premise product delivery model doesn't provide full multi-tenancy, some multi-tenancy can be achieved when deployed with Evidian's IGA solution.

With a few exceptions, most Identity Federation related standards are supported and Evidian supports federation and provisioning to most major cloud services out-of-the-box. Their Web Access Management is very mature and is one of their strongest capabilities in the leadership compass.

An interesting capability is support for Dynamic Authorization Management. The Evidian IAM Suite provides fine-grained access control in which can connect to their Web Access Management either directly or through the use of their XACML based authorization server.

Evidian's strong authentication includes a wide range method, as well as support for social logins such as Facebook, LinkedIn, Twitter, and FranceConnect. Their Adaptive Authentication can evaluate common risk factors, such as device fingerprint, time of day/week, IP address, geo-location, geo-velocity, as well as user attributes.

Evidian shows strong support in the area of user management, self-service and workflows as well as rating high in product usability.



Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 12: Evidian rating

Overall, Evidian delivers a well-rounded offering. Evidian has a significant number of system integration partners within Europe, but few in other regions. Evidian appears in both the market and product leadership categories of this leadership compass and should be considered in product evaluation processes for this market.

5.6 F5 Networks – BIG-IP APM

F5 Networks core product is their BIG-IP in which their Access Policy Manager (APM) is a part of that product line and provides their Identity Federation and Web Access Management capabilities. Established in 1996, F5 Networks has a strong presence with large companies in North America as well as a presence in other countries.

Strengths	Challenges
• Strong Web Access Management • Good reporting capabilities • Good integration support for SIEM/Security Intelligence Platforms • Support for social logins using OAuth2	• Limited strong authentication options • Little adaptive authentication support and requires 3rd party support • Limited user management and self-service • Limited mobile support • Federation provisioning to cloud services is not supported

Table 13: F5 Networks major strengths and challenges

F5 BIG-IP APM greatest strength is their Web Access Management capabilities. Their non-federation authentication and authorization methods include support for Headers, Forms, Kerberos, NTLM, JWT, custom header, certificate, and Oracle OAM. Authorization policy support includes Attribute, Role, and Context-based access control capabilities to managing user's access to resources.

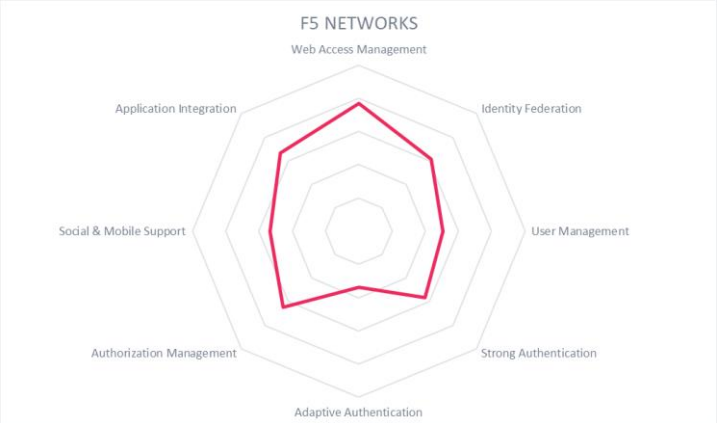
Most Identity Federation related standards are supported, and although federation to major cloud services is supported out-of-the-box, federation provisioning to cloud services are not.

F5 APM provides good reporting capabilities with large number of out-of-the-box reports available, which includes pre-defined compliance report for HIPAA and PSD2.

F5 shows good support for integrations with SIEM/Security Intelligence Platforms which includes out-of-the-box integration support for HP ArcSight, IBM Qradar, RSA NetWitness, Splunk, and the Elastic stack.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 14: F5 Networks rating



Overall, F5 Networks BIG-IP APM has strong Web Access Management capabilities with weaknesses in the other categories of the leadership compass evaluation. F5 is well known in most large companies for the network traffic management products and application security, as well as other market qualities that give them a presence in the Market Leader segment.

5.7 ForgeRock – The ForgeRock Identity Platform

ForgeRock is a leader in the IAM space, providing a single integrated suite based on their Identity Platform. The Access Management and Identity Gateway components of that platform give broad support for the Web Access Management & Identity Federation. ForgeRock supports large companies split evenly between North America & EMEA and has a growing presence and partner ecosystem in the APAC region.

Strengths	Challenges
• Wide range of MFA options out-of-the-box • Strong Adaptive/Risk-based authentication • FIDO2 - W3C WebAuthn standards supported • Good mobile device management • Good integration support for backend services • Broad platform support	• Support for older versions of FIDO currently requires partner and community models. • Only basic reporting capabilities without 3rd party tools or products

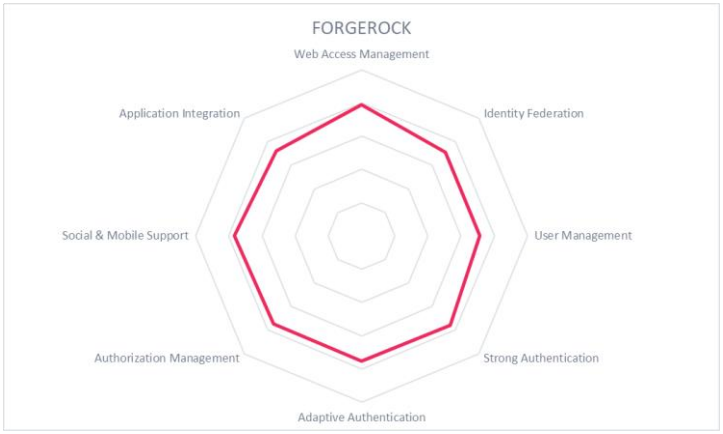
Table 15: ForgeRock major strengths and challenges

ForgeRock provides solid Web Access Management capabilities and supports most Identity Federation related standards including UMA. Federation and provision to most major cloud services are given as well as support for the SCIM standard.

Mobile device management support has become an expected capability for the modern IT. ForgeRock gives good support for device management allowing for device tracking, registration, workflows and fingerprinting. Both a REST API and UI are given to manage the device lifecycle.

ForgeRock's Access Management has centralized storage and a policy definition point. Their authorization engine can be invoked at any point in the user session, and access policies can be exported in XACML format for customers that are interested in using this standard. ForgeRock also provides extensive audit logging capabilities, but only provides options for basic reports and often requires 3rd party tools and products for more advanced reporting capabilities.

ForgeRock provides strong authentication options out-of-the-box for MFA, Adaptive, and Social Logins. ForgeRock supports FIDO2 – W3C WebAuthN standards as of version 6.5, although FIDO U2F support is available via a partner authentication module and UAF support from a community supported module. Also, ForgeRock's Intelligent Authentication UI drag and drop interface greatly simplifies the creation and configuration of the user login experience.



Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 16: ForgeRock rating

ForgeRock provides a well-balanced solution for Web Access Management & Identity Federation and continues to be venture-financed, allowing them to invest in product development heavily. This investment shows by their rapidly improving capabilities, moving them up in the Innovation Leadership category. Overall, ForgeRock is amongst the leading-edge vendors in the IAM space and should be considered in product evaluations.

5.8 IBM – Security Access Manager

IBM Security Access Manager (ISAM) is a well-established product in the market, and IBM has one of the largest customer bases of all vendors in this market segment with many very large deployments of their products. Although ISAM provides standard IAM functionality, it is also marketed as an Access Management and Identity Federation platform with some WAF capabilities for Web Access Management.

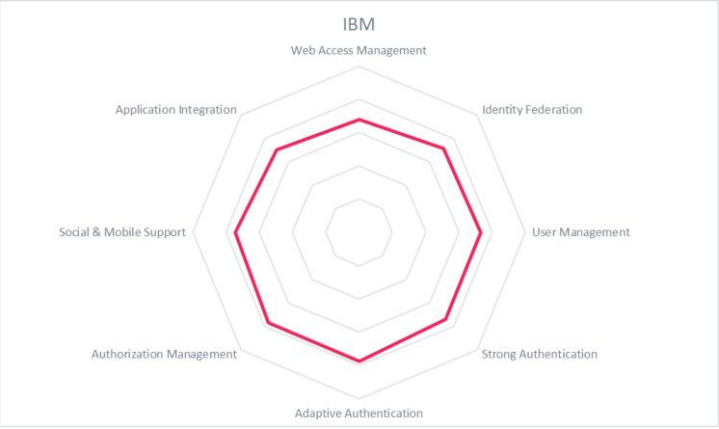
Strengths	Challenges
• Large installation base and professional services worldwide • Strong partner ecosystem globally • Mature access management • Strong and Adaptive authentication • Good user management • Good social and mobile support	• Requires integration with other IBM products for some more advanced features • Limited multi-tenancy

Table 17: IBM major strengths and challenges

ISAM provides broad support for many related areas of Web Access Management including methods for non-federated authentication and authorization typically deployed as a reverse proxy in front of a web application, and it also provides REST APIs that can be called directly. Their WAM also gives good session protection but requires the use of their QRadar product for detection of session attacks.

Most federation related standards are supported as well as identity provisioning to major cloud services out-of-the-box. Stronger support is given to federation to cloud services with a very large number of connectors to SaaS applications.

ISAM provides mature Access Management for authorization which is improved through the use of risk-based authentication. Strong and adaptive authentication capabilities are also given meeting the majority of context-based authentication factor criteria. Good support for social and mobile device management is available as well.



Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 18: IBM rating

IBM Security Access Manager (ISAM) is a very mature product with nearly 20 years in the market. In that time, ISAM has continued to evolve to meet the growing list of IT security requirements through broad feature support, and it is amongst the leading products in the Access Management and Federation market. IBM offers a large number of system integration partners on a global scale and substantial experience in large-scale deployments.

5.9 Micro Focus – Access Manager

Micro Focus 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 architecture. Customers are evenly spread across small, medium and large companies with a focus in North America and EMEA, with a smaller presence in the APAC region.

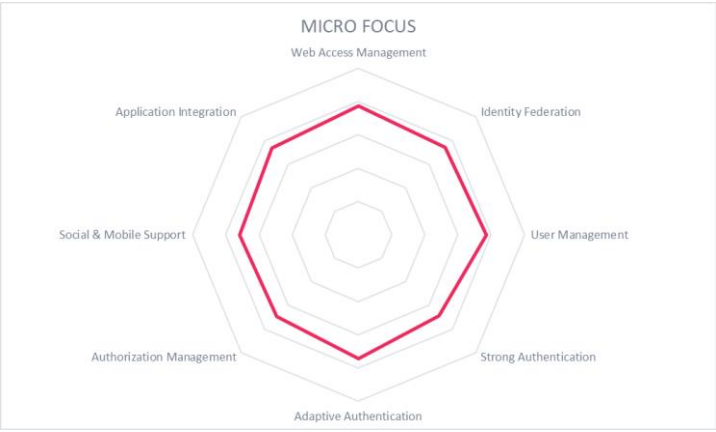
Strengths	Challenges
• Comprehensive Web Access Management • Broad Identity Federation capabilities • Growing partner ecosystem on global scale • Good standard support • Both UI and API configuration options	• Some Advanced Multi-Factor Authentication features requires additional licenses • Limited integrated development environment for customization

Table 19: Micro Focus major strengths and challenges

Micro Focus gives consistently good levels of support for the different categories of this Leadership Compass. Their Web Access Management is comprehensive and provides broad support for identity federation and coverage of related standards include support Liberty Alliance standards.

Most industry standard Multi-Factor Authentication (MFA) methods are supported, including biometrics. At this time, some MFA functionalities require additional licenses. REST APIs are available to allow the integration of any systems not directly supported by SAML, OAuth2 or RADIUS interfaces. REST can also be utilized to connect their Risk-engine to external systems for risk and context information. Intelligence roadmap features will include improved identity analytics with threat detection and automated risk remediation, as well as transaction risk analysis to prevent fraud. Micro Focus will also extend their policy-based access management capabilities to include API's with the release of their Secure API Manager, allowing organizations to secure and manage API's and Applications through a single policy engine. With their future improvements to provide better visibility of events and risk within the system moves their capabilities in the right direction.

Solid user management is given as well as social and mobile management support. For mobile device management, registration and administration of devices can be conducted either through their UI or APIs.



Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 20: Micro Focus rating

Micro Focus has an extensive partner ecosystem on a global scale. The product is widely deployed, with a significant number of large-scale implementations at customer sites. Overall, Micro Focus Access Manager is one of the leading products in the Web Access Management and Identity Federation market segment. They remain in the leadership categories for both product and market segments, although they fall out of the leadership category for innovation.

5.10 One Identity - Cloud Access Manager

One Identity has emerged through a number of different company acquisitions (Quest and Dell) and is now a separate legal entity as of 2017. Their Cloud Access Manager provides the Web Access Management and Identity Federation capabilities. While their product name indicates a cloud-based solution, it actually provides an on-premise solution for Web Access Management and Identity Federation. They offer an integrated IAM suite in a modular fashion, where each product in the suite can connect to another using a "one-click" strategy. Suite products residing on premises can also connect to their IDaaS offerings as well.

Strengths	Challenges
• Strong adaptive capabilities • Good policy and role-based approach to access management • Good MFA support • Out-of-the-box federation support for most major cloud services	• User self-registration is not supported • Device management is missing • Limited multi-tenancy support

Table 21: One Identity major strengths and challenges

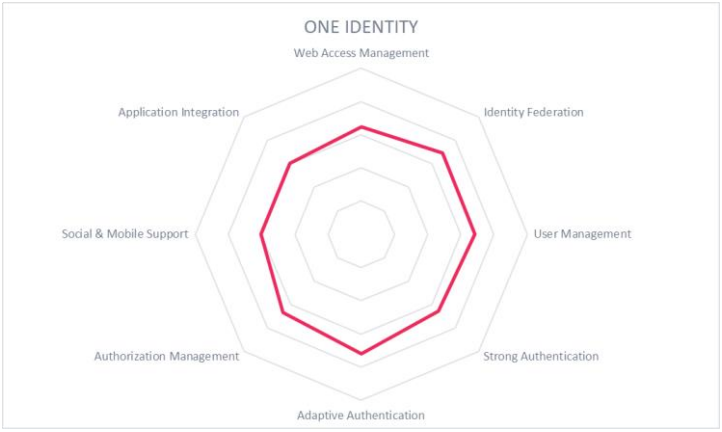
One Identity's Cloud Access Manager offering includes Web Access Management, Federation and Single Sign-On support as well as password, role, and directory management. Cloud Access Manager shows strength by supporting the major federation standards as well as providing out-of-the-box support for federation and provisioning to cloud services. Good user management is given, although user self-registration is not supported.

Most strong authentication methods are supported including biometric factors. For adaptive authentication, Cloud Access Manager includes a security analytics engine that delivers risk-based authentication as well as step-up authentication based on a risk score and most context-based authentication factors are supported as well.

One Identity provides good social login authentication support. And with mobile device support becoming an expected capability in the IAM space, currently, they do not support mobile management. Another area of possible improvement is with monitoring and alerting. Even though they give centralized and automatic logging of events, there is still some room for improvement to allow automated alerts as well as integration with health monitoring and security intelligence platforms.

Security	positive
Functionality	positive
Integration	neutral
Interoperability	neutral
Usability	positive

Table 22: One Identity rating



One Identity customer focus is in North America and some presence in the EMEA and APAC regions with a proportional partner ecosystem in those areas. Missing are important device management capabilities as well as some other limitations in areas such as monitoring and alerting capabilities and integration options. Although some improvements can be made, One Identity Cloud Access Manager provides fairly good adaptive and MFA support, with some strengths in Identity Federation and user management.

5.11 Oracle - Access Management Suite Plus

Oracle Access Management Suite Plus is a single integrated suite that includes their Access Manager, Identity Federation, Entitlements Server, Adaptive Access Manager and Secure Token Services. This product suite provides customers with a broad range of features, beyond the core area of Access Management and Federation.

Strengths	Challenges
• Strong Web Access Management • Wide range of MFA options • FIDO support • Good adaptive authentication capabilities • Full support for multi-tenancy	• Limitations on application server and database integration • User Management & Self Services workflows require Oracle Identity Governance • Product suite is powerful but complex

Table 23: Oracle major strengths and challenges

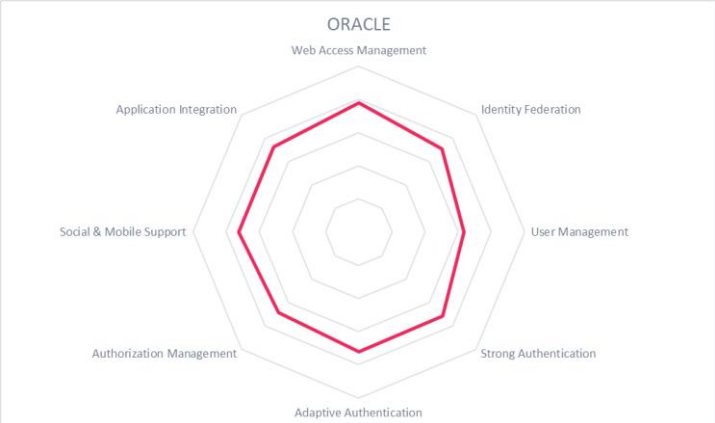
Oracle provides a strong offering in Web Access Management and includes APIs using their Access SDK. Good management of user access is also given. Support for the majority of the federation standard is available as well as out-of-the-box federation to cloud services, although out-of-the-box federation provisioning to significant cloud services is not.

MFA and risk-based authentication are supported through Oracle's Adaptive Access Manager, which includes custom plugins. A wide range of authentication methods are given included biometrics, and most context-based factors are supported in the risk ratings with the exception of user behavior. Strong support for FIDO U2F and UAF is also available.

Oracle Access Management Suite Plus is an integrated suite with full support for multi-tenancy, but components of the suite cannot be replaced by other COTS products or home-grown solutions which should be considered when planning product replacements. Also, with the exception of directory services, Oracle limits support to application server and databases to their own products Oracle Weblogic and Oracle Database respectively.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 24: Oracle rating



Overall, the Oracle Access Management Suite Plus provides a strong offering in the Access Management and Federation market segment. Although the complexity of the suite should not be underestimated, Oracle Access Management Suite Plus provides a strong offering in the market and should be considered for a product evaluation shortlist.

5.12 Ping Identity - Federated Access Management

Ping Identity was founded in 2002 with a primarily focused in the area of Identity Federation. Since then, Ping Identity has steadily grown to add features to fill out their Web Access Management and other areas of their platform. The Ping Identity Platform made up of a number of software products and cloud services, but for this leadership compass only PingFederate, PingAccess, and PingOne have been evaluated.

Strengths	Challenges
• Good Web Access Management • Solid Identity Federation capabilities • Provides API support for access management and identity federation • Good customer support	• User management can use some improvements. • Limited biometric MFA options

Table 25: Ping Identity major strengths and challenges

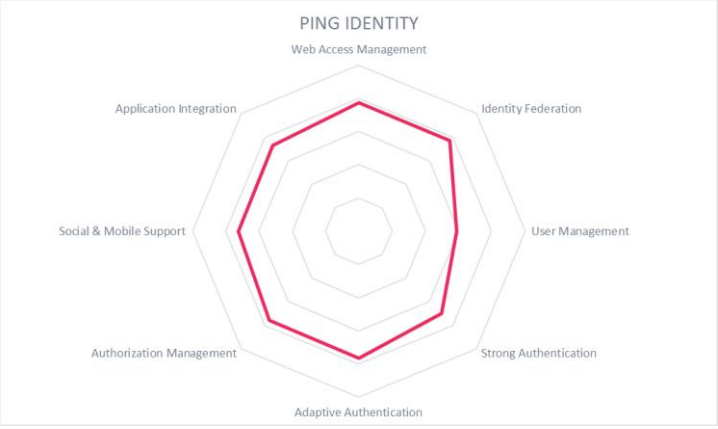
Ping Identity has evolved to provide strong Web Access Management and it includes mechanisms to allow for session lifecycle management as well. Detection of session-based attacks is also offered but requires integration between Ping's identity intelligence and access management offerings. Also, APIs are given to administer and retrieve access policy decisions. APIs for retrieving identity information is given, among others.

Good coverage is given in the area of adaptive authentication, and most MFA options are provided with the exception of biometrics. Support for FIDO2 and U2F-compatible security keys is currently in beta with full support coming in a near future release. In addition, good capabilities are provided for social logins and device management.

Ping Identity has filled out many areas of their Web Access Management and other capabilities evaluated in this Leadership Compass, although some improvements in the user management category can still be made. User self-service is provided via customizable templates, not ready to go out-of-the-box. Some useful user management workflows are not offered or require integration with other third-party solutions.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 26: Ping Identity rating



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

5.13 Rohde & Schwarz – Web Access Manager

The Web Access Manager product was developed by the French company formally DenyAll, and more recently acquired the German company Rohde & Schwarz Cybersecurity. The Web Access Management is part of their platform that also provides Web Application Firewall capabilities.

Strengths	Challenges
• Web Access Management • User Access Management • Adaptive Authentication	• Missing federation and provisioning to cloud services • Limited multi-tenancy support • Missing device management capabilities • User management with self-service workflows not available

Table 27: Rohde & Schwarz major strengths and challenges

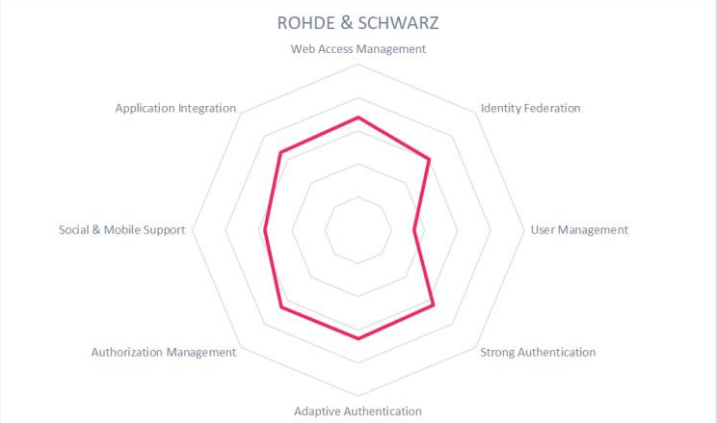
Web Access Manager gives good support for Web Access Management including full detection of session attacks as well as managing access of users. Their Identity Federation has both SP and IdP capabilities and support most federation related standards but does not provide federation and provisioning to cloud services. Support for most Identity Federation related standards, which includes OAuth, OpenID, and JWT management, as well as more traditional standards such as SAML, SWT, WS-Federation, and Trust.

Good Adaptive Authentication is given with workflows, and basic MFA factors are provided, although biometric factor support is not available, although unified authentication through web single sign-on is provided. The Web Access Manager is agent-less, which improves the deployment process. Other capabilities include intelligence in learning application usage enhancing the creation of access rules.

User management with self-service workflows is missing, as well as support for device management. Both of these areas could be an opportunity for improvement. An interesting future enhancement on their roadmap includes Bot mitigation, which addresses one of the current threats in today's cyber security landscape.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	positive
Usability	positive

Table 28: Rohde & Schwarz rating



Rohde & Schwarz Cybersecurity Web Access Manager support smaller companies primarily in the EMEA region, with some presence in Brazil & Mexico as well as North America. Their partner ecosystem is strong again in the EMEA region, weaker in the other regions. Their Web Access Manager focuses on Web Access Management with strength in adaptive authentication, although other features evaluated in the Leadership Compass can be improved upon.

5.14 Ubisecure - Identity Server

Ubisecure is a Finland based company established in 2002 with a customer base primarily in the Nordic region. Their Identity Server is delivered as a single integrated IAM suite that provides both Web Access Management and Identity Federation capabilities with a fully integrated database and application server.

Strengths	Challenges
• Comprehensive Web Access Management • Good Identity Federation • Good mobile and device management support • GSMA Mobile Connect support • Strong support for user management and self-service workflows	• Small partner ecosystem & limited global reach • Limited multi-tenancy support • Missing adaptive authentication capability • Only basic MFA options

Table 29: Ubisecure major strengths and challenges

Ubisecure's strength is in their Web Access Management. The Identity Server provides good support for managing user access using an attribute, role, and context-based access control. Support to websites that do not support federation as well as non-federation authentication for TUPAS (Finnish bank authentication) is also given, although there is limited ability to detect sessions attacks.

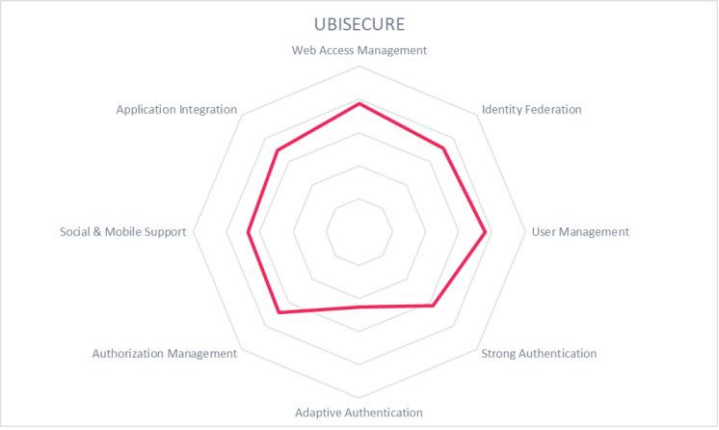
Identity federation support for most major related standards including TUPAS. Although only some support is given to federation to popular cloud services out-of-the-box, more capabilities are given to federation provision to these cloud services.

Adaptive and risk-based authentication is becoming an expected capability with IAM solution today. While Ubisecure's Identity Server is missing this capability natively, system integrators can add other third-party solutions, such as biometric authentication. Strong authentication is somewhat limited. Only basic MFA factors are supported, and no biometric authenticating factors options are given.

Alternatively, good support for mobile and device management is given. Interestingly, Ubisecure provides GSMA Mobile Connect support and is an early adopter of this strong mobile authentication solution. Additionally, strong support for user management and self-service workflows is provided. Also, Ubisecure is actively preparing for future development in their product capabilities by participating in some standards working groups such as MODRNA, IETF for the W3C Web Authentication (WebAuthn / FIDO) specification and the Kantara Initiative to name a few.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 30: Ubisecure rating



Ubisecure has a relatively small presence outside the Nordic region and a limited partner ecosystem. Although they provide some interesting features in some specific areas, and their Identity Server has a good focus on Web Access and user management, they lack some modern authentication capabilities.

5.15 WSO2 - Identity Server

WSO2 Identity Server is based on open source and provides Identity and Access Management (IAM) capabilities as a single integrated IAM suite. For the purpose of this Leadership Compass evaluation, WSO2 Identity Server focuses primarily on Identity Management.

Strengths	Challenges
• Identity Federation • Good User Management • Good MFA • Good Authorization Management • Support for XACML v2 & 3 standards • Support for UMA and SCIM • FIDO U2F support	• Little focus on Web Access Management • Missing device management capabilities • Basic Adaptive Authentication

Table 31: WSO2 major strengths and challenges

Good Identity Federation capabilities are provided such as support for most federation standards including UMA and SCIM, and federation and provisioning to major cloud services are supported out-of-the-box. Support for the different types of access controls are given for managing access of users and for fine-grained Dynamic Authorization Management, WSO2 Identity Server provides support for both XACML 2.0 and 3.0 standards. Limited focus is given to Web Access Management

For authentication, WSO2 Identity Server provides good social login support and MFA with many out-of-the-box connectors to other second factor implementations, as well as FIDO U2F support is given although biometrics requires third-party vendor support. Some adaptive/risk-based capabilities are provided with limitations on the context-based authentication factors options.

Although device management capabilities that include device ID tracking, mapping, fingerprinting, or workflows are not available, user management, self-service, and their other workflows are well supported.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 32: WSO2 rating

WSO2 customers are focused in North America and the EMEA regions with some presence in the APAC supporting small to large company sizes, with a good partner ecosystem. WSO2 Identity Server provides some strengths in the areas of Identity Federation, User, and Authorization Management, but may not be the choice for those looking for strong Web Access Management as well as device management capabilities. Overall, WS02 continues to make improvements in a positive direction moving them from product challenger in 2016 to the product leader category of this current version of the report.

6 Vendors to watch

Besides the vendors covered in detail in this Leadership Compass document, we observe some other vendors in the market that have credible Access Management and Federation capabilities in the market. A few of these vendors have decided not to participate in this KuppingerCole Leadership compass for their own reasons, but since we find them interesting and worth a mention, we decided to include them here. These vendors may not fully fit into the market segment of Access Management and Federation or do not meet our eligibility criteria to be considered in this evaluation. We provide short abstracts for these vendors below.

6.1 Atos DirX Access

DirX Access is the Access Management and Federation solution within the Atos DirX product portfolio. Atos, having been acquired by Evidian indirectly via the Groupe Bull acquisition, has also acquired the former Siemens Business Services which includes the Siemens DirX portfolio. Both the products and capabilities from these acquisitions are now united under the brand Evidian, although the traditional DirX products will still be available and maintained by Atos.

Now, the Evidian DirX product line for IAM includes web access management, single sign-on, identity federation and directory services. Deployment models comprise of on-premise, managed or cloud-based options. DirX Access provides the standard Web Access Management capabilities and support for Identity Federation based on SAML, OAuth 2.0, and OpenID Connect. Broad support for various authentication mechanisms, including risk-based authentication is one the strengths provide by DirX Access.

6.2 Fischer International Identity

Fischer International Identity provides Web Access Management and Identity Federation both as on-premise and cloud deployments. Their Identity products show its strength in innovation which includes automation of identity provisioning, self-service access requests, and workflows, as well as federation and single sign-on when accessing web and SaaS applications.

Fischer International is a mid-sized company founded in 1982 and is headquartered on the east coast of the southern U.S. Their partner network is mainly based in the U.S. with a small presence in eastern Europe.

6.3 Forum Systems - Sentry API Security Gateway

Forum Systems is a privately held independent engineering company based in Newton, Massachusetts, USA. Founded in 2001, the company can provide a combined Web Access Management and Identity Federation offering using a gateway-based approach that sits on the edge of an organizations network which can be deployed as a FIPS 140-2-certified hardware appliance, a virtual appliance, or software.

All solutions provided by Forum Systems are based on the same core technology, the company's Forum Sentry API Security Gateway product. Their portfolio of security and access control gateways for various scenarios, such as mobile access control or cloud storage provider integration**. A**lso include**d is** unified management of identities, and support for Single Sign-On (SSO).

6.4 Identity Automation RapidIdentity

Identity Automation started in 2004 as consulting firm helping companies with their Identity and Access Management (IAM) integrations such as provisioning automation, access, and user account management. Since 2009 they developed their own IAM platform called RapidIdentity.

RapidIdentity focuses on support for the complete identity and access lifecycle provided through a well-integrated solution with strong out-of-the-box capabilities. Their Single Sign-On (SSO) has become more standards compliant, since our last evaluation, allowing integration with on-premises and cloud-based applications using SAML 2.0, OAuth, OpenID Connect, WS-Federation. SSO mobile access support to cloud application for iOS and Android devices.

Although being more an integrated platform for broad coverage of various IAM requirements than a specialized solution for Web Access Management and Identity Federation, Identity Automation RapidIdentity delivers baseline capabilities in the market segment.

6.5 Indeed Identity

Indeed Identity is a Lithuanian-based software company that provides Enterprise Authentication and Enterprise Single Sign-On products. Although a relatively small company founded in 2005, their partner network includes some large companies based internationally.

The Indeed Access Manager gives some advanced multi-factor authentication options using push authentication, biometrics such as fingerprint, palm vein pattern, and 3D face recognition to allow access to Windows systems, in addition to other MFA options for web applications, Remote Desktop, VDI, Citrix and RADIUS-compatible applications.

The Indeed Identity product offering is clearly positioned as a specialist vendor in this market segment. Nonetheless, due to their strong authentication, enterprise SSO, user self-service and their potential for adding in Identity Federation with their recent SAML support, they are worth looking at as a complementary offering to other vendors' products.

6.6 OpenIAM

OpenIAM has been in the IAM market since 2008. They moved from an open source model to a model which mandatorily involves a commercial component and open source. OpenIAM is a is a mid-sized company that faces the challenges of a limited partner ecosystem and growing unwillingness of organizations to adopt open source software options for security.

OpenIAM product suite has two distinct components: OpenIAM Identity Manager delivering Identity Provisioning and auditing capabilities, and the OpenIAM Access Manager providing access management including identity federation, web-based access management, and SOA security. Their Web Access Control provides advanced authentication, single sign-on, federation, and dynamic authorization management. Their IAM offering started as an appliance form of deployment model, which now also can be run from the cloud, providing an IDaaS (Identity as a Service) offering targeted at managing identities and their access in hybrid IT infrastructures. Furthermore, it is available as a software installation for both on-premises and private cloud deployments.

6.7 SecureAuth IdP

SecureAuth has been in the market since 2006 and headquartered in Irvine, CA. Their strength is not only providing Web Access Management and Identity Federation capabilities but strong authentication as a mix of service and on-premises capabilities. SecureAuth supports both Cloud and on-premises deployments.

SecureAuth IdP provides Web Access Management and Identity Federation, although primarily targeted at strong authentication with their wide range of MFA options, as well as adaptive authentication capabilities. Mobile access support is given as well as identity federation and user self-service functionality that includes device enrollment.

6.8 United Security Providers (USP)

Founded in 1994, United Security Providers (USP) is a Swiss software vendor and service provider with offices in Bern (headquarters), Zurich, London, and Minsk. USP has more than 100 security professionals and operates its own 24/7 Security Operations Center. While their initial and primary target market is Switzerland, they are sustaining a growing market reach beyond their domestic market, primarily in Germany, Austria, and the UK.

The USP Secure Entry Server® (SES) offers a comprehensive Web Access Management and Identity Federation solution with Single Sign-on and Web Application Firewall capabilities. Their solution includes modern MFA (Multi-Factor Authentication), risk-based and adaptive authentication features. SES provides versatility in deployment models which can be delivered as hardware or a virtual appliance, containerized or in the cloud. Their solution is also available as a fully managed service or by partner hosting and platform-as-a-service providers. United Security Providers Secure Entry Server is considered a strong, unified and interoperable access management solution offering for customers located in their primary target regions of D/A/CH and the UK.

7 Methodology

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

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

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

7.1 Types of Leadership

We look at four types of leaders:

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

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

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

Our rating is based on a broad range of input and long experience in 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, as well as other sources.

7.2 Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management[1]). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

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

Integration—integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated.

[1] http://www.kuppingercole.com/report/mksecnario_understandingiam06102011

And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability—interoperability also can have many meanings. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

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

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

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

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

[2] http://www.kuppingercole.com/report/cb_apieconomy16122011

7.3 Vendor rating

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

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

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

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

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

7.4 Rating scale for products and vendors

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

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

7.5 Spider graphs

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

Web Access Management	The solutions ability to provide WAM capabilities to websites such as authentication and authorization for sites that do not support federation protocols, session management, and its protection.
Identity Federation	The depth in which standards support the Identity Federation solution, can supply Service Provider (SP) and/or Identity Provider (IdP) functionality, and federation provisioning to cloud services for example.
User Management	The level of support for user management capabilities such as user-self-service and managed registration, access request/approval workflows, password management, and the types of user directories and protocols used.
Strong Authentication	The range of supported standards and methods for strong authentication, which includes multi-factor and social logins.
Adaptive Authentication	The measure of various aspects of adapted authentication supported by the solution such as step-up authentication, risk-based authentication as well as the different types of context factors used in the risk ratings.

Authorization Management	The level of support for the management of access policies including storage and type of controls used whether role, context or attribute based for both administrators and users, as well as the related authorization standards used by the solution.
Social & Mobile Support	The use of federation and standards for social Single-Sign-On, as well as mobile device management such as registration and associated device identities, fingerprinting, and workflows.
Application Integration	The extent of the solution's ability to integrate with itself as well as backend applications and other services.

The spider graphs add an extra level of information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas while being strong in other areas. These might be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic decisions on Web Access Management & Identity Federation.

7.6 Inclusion and exclusion of vendors

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

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

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

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

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

8 Copyright

The Future of Information Security – Today

KuppingerCole supports 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 Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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

KuppingerCole Analysts AG
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com