Access Management and Federation

Leaders in innovation, product features, and market reach for Access Management and Identity Federation.
Your compass for finding the right path in the market.

by Martin Kuppinger
mk@kuppingercole.com
March 2016
Content

1 Management Summary ........................................................................................................5
  1.1 Overall Leadership ........................................................................................................ 6
  1.2 Product Leadership ........................................................................................................ 7
  1.3 Market Leadership .......................................................................................................... 8
  1.4 Innovation Leadership .................................................................................................... 9

2 Methodology .......................................................................................................................... 11

3 Product Rating .......................................................................................................................... 13

4 Vendor Rating .......................................................................................................................... 15

5 Vendor Coverage .................................................................................................................... 16

6 Market Segment ........................................................................................................................ 17

7 Specific features analyzed ..................................................................................................... 21

8 Market Leaders ...................................................................................................................... 22

9 Product Leaders ..................................................................................................................... 23

10 Innovation Leaders ............................................................................................................... 24

11 Product Evaluation ............................................................................................................... 25
  11.1 AdNovum – Nevis Security Suite .................................................................................. 26
  11.2 Atos – DirX Access ......................................................................................................... 27
  11.3 CA Technologies – CA Single Sign-On ......................................................................... 28
  11.4 Dell – One Identity Cloud Access Manager ................................................................. 29
  11.5 EmpowerID – EmpowerID SSO Manager ................................................................... 30
  11.6 Ergon Informatik – Airlock Suite ................................................................................... 31
  11.7 Evidian – Web Access Manager ................................................................................... 32
  11.8 ForgeRock – OpenAM ................................................................................................. 33
  11.9 Forum Systems – Forum Sentry .................................................................................... 34
  11.10 GlobalSign IAM .......................................................................................................... 35
  11.11 IBM – Security Access Manager ................................................................................. 36
  11.12 Identity Automation - RapidIdentity ........................................................................... 37
  11.13 Micro Focus – Access Manager .................................................................................. 38
  11.14 Oracle – Access Management ...................................................................................... 39
  11.15 Ping Identity – Federated Access Management ............................................................. 40
  11.16 SecureAuth - IdP ........................................................................................................ 41
  11.17 WSO2 – Identity Server ............................................................................................. 42

12 Products at a glance .............................................................................................................. 43
  12.1 The Market/Product Matrix .......................................................................................... 45
  12.2 The Product/Innovation Matrix ..................................................................................... 47
  12.3 The Innovation/Market Matrix ...................................................................................... 48

13 Overall Leadership – the combined view ............................................................................ 49
Content Tables

Table 1: AdNovum Nevis Security Suite major strengths and weaknesses................................................................. 26
Table 2: AdNovum Nevis Security Suite rating........................................................................................................... 26
Table 3: Atos DirX Access major strengths and weaknesses.......................................................................................... 27
Table 4: Atos DirX Access rating...................................................................................................................................... 27
Table 5: CA Single Sign-On major strengths and weaknesses.......................................................................................... 28
Table 6: CA Single Sign-On rating...................................................................................................................................... 28
Table 7: Dell Cloud Access Manager major strengths and weaknesses.......................................................................... 29
Table 8: Dell Cloud Access Manager rating.................................................................................................................. 29
Table 9: EmpowerID SSO Manager major strengths and weaknesses.............................................................................. 30
Table 10: EmpowerID SSO Manager rating.................................................................................................................... 30
Table 11: Ergon Airlock Suite major strengths and weaknesses........................................................................................ 31
Table 12: Ergon Airlock Suite rating.................................................................................................................................. 31
Table 13: Evidian Web Access Manager major strengths and weaknesses......................................................................... 32
Table 14: Evidian Web Access Manager rating................................................................................................................ 32
Table 15: ForgeRock OpenAM major strengths and weaknesses........................................................................................ 33
Table 16: ForgeRock OpenAM rating................................................................................................................................ 33
Table 17: Forum Systems Sentry major strengths and weaknesses.................................................................................... 34
Table 18: Forum Systems Sentry rating.............................................................................................................................. 34
Table 19: GlobalSign IAM major strengths and weaknesses.............................................................................................. 35
Table 20: GlobalSign IAM rating....................................................................................................................................... 35
Table 21: IBM Security Access Manager major strengths and weaknesses........................................................................ 36
Table 22: IBM Security Access Manager rating................................................................................................................ 36
Table 23: Identity Automation RapidIdentity major strengths and weaknesses................................................................. 37
Table 24: Identity Automation RapidIdentity rating.......................................................................................................... 37
Table 25: Micro Focus Access Manager major strengths and weaknesses....................................................................... 38
Table 26: Micro Focus Access Manager rating................................................................................................................ 38
Table 27: Oracle Access Management major strengths and weaknesses............................................................................ 39
Table 28: Oracle Access Management rating................................................................................................................... 39
Table 29: Ping Federated Access Management major strengths and weaknesses............................................................ 40
Table 30: Ping Federated Access Management rating..................................................................................................... 40
Table 31: SecureAuth IdP major strengths and weaknesses............................................................................................... 41
Table 32: SecureAuth IdP rating.......................................................................................................................................... 41
Table 33: WSO2 Identity Server strengths and weaknesses.............................................................................................. 42
Table 34: WSO2 Identity Server rating................................................................................................................................ 42
Table 35: Comparative overview of the ratings for the product capabilities .............................................. 43
Table 36: Comparative overview of the ratings for vendors ................................................................. 44

Table of Figures

Fig. 1: Overall Leaders in the Access Management/Federation segment ............................................. 6
Fig. 2: Product Leaders in the Access Management/Federation segment ......................................... 7
Fig. 3: Market Leaders in the Access Management/Federation segment ........................................... 8
Fig. 4: Innovation Leaders in the Access Management/Federation segment .................................... 9
Fig. 5: The Computing Troika ............................................................................................................. 17
Fig. 6: Supporting the Extended Enterprise ......................................................................................... 18
Fig. 7: Dealing with all types of user populations .............................................................................. 19
Fig. 8: Federation and Web Access Management .............................................................................. 20
Fig. 9: Market Leaders in the Access Management/Federation market segment .......................... 22
Fig. 10: Product Leaders in the Access Management/Federation market segment ..................... 23
Fig. 11: Innovation Leaders in the Access Management/Federation market segment .................. 24
Fig. 12: The Market/Product Matrix .................................................................................................. 45
Fig. 13: The Product/Innovation Matrix ............................................................................................... 47
Fig. 14: The Innovation/Market Matrix ............................................................................................... 48
Fig. 15: The Overall Leadership rating for the Access Management/Federation ......................... 49

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: SecureAuth IdP - 70844
Executive View: CA SiteMinder® - 71022
Executive View: Dell One Identity Cloud Access Manager - 71250
Executive View: Ergon Airlock/Medusa - 71047
Executive View: Evidian Identity & Access Manager - 70871
Executive View: ForgeRock OpenAM - 71405
Executive View: Forum Sentry API Gateway - 71204
Executive View: GlobalSign - 71051
Executive View: IBM Cloud Security Enforcer - 71290
Executive View: Identity Automation RapidIdentity - 71203
Executive View: NetIQ Access Manager - 71054
Executive View: Oracle Identity and Access Management Suite Plus 11g R2 - 70917
Executive View: PingOne® - 70870
Executive View: WSO2 Identity Server - 71129
Leadership Compass: Privilege Management - 71100
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
Leadership Compass: Identity Provisioning - 70949
Product Report: EmpowerID - 71115
Vendor Report: Atos DirX - 70741
Vendor Report: Dell IAM - 70812
Vendor Report: Dell IAM - 70812
1 Management Summary

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 key 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 Extended and Connected Enterprise.

While Web Access Management technologies are well established and Identity Federation has also been around for years, we have observed a 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 a number of 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 take the fact into account that several of these solutions also are offered from as cloud services. This can be valuable to customers if they want 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 growing rapidly. 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 products.

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 purely focusing on that part of the overall IAM (Identity and Access Management) market.

Picking solutions always requires 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 his requirements. However, this Leadership Compass will help identifying those vendors that customers should look at more closely.

### 1.1 Overall Leadership

![Overall Leaders in the Access Management/Federation segment](image)

Overall Leadership is the combined view on the three Leadership categories, i.e. Product Leadership, Innovation Leadership, and Market Leadership. This combined 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 falling apart 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. Thus, we strongly recommend looking at all Leadership categories and the individual analysis of the vendors and their products for gaining a comprehensive understanding of the players in that market segment.

In the market for Web Access Management and Federation, we currently see five companies in the Leaders segment for Overall Leadership. 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 gained significant market share over the past years and made it into the Leaders segment.

The Challenger segment is very crowded, with most vendors being placed in that segment. Here we find a variety of players, including large and established vendors such as Oracle, Dell, Evidian, or Atos, which provide mature offerings, however being not always as feature-rich and innovative as the companies in...
the Leaders segment. We also find a number of still relatively new companies such as EmpowerID and GlobalSign, the latter after their acquisition of former Ubisecure. AdNovum and Ergon are two vendors based in Switzerland, which both offer strong integrated Web Application Firewall capabilities.

Furthermore, we find a number of specialists in the Challengers section, including Forum Systems with their gateway-based approach also delivering strong API Security features, SecureAuth focusing on multi-factor authentication to the cloud, and WSO2 with a platform-based open source approach showing its particular strength in supporting the rapid development of complex custom solutions.

Finally, we have one vendor being placed in the Followers section. Identity Automation is a rather small companies with a product offering that delivers baseline capabilities, but still does not have the breadth of functional coverage as other products in the market. However, they are on their way towards becoming a challenger for the more established players in the market and might be a good choice for certain specific use cases and customer requirements.

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 features provided by the vendor’s products is mandatory.

1.2 Product Leadership

![Product Leadership Diagram]

Fig. 2: Product Leaders in the Access Management /Federation segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

The second view we provide is about Product Leadership. That view is mainly based on the analysis of product features and the overall capabilities of the various products.

Here we see a number of companies being placed in the Leaders segment. Again, the Overall Leaders are in that segment, i.e. CA Technologies, ForgeRock, IBM, Micro Focus, and Ping Identity (in alphabetical order). All of them have mature product offerings.
Other vendors in the Leaders segment include both Swiss vendors AdNovum and Ergon, but also EmpowerID as a still relatively unknown player in this market and SecureAuth with their strong support for multi-factor authentication. Forum Systems and Dell also made it to the Leaders segment.

Evidian is close to entering the Leaders segment, followed by GlobalSign, Atos, and Oracle. Furthermore, we find WSO2 in that segment, again with a specialized type of offering.

In the Follower section we again find Identity Automation, with them being close to reaching the Challengers segment.

Again, to select a product it is important to look at the specific features and map them to the customer requirements. There are sufficient examples where products that weren’t “feature leaders” still were the better fit for specific customer scenarios.

1.3 Market Leadership

![Market Leadership Diagram]

Fig. 3: Market Leaders in the Access Management/Federation segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

We expect Market Leaders to be leaders on a global basis. Companies which are strong in a specific geographic region but sell little or nothing to other major regions are not considered Market Leaders. The same holds true for the vendor’s partner ecosystem – without global scale in the partner ecosystem, we don’t rate vendors as Market Leaders.

Market Leadership is an indicator of the ability of vendors to execute on projects. However, this depends on other factors as well. Small vendors might well be able to execute in their “home base”.

Small vendors are sometimes more directly involved in projects, which can be positive or negative – the latter, if it leads to branches in product development, which aren’t managed well. Besides that, the success of projects depends on many other factors, including the quality of the system integrator – so even large vendors with a good ecosystem might fail in projects.

It comes to no surprise that the large and established software vendors dominate the Leaders segment. IBM, Oracle, CA Technologies, Ping Identity, and Micro Focus all made it into the Leaders segment.
ForgeRock, with their massive growth in the past years, also made it into that segment, now being considered as one of the Market Leaders in Access Management and Federation.

In the Challenger section we find a number of further players, including Dell as the company being closest to the Leaders segment. Other vendors in this section include – in alphabetical order – AdNovum, Atos, EmpowerID, Ergon, Evidian, Forum Systems, GlobalSign, SecureAuth, and WSO2. The reasons for being placed in that segment vary. Some of the vendors such as AdNovum and Ergon still lack a global partner ecosystem, while others are specialists with a still relatively small customer base.

Finally, we again see Identity Automation in the Followers segment, with a fairly small customer base and partner ecosystem and being focused on certain geographies.

It has to be noted that this Market Leadership rating doesn’t allow any conclusion about whether the products of the different vendors fit the customer requirements.

1.4 Innovation Leadership

![Innovation Leaders in the Access Management/Federation segment](image)

The third angle we take when evaluating products is about innovation. Innovation is, from our perspective, a key distinction in IT market segments. Innovation is what customers require to receive new releases that meet new requirements. Thus, a look at Innovation Leaders is also important, beyond analyzing product features.

Here we see ForgeRock in front, followed by a number of other companies. Other Leaders include Ping Identity, EmpowerID, CA Technologies, Ergon, and IBM. All of them showed significant innovation and strong support of the list of features we consider as innovative in the Web Access Management and Identity Federation market, starting with broad standards support. AdNovum just made it into the Leaders segment, with significant improvements and innovations being added in recent releases.
SecureAuth and Micro Focus are leading the crowded Challenger segment, all being close to entering the Leaders segment. Most of the other vendors such as Oracle, GlobalSign, Evidian, Forum Systems, WSO2, Atos, and Dell are also well placed in the Challenger segment, indicating that they show significant innovation in this market.

Identity Automation again populates the Followers section. They have some innovative features, however due to the still relatively small overall feature set they lack support for some of the innovative features we’d like to see.

Again, in some cases products that appear more to the left of that figure do not necessarily fail in innovation but are focused on specific requirements or highly focused approaches.

Some vendors have demonstrated a significant amount of innovation in recent time, driving standards evolution forward. Others are innovative with respect to new features such as backend integration or integration with Enterprise Single Sign-On or Web Application Firewalls. Overall, this view reflects the fact that there is still a lot of innovation happening in the Access Management and Federation market, with significant room for some of the vendors to enhance their offerings.
2 Methodology

KuppingerCole’s Leadership Compass is a tool that provides an overview of a particular IT market segment and identifies the leader in that market segment. It is the compass that assists you in identifying the vendors and products 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 does not 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.

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 of global presence or breadth of partners can prevent a vendor from becoming a Market Leader.

- **Innovation Leaders**: Innovation Leaders are those vendors which are driving innovation in the particular market segment. They provide several of the most innovative and upcoming features we hope to see in the particular 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 most 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 a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.
In addition, we have defined a series of matrixes which:

- Compare ratings, for example the rating for innovation against the one for the overall product capabilities, thus identifying highly innovative vendors which are taking a slightly different path than established vendors, but also established vendors which no longer lead in innovation. These additional matrixes provide additional viewpoints on the vendors and should be considered when picking vendors for RFIs (Request for Information), long lists, etc. in the vendor/product selection process.

- Add additional views by comparing the product rating to other feature areas. This is important because not all customers need the same product features, depending on their current situation and specific requirements. Based on these additional matrixes, customers can evaluate which vendor fits best to their current needs but is also promising regarding its overall capabilities. The latter is important given that a product typically not only should address a pressing challenge but become a sustainable solution. It is about helping now and being good enough for the next steps and future requirements. Here these additional matrixes come into play.

Thus, the KuppingerCole Leadership Compass provides a multi-dimensional view on vendors and their products.

Our rating is based on a broad range of input and a 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, plus a variety of other sources.
3 Product Rating

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

- Security
- Functionality
- 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). 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 state of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the state 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 the portfolio. Thus, when we use the term integration, we are referring to the extent in which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.
Interoperability—interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to insure 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) 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, overall we have strong expectations 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 both 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 increase costs, but inevitably lead 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 is of highest importance. This is because lack of excellence in any or all of these areas will lead to inevitable identity and security breakdowns and weak infrastructure.
4 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 particular 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. Innovativeness, despite being part of the vendor rating, looks at the innovativeness in the particular market segment analyzed in this KuppingerCole Leadership Compass.

**Market position** – measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active, e.g. being weak in one segment doesn’t necessarily lead to a very low overall rating. This factor takes into account the vendor’s presence in major markets. Again, while being part of the vendor rating, this mainly looks at the market position in the particular market segment analyzed in this KuppingerCole Leadership Compass. Thus a very large vendor might not be a market leader in the particular market segment we are analyzing.

**Financial strength** – even while KuppingerCole doesn’t consider size to be a value in 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 for the particular product covered in this Leadership Compass document. 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.
5 Vendor Coverage

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, the US, or the APAC region.

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 a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

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

For this Leadership Compass document, all major vendors we approached responded to the questionnaire. However, some of the vendors which have their main focus on network security and provide Web Access Management and Federation capabilities more as an add-on didn’t respond to the questionnaire. These vendors commonly are not the primary focus of organizations looking for Web Access Management and Identity Federation, however they might become an alternative for certain scenarios.

Furthermore, there are a number of point offerings in the market that have a limited market visibility and were not included in the leadership analysis for this KuppingerCole Leadership Compass. Some of these vendors are listed in the final section of this document and might become part of the next edition of this document, depending on how they evolve.
6 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 “supporting the Extended and Connected 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. IT has to provide an infrastructure for this Extended Enterprise, both for incoming and outgoing access; both for customers and other externals such as business partners; and both for existing and new on-premise applications and cloud services.

![Cloud Computing Diagram](image)

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. Customers today expect that they have access to far more information at their vendor’s systems than ever before. While organizations always had these external relations, the density has changed as well as the need for IT support of the Extended Enterprise.

All three major trends that affect today’s IT - the Computing Troika of Cloud Computing, Mobile Computing, and Social Computing - stand for a shift towards an open, integrated enterprise that is extended beyond the perimeter of the organization itself. Whether you tend to name this the Extended Enterprise or opt for Connected Enterprise does not matter. It is about the need for connecting today’s on-premise IT with the outer world in various ways.
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.
- **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 own 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.
- **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 Extended 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 then is used by the backend application. Some tools also support APIs for authorization calls to the system.
Identity Federation, on the other hand, allows splitting authentication and authorization between an IdP (Identity Provider) and a Service Provider (SP) or Relying Party (RP). 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 Extended 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 enabling new forms of collaboration in industry networks or by adding more flexibility in the R&D supply chain), and the underlying collaboration & communication.

The Extended 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 managed in internal systems so far, more business partners, customers, and even potential customers are added. They shall have 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 own, internal directories, others will be federated in from external Identity Providers or will be managed by means of 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.

Fig. 7: Dealing with all types of user populations will require both federation and locally managed user accounts.
Web Access Management, on the other hand, comes into play for 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.

The focus is on on-premise solutions for that purpose. We also see a growing number of cloud services providing 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 have also 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 covers companies such as Okta, OneLogin, Microsoft with their Azure Active Directory, and many more.
7 Specific features analyzed

When evaluating the products, besides looking at the aspects of

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

we also considered several specific features. These include:

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.

Federation support

Clearly one of the most important criteria is the support for federation protocols such as SAML 2.0, OAuth 2.0, and others.

User self-services

Particularly for Web Access Management, user self service capabilities such as registration and password reset are another important feature that we analyze.

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.

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.
8 Market Leaders

Based on our evaluation of the products, we’ve identified (as mentioned above) different types of leaders in the Access Management and Federation market segment. The Market Leaders are shown in figure 9.

We expect Market Leaders to be leaders on a global basis. Companies which are strong in a specific geographic region but sell little or nothing to other major regions are not considered Market Leaders. The same holds true for the vendor’s partner ecosystem – without global scale in the partner ecosystem, we don’t rate vendors as Market Leaders.

Market Leadership is an indicator of the ability of vendors to execute on projects. However, this depends on other factors as well. Small vendors might well be able to execute in their “home base”.

Small vendors are sometimes more directly involved in projects, which can be positive or negative – the latter, if it leads to branches in product development, which aren’t managed well. Besides that, the success of projects depends on many other factors, including the quality of the system integrator – so even large vendors with a good ecosystem might fail in projects.

![Market Leaders in the Access Management/Federation market segment](image)

It comes to no surprise that the large and established software vendors dominate the Leaders segment. IBM, Oracle, CA Technologies, Ping Identity, and Micro Focus all made it into the Leaders segment. ForgeRock, with their massive growth in the past years, also made it into that segment, now being considered as one of the Market Leaders in Access Management and Federation.

In the Challenger section we find a number of further players, including Dell as the company being closest to the Leaders segment. Other vendors in this section include – in alphabetical order – AdNovum, Atos, EmpowerID, Ergon, Evidian, Forum Systems, GlobalSign, SecureAuth, and WSO2. The reasons for being placed in that segment vary. Some of the vendors such as AdNovum and Ergon still lack a global partner ecosystem, while others are specialists with a still relatively small customer base.
Finally, we again see Identity Automation in the Followers segment, with a fairly small customer base and partner ecosystem and being focused on certain geographies.

It has to be noted that this Market Leadership rating doesn’t allow any conclusion about whether the products of the different vendors fit the customer requirements.

Market Leaders (in alphabetical order):

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

9 Product Leaders

The second view we provide is about Product Leadership. That view is mainly based on the analysis of product features and the overall capabilities of the various products.

![Product Leaders in the Access Management/Federation market segment](image)

Here we see a number of companies being placed in the Leaders segment. Again, the Overall Leaders are in that segment, i.e. CA Technologies, ForgeRock, IBM, Micro Focus, and Ping Identity (in alphabetical order). All of them have mature product offerings.

Other vendors in the Leaders segment include both Swiss vendors AdNovum and Ergon, but also EmpowerID as a still relatively unknown player in this market and SecureAuth with their strong support for multi-factor authentication. Forum Systems and Dell also made it to the Leaders segment.

Evidian is close to entering the Leaders segment, followed by GlobalSign, Atos, and Oracle. Furthermore, we find WSO2 in that segment, again with a specialized type of offering.
In the Follower section we again find Identity Automation, with them being close to reaching the Challengers segment.

Again, to select a product it is important to look at the specific features and map them to the customer requirements. There are sufficient examples where products that weren’t “feature leaders” still were the better fit for specific customer scenarios.

Product Leaders (in alphabetical order):

- AdNovum
- CA Technologies
- Dell
- EmpowerID
- Ergon Informatik
- ForgeRock
- Forum Systems
- IBM
- Micro Focus
- Ping Identity
- SecureAuth

10 Innovation Leaders

The third angle we took when evaluating products was about innovation. Innovation is, from our perspective, a key distinction in IT market segments. Innovation is what customers require to receive new releases that meet new requirements. Thus, a look at Innovation Leaders is also important, beyond analyzing product features.

Here we see ForgeRock in front, followed by a number of other companies. Other Leaders include Ping Identity, EmpowerID, CA Technologies, Ergon, and IBM. All of them showed significant innovation and strong support of the list of features we consider as innovative in the Web Access Management and Identity Federation market, starting with broad standards support. AdNovum just made it into the Leaders segment, with significant improvements and innovations being added in recent releases.
SecureAuth and Micro Focus are leading the crowded Challenger segment, all being close to entering the Leaders segment. Most of the other vendors such as Oracle, GlobalSign, Evidian, Forum Systems, WSO2, Atos, and Dell are also well placed in the Challenger segment, indicating that they show significant innovation in this market.

Identity Automation again populates the Followers section. They have some innovative features, however due to the still relatively small overall feature set they lack support for some of the innovative features we’d like to see.

Again, in some cases products that appear more to the left of that figure do not necessarily fail in innovation but are focused on specific requirements or highly focused approaches.

Some vendors have demonstrated a significant amount of innovation in recent time, driving standards evolution forward. Others are innovative with respect to new features such as backend integration or integration with Enterprise Single Sign-On or Web Application Firewalls. Overall, this view reflects the fact that there is still a lot of innovation happening in the Access Management and Federation market, with significant room for some of the vendors to enhance their offerings.

Innovation Leaders (in alphabetical order):

- AdNovum
- CA Technologies
- EmpowerID
- Egon Informatik
- ForgeRock
- IBM
- Ping Identity

## 11 Product Evaluation

This section contains a quick rating for every product we’ve included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and KuppingerCole Executive View Reports available, providing more detailed information.
11.1 AdNovum – Nevis Security Suite

AdNovum is a Swiss-based software vendor. They support what they call “secure web interaction” with their Nevis Security Suite. The suite consists of various components for Web Access Management, including Federation support, and Web Application Firewall, authentication, user management including delegated administration and self-registration, support for digital signatures, and an administration console. All features are provided by separate components. However, these components are tightly integrated.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broad support for authentication mechanisms, including several national ID cards</td>
<td>Currently focused on few markets, including Switzerland and Singapore, but following a defined expansion strategy into other markets</td>
</tr>
<tr>
<td>Proven strength in various customer deployments</td>
<td>Still small but growing partner ecosystem</td>
</tr>
<tr>
<td>Additional, uncommon features such as delegated administration and digital signature support</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: AdNovum Nevis Security Suite major strengths and weaknesses.

AdNovum started developing the AdNovum Nevis Security Suite some fifteen years ago, thus having a long history and experience in this market segment. They provide a broad set of features around classical Web Access Management, managing access of external users to internal applications. That includes providing security tokens, coarse-grained authorization, but also advanced features - such as content inspection - that go beyond the common scope of Web Access Management products.

The product provides strong capabilities for flexible and extensible authentication with a broad set of authentication mechanisms, including some national eID cards. Due to the specific customer requirements (especially in government and insurance companies), there is also support for digitally signing documents, which is a rather uncommon add-on to that category of products.

AdNovum executes well on their roadmap and has added several features that had been lacking previously, such as extended standards support. Another strength is the reverse proxy functionality and, based on that, their support for Web Application Firewall features.

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

Table 2: AdNovum Nevis Security Suite rating.

The AdNovum Nevis Security Suite is an interesting offering from a feature perspective. The product has a well-defined architecture that is componentized. It provides several interesting and rather unique features, moving the product into the Product Leader’s category. The biggest challenge however is the still small number of partners and the limited regional reach, being mainly focused on the Swiss and Singapore markets as of now. However, AdNovum follows a defined expansion strategy into further markets.
11.2 Atos – DirX Access

DirX Access is the Access Management and Federation solution within the Atos DirX product family. These products came to the Atos portfolio as part of the Siemens SIS acquisition. Atos executes on a well-defined roadmap and has always been focused on providing solutions for enterprise customers with complex requirements and large-scale environments. The product differentiates through its support for runtime authorization management based on XACML queries.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proven solution with focus on large-scale environments, including its own managed services</td>
<td>Several features such as workflows, user self-registration and audit require additional DirX products</td>
</tr>
<tr>
<td>Support for applications requesting access at runtime through APIs, including XACML support</td>
<td>Limited support for mobile users</td>
</tr>
<tr>
<td>Broad support for various authentication mechanisms</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Atos DirX Access major strengths and weaknesses.

DirX Access provides standard Web Access Management capabilities and support for Identity Federation based on SAML, OAuth 2.0, and OpenID Connect 1.0. 2.0. A strength of the product is the broad support for various authentication mechanisms, including risk-based authentication.

While some other products in the market provide APIs for applications to request access decisions, support for fine-grained authorizations based on the XACML standard is rather uncommon. Separate products that are categorized as Dynamic Authorization Management solutions usually provide this capability. This feature might be relevant to some customers.

A challenge for some scenarios might result from the fact that many features such as workflow capabilities, user self-registration, or advanced audit functions are not supported by DirX Access itself but by other DirX components, i.e. DirX Identity and DirX Audit. Such modularity is fine from an architectural perspective, however deployments become more complex and license costs will increase. However, for existing DirX customers, this might be considered being an advantage.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>neutral</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>positive</td>
</tr>
</tbody>
</table>

Table 4: Atos DirX Access rating.

Atos DirX Access is an established product in the Access Management and Federation market. There should be improvements regarding the support for standards and, in particular, for mobile users. On the other hand, the product provides a mature and well thought out internal security model and support for Dynamic Authorization Management, which is relevant for several use cases.
11.3 CA Technologies – CA Single Sign-On

CA Single Sign-On, formerly known as CA SiteMinder, is one of the most established products in the Web Access Management market. It offers comprehensive Web Access Management and Identity Federation capabilities. The product has a very large number of customers, being very mature. It delivers excellent platform support.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mature product with a very large installed base</td>
<td>Some features such as workflows for management of external users are delivered by other CA Technologies products</td>
</tr>
<tr>
<td>Flexible access policies and good UI for managing those policies</td>
<td></td>
</tr>
<tr>
<td>Strong integration capabilities for applications</td>
<td></td>
</tr>
<tr>
<td>Outstanding platform support.</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: CA Single Sign-On major strengths and weaknesses.

Given the large number of deployments of CA Single Sign-On, it comes as no surprise that the products are leading-edge regarding the options for integration into existing IT environments. They provide broad support for different application server infrastructures, operating systems, etc. Also, there is an extensive set of APIs for integrating existing applications.

The core Web Access Management capabilities are also proven, mature, and comprehensive. There are various ways of interfacing to web applications and controlling access. Access can be managed very flexibly based on granular access policies. The features also include built-in support for connecting to various user stores such as directory services and the capability for virtualizing these environments.

The product provides extensive support for established standards such as SAML and WS-Federation. Support for OAuth 2.0 also has been added, while support for some emerging standards such as UMA is still lacking. However, we expect that this will change quickly based on the fact that CA Single Sign-On is leading-edge with respect to supporting heterogeneous infrastructures. Some complementary features such as self-service user registration are provided by CA Identity Manager.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>strong positive</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>strong positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 6: CA Single Sign-On rating.

CA Single Sign-On is well-established amongst the leading products in the Access Management and Federation market, being mature and widely deployed. CA Technologies has a good partner base for that product and delivers leading-edge support for heterogeneous IT infrastructures. This makes the product a clear pick for shortlists when looking for Access Management and Federation products.

CA Technologies

KuppingerCole Leadership Compass
Access Management and Federation
Report No.: 71102
11.4 Dell – One Identity Cloud Access Manager

Dell Software is one of the leading software vendors, with a broad portfolio in particular around infrastructure management and security. Part of this portfolio is Dell One Identity Cloud Access Manager (subsequently referred to as Cloud Access Manager). While the name indicates a cloud-based solution, the product in fact is an on-premise solution for Web Access Management and Identity Federation.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong policy- and role-based approach for managing access</td>
<td>No support for self-registration of external users</td>
</tr>
<tr>
<td>Support for dynamic roles and risk information including data delivered by firewalls, blacklist services etc.</td>
<td>Windows platform only, might be an inhibitor for some customers</td>
</tr>
<tr>
<td>Out-of-the-box integration with MFA (Multi-Factor Authentication) solutions</td>
<td></td>
</tr>
<tr>
<td>Integrated just-in-time provisioning for leading cloud services, support also for on-premise services</td>
<td></td>
</tr>
</tbody>
</table>

Table 7: Dell Cloud Access Manager major strengths and weaknesses.

Cloud Access Manager is a well thought-out solution with a number of rare features, such as risk-based policy decisions and integrated support for MFA both as a service and on-premises, through Dell Software’s Defender offerings. It provides a number of innovative features by integration with other Dell Software solutions, in particular integration with network threat information.

Cloud Access Manager is a strong entry into access management for both internal and external services and enables an SSO experience for users to all types of web-based services. In the recent version, some important additions have been made, such as support for OAuth 2.0. Overall, the functional breadth of the product is good. A particular strength is the integrated support for reverse proxy capabilities, allowing to control both inbound and outbound access well.

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

Table 8: Dell Cloud Access Manager rating.

There is still some room for improvement, e.g. by adding self-registration capabilities – including the required workflows – for external users that are not federated in. However, overall the product is an option that should be considered in product selections in that market segment.
11.5 EmpowerID – EmpowerID SSO Manager

EmpowerID, formerly known as The Dot Net Factory, provides a set of products based on the common EmpowerID platform. The Access Management and Federation features are provided by EmpowerID SSO Manager. This component offers both groups of services, including support for social logins and standard interfaces to various Cloud services such as Salesforce.com.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated platform with high flexibility in customization, based on workflows</td>
<td>Small but growing partner ecosystem</td>
</tr>
<tr>
<td>Strong support for new requirements such as social logins and SSO to cloud services</td>
<td>Limited but growing integration into SIEM tools and other advanced auditing tools</td>
</tr>
<tr>
<td>Strong support for federation standards</td>
<td></td>
</tr>
</tbody>
</table>

Table 9: EmpowerID SSO Manager major strengths and weaknesses.

EmpowerID has built its product portfolio on a common platform that supports flexible customization based on its workflow capabilities. Rapid deployment is supported based on a set of standard workflows for Access Management and Federation. This platform both eases deployment and provides good integration with other IAM features provided by EmpowerID.

The major focus of the EmpowerID SSO Manager is support for Identity Federation, including advanced features such as out-of-the-box support for social logins or standard interfaces to common Cloud providers such as Salesforce.com and others. In the area of Web Access Management, the feature set is rather standard, with HTTP header injection as the standard capability. Besides the support of social logins, there is good support for other authentication mechanisms. The breadth of support for current standard protocols for Identity Federation can be rated as state-of-the-art.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>strong positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>strong positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 10: EmpowerID SSO Manager rating.

EmpowerID SSO Manager has made it in both the Product Leader’s and Innovation Leader’s segments of this Leadership Compass, based on their good support for standards and some innovative capabilities especially around Identity Federation. The still rather small partner ecosystem might become an inhibitor for customers. Thus, it is clearly a solution that is worth evaluation, especially for customers that build on Microsoft Windows Server infrastructures.
11.6 Ergon Informatik – Airlock Suite

Ergon Informatik is a Swiss vendor that offers an integrated solution consisting of various components, which in combination provide the Web Access Management and Identity Federation capabilities. Airlock Suite provides authentication capabilities, workflow features, Web Application Firewall capabilities, and at its core Web Access Management and Identity Federation capabilities.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broad support for various authentication</td>
<td>Limited support for standards beyond SAML,</td>
</tr>
<tr>
<td>mechanisms</td>
<td>OAuth 2.0 and JWT; support for WS-standards lacking</td>
</tr>
<tr>
<td>Integrated support for features such as user</td>
<td>Still rather small partner ecosystem and</td>
</tr>
<tr>
<td>self-registration and password reset with</td>
<td>limited global reach</td>
</tr>
<tr>
<td>strong flexibility</td>
<td></td>
</tr>
<tr>
<td>Strong Web Access Management capabilities</td>
<td></td>
</tr>
</tbody>
</table>

Table 11: Ergon Airlock Suite major strengths and weaknesses.

Ergon has integrated two formerly separate products, Airlock and Medusa, into one suite. Based on that, the Airlock Suite provides a good foundation for addressing Web Access Management requirements and also Identity Federation challenges. However, the support for new standard protocols in Identity Federation is still somewhat limited and leaves room for improvement. On the other hand, the product provides excellent capabilities for traditional Web Access Management with a mass of integration capabilities to existing applications. A particular strength are the Web Application Firewall and reverse proxy capabilities.

We positively recognize that Ergon has made massive progress in moving from a separate set of products towards an integrated suite. That eases deployments and gives customers access to an integrated offering, while particular capabilities still can be licensed separately, based on the now three different components Airlock WAF (Web Application Firewall), Airlock Login (strong authentication, SSO), and Airlock IAM (user & token management, cross-domain SSO, and self-services).

Overall, the products provide a good set of capabilities especially when it comes to Web Access Management and Identity Federation requirements, with still some room for improvement in the area of Identity Federation.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>strong neutral</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 12: Ergon Airlock Suite rating.

As with many smaller vendors, the partner ecosystem of Ergon Informatik is still rather small and global reach is limited. On the other hand, there are a significant number of customers especially in Central Europe. Based on the improvements the company has made in the past two years, Ergon Airlock Suite has emerged to an interesting alternative to established solutions in this market segment.
11.7 Evidian – Web Access Manager

Evidian is a vendor based in France that is part of Groupe Bull, a large IT vendor and systems integrator. The company provides a comprehensive portfolio in the area of IAM. Their key product for Web Access Management and Identity Federation is named Evidian Web Access Manager. It is integrated with other Evidian solutions both in the area of Identity Provisioning and Enterprise Single Sign-On.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration with Enterprise-SSO and Mobile E-SSO features</td>
<td>Few system integration partners outside of EMEA</td>
</tr>
<tr>
<td>Strong Web Access Management capabilities and good support for Identity Federation standards</td>
<td>Limited multi-tenancy support</td>
</tr>
<tr>
<td>Authorization Management capabilities available as add-on module</td>
<td>Standard support focused on main standards such as SAML and OAuth</td>
</tr>
</tbody>
</table>

Table 13: Evidian Web Access Manager major strengths and weaknesses.

Evidian Web Access Manager is a mature solution for Web Access Management and Identity Federation, with support for various Identity Federation protocols. It also supports a wide range of authentication mechanisms. A unique feature is the tight integration with the Enterprise Single Sign-On product of Evidian. This allows users that have signed-on via E-SSO – including mobile devices – to directly access web applications via Evidian Web Access Manager. In some areas, there is some integration and dependency on the Evidian Identity & Access Manager for advanced features. It also provides self-service capabilities and other features required for efficient deployments to external users.

Another strength is the broad platform support of the product. It runs on various Linux, UNIX, and Windows Server versions. All backend components such as databases are delivered with the product. However, there are no managed services or Cloud offerings for that product as of now.

As an add-on, the product can be integrated with the Evidian Identity & Access Manager to support fine-grained run-time authorizations. This is a rarely found feature in that type of product but is relevant to some customers.

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

Table 14: Evidian Web Access Manager rating.

Overall, Evidian delivers an interesting offering in the area of Access Management and Federation, particularly through its integration with the Enterprise SSO offering. There is a significant number of system integration partners in Europe, but few in other regions. Overall, the Evidian offering is an interesting alternative to the established players in the market and deserves evaluation in decision making processes.
11.8 ForgeRock – OpenAM

ForgeRock over the past years has emerged from a start-up towards a leading vendor in the IAM space. While their products are open source, both technology and support are enterprise grade today. Their offering for Web Access Management and Identity Federation is named OpenAM. The product provides comprehensive support for the Access Management/Federation requirements. All ForgeRock products are based on a common platform, the ForgeRock Identity Platform.

### Strengths/Opportunities
- Strong features for Identity Federation
- Very broad support for various authentication methods, strong security and authorization model
- Broad platform support

### Weaknesses/Threats
- More advanced functionalities in self-registration and user management might require OpenIDM in addition

Table 15: ForgeRock OpenAM major strengths and weaknesses.

OpenAM is the leading open source solution in the area of Access Management and Federation, but also amongst the leading-edge products when compared with the “closed source” offerings. The products are freely available; however, for production use a subscription is required. The product offers a comprehensive set of features in both Identity Federation and Web Access Management, with various ways of supporting existing web applications. In the area of Identity Federation, all relevant standard protocols are supported.

It offers great multi-platform support, for user stores, operating systems, and databases. It also offers broad support for various authentication mechanisms. The authorization model is based on a policy engine. Policies are stored in a central policy store. This approach allows for implementing both coarse-grained and fine-grained policies.

The product also offers basic features for user self-service, including registration and password management. However, ForgeRock recommends using their OpenIDM product for more complex requirements. Given that both products are based on a common stack, this is fairly straightforward. However, it will affect licensing cost.

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

Table 16: ForgeRock OpenAM rating.

ForgeRock is venture-financed and currently investing heavily in product development. This results in both rapidly improving the (already good) capabilities of the product and already has led to a large partner ecosystem on global scale. ForgeRock OpenAM is amongst the leading-edge products in the Access Management and Federation market segment and should be considered in product evaluations.
11.9 Forum Systems – Forum Sentry

Forum Systems differs from all other solutions in this Leadership Compass by the fact that it is delivered also as a hard or soft appliance. The product delivers a broad set of functionality in particular around Identity Federation and federated SSO, but also additional capabilities such as integrated Web Application Firewall functionality.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong features for Identity Federation</td>
<td>Appliance- and gateway-based approach</td>
</tr>
<tr>
<td>Very broad support for various authentication methods</td>
<td>differs from other solutions, requires in-depth</td>
</tr>
<tr>
<td>Strong security model</td>
<td>evaluation</td>
</tr>
<tr>
<td>Additional capabilities for API Management and Web Application Firewall</td>
<td>Only baseline support for traditional Web Access Management</td>
</tr>
</tbody>
</table>

Table 17: Forum Systems Sentry major strengths and weaknesses.

Forum Systems started in the API Management space, with a solution built as hard appliance for controlling API-based access to systems. However, most of the standards in that area are anyway similar to the ones relevant for Web Access Management and Identity Federation, thus the extended support and positioning for the latter market segment is just a logical extension.

Standard support is comprehensive, with UMA planned for support in 2016. For traditional Web Access Management, the feature set is more baseline, however the added capabilities provided through their reverse proxy and Web Access Management capabilities make it an interesting offering in that space as well. Furthermore, many of the common features of Web Access Management can be replaced by the gateway-based approach of Forum Sentry, being also agent-less and thus simple to deploy.

The deployment of Forum Sentry as hard appliance can be a benefit or challenge to customers, depending on the way customers build their infrastructure and their specific preferences. However, with the alternative deployment options, Forum Systems gives customers full choice. Furthermore, having a ready-to-use solution which just must be plugged into the network is an advantage for rapid deployment.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>strong positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 18: Forum Systems Sentry rating.

Forum Systems with its Sentry product is a challenger to the established players in the markets for Web Access Management and Identity Federation. Due to their gateway-based approach, they differ from most other offerings. Forum Systems should be considered in product evaluations in this market segment, in particular also due to their alternative approach for form factor and thus deployment and the integration with API Security capabilities.
11.10 GlobalSign IAM

GlobalSign has acquired Ubisecure a while ago. GlobalSign is a leading provider of digital certificates and extends its portfolio into other areas. GlobalSign IAM is different from most other solutions in the market in its focus on service providers instead of end-user organizations. Thus, the feature set concentrates on the specific requirements for these groups of users. However, we see the product also as an interesting solution for end-user organizations.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong support for authentication methods, including national ID cards and banking ID cards</td>
<td>Still a relatively small partner ecosystem</td>
</tr>
<tr>
<td>Strong capabilities for service providers, especially around self-registration</td>
<td>Main presence in EMEA as of now, but growing in other regions</td>
</tr>
<tr>
<td>Integrated Identity Management capabilities, for instance to manage group membership and consolidate users</td>
<td>Limited support for emerging standards such as UMA</td>
</tr>
</tbody>
</table>

Table 19: GlobalSign IAM major strengths and weaknesses.

When looking at the standard feature areas of Web Access Management and Identity Federation, the Ubisecure IAM Suite provides strong support, including more specific standards such as ETSI MSS 102-204 and the most recent standard from GSMA, Mobile Connect. GlobalSign has shown commitment to innovation by adding that standard and thus enabling advanced and convenient mobile-based authentication such as biometrics for end users.

The primary focus of the product is supporting service providers in providing controlled access for customers or citizens, which also serves well for use cases of large organizations that need to support consumer and customer access. The product supports a broad range of authentication methods, including banking cards and national ID cards. There are also fully configurable registration workflows as a standard feature, as well as functions that allow identifying, cleansing, and enhancing data on registration.

The product integrates basic identity management capabilities for these specific use cases, resulting in a complete solution for the targeted customers.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 20: GlobalSign IAM rating.

With the acquisition by GlobalSign, there is a far better scale than before. However, most customers are still in EMEA and the partner ecosystem is rather small. On the other hand, the product is highly attractive for service providers, mobile network operators, and governments but also large organizations due to its specific features for use cases that primarily focus on the integration of customers or citizens at large scale.
11.11 IBM – Security Access Manager

IBM Security Access Manager integrates the formerly separate products IBM Tivoli Access Manager (TAM) and IBM Tivoli Federated Identity Manager (TFIM). The solution is delivered as a soft/virtual appliance as well as a hardware appliance with full integration of the capabilities of the formerly separate offerings, plus a number of functional improvements that have been added in the latest releases. It thus fully covers both the traditional Web Access Management and the Identity Federation use cases.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very large customer base with many large-scale deployments</td>
<td>Advanced workflow features require integration with IBM Security Identity Manager</td>
</tr>
<tr>
<td>Good support for federation standards</td>
<td>Limitations for multi-tenancy</td>
</tr>
<tr>
<td>Very strong support for Web Access Management</td>
<td></td>
</tr>
<tr>
<td>Very good platform support</td>
<td></td>
</tr>
</tbody>
</table>

Table 21: IBM Security Access Manager major strengths and weaknesses.

IBM has one of the largest customer bases of all vendors in this market segment. There are many very large deployments of the products. Thus, it comes as no surprise that the products provide strong support for various authentication mechanisms, but also very broad platform support and comprehensive integration capabilities with existing web applications.

Besides the strength in Web Access Management, IBM Security Access Manager also offer strong support for federation standards. Like several other solutions, advanced features for workflows and user self-service management require the use of an additional product, in that case the IBM Security Identity Manager. Integration is straightforward, as it is between the two core products of the IBM Access Management solution. Furthermore, there is integration into other IBM Security offerings such as QRadar, supporting e.g. advanced threat analytics, Trusteer Pinpoint for fraud and malware protection, and others.

With the recent improvements, there remain few limitations. One is the limited support for multi-tenancy. One challenge in that area is that audit logs are not separated per tenant. Another challenge is that the transport of environments from development to test to production, i.e. staging, is only supported via command-line interfaces or REST APIs by scripting. This can become a little cumbersome. However, IBM Security Access Manager overall delivers excellent capabilities.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>strong positive</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 22: IBM Security Access Manager rating.

In sum, the IBM Security Access Management Solution is amongst the leading products in the Access Management and Federation market for good reasons. It provides broad feature support and is a very mature solution. In addition, IBM offers a large number of system integration partners on global scale and strong experience in large-scale deployments.
11.12 Identity Automation - RapidIdentity

Identity Automation has been in the market for more than a few years, however it was initially in the system integrator business around IAM, before becoming a software vendor. Based on the experience and expertise from the integration business, Identity Automation has developed its own software product, RapidIdentity, focusing on support for the complete identity and access lifecycle provided through a well-integrated solution with strong out-of-the-box capabilities.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated platform covering a broad range of IAM requirements</td>
<td>Baseline support for standards, focusing on major federation standards</td>
</tr>
<tr>
<td>Integrated support for multi-factor authentication</td>
<td>No support for social logins yet, limited support for authentication methods</td>
</tr>
<tr>
<td>Registration and self-service as standard capability</td>
<td>Relatively small vendor with limited ecosystem, no global scale yet</td>
</tr>
<tr>
<td>Proven scalability even for very large environments</td>
<td></td>
</tr>
</tbody>
</table>

Table 23: Identity Automation RapidIdentity major strengths and weaknesses.

RapidIdentity is a product focusing on support for a broad variety of IAM capabilities. One of the features is RapidFederation, which also can be licensed separately. As all functional feature sets of RapidIdentity, RapidFederation relies on the core platform capabilities and adds additional services.

RapidFederation provides support for federating out to cloud applications and other types of applications supporting the SAML standard. Thus, the solution also acts as a Cloud Single Sign-On product, beyond the standard IAM/IAG capabilities, which is yet a quite rare combination. However, support as-of-now is limited to the SAML v2 standard, while support for OAuth 2.0 is yet missing. Furthermore, there is no extended support for federated provisioning of users to cloud services based on SCIM or custom integrations. Also support for traditional Web Access Management requirements is lacking.

<table>
<thead>
<tr>
<th>Security</th>
<th>neutral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>neutral</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>neutral</td>
</tr>
<tr>
<td>Usability</td>
<td>positive</td>
</tr>
</tbody>
</table>

Table 24: Identity Automation RapidIdentity rating.

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 evaluated here. However, due to their integrated approach, the product is an interesting option for organizations looking for such type of solution that is well integrated and rapid to deploy.
11.13 Micro Focus – Access Manager

Micro Focus has been the first vendor in the market to integrate Identity Federation capabilities from the very beginning with Web Access Management features. Thus, there is a fully integrated solution for Access Management/Federation now, built on a consistent architecture. The product is widely deployed and mature.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full integration between Web Access Management and Identity Federation</td>
<td>No SCIM support yet</td>
</tr>
<tr>
<td>Flexible configuration of access policies</td>
<td>Workflow support requires use of NetIQ Identity Manager</td>
</tr>
<tr>
<td>Good support for most federation-related standards</td>
<td></td>
</tr>
</tbody>
</table>

Table 25: Micro Focus Access Manager major strengths and weaknesses.

The support for managing access to existing web applications already is comprehensive. In the areas of standards support, Micro Focus has a clear commitment on supporting new standards. However, some standards such as SCIM for provisioning in federated environments are not yet supported.

The product offers self-service password reset along with self-registration capabilities. However, for more advanced features such as workflow capabilities, either 3rd party solutions or the Micro Focus Identity Manager might be needed as additional components. Support for authentication mechanisms and for operating system platforms is good. Micro Focus Access Manager also provides good capabilities for managing access policies and a high degree of flexibility in that area.

A shortcoming of the product is the lack of APIs that can be used by applications to request authorization decisions or by administrators to control and configure the product. These should be available in an upcoming release.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>strong positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 26: Micro Focus Access Manager rating.

Micro Focus can build on a large partner ecosystem on a global scale. The product is widely deployed, with a significant number of large-scale implementations at customers. Overall, Micro Focus Access Manager is one of the leading products in the Access Management/Federation market segment, even while some improvement in innovation performance is recommended.
11.14 Oracle – Access Management

Oracle Access Management is a multi-functional product that consists of several services, including Oracle Access Manager (OAM), Mobile and Social, Identity Federation and Secure Token Services, as well as Adaptive Access Manager (OAAM), Entitlement Server (OES) and API Gateway (OAG). This provides customers with a broad range of features, beyond the core area of Access Management and Federation. Given that not all of these features apply to the market segment evaluated in this KuppingerCole Leadership Compass, not all of them are taken into account for the rating. For customers looking for a strategic approach beyond these areas, integrating risk- and context-based authentication and authorization as well as Dynamic Authorization Management, Oracle Access Management Suite Plus provides a unique feature combination in the market. Another strength is the support for social logins and mobile security.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong feature set for Access Management and Federation</td>
<td>Suite converging but still based on separate products</td>
</tr>
<tr>
<td>Several additional features such as risk- and context-based authentication and authorization and support for social and mobile access</td>
<td>Limitations in multi-tenancy, but alternative Cloud offering available and defined roadmap for on-premise solution</td>
</tr>
<tr>
<td>Large installed base</td>
<td>Workflows require use of an Oracle sister product</td>
</tr>
</tbody>
</table>

Table 27: Oracle Access Management major strengths and weaknesses.

With its approach to combining formerly separate products into a comprehensive access platform, Oracle has decided to move away from a large number of point solutions. That provides opportunities for customers to have access to a very broad range of capabilities, but requires good planning of the deployments and the overall approach to Access Management. A clear advantage is the well-defined path towards new types of capabilities.

The product provides strong support for various features such as authentication methods, management and flexibility of access policies, and platform support. Oracle also is clearly committed to supporting open federation standards.

However, there are also some areas with room for improvement. This holds especially true for the support of multi-tenancy. This can be solved; however, the product still lacks full support for multi-tenancy.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>neutral</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 28: Oracle Access Management rating.

Overall, the Oracle Access Management platform is a strong offering in the Access Management and Federation market segment. It is a logical pick for product shortlists. However, the complexity of the suite should not be underestimated and balanced with the current and future requirements.
11.15 Ping Identity – Federated Access Management

Ping Identity is, in contrast to most other vendors in the Access Management and Federation market segment, primarily focused on the area of Identity Federation in its early days and amongst the recognized leaders in that area, particularly for its leading role in innovation for this market segment. The core product in that area is PingFederate, a widely deployed and mature solution. Ping has expanded its product offering to include additional capabilities, such as, multi-factor authentication, access security and multi-tenant SaaS delivery, packaged as Ping Identity Federated Access Management.

**Strengths/Opportunities**
- Excellent support for all Identity Federation requirements
- Very innovative and excellent standards support
- Integrated native mobile strong authentication capabilities
- Strong track record in rapid deployments
- Good support for both on-premise and Cloud deployments

**Weaknesses/Threats**
- No full support for traditional Web Access Management, but offers lightweight Web Server integration kits and reverse proxy functionality as alternative solutions
- No full support for multi-tenancy but alternative cloud offerings

Table 29: Ping Federated Access Management major strengths and weaknesses.

Ping Identity’s Federated Access Management product includes an access policy server which provides access security services for Web, mobile and API security through a central policy administration server, and also provides proxy, agent and RESTful API enforcement points. The access policy server integrates with the federation server and authentication services through standard-based interfaces to enable cross-domain federation, authentication and authorization services for legacy and modern security and application infrastructures.

Ping Identity offers Identity as-a-Service (IDaaS) as part of the Federated Access Management (FAM) product, which supports identity administration and self-service administration features. Device registration and identification are also provided with the IDaaS authentication service. In addition, password change and reset is available in both software and IDaS depending on the deployment model their customers need.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>strong positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Table 30: Ping Federated Access Management rating.

Due to the specific role as one of the Innovation Leaders and overall leading-edge solution for Identity Federation, we see PingFederate as a must in shortlists for Identity Federation. Additionally, based on the various integration approaches, the product can also serve well for environments where some traditional Web Access Management still is required.
SecureAuth is one of the vendors in the market that have been around for quite some time. As the name implies, their specific strength is not only providing Web Access Management and Identity Federation capabilities but strong authentication as a mix of service and on-premises capabilities. In contrast to most other offerings, SecureAuth supports both Cloud and on-premises deployments.

### Strengths/Opportunities
- Strong support for strong authentication mechanisms
- Tight integration especially with on-premises Microsoft Active Directory
- Strong standards support
- Well thought-out approach on security and data privacy

### Weaknesses/Threats
- Good baseline support for Identity Federation, but not leading-edge
- Limited support for traditional Web Access Management capabilities

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>positive</td>
</tr>
<tr>
<td>Integration</td>
<td>strong positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>strong positive</td>
</tr>
<tr>
<td>Usability</td>
<td>strong positive</td>
</tr>
</tbody>
</table>

Even while SecureAuth commonly is considered being a cloud provider, the traditional deployment is on premises. For customers looking for strong integration with enterprise infrastructures and strong authentication, SecureAuth is an interesting pick despite their shortcomings regarding traditional Web Access Management. The product also can work complementary to established Web Access Management solutions, adding e.g. strong authentication support.
11.17 WSO2 – Identity Server

WSO2 is a provider of an open-source suite of products positioned as “lean enterprise middleware”. That term describes well where WSO2 positions themselves: as a provider of a comprehensive suite of middleware functions covering the needs of connected enterprises and supporting business processes within and beyond the perimeter of the organization. This includes support in particular for Identity Federation use cases.

<table>
<thead>
<tr>
<th>Strengths/Opportunities</th>
<th>Weaknesses/Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development platform approach, allowing for flexible</td>
<td>No focus on traditional Web Access Management</td>
</tr>
<tr>
<td>customization</td>
<td>Platform approach with growing support for out-of-the-box usage scenarios</td>
</tr>
<tr>
<td>Strong standard support</td>
<td>Few specific connectors to target systems</td>
</tr>
<tr>
<td>Broad IAM capabilities, beyond Access Management and</td>
<td></td>
</tr>
<tr>
<td>Federation</td>
<td></td>
</tr>
<tr>
<td>Excellent scalability for large scale deployments</td>
<td></td>
</tr>
<tr>
<td>Growing partner ecosystem on global scale</td>
<td></td>
</tr>
</tbody>
</table>

Table 33: WSO2 Identity Server strengths and weaknesses.

It supports multifactor authentication with FIDO U2F and Single Sign-On (SSO). SSO is supported via OpenID, OpenID Connect, SAML2, WS-Federation, and Kerberos KDC. The latter allows integration with Microsoft Active Directory authentication. SAML2 support also provides integration with Cloud applications and SSO to these. Beyond SAML2 as one of the most important federation standards, there is also support for other standards such as OAuth 2.0 and WS-Trust. API Security for REST-based communication can be implemented using OAuth 2.0 and XACML.

For fine-grained Dynamic Authorization Management, WSO2 Identity Server provides support for both XACML 2.0 and 3.0 standards. It allows using various PIPs (Policy Information Points) and can work with a number of PEPs (Policy Enforcement Points).

While the standards support is excellent and the above paragraphs list only a portion of these, there is somewhat limited support for standard integrations. However, WSO2 is consequently working on enhance the breadth of support for out-of-the-box use of the product, beyond the platform approach.

<table>
<thead>
<tr>
<th>Security</th>
<th>strong positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality</td>
<td>neutral</td>
</tr>
<tr>
<td>Integration</td>
<td>positive</td>
</tr>
<tr>
<td>Interoperability</td>
<td>positive</td>
</tr>
<tr>
<td>Usability</td>
<td>positive</td>
</tr>
</tbody>
</table>

Table 34: WSO2 Identity Server rating.

The clear strength of WSO2 Identity Server is the platform approach, which allows creating custom solutions e.g. for consumer identity management. For customers looking for a ready-to-use solution, WSO2 Identity Manager is not the first choice. However, with their excellent support for standards, the product is well worth an evaluation in many customer scenarios.
12 Products 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 35.

<table>
<thead>
<tr>
<th>Product</th>
<th>Security</th>
<th>Functionality</th>
<th>Integration</th>
<th>Interoperability</th>
<th>Usability</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdNovum Nevis Security Suite</td>
<td>strong positive</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Atos DirX Access</td>
<td>strong positive</td>
<td>positive</td>
<td>neutral</td>
<td>positive</td>
<td>positive</td>
</tr>
<tr>
<td>CA Single Sign-On</td>
<td>strong positive</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Dell One Identity Cloud Access Manager</td>
<td>strong positive</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>EmpowerID SSO Manager</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Ergon Airlock Suite</td>
<td>strong positive</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Evidian Web Access Manager</td>
<td>strong positive</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>ForgeRock OpenAM</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Forum Systems Forum Sentry</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>GlobalSign IAM</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>IBM Security Access Management</td>
<td>strong positive</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Identity Automation RapidIdentity</td>
<td>neutral</td>
<td>neutral</td>
<td>positive</td>
<td>neutral</td>
<td>neutral</td>
</tr>
<tr>
<td>Micro Focus Access Manager</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Oracle Access Management</td>
<td>strong positive</td>
<td>positive</td>
<td>neutral</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Ping Identity Federated Access Management</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>SecureAuth IdP</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>WSO2 Identity Server</td>
<td>strong positive</td>
<td>neutral</td>
<td>positive</td>
<td>positive</td>
<td>positive</td>
</tr>
</tbody>
</table>

Table 35: Comparative overview of the ratings for the product capabilities.
In addition we provide in table 38 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.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Innovativeness</th>
<th>Market Position</th>
<th>Financial Strength</th>
<th>Ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdNovum Informatik</td>
<td>positive</td>
<td>weak</td>
<td>positive</td>
<td>weak</td>
</tr>
<tr>
<td>Atos</td>
<td>positive</td>
<td>neutral</td>
<td>positive</td>
<td>neutral</td>
</tr>
<tr>
<td>CA Technologies</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Dell</td>
<td>positive</td>
<td>neutral</td>
<td>strong positive</td>
<td>positive</td>
</tr>
<tr>
<td>EmpowerID</td>
<td>strong positive</td>
<td>neutral</td>
<td>positive</td>
<td>neutral</td>
</tr>
<tr>
<td>Ergon Informatik</td>
<td>strong positive</td>
<td>neutral</td>
<td>positive</td>
<td>neutral</td>
</tr>
<tr>
<td>Evidian</td>
<td>positive</td>
<td>neutral</td>
<td>positive</td>
<td>neutral</td>
</tr>
<tr>
<td>ForgeRock</td>
<td>strong positive</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Forum Systems</td>
<td>positive</td>
<td>neutral</td>
<td>positive</td>
<td>positive</td>
</tr>
<tr>
<td>GlobalSign</td>
<td>positive</td>
<td>neutral</td>
<td>positive</td>
<td>positive</td>
</tr>
<tr>
<td>IBM</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Identity Automation</td>
<td>weak</td>
<td>critical</td>
<td>weak</td>
<td>critical</td>
</tr>
<tr>
<td>Micro Focus</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Oracle</td>
<td>positive</td>
<td>strong positive</td>
<td>strong positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>Ping Identity</td>
<td>strong positive</td>
<td>positive</td>
<td>positive</td>
<td>strong positive</td>
</tr>
<tr>
<td>SecureAuth</td>
<td>positive</td>
<td>neutral</td>
<td>neutral</td>
<td>positive</td>
</tr>
<tr>
<td>WSO2</td>
<td>positive</td>
<td>neutral</td>
<td>neutral</td>
<td>neutral</td>
</tr>
</tbody>
</table>

Table 36: Comparative overview of the ratings for vendors.

Table 36 requires some additional explanation in case that a vendor has got a “critical” rating.

In the area of **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, advanced analytical capabilities, and others. However, in this analysis all vendors scored at least neutral regarding this criterion.

The **critical** ratings are applied for **Market Position** in the case of vendors which have a very limited visibility (with that particular product and in general) 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 the area of *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 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 the own consulting and system integration business. However, our strong believe is that growth and successful market entry of companies into a market segment relies on strong partnerships.

### 12.1 The Market/Product Matrix

![Market/Product Matrix](image)

Fig. 12: 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.

Beyond that analysis, we have compared the position of vendors regarding combinations of our three major areas of analysis, i.e. Market Leadership, Product Leadership, and Innovation Leadership. That analysis provides additional information.

These comparisons, for instance, use the rating in Product Leadership on the horizontal axis and relate it with the rating in other areas, which is shown on the vertical axis. The result is split into four quadrants. The upper right quadrant contains products with strength both in the product rating and in the second rating we’ve looked at in the particular matrix, e.g. innovation. The lower right quadrant contains products that are overall strong but are lacking in the dimension shown on the vertical axis.

For example, this can be products that have strong technical capabilities but are relatively new to the market, resulting in a small customer base. The upper left quadrant contains products which are typically below average in the product rating but have specific strengths regarding the second dimension we look at in the particular matrix. They might be highly innovative or very mature and established, but not being leading edge when looking at the product rating. Finally, there is the lower left quadrant that contains products suffering on both axes. However, these products might have specific strengths that are highly valuable for some specific use cases.
In that 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 frequently are innovative but focused on specific regions.

We’ve defined four segments of vendors to help in classifying them:

**Market Leaders:** This segment contains vendors which have a strong position in our categories of Product Leadership and Market Leadership. These vendors have an overall strong to excellent position in the market.

**Strong Potentials:** This segment includes vendors which have strong products, being ranked high in our Product Leadership evaluation. However, their market position is not as good. That might be due to various reasons, like a regional focus of the vendors or the fact that they are niche vendors in that particular market segment.

**Market Performers:** Here we find vendors which have a stronger position in Market Leadership than in Product Leadership. Typically, such vendors have a strong, established customer base due to other market segments they are active in.

**Specialists:** In that segment we typically find specialized vendors which have – in most cases – specific strengths but neither provide full coverage of all features which are common in the particular market segment nor count among the software vendors with overall very large portfolios.

This chart shows an interesting distribution of the vendors. On one hand, we see a number of companies in the Market Leaders segment. These include the overall leaders such as CA Technologies, ForgeRock, IBM, Micro Focus, and Ping Identity, but also Oracle and Dell Software.

The Strong Potentials segment also contains a number of vendors, with EmpowerID, GlobalSign, SecureAuth, Evidian, Forum Systems, and Ergon all being close to entering the Market Leaders segment. Also Atos and WSO2 are found in that segment. AdNovum is also positioned here, but still has to improve its positioning in the Market Leaders rating.

While there are no Market Performers, we see one company. Identity Automation is a real specialist, focusing on certain aspects of the market.
12.2 The Product/Innovation Matrix

![Product/Innovation Matrix Diagram]

Fig. 13: The Product/Innovation Matrix. Vendors below the line are less innovative, vendors above the line are, compared to the current Product Leadership positioning, more innovative.

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with few exceptions. This distribution and correlation is typical for mature markets with a significant number of established vendors plus a number of smaller vendors.

Again we’ve defined four segments of vendors. These are

- **Technology Leaders:** This group contains vendors which have technologies which are strong regarding their existing functionality and which show a good degree of innovation.

- **Establishment:** In that segment we typically find vendors which have a relatively good position in the market but don’t perform as strong when it comes to innovation. However, there are exceptions if vendors take a different path and focus on innovations which are not common in the market and thus do not count that strong for the Innovation Leadership rating.

- **Innovators:** Here we find highly innovative vendors with a limited visibility in the market. It is always worth having a look at this segment because vendors therein might be a fit especially for specific customer requirements.

- **Me-toos:** This segment mainly contains those vendors which are following the market. There are exceptions in the case of vendors which take a fundamentally different approach to providing specialized point solutions. However, in most cases this is more about delivering what others have already created.

In that chart, most vendors are placed in the Technology Leaders segment, with a strong correlation of Innovation and Product rating. This is typical for more mature markets, where most vendors deliver a broad set of features, including at least a significant portion of the more innovative features.
Anyhow, within the segment we see a number of vendors more to the upper right edge, indicating strength in both product capabilities and innovativeness, while others are more to the lower left, showing that these are not as strong in these ratings.

Finally, we see Identity Automation with their more specialized offering in the “Me-toos” segment.

### 12.3 The Innovation/Market Matrix

![Innovation/Market Matrix Diagram]

Fig. 14: The Innovation/Market Matrix. Vendors below the line are performing well in the market compared to their relatively weak position in the Innovation Leadership rating, while vendors above the line show based on their ability to innovate, the biggest potential for improving their market position.

The third relation shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position.

On the other hand, vendors which are highly innovative have a good chance for improving their market position but might also fail, especially in the case of smaller vendors.

The four segments we have defined here are

**Big Ones:** These are market leading vendors with a good to strong position in Innovation Leadership. This segment mainly includes large software vendors.

**Top Sellers:** In that segment we find vendors which have an excellent market position compared to their ranking in the Innovation Leadership rating. That can be caused by a strong sales force or by selling to a specific community of “customer customers”, i.e. a loyal and powerful group of contacts in the customer organizations.
Hidden Gems: Here we find vendors which are more innovative than would be expected when looking at their Market Leadership rating. These vendors have a strong potential for growth, however they also might fail in delivering on that potential. Nevertheless, this group is always worth a look due to their specific position in the market.

Point Vendors: In that segment we find vendors which typically either have point solutions or which are targeting specific groups of customers, like SMBs, with solutions focused on these, but not necessarily covering all requirements of all types of customers and thus not being amongst the Innovation Leaders. These vendors might be attractive if their solution fits the specific customer requirements.

Hidden Gems: Here we find vendors which are more innovative than would be expected when looking at their Market Leadership rating. These vendors have a strong potential for growth, however they also might fail in delivering on that potential. Nevertheless, this group is always worth a look due to their specific position in the market.

Point Vendors: In that segment we find vendors which typically either have point solutions or which are targeting specific groups of customers, like SMBs, with solutions focused on these, but not necessarily covering all requirements of all types of customers and thus not being amongst the Innovation Leaders. These vendors might be attractive if their solution fits the specific customer requirements.

Here we see a number of companies being both highly innovative and having a strong position in the market. These companies, being placed in the Big Ones segment, include CA Technologies, Dell, ForgeRock, IBM, Micro Focus, Oracle, and Ping Identity.

While the Top Sellers segment is empty, the Hidden Gems segment is very crowded as well, containing most of the other vendors such as AdNovum, Atos, EmpowerID, Ergon, Evidian, Forum Systems, GlobalSign, SecureAuth, and WSO2.

Again, Identity Automations fall somewhat apart due to their specialized offering, being placed in the Point Vendors segment.

13 Overall Leadership – the combined view

Finally, we’ve put together the three different ratings for Leadership, i.e. Market Leadership, Product Leadership, and Innovation Leadership and created an Overall Leadership rating. This is shown below in figure 15.

Fig. 15: The Overall Leadership rating for the Access Management/Federation market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].
In the market for Web Access Management and Federation, we currently see five companies in the Leaders segment for Overall Leadership. 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 gained significant market share over the past years and made it into the Leaders segment.

The Challenger segment is very crowded, with most vendors being placed in that segment. Here we find a variety of players, including large and established vendors such as Oracle, Dell, Evidian, or Atos, which provide mature offerings, however being not always as feature-rich and innovative as the companies in the Leaders segment. We also find a number of still relatively new companies such as EmpowerID and GlobalSign, the latter after their acquisition of former Ubisecure. AdNovum and Ergon are two vendors based in Switzerland, which both offer strong integrated Web Application Firewall capabilities.

Furthermore, we find a number of specialists in the Challengers section, including Forum Systems with their gateway-based approach also delivering strong API Security features, SecureAuth focusing on multi-factor authentication to the cloud, and WSO2 with a platform-based open source approach showing its particular strength in supporting the rapid development of complex custom solutions.

Finally, we have one vendor being placed in the Followers section. Identity Automation is a rather small companies with a product offering that delivers baseline capabilities, but still does not have the breadth of functional coverage as other products in the market. However, they are on their way towards becoming a challenger for the more established players in the market and might be a good choice for certain specific use cases and customer requirements.

Again: 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 features provided by the vendor’s products is mandatory.

Overall Leaders are (in alphabetical order):

- CA Technologies
- ForgeRock
- IBM

- Micro Focus
- Ping Identity
14 Vendors and Market Segments to watch

Besides the vendors covered in this KuppingerCole Leadership Compass on Access Management and Federation, there are several other vendors which either declined participation in this KuppingerCole Leadership Compass, have only a slight overlap with the topic of this document, or are not (yet) mature enough to be considered in this document. This includes the following vendors:

**Fischer International**

Fischer International is another vendor that provides Web Access Management and Identity Federation both as on-premise and cloud deployments. This product most likely will be included in a future version of the KuppingerCole Leadership Compass on Access Management and Federation.

**Indeed Identity – Enterprise Authentication and Enterprise Single Sign-On**

Indeed Identity is a software vendor based in Russia that delivers solutions for authenticating users, encrypting messages, and securing information on mobile phones. Part of their solution portfolio are Indeed Enterprise Authentication, providing various strong authentication methods, and Indeed Enterprise Single Sign-On, delivering standard Single Sign-On capabilities to both standard web services and cloud applications.

With their product offering, Indeed Identity is clearly positioned as a specialist vendor in this market segment. They do not yet provide a full Web Access Management and Identity Federation offering, however can support the baseline requirement for Single Sign-On to such applications and also strong authentication with their offerings.

Indeed Identity also might be considered as a complementary solution to the other products in scope, by adding traditional Enterprise Single Sign-On features and strong authentication capabilities to the Web Access Management and Identity Federation infrastructure. Furthermore, we expect Indeed Identity adding in particular Identity Federation support to its products for increased support of the use cases in the market segment in scope.

As of now, Indeed Identity takes a specialist role in this market segment, with limited support for major features. However, due to their specific strength in certain areas and their potential for adding in particular Identity Federation support, they are worth a look in specific as a complementary offering to other vendors’ products.

**Layer 7**

Layer 7, now a part of CA Technologies, provides support for various federation standards. However, their approach is targeted to application-to-application communication at the API (Application Programming Interface) level, in contrast to the user-centric approaches of the products covered in this KuppingerCole Leadership Compass on Access Management and Federation. Layer 7 is the subject of research and reports of KuppingerCole in the area of the “API Economy”. There will be further publications on that type of solution and security for application-to-application communication in future. With this acquisition, CA Technologies has a portfolio covering both user-to-system and system-to-system federation.
Microsoft ADFS

Besides the Microsoft Windows Azure Active Directory (WAAD) mentioned above, there are also the Microsoft Active Directory Federation Services. These are part of the Microsoft Windows Server platform. They were not selected for this KuppingerCole Leadership Compass document due to their limitations regarding the user store, being focused on the Microsoft Active Directory.
Kuppinger Cole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company Kuppinger Cole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.


For further information, please contact clients@kuppingercole.com